Advanced Sciences and Technologies for Security Applications

Hamid Jahankhani
Stefan Kendzierskyj
Arshad Jamal
Gregory Epiphaniou
Haider Al-Khateeb

Blockchain and Clinical Trial

Securing Patient Data

Springer

Advanced Sciences and Technologies for Security Applications

Series editor

Anthony J. Masys, Associate Professor, Director of Global Disaster Management, Humanitarian Assistance and Homeland Security, University of South Florida, Tampa, USA

Advisory Editor

Gisela Bichler, California State University, San Bernardino, CA, USA
Thirimachos Bourlai, West Virginia University, Statler College of Engineering and Mineral Resources, Morgantown, WV, USA
Chris Johnson, University of Glasgow, Glasgow, UK
Panagiotis Karampelas, Hellenic Air Force Academy, Attica, Greece
Christian Leuprecht, Royal Military College of Canada, Kingston, ON, Canada
Edward C. Morse, University of California, Berkeley, CA, USA
David Skillicorn, Queen's University, Kingston, ON, Canada
Yoshiki Yamagata, National Institute for Environmental Studies, Tsukuba, Ibaraki, Japan

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Hamid Jahankhani • Stefan Kendzierskyj
Arshad Jamal • Gregory Epiphaniou
Haider Al-Khateeb
Editors

Blockchain and Clinical Trial

Securing Patient Data

Springer

Editors
Hamid Jahankhani
London Campus
Northumbria University
London, UK

Arshad Jamal
London Campus
Northumbria University
London, UK

Haider Al-Khateeb
University of Wolverhampton
Wolverhampton, UK

Stefan Kendzierskyj
London Campus
Northumbria University
London, UK

Gregory Epiphaniou
University of Wolverhampton
Wolverhampton, UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-030-11288-2 ISBN 978-3-030-11289-9 (eBook)
https://doi.org/10.1007/978-3-030-11289-9

Library of Congress Control Number: 2019934757

© Springer Nature Switzerland AG 2019
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

In the USA, over 350k people suffer 'digital deaths' due to information errors, whilst in the UK, the number is around 30k. Poor information management is the culprit: spanning R&D results, Doctor and Surgeon notes, incorrect diagnosis, drug dispensing errors and so on. Even more basic, around 23% of all patient paper documentation is lost or not in the right place at the right time.

ICT and medical professionals have struggled for decades with these thorny problems that ultimately condense down to inadequate management systems, processes, security and governance. Probably the earliest crystallisation was around patient records and a perceived need for absolute security with access anytime, anywhere. But until recently, there was no tried and tested technology offering the capabilities to satisfy every aspect of the identified need. However, blockchain or distributed ledger fits the bill perfectly!

The basic technology has been around for over a decade and has now been widely adopted. And I think we can safely assume that if blockchain is sufficiently secure for cryptocurrencies, military, intelligence, government banking and legal applications, it is good enough for the medical sector. So the subject and content of this book turns out to be both timely and pertinent but, more importantly, sufficiently broad and deep to be both illuminating and enlightening.

The edifying treatment of blockchain technology thoughtfully argues the case for general application across the medical sector. Personally, I appreciated the detail and the vision, along with the prognosis for future application in a sector that we all rely upon. I therefore have no hesitation in commending this book to professional and lay readers alike.

It really is important to understand what blockchain is and how it complements Big Data, the IoT and AI whilst providing a governance tool that can mean the difference between life and death.

Do enjoy the read, and be prepared to be challenged.

Sentient Systems Research
The University of Suffolk,
Suffolk, UK

Peter Cochrane

Contents

Chapter 1
Blockchain and Healthcare

Gregory Epiphaniou, Herbert Daly, and Haider Al-Khateeb

Abstract Distributed Ledger Technologies are promised to be genuinely disruptive in a variety of industries and sectors, from the food supply, pharmaceutical, real estate, financial services, academia and healthcare. Blockchain technologies vastly improve the flow of data within and among companies and people and transform the way that the Internet is used to exchange value. The use of distributed applications can revolutionise and simplify complex system tasks and create new substructures in a fully developing distributed economy as part of Industry 4.0. Blockchain technologies have the enormous potential to transform healthcare and existing security, privacy and interoperability issues allowing more flexibility and freedom to patients and their data. New economies of scale are emerging for health information exchange that makes the management of electronic records easier while eliminating fictions and costs associated with current intermediaries. This chapter seeks to explore the idiosyncrasies of Blockchain technology and its adaptation in healthcare with an emphasis to its core features and applications. We expand to the key risks and opportunities of Blockchain and briefly discuss this pilot studies in healthcare.

Keywords Blockchain · PoS · DPoS · PoW · PoA · PoET · Raft · Hyperledger · HIS

1.1 Introduction to Blockchain Technology: Features and Application in Healthcare

Blockchain was initially described as the fundamental block of bitcoin a cryptocurrency solution introduced by Satoshi Nakamoto to his White Paper in 2009 (Nakamoto 2009). The technology seeks to establish a consensus of trust in cases where there is a need to store a state (transaction) by multiple writers often unknown and untrusted. It is often regarded and celebrated as a disruptive technology using

G. Epiphaniou (✉) · H. Daly · H. Al-Khateeb
University of Wolverhampton, Wolverhampton, UK
e-mail: g.epiphaniou@wlv.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_1

public verifiability aspects to assure immutability and audit trail of cryptographically secure transactions executed by online users (Ryan Henry 2018). Blockchain can be seen as a revolutionary technology in which a sequence of blocks holds a complete list of transaction records much like a general public ledger. Although several limitations have been recorded with this technology such as the restrictions on the block size and the rate of the transactions, these do not constitute significant issues for the validation of records given both the nature of the records held, transmitted as well as their total size (Mettler 2016). It is vital to ensure that these records are treated in such a way within the network path and between the software or devices collecting and transmitting them that their integrity, authenticity and confidentiality is maintained. The innovative idea behind this approach is that all transactions are stored in a decentralised fashion inside the communication environment.

At its basic form, Blockchain is a decentralised distributed ledger of all the transactions executed amongst multiple parties. This virtual ledger is replicated and produced collaboratively using strong cryptographic protection and distributed validation amongst all peers. Business logic is embedded in the ledger and is often executed together with transactions using distributed applications (e.g. smart contracts) (Ariel Ekblaw 2016). The technology enables anonymous transactions that are impossible to tamper, erase or dispute transparently. Transactions are considered irreversible with no centralised authority controlling the communication process and in the health sector, in particular, provides a means to electronically regulate the sharing of patients' health records with other entities in the sector. All entities involved in the collection, storage and processing of medical information, will have access to a private and transparent distributed ledger that can also improve health research. The technology seeks to establish a minimum acceptable threshold within which the delegation of responsibility and accountability of health service providers can be established (Angeletti et al. 2017). Since medical sensors and integrated IT medical devices have evolved from sensing and processing to decision-making, the security of the patients' health records dictates the design and implementation of new solutions that can give data owners control over their data. It is essential that decisions made upon data-processing related to medical information should always be based on reliable facts about the clarity, relevance, and integrity of the data processed. Recently, there are examples of Blockchain technology adapted to monitor the production processes for drugs. Counterfeit medicines are an increasing issue worldwide, spanning a whole range of drugs from lifestyle products to drugs for the treatment of cardiovascular disease and cancer. The World Health Organisation estimates a steep increase of such counterfeits, from 10% to 30% globally (Zonyin Shae 2018).

Hyperledger has recently launched the counterfeit medicines project, using a combination of timestamps and Blockchain technology to verify the ownership and quality of drugs within the supply chain (Androulaki et al. 2018). Additional platforms have been developed for clinical trial precision medicine, using verifiable anonymous identity management components under different medical use cases utilising the distributed parallel computing paradigms (Herlihy 2017; Wang et al. 2018). Similar approaches have been published in the public domain that utilises

Blockchain technology to regulate and control the data flows of personal data of participants in clinical trials while privacy and anonymity are preserved (Alevtina Dubovitskaya 2018; Gordon and Catalini 2018; Alhadhrami et al. 2017). In all cases, there is a difficulty to move and share medical data promptly securely that seems to have a detrimental effect on patient's care. Also, specific legal and regulatory compliance requirements restrict patients and the proxies from accessing data about their health posing Blockchain-based medical record storage, and data exchange systems is a suitable solution to these problems (Rifi et al. 2017).

The blockchain through its decentralised structure promises to be resilient against the data outages and provide a certain degree of data contingency within the communication network. The reliability of data often depends on the controls imposed for the creation of the transactions by specified authorities. It is therefore essential to identify the exact means by which these medical records are created before their input onto the Blockchain network. Some aspects around the authenticity of data are often outside the scope of the Blockchain operation, and it must always be assured utilising defensive measures outside the Blockchain network (Mayo 2016).

Each block in the Blockchain consists of the block header and its body where the block version, the Merkle tree root has, timestamp, nonce, nbits and the parent block hash (except for the first block) are included. Consent of the next block in the chain is found by solving, i.e. mining a hashed-based proof of work (hash puzzle) with high computational overhead. Changes in the blocks cannot be granted without re-calculating the hash puzzle. The main idea is that after several blocks, it should be computationally infeasible to change a block containing transactions (Scheuermann 2016). The complexity of the proof of work scales dynamically with the combined computation in the network. The maximum number of transactions that a block can contain depends on the block size of each transaction. Concepts of asymmetric cryptography are used to validate the authentication of these transactions using a pair of private and public keys. The digitally signed transactions use Elliptic curve digital signature algorithm (ECDSA) and variations of it (Yi 2018; Liu et al. 2018). The transactions made can be validated quickly, and invalid transactions would not be admitted to the Blockchain network. The discovery of invalid transactions in the Blockchain is almost immediate. However, immutability aspects might be considered as the number of participants in private Blockchain can affect the possibility of tampering these transactions. It is also available to control nodes/participants who can join the consensus process of the private Blockchain (Ana Reyna 2018).

The adaptation of Blockchain technology in the provision of secure healthcare data management systems attracts much of the attention recently due to its ability to build and deploy distributed ledgers consisting of different data structures relevant to healthcare information. The technology promises to achieve a certain level of global visibility to individualised medical histories entirely immutable and distributed within a patient's network leveraging strong cryptographic primitives to ensure that trust is established among peers. Access to these medical histories can be done in a more efficient, verifiable and permanent way, where modifications to an exist-

ing block encapsulating a particular patient record cannot be modified without modifying all subsequent blocks (Chang 2018). The ability to offer and achieve decentralised consensus means that an agreement can be reached without the involvement of the trusted mediator while modifications to the blocks, are globally visible and audible by all participants including the persons themselves. Unauthorised modifications are easily detectable and to a certain extent attributable. The Blockchain network offers strong integrity and immutability aspects but also perpetual data storage which might conflict with new regulations related to personal data retention periods (e.g. GDPR). Some additional challenges include the size of the data that needs to be stored as well as existing searching capability offered by the Blockchain, especially, when hashes will be regarded as personal data by the Information Commissioner Officer (ICO) in the future (Lima 2018).

Personalised healthcare, data sharing processes, and recent developments in legislation require patients to engage in the details of their electronic medical records often stored in remote and decentralised platforms. Data in these platforms is often scattered across different organisations with significant issues presented with regards to its accuracy and clarity. Medical record management has been proved quite challenging to initiate as patients have limited access to their records and are in some cases discouraged from accessing their full medical profile (Ross and Lin 2003). This proves to be a crucial factor in establishing trust and participation in the medical system and services as patients are often mistrusting the existing processes and protocols that underpin data sharing across different providers. For healthcare practitioners that also means slow access to fragmented data that could impair their ability to analyse information and make informed decisions on identifying health risks, targeted treatments and too many cases verify prognoses (Kabene et al. 2006).

Specific issues around privacy also apply as the existing systems must recognise that not all healthcare providers and practitioners should have access to the whole dataset for patients. The viewing and data retrieval permissions are often complicated to establish given the fact that different members of the healthcare sector frequently share data processing and viewership. It has been noticed a progressive shift of data and healthcare services to the cloud due to its convenience, savings and near real-time access (Ariel Ekblaw 2016). However, certain limitations and security implications have been recorded with the integrity of the patient's medical history, conventional cryptographic algorithms used, and legacy access control systems applied. Economies of scale are slowly emerging to cybercriminals who seek to benefit financially from the theft of medical records. For example, medical records can be sold to third-party providers who have a vested interest to identify individuals' conditions or the potential to develop them in the future. Unauthorised access to electronic medical records intentional or otherwise must be heavily penalised also, why adequate and relevant access control models are applied to regulate and limit access to the data.

Healthcare -related data is regarded as high volume, high velocity and high variety that poses significant challenges in storage, processing and sharing in traditional Information Systems. Existing data and information record protocols often propagate data entry errors that could lead to medical decisions made with incom-

plete or missing information increasing the overall cost to the health system (Vimalachandran et al. 2016). Due to nature, criticality and sensitivity of this data, the retrieval and analysis must be contacted in a secure and regulated manner to better support the existing capability of health information systems dealing with patient mobility, data. The electronic medical records have to unify their data structures in an attempt to represent better and express information available to multiple healthcare providers (Bush et al. 2017). The integration of Healthcare Information Systems (HIS) and traditional IT infrastructures combined with the pervasiveness of smart devices has sifted the paradigm within the healthcare industry. Medical sensors available to patients allow healthcare providers to measure and monitor the wellbeing of users with increased use of mobile applications and embedded devices that continuously gather, process and translate data (Ko et al. 2010). These medical records generated become private health records blurring the boundaries between entities accessing and processing data collected. Machine to machine communications will open new frontiers in the real-time personalised healthcare but equally create legal disputes and liabilities related to misdiagnosis due to decisions made based on the data sent from these devices.

1.2 Overview of Blockchain Types and Consensus Mechanisms

Current Blockchain technologies can be categorised into three main types: Public blockchains, Private blockchains and consortium blockchains. In public blockchains, all transactions and records are publicly accessible to all participants in the consensus process. In cases, where only a group participates in the consensus process then the Blockchain type is a consortium one. A private Blockchain consists of a network of nodes that belong to the same organisation or entity that controls the whole platform. In cases where untrusted nodes within the Blockchain network require public verifiability for transactions to be admitted a public permissioned Blockchain model is deployed (Tama et al. 2017). In cases that public verifiability he is not required then a private permissioned Blockchain it is used. In public Blockchain all nodes are unknown, but all can take part in the consensus process. Increased latency has been contributed as one of the critical issues on public Blockchain networks because a large number of nodes could increase the time it takes to propagate transactions and blocks within the network. The main difference between all three types is the concept of decentralisation, and the technology manifests the weight. Public blockchains offer full decentralisation whereas Consortium blockchains our only partially decentralised. Private blockchains are regarded as closed groups often centralised. Another difference is that in the case of private Blockchain and consortium Blockchain types all nodes are known, and there are cases in which the immutability could have tampered. Given the fact that in all BC types nodes are not trusted a mechanism must be used to reach a consensus amongst

these untrustworthy nodes about the consistency of the distributed ledger (Jayachandran 2017). All nodes in the network should mutually agree on the final state of data. The consensus mechanism is a process utilised to agree on data state whereby all nodes agree on the same value. There should be clear termination criteria to be fulfilled for a consensus to be reached, and the value agreed by all nodes must be the same as the initial value proposed by honest node(s). The expectation is that the consensus mechanisms should be able to work in the presence of adversaries or untrustworthy nodes and should require a decision made only once in a single consensus cycle. The broad categories that consensus mechanisms fall under are *Byzantine fault tolerance-based and Leader-based* (Lamport et al. 1982), (Achour Mostéfaoui 2001). The former used signed messages to reach an agreement without intensive computational tasks, and the latter requires all nodes to compete for the proposal of the final value. A list of these consensus mechanisms and their different characteristics are given as follows:

Proof of Work (POW) This often involves some heavy computer calculations to prove that any given node that performs these calculations (mining) is unlikely to attack the network. The mechanism assumes the output of the calculation to be equal to or smaller than a certain value from the calculated hash value off the block header. Once one node inside the network identifies the value, the block is broadcasted to the rest of the nodes to verify the correctness of the hash value mutually. If the validation process is successful, all nodes within the network are obliged to update their Blockchains (Gervais et al. 2016). Every newly created block is linked to the previous one, and the length of the chain is proportional to the amount of work each node must place following a rewarding mechanism for miners. This underpins the cryptographic resistance of the system against tampering as its threat model dictates that at least 50% of the hashing power of all nodes must be controlled in order for an attack to be successful. Elements like the number of nodes, available processing power at any given time instance and network load can influence the complexity of the work required by miners to solve a puzzle and admit a block into the blockchain network within an average time of 10 min (Eyal and Sirer 2018). The hash value of each block is incorporated into the next block in an attempt to increase the security and integrity of the chain. The computational power required in PoW renders this consensus mechanism suitable in several environments such as defence from DoS attacks. Mining requires strong computational capacity that can be considered as a limitation of the PoW consensus mechanism. This is often translated to highly specialised and expensive computer hardware to run the complicated algorithms required (Tosh 2017). Attackers can also monopolise computational power within the network by preventing other miners from completing blocks. The computational power may allow adversaries to create lengthier chains and prevent legitimate transactions taking place.

Proof of Stake (PoS) In PoS a node is required two show ownership of a certain number of cryptocurrency units. New block creators are often selected in a pseudorandom way based on their health which is also defined as a stake. The num-

ber of cryptocurrencies is fixed the rewards given are usually transaction fees. In order to validate transactions and create blocks, node must first put their coins at stake. If these nodes validate a fraudulent transaction, they lose their holdings as well as their permission to participate as a forger in the future. The selection process for these forgers is often based on unique methods of selection such as the randomised block selection and Coin Age-Based selection. The former base their selection on the combination of the lowest hash value and the size of the stake whereas the latter on the coinage. Coinage multiplies the number of coins being at stake by the period at which those coins are staked. Nodes that have a high number of coins for a more extended period staked are the candidates to construct a block an add it to the Blockchain. Once a block is created the coin age is reset to 0, and the node must wait at least for 30 days before they can sign another block (Judmayer et al. 2017). This consensus mechanism is affordable and environmentally friendly due to low electricity consumption and reduced hardware costs. With the adaptation of this consensus mechanism, the Blockchain it is no longer rely on the proof of work. The adversaries must accumulate enough number of coins and hold them for long enough in order to attack the network. This has proved it to increase the computational complexity and sophistication needed by an adversary to model a successful attack. The proof of stake moves the mining power, inside the Blockchain where the nodes themselves become the core components to passively generating income. Illegal activities are discouraged by the participating nodes on to the Blockchain as nodes that validate existing blocks maintain their coins in a stacked state. This action seems to deter illegal activities such as submitting a defective block or try to double spend a coin.

Delegated Proof of Stake (DPoS) The ability to use the CPU power for mining purposes was embedded in the initial idea design and implementation of bitcoin. The process of mining gave equal opportunities to all nodes to participate in the decision-making process of block creation and storage in the Blockchain network. The DPoS delegates the hashing power required to a group of nodes (witnesses) that have been designated for mining purposes using bespoke hardware and software. Each node within the network selects the actual miners based on their stake using a voting system that always assures a certain decentralisation threshold throughout the process. The selected miners are responsible for creating new blocks and get rewards as appropriate (Wen 2018). DPoS has proved to be a fast and efficient consensus mechanism using approval voting to solve the problem of fair and democratic participation in the block creation process. The elected delegates can control specific parameters from block intervals to transaction sizes using a deterministic selection running by all nodes within the network (Quenetain 2017). A formal process of approval voting is initiated where each node is allowed one vote per share per witness. A group of these witnesses are selected in such a way that at least 50% of nodes believe there is sufficient decentralisation assured throughout the process by voting for at least that many witnesses as the initial number they expressed. Each witness is given a fair chance of producing a block at a fixed schedule, and once all witnesses have produced at least one block, they are reshuffled to start over. Failure

to produce a block in a given timeslot means that a witness loses their turn and the next witness produces the next block (*Delegated Proof-of-Stake Consensus*2018). Monitoring the rate of participation is easy and dropping to the rate should assure specific controls in place to confirm the transactions (e.g. more time allocated).

Practical Byzantine Fault Tolerance (PBFT) Focuses on establishing a Byzantine state machine that tolerates Byzantine faults using a leader for validating and invalidating nodes (Liskov 1999). All nodes in the network are sequentially ordered with all node except their leader referring to as backup nodes. There is a substantial communication between nodes not only validating messages but also to verify the integrity of messages received from a specific node at any given instance (Sukhwani et al. 2017). The threat model for PBFT assumes that the network can function in a trustworthy manner even if adversaries account for up to 1/3 of the overall nodes in the network. The rounds of PBTF is split into four different phases where all backup nodes are treated equally to the presence of a leader (Byzantine General's problem). A request is sent by a node to the leader and the leader multicasts the request to the backup nodes. The nodes execute the request, and a reply is then sent back to the client. The client waits for the multiple identical replies from different nodes. All nodes are deterministically allocated and all start at the same state (Spiegelman 2016). The final identical reply is often the one that all honest nodes agree and either accept or reject it. A round Robbin approach is used to change the leader node for each iteration of the PBFT in case that time exceeds the period within which the leader node is expected to multicast a request. PBFT seems to reduce the overall energy and computational complexity required to reach a consensus and provides transaction finality in the absence of transaction confirmation.

Given that heavy communication and messages' exchange is required in the case of PBFT, the model seems to work better in small-scale environments (consensus groups) with additional cryptographic overheads as part of the digital signing processes and message authentication presented. Identity manipulation and propagation can be allowed in the network that makes PBFT susceptible to Sybil attacks. This can be partially mitigated with increased network sizes although that contradicts the model as a function of the increased network size.

Raft Raft is a consensus mechanism developed by Stanford University for managing replicated logs. This consensus mechanism it has proved to be easy to use and simplifies further the process of the leader's selection, local application, and safety by imposing a substantial degree of coherency and reduce the number of states as a result. Raft also identifies a novel mechanism for changing cluster members using overlapping majorities (Ongaro and Ousterhout 2014). Log entries flow from the leader node to the backup nodes and other services. That makes management of replicated logs easier within the network. The election of the leader uses randomised timers with negligible overhead imposed on the overall operation of the Blockchain that can be considered another benefit of this consensus mechanism. The elected leader is responsible for managing the replicated logs within the network and verify acceptance of the logs to the state machines. The Raft consensus mechanism utilises

a cluster of several servers which can act as leader, follower, or candidate. During normal operation, there is only one leader all the other entities are passive followers do not issue requests on their own but respond to requests from other entities within the network. A heartbeat mechanism he is used for the leader's election using a valid RPCs from other entities and as a mean to assure leaders' authority. The consensus mechanism also produces an additional algorithmic process to ensure that each state machine executes the same commands in the same this is done order. This is done using a restriction on which servers may be elected as leaders. The mechanism addresses the issue of distributed consensus using a simplified and more understandable implementation of the state space.

Proof of Authority (PoA) This consensus mechanism can be characterised as an optimised version of PoS model where a small group of validators stakes the identity. This allows the network to be managed more efficiently and securely (Proof of Authority Chains 2017). The mechanism is proved to be energy-efficient and less computationally intensive than POW with three basic requirements needed to become a validator. These requirements have significant implications on the overall incentive structure of the model in order to achieve correct behaviour overall by all nodes participating in the Blockchain network. (1) The identities must be formally identified on-chain with the ability to verify them off-chain. (2) it should be computationally expensive to become a validator and maintain clear incentives to justify honest behaviour in the long term. (3) The identification and establishment of validators must be uniformly distributed. The incentive structure uses reputation as a key component to deter dishonest behaviours. The model simplifies the process of removing honest validators who act maliciously by damaging their reputation and exclude them from future financial gains.

Proof of Elapsed Time (PoET) This mechanism introduces the basic idea of random waiting time for every new block the validator was to create. The new block it has created by the validator whose timer expires first in an attempt to provide equal chances to all nodes within the network to participate onto the block creation (Chen et al. 2017). The correct execution of the time process is realised by using Intel's software Guard extension (SXG) that enables the execution of programs in memory constraint space. These constrained memory spaces are cryptographically encoded by the processor using a measurement hash, allowing remote entities to verify the integrity of the memory space (Tian et al. 2017). The provision of the mechanism requires several Intel services running on local and remote nodes. It also adds complexity during the block verification process in comparison to PoW. The overall security of the mechanism is proportional to the cryptographic resistance of the software regard extension, causing a single point of failure scenario in which a single compromised node can render several attacks possible.

Proof of Importance (PoI) Similar to other approaches the proof of importance (PoI) consensus mechanism is used to identify which network nodes are eligible to add a block in the Blockchain network. This consensus mechanism tries to over-

come the problems that can be found in the proof of Stake model by identifying three fundamental components namely, vesting, transaction partners and number and size of transactions (Asolo 2018). Each node within the network has an account proof of their importance score. The higher the vested coins required for harvesting, the higher the importance score for that node the number of transactions conducted also contributes to the importance score, the larger the transactions, the greater the impact on the importance score.

1.3 Blockchain Security Risks and Opportunities: Identifying the Threat Landscape

Despite the innovative solutions Blockchain promises to bring to the data decentralisation, storage and processing capability, the technology itself seems to present some inherent security risks. The way that the decentralisation of consensus and self-organisation of the network are manifested in the Blockchain platform seems to increase the attack surface and further propagate security problems related to technical, storage, cryptographic and platform dependent components of the technology. Currently, there is a clear trade-off between the block size and the ability of the Blockchain network to resist against possible DDoS attacks. Bigger blocks allow more records to be stored at the expense of complicating the running and managing processes in the Blockchain nodes. The distributed data storage capability creates an increased attack surface that can provide skilful adversary for alternative ways to access data stored at the nodes. Data mining, data correlation and traffic analysis can be utilised by skilful adversaries to retrieve valuable information related to smart contracts, users, network structure and applications running. Limitations concerning the conceptual design and implementation of consensus mechanisms they also allow disruptive attacks and malicious activities within the Blockchain network. Issues related with traditional Public key cryptography are also manifested with regards to the private key management, confirmation of the user's identity and assumptions about key usage, key freshness and key generation. In typical scenarios, nodes are solely responsible for the generation, secure storage and use of their private key often without the necessary entropy required. That can lead to vulnerabilities that can expose private key information to an adversary, tampering the user's Blockchain account and difficulties related to tracking criminal behaviour against modified Blockchain information.

Cryptoviral extortion software increasingly uses Blockchain as a mean to link the transaction that pays the ransom to the decryption key for the filesystem. Adversaries utilise conventional spreading techniques in traditional social engineering to infect their victims and make resources unavailable. The attackers announced payment instructions to the afflicted systems and they can verify payments via the Blockchain network (e.g. CTB-Locker and WannaCrypt) (Kao 2018). Figure 1.1 lustrates the evolution of cryptoviral extortion software. Blockchain offers a certain

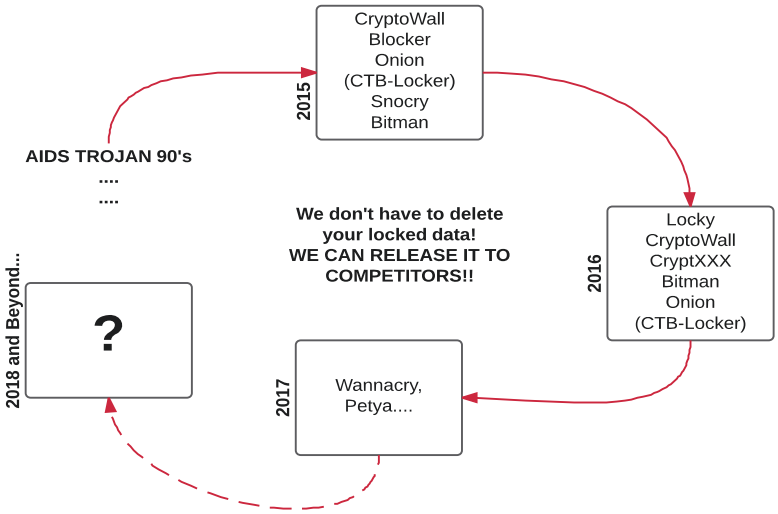

Fig. 1.1 Evolution of cryptoviral extortion software

degree of anonymity and a network of virtual payments that can enable adversaries to encrypt transaction information a mix user's valid coins making money-laundering much easier (Irwin 2017). Skilful adversaries can also perform double spending attacks it which a cryptocurrency is used multiple times for transactions by exploiting the intermediate time between consecutive transactions and their confirmation assuming that an attacker knows the vendor address before the attack. If any legal transaction is added to the wallet of the targeted vendor and this transaction is mined into a successful block, then the attacker can use a service without paying any fee. Blockchain technology has also been criticised with regards to the privacy protection measures it deploys. There are cases of privacy leakage for a sender allowing an attacker to identify the actual transaction with a high degree of accuracy. Information leakage can facilitate confidential information exposure, theft of cryptographic material, and further electronic crimes.

Malicious contracts can be developed by skilful adversaries (CriminalSmartContracts) to carry out illegal activities or exploit security vulnerabilities caused by software defects in other legitimate smart contracts (Juels et al. 2016). Significant risks apply when external contracts are called without controlling their flow, allowing changes to the data in an unexpected way (Atzei et al. 2017). Irregularities and exception handling, privacy values leaked by miners and altering contracts during or after deployment are typical attack vectors manifested in the Blockchain network. Skilful adversaries can convince honest miners to perform operations that waste resources and gain a competitive advantage to the selection and participation process during the block creation. This allows selfish miners to simultaneously perform computations on multiple chains and gain multiple rewards for the block creation process at the same time. Attacks against BGP (Border Gateway Protocol) and the way that IP packets are regulated can be used to intercept

traffic within the Blockchain network. These attacks can delay the block creation by introducing artificial delays and impacts on the decentralisation processing capacity of nodes within the mining pools leading to bitcoins being stolen (Apostolaki et al. 2017). A variation of this attack can allow an adversary to control the access a legitimate node has within the network, and leverage the victim's computational capacity for illegal purposes. The victim has limited visibility and access within the network resources, rendering this approach the basis for further attacks to conduct such as transaction denial, re-write blocks and double spending (Steward 2017).

Blockchain support interoperation between different users, applications, and processes. The way that data is stored, processed and updated create a substantial economic benefit and motivation for adversaries to interfere with the security management and self-organisation of the platform. Certain elements related to privacy enhancement as part of the Blockchain operation might render impossible to verify and trace users true identity. Also, the real value of information exchange lies the distributed technologies leverage information flow across different Blockchain integration platforms, payment processors, smart contracts and traditional IT infrastructures (Piekarska 2017). Scalability is inherently embedded into the Blockchain technology where an organic expansion over time might a introduce significant security issues and as with every new technology, the direct and indirect impact the Blockchain security failure has not yet been measured or quantified. The majority attack (51% problem) previously described poses a significant theoretical threat that could materialise considering the large number of nodes, users and mining firms across the globe. Exploiting software vulnerabilities in the decentralised Autonomous Organisation (DAO) it is another area of concern where a skilful adversary can execute arbitrary code and transfer tokens between accounts or iterate transfer requests without updating account balances (Atzei et al. 2017). The systematic testing and performance management of smart contracts is of paramount importance to the process of identifying the flaws that can result in the exploitation of DAO code. It is therefore essential to peer review code before deployment and apply strong, secure software development lifecycles towards the development of more robust and secure Blockchain components. The block propagation mechanisms it is also an area of interest as these considered the foundation building blocks of consensus and trust in Blockchain.

Attacks against the propagation mechanisms can reverse transactions and initiate double spending, tamper with the ordering of transactions, prohibit normal mining operations by legitimate nodes and impair with the confirmation operations of standard transactions (Oguzhan Ersoy 2017). Multi-signature techniques are often used during the contracts' creation using dedicated scripts. There are possibilities of misconfigured transactions increasing the complexity of the script that controls the contract. These contract-type transactions must be verified and the accuracy of the script that controls them should be tested. The verification process becomes a necessity especially in cases that the Blockchain network grows more complex and transaction facilitators are scattered. This can lead to violations where an attacker can generate a block containing altered data or make race attacks possible where hundreds of transactions are sent two multiple users (Xiaoqi Li 2017). A significant

risk identified is the lack of regulation and standards when it comes to Blockchain operation and interoperability aspects. Keeping the consensus architecture healthy and consistent also proved to be a more challenging issue as it might seem. There is also a systematic lack of standard protocols that prohibits developers from propagating coding errors across different platforms. There is a clear need for self-imposed regulatory standardisation amongst different Blockchain consortiums both internally and externally to organisations. Given the fact, the Blockchain is primarily intended for Internet transactions do not necessarily compete with traditional currencies but rather with online payment processors such as PayPal and credit cards. Elements related to supply and demand to control the value of cryptocurrencies used in Blockchain as they are not denominated in other physical currencies. Therefore, the current regulatory landscape is quite immature and complex depending on the component of the distributed ledger one is referring to. Given the fact that regulatory requirements often have a local component, several approaches have been recorded in the literature to identify the key role of regulators in Blockchain consortia based on local and regional specificities (Cermeno 2016).

1.4 Benefits and Challenges of Blockchain Technology in Healthcare Sector

Having discussed the general features of Blockchain technology in previous our sections, we now turn our attention to healthcare technology and the unique challenges if this area. Swan (2015), a relatively early work, reviews the possible uses of the new technology, which suggests that Blockchain offers "reconfiguration possibilities to all industries and even more broadly to all areas of human endeavour". Disintermediated transactions are as seen as key to offering decentralised models of services we depend on while affording a "global scope and scale that was previously impossible" (Swan 2015). Though there are many lofty aspirations relatively few applications focus on health, although those which do we shall discuss the return to for discussion later. None the less it appears that on the whole, early discussion of Blockchain within the community of developers failed to engage well with the conversations within the healthcare industry and its considered direction of travel. However, it could, therefore, be argued that given the requirements of future Healthcare Information Systems (HIS), the use of Blockchain technology may present the only practical choice. HIS have been in existence for some time, the Healthcare Information and Management Systems Society (HIMSS), for example, was founded in 1961 with the aim of representing organisations and professionals with interest in management and innovation of systems dealing with healthcare data. Large scale national programmes of research and investment in this area, however, have become most prevalent from the beginning of the twenty-first century onwards. Many factors have served to create new avenues of potential, among them the widespread use of mobile technologies and cloud computing, improved

standards for file compression, encoding and transfer, as well as the relatively low cost of storage and processor power. Blockchain then may serve as another enabling factor in this development.

At around the same time Nakamoto (2009) was proposing the Bitcoin model for Cryptocurrency a group of technology authors were advocating a new way of organising healthcare systems which they named "Cybercare" (Koop et al. 2008). Their vision arguably forms an ideal for the direction of travel in Health Information Systems (HIS) and though it differs in detail it is interestingly couched in somewhat similar terms. Written primarily at addressing shortcomings in the US healthcare systems the aims of "Cybercare" were to "help reduce costs, improve quality of care and potentially make insurance more affordable to all citizens". The issues they describe, problems stemming from centralisation, resource intensive treatments and the prevalence bureaucratic processes between systems which struggle to interoperate effectively.

Koop et al. (2008) describe a vision of integrated, yet distributed, information services supporting the delivery of healthcare in a new kind of ecosystem, shifting the emphasis of the healthcare system to new modes and patterns of performance. At the heart of their vision is a decentralised model summarised in Fig. 1.1 based on Koop et al. (2008). This new model aims to solve contemporary failures through "a new system that move medical care away from the hospital and into the community clinic." This they claim would enable primary care providers to "use telemedicine over a distributed network to link to tertiary medical providers and systems worldwide." The technology proposed can rebalance the provision of healthcare from specialised centres to patients' homes. Koop et al. (2008) give a 20-year time horizon for the development of these new systems which integrates the needs of public healthcare, private healthcare and security. The issue of security is drawn rather broadly, as the interests of the authors include issues of "National Security" and the needs of military hospitals. However, reflecting on this 10 years after the original proposal the information security needs of individuals and health care organisations are arguably no less significant than those of the military then. Arguably, in fact, the challenges in non-military scenarios are more significant due to a lack of infrastructure, awareness and security oriented culture (Fig. 1.2).

Targeting cost and quality, though definitions vary, the Cybercare model looks to reduce processes that add little value to care and enable more localised preventative healthcare strategies based on the availability of patient data. Broadly then we can understand where the features of Blockchain systems may have the most impact on this vision.

Various previous initiatives have driven investment in healthcare technology. In the United States estimates of the savings resulting from better management of healthcare data are as high as $81billion annually and legislation such as the 2010 Patient Protection and Affordable Care Act and American Recovery and Reinvestment Act 2008 more than $19 Billion were allotted for the modernisation of healthcare systems (El-Yafouri and Klieb 2014). Previous investment in health data systems may prove to be either an enabler or a hindrance to the adoption of Blockchain systems in healthcare. Existing systems, which are successful, provide

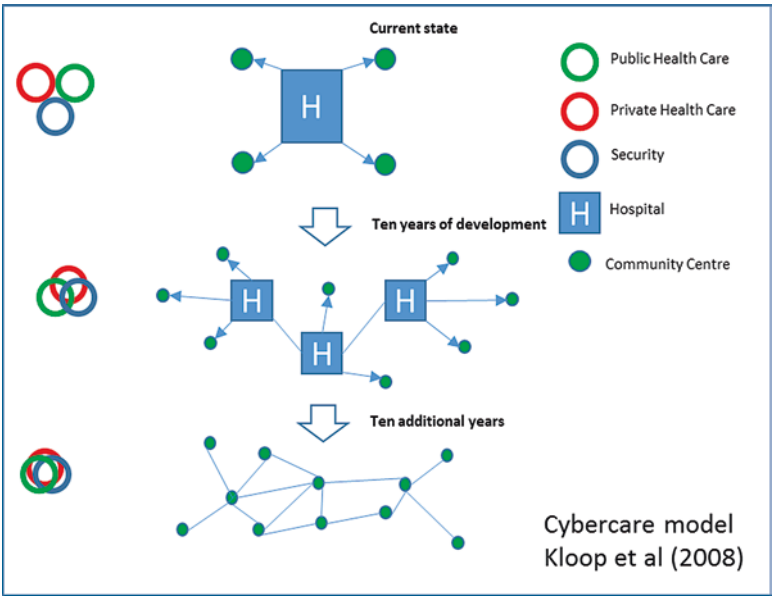

Fig. 1.2 Evolution towards Cybercare. (Koop et al. 2008)

a demonstration of the effectiveness of electronic solutions and can be used as a way of explaining how distributed solutions can bring practical benefits. They will have typically have dedicated technological infrastructure e.g. private clouds, mobile gateways, data clusters, which Blockchain systems may draw on. There is also the data itself which has been chosen to support the broader goals of the healthcare organisation or a network of organisations. This has the potential to be used as part of the new systems. Existing systems however also have the potential to cause inertia in future developments. Systems can become "legacy systems", obstacles to change and resistant to improvement. It is also the case that issues of data design can determine the functions that are most easily used or developed. The underlying data models and the potential for interoperation with other systems are key in planning innovative services and extensions. Koop et al. (2008) describe a scenario where shared patient-centric data records could be used to speed communications and reduce the occurrence of medical errors. Existing "islands of information" such as dental records and vaccine registries, could be integrated with other organisations such as hospitals and the insurance companies who authorise care. Such a patient record would be mobile and accessible by the patient as they interact with institutions of their choice. This integrated approach could draw on data from personal fitness devices to support early diagnosis and preventative interventions.

Though there have been significant developments in Health Information Systems (HIS) in recent years many of the key ideas were laid down much earlier as a survey of these concepts Saranummi (2009) illustrates. Saranummi (2009) draws on the Health Information Management Systems Society (HIMSS) definitions of health-

care data and interoperability. Service providers and researchers will typically use medical history in order to make decisions about planning and care. Saranummi (2009) distinguishes between the Electronic Health Record (EHR) and the Personal Health Record (PHR). The first for data within a single Care Delivery Organisation (CDO), the second recording the medical history of an individual, owned by the patients themselves. Key then to effective HIS design, whether based on Blockchain technology or not, is the ability to store the most useful and relevant data about treatments and patients which may also include complex data such as digital images, audio, and video. Table 1.1 provides a list of key concepts for understanding existing networks and HIS provision.

El-Yafouri and Klieb (2014) discuss the adoption of information technologies in the health sector using and expanding on EMRAM, a HIMSS model for understanding the influences on organisations adopting HIS and describing their level of adoption. El-Yafouri and Klieb (2014) also provide a number of concepts to understand the potential benefits and challenges for organisations looking to adopt new technology. Figure 1.3 describes the maturity levels of organisations and groups with HIS based on their level of integration.

The main benefits of adoption El-Yafouri and Klieb (2014) describe are the cost savings and improved quality of care based on efficiencies and analysis of collected data. Use of techniques such as machine learning can support a reduction in hospitalisations, visits to surgery, administrative nurse work and better allocation of physical services and resources. When applied across a network of CDOs the interchange of information can spread these benefits across a network of partners. Analysis of appropriate data feeds can be used for better disease prevention and the management of patients with chronic health conditions. These factors directly favour healthcare funders such as insurance companies, national government programmes which have faced issues with the growing cost of care. Moreover, El-Yafouri and Klieb (2014) argue that the improved health outcomes of such initiatives ultimately benefit patients. Drivers for adoption then are based on the demand from stakeholders and funders for improved levels of service. While there are management factors in ensuring that improvements are achieved, interconnected HIS enable the initiatives which can make this occur. The coded categorisation of levels of HIS adoption presented by El-Yafouri and Klieb (2014) are summarised in Table 1.2, helping to describe the degree of technological penetration; an indication of what it is possible to achieve within a given network of CDOs. While useful the classification could be more complete, for example, some discussion of how networks containing members with different EM levels may be managed or developed.

Koop et al. (2008) list a number of barriers in progress towards a Cybercare model. Some of these concern the information itself and how it is managed by in the system. For example, ensuring that only high quality information is accessed or stored. The development of special technologies to support interoperability of systems and the exchange of data are also a concern. Privacy issues, including authentication, are listed as critical for the generation of patient oriented records and for broadening the network of CDOs and medical practitioners. Other barriers relate to

Table 1.1 Health information systems terms acryonyms and abbreviations

Acronym	Explanation
ARRA	American Recovery and Reinvestment Act 2009 – also known as the Stimulus and Recovery act. Provided incentives for healthcare organiations to modernise their HIT systems.
CDO	Care Delivery Organisations – Organisation responsible for the delivery of healthcare services. These may include hospitals, clinics, specialist centres and some care homes.
CPR	Computerised Patient Record – Traditional patient record transposed into digital format. Often an initial step in small independent CDOs becoming digital
EMR	Electronic Medical Records – Organisational records used by an HIS to record information about
EMRAM	EMR Adoption Model – Technology adoption model developed by the HIMSS based on the
HER	Electronic Health Records – Term often used interchangeably with EMR, however the EHR collates multiple records from different CDOs
HIMSS	Healthcare Information and Management Systems Society – Organisation founded in 1961 to support and advise stake holders on the effective use of information technology in the health care sector. Responsible for several studies the adoption and diffusion of technology in the sector.
HIPPA	The Health Insurance Portability and Accountability Act (HIPAA) – details requirements for storage and security measures that must be in places for the storage and use of sensitive patient data. HIPAA compliance is required for most active HIS in the United States.
HIS	Health Information Systems – Systems typically owned be a single CDA for manging care related data which may inform patient care as well as relationships with organisations and suppliers
HIT	Health Information Technology – Use of technology in a healthcare context including mobile hardware, image processing, and sensor technology
HL7	Health Level Seven – An early standard to facilitate the exchange of data between organisations processing healthcare data. Considered legacy by some it has declined in use as other more widely applicable interoperability standards have emerged.
PHR	Personal Health Record – Personalised universally accessible health record, patient centric it is used to manage individual health and wellness securely
Snomed-CT	Systemised Nomenclature of Medicine – Clinical Terms – Specialised code for recording data about medical statuses, procedures and diagnoses. Used to record data in medical records.

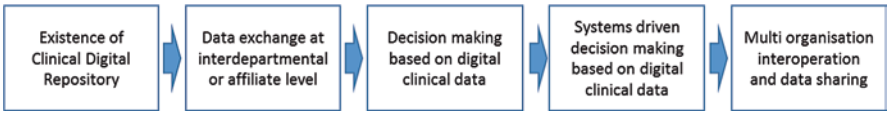

Fig. 1.3 Maturity levels for HIS adoption

Table 1.2 EM Level categories of HIS Adoption

Category	Explanation
EM1	Single care provider with a partial HIS supporting the needs of at least one department
EM2	Single care provider with organisation wide HIS using standards and internal data sharing. Data used in testing and decision making.
EM3	As EM2 with HIS widespread organisation use with supporting paperless administration process. Capable of decision making activities as well as automated alerts and recommendations.
EM4	As EM4 with all departments interconnected with real-time sharing of information. Inter-organisation information exchange capability.
EM5	As EM5 with all organisations in network (typically regional) capable of data exchange supported by national or international standards.

Adapted from El-Yafouri and Klieb (2014)

levels of education among patients, medical staff and also technologists. Each of these may be significant factors in the adoption and use of new systems based on Blockchain technology. Given the previously discussed properties of Blockchain systems and the broader needs of Health Information Systems, some patterns for their potential use emerge. Based on the original purpose of such systems to record Crypto-currency exchanges, there is potential to benefit from applications which include electronic payments and also from the ability to automate related activities, using smart contracts. This could result in offering some intermediate accounting services or possibly even a localised currency, exchanging value between partners in a network. It may be possible to realise the Personal Health Record (PHR) concept using Blockchain based identity management. The Electronic Health Records (EHR) where multiple agencies collaborate to keep common records up to date may also be realisable by capturing immutable transactions from multiple sources across a network of care providers together with that patients own data. Additionally, as healthcare services typically require complex supply chains for delivery, Blockchain architectures could be used to help strengthen these partnership networks providing their validation and dynamic customisation where needed. By applying features that ensure trustworthiness and seamlessly handle disputes, existing networks may be extended to include partners who are currently too disparate to disparate to engage with. This may enable some aspects of the integrated partnerships described by EM5 category of HIS adoption (See Table 1.2). On the periphery, we have applications in areas that directly support healthcare systems such as authentication of medical staff credentials, quality assurance in the supply chain of pharmaceuticals and supplies, verification of medical images and other critical data files. The opportunities are extensive, and the most pertinent question is when and how they can be exploited most successfully. At the moment a few specific platforms with different features, advantages and disadvantages have emerged, as will be discussed in the next section. It is a challenge to find the most appropriate way to design and such systems, though as we shall discuss in the penultimate section several early systems and interesting prototypes are currently gaining attention in this field.

1.5 Blockchain Healthcare Platform Examples

The essential features of the Blockchain as originally defined, mean that it provides a secure mechanism for implementing a Distributed Ledger, a system of records shared across multiple nodes, which making use of a communications network are potentially remote (Fig. 1.4). This is implemented in a peer-to-peer configuration, implying the ability for all stakeholders to take an equal part in the ownership management and store of the data. The ledger contains records of the transactions processed by the systems relating to the legitimate exchange of assets. Assets in the case are any item of value which may be some information, or if a link to a unique identity can be found, some physical thing also. The Blockchain then, in its simplest form, maintains a mutually agreed record of the state of asset ownership throughout the network of participants. The combination of the ledger fragments stored at each of the nodes gives the agreed state of the system, which can be used as a reference by all participants. Problems in healthcare resulting from the ineffective tracking of assets between participants are potentially addressable through such solutions. The proviso, however, is that both the assets and the participants must be uniquely identified and authenticated. This could be seen as a way for informal networks of actors within a Care Delivery Organisation (CDO) to form and interact in a trusted way. Moreover, it could be a mechanism for networks of CDOs to form and exchange shared assets from a shared pool. This provides the potential for, collaboration around assets.

In the peer-to-peer model, distributed ledger fragments are stored at each node and when combined they provide the global state of the ledger. Reasoning about this global state requires the initial state transformed incrementally by the transactions between the participants. The transactions themselves are stored immutably in uniquely identifiable blocks across the nodes, supported by the mechanisms of authentication discussed previously.

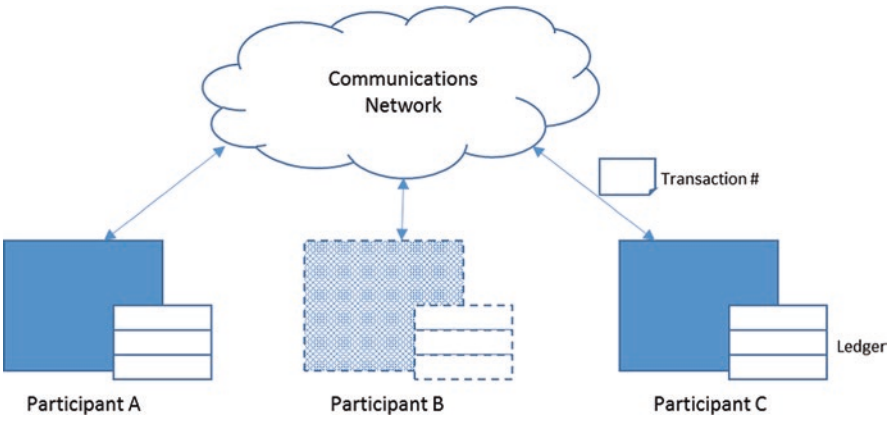

Fig. 1.4 Ledger distributed between business network participants

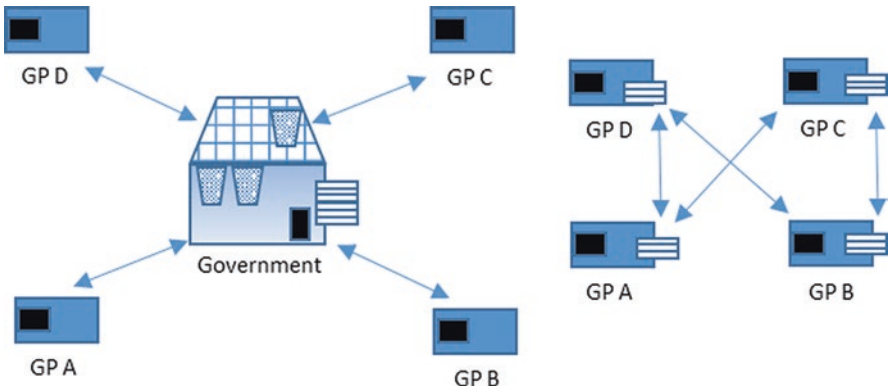

Fig. 1.5 Network of General Practitioners sharing data via government vs disintermediated peer-to-peer

Given the facility to share data securely, from authenticated sources across a network of partners, the obvious applications are those which either require consensus or those which could be made more efficient through disintermediation. Disintermediation simplifies a network of participants by removing the necessity of verifying parties. A disintermediated network need not heterogeneous, in the sense that all partners are of the same type of having the same role, merely that the network is designed so that participants whose only real role is verification have been removed (Fig. 1.5). In complex networks, verifiers require resources and may act as a bottleneck to the flow of transactions. In the context of healthcare, consider the possible parties that may be connected as participants in a network processing the exchange of funds relating to treatment; CDOs of different kinds could be connected with, lawyers, Insurance companies or possibly state providers. The exchanges of funding, would be managed by banks unless systems of credit or crypto-currency are used.

Perhaps the most significant feature of Blockchain solutions enable is the ability to attach active logic to each transaction using smart contracts. These smart contracts, as previously discussed, can invoke specialist behaviour, including referencing or altering the current state of the global ledger. An example of this would be a network where a hospital, and specialist clinic and insurance company were involved in the diagnosis and treatment of patients with payment approval respectively. Smart contracts can be used to co-ordinate the stages of the patients care as they occur. The hospital diagnosis automatically raising an appointment with the specialist clinic with payment approval checked against the insurance records. The global state of the ledger allows disputes of anomalies to be discovered early and straight forward cases can be dealt with automatically using the contract. An extension of this could even include the allocation of work to medical staff. Smart contracts could interrogate records on staff experience to allocate work to those who are both qualified and available (Fig. 1.6).

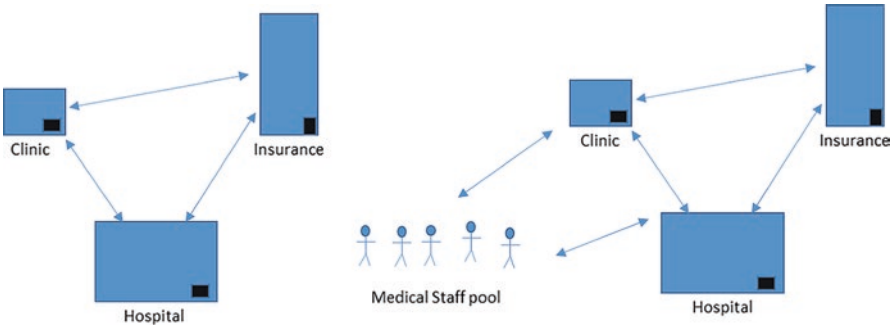

Fig. 1.6 Healthcare networks where Smart Contracts could simplify interaction

None the less as Swan (2015) explains smart contacts of themselves cannot provide new, previously unavailable functionality, rather they "allow common problems to be solved in a way that minimizes the need for trust. Minimal trust often makes things more convenient by taking human judgment out of the equation, thus allowing complete automation." (Swan 2015). Inherent in the security and cryptographic features previously discussed are the issues of identity and non-repudiation. The ability to ensure identity create special opportunities to record ownership of intangible assets such as patient data. This opens the way potentially for patients to assert ownership of information stored within the network about them. There is a transition from numerous Computerised Patient Records (CPR) to distributed CPR across multiple CDOs to the Personal Health Record (PHR) where an assured identity can be used to access data for individuals from across the network or participants.

Additionally, auditors and regulators can use digitally signed and timestamped data stored in the ledgers for managing the activities of network participants. As with smart contracts, this cannot replace the process of auditing though it could simplify the process, therefore, allow it to be more thorough using the same resources (Fig. 1.7). Central to this, of course, is applying adequate cryptographic security features to the network of participants. Different Blockchain frameworks and platforms make a variety of tools available to developers in this respect, the features of which we have discussed previously.

Ethereum (www.ethereum.org) is a framework for the implementation of distributed applications based on public Blockchain systems. The project is overseen by the non-profit Enterprise Ethereum Alliance (EEA) a group with more than 150 members created in 2017. Wood (2014) provides a comprehensive, formal description of the features and architecture of the system. Central to Ethereum, as well as the underlying Blockchain model, is the Ethereum Virtual Machine (EVM) which executes the code implementing the application. There are also suites of specialist protocols for managing distributed relationships such as specialised secure messaging. From its inception, it received a great deal of interest as a general platform for creating applications using smart contracts as their primary building block. The EVM is a Turing complete distributed virtual machine, running smart contracts

Fig. 1.7 Healthcare models based on assured identity and non-repudiation

Table 1.3 Names of ether denominations

Multiplier	Name
10^0	Wei
10^9	Giga-Wei
10^{12}	Szabo
10^{15}	Finney
10^{18}	Ether

code compiled from a number of specialist languages including Solidity and Viper, which are similar to JavaScript and Python respectively. As a public Blockchain, the mechanism for promoting the verification of transactions is based on its own Cryptocurrency, Ether. This typically follows the Proof of Work model (PoW) where Miners are rewarded with Ether for carrying out verification of transactions. Operations in smart contracts have a cost in Ether, paid by the owners in order to deter unnecessary code. Ether is publicly traded with denominations in Table 1.3 more common than Ether itself. Smart contract code compiled as instructions on the EVM are charged to those invoking them according to the specific type or their class with a cost function denoted as "gas" (See Wood 2014 Appendix G Fee Schedule for full details). When projects are initially created they purchase a certain amount of Ether coins to use as "fuel" which may eventually, according to the project's business model become self-sustaining.

As an extensible system optimised for widespread public use, many early implementations were focused on domain specific coins. In the Healthcare context, described by Swan (2015) coins would be created and sold in an Initial Coin Offering (ICO) by a group of clinics who had organised and funded the system. These would either be traded openly or as token values established and managed by the group of clinics. The coins themselves would be stored in unique electronic wallets by their owners, who would include the clinics in the group, their patients and perhaps were the group big enough, insurance companies too. As transactions for care occur, encoded as smart contracts, records would be stored to the Blockchain and verified by miners using proof of work in exchange for Ether. Such a configuration is described in Fig. 1.8. DentaCoin (Den) provides an early example of such an

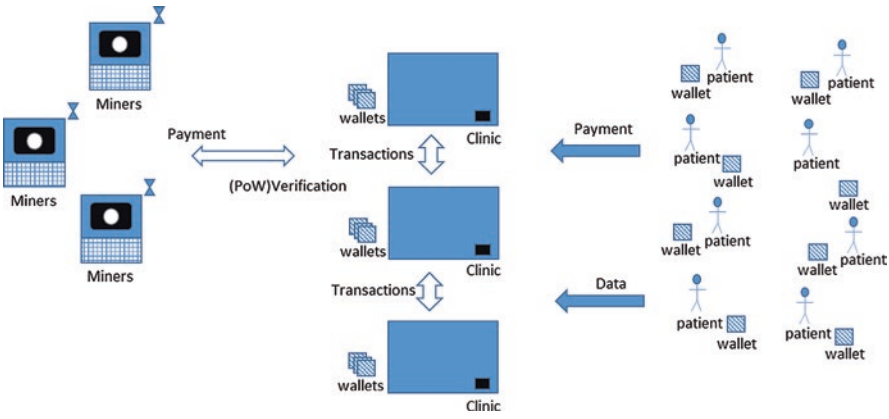

Fig. 1.8 Example of a healthcare coin implementation

approach to healthcare coins, although this platform has developed over time to include patient data and more general cryptographic infrastructure for clinics.

Hyperledger (www.hyperledger.org) is an Open Source project under the governance of the Linux Foundation (Hyperledger 2018). The project began in 2015 providing a codebase for implementing with the aim of providing permissioned Blockchains for Enterprise applications (Hyperledger 2018). Androulaki et al. (2018) describe Fabric as a "distributed operating system for permissioned Blockchains". Currently more the 230 organisations are involved as members. The project includes five code incubation frameworks; Burrow, Fabric, Indy, Iroha and Sawtooth, which offer implementations which provide different features, such as varied consensus mechanisms described in Table 1.4. The frameworks are modular and extensible based on common reusable building blocks. The original implementation Hyperledger Fabric 1.0 was released in 2017, though development based on the framework predated this. As well as Distributed Ledger implementation, Hyperledger features smart contracts implemented using "chaincode" with APIs in standard programming languages including Go, JavaScript and Node.js.

Hyperledger (2018) provide an example where Hyperledger Indy is used as the basis for a credentialing system for medical staff. Hospitals use "credentialing" to ensure that medical staff are both qualified and competent. Digital identity recorded on a Blockchain allows this task to happen more efficiently than is currently possible, hence reducing the costs. (Figs. 1.5 and 1.9).

1.6 Blockchain Healthcare Pilots and Initiatives

In previous sections, we have looked at the technology and concepts behind Blockchain systems regarding their security properties. We reviewed the broad aspirations for the development of Health Information Systems to support in supporting

Table 1.4 Hyperledger frameworks

Framework	Description
Burrow	A platform which implements Ethereum virtual machine supporting both permissioned and permission less
Fabric	The original system providing a modular framework for permissioned enterprise Blockchain using customisable channels and byzantine fault tolerance
Indy	Blockchain framework focussed on the verification of digital identity
Iroha	Specialised implementation based on the Fabric framework with a focus on mobile applications
Sawtooth	A lightweight platform for high volume asset tracking and IOT applications with pluggable dynamic consensus algorithms

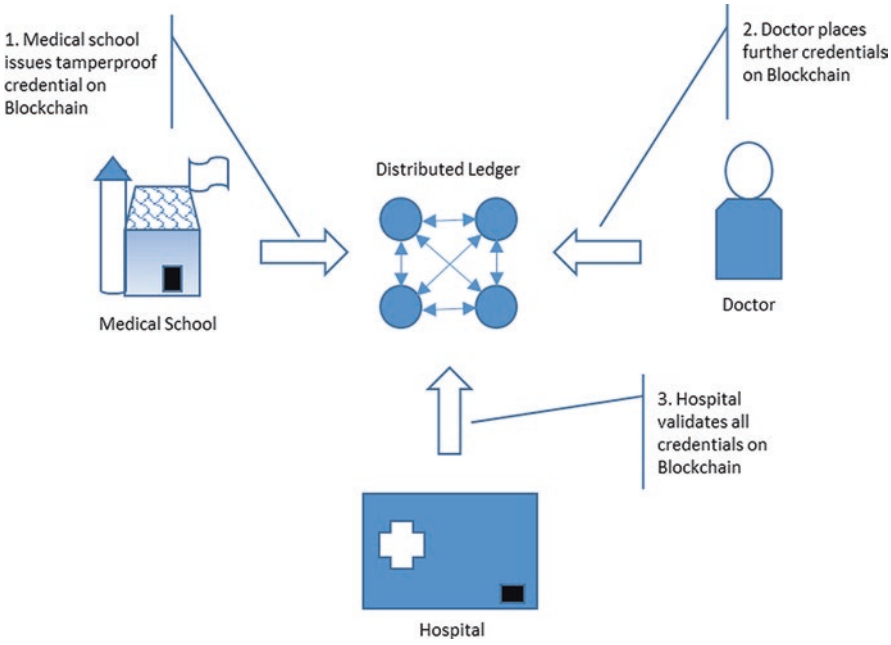

Fig. 1.9 Credentialing medical staff using Indy. (Hyperledger 2018)

the long term goals of evolving the way that healthcare organisations operate. Having explored the patterns for applications and the platforms that support them, we now turn our attention to established projects initiatives already applying this technology. Swan (2015) suggests a number of distinct healthcare applications that might emerge; Healthcoin, Personal Health Records, Research Commons and Notary services. Healthcoin, as previously discussed, is the concept of a domain specific cryptocurrency for the denomination and payment of healthcare services. The benefit of this being that a common currency would help with transparency in multi payer systems and if widespread enough could help to control inflation and simplify the transfer of resources healthcare organisations. The main drawback for

such an implementation would be the widespread support required to make the system work well. Swan (2015) suggests the Personal Health Records stored on a Blockchain could promote common standards for interoperability as well as providing patients with secure access and selective access to their health records. Research commons generalise the theme of secure personal records, with anonymous individualised data, combined with personal fitness data collected from mobile devices used in healthcare research projects, applying privacy controls. Notary services could provide verification required to enact services such as proof of insurance, authenticated test results, or digitised consent. These clearly echo the aspirations of Cybercare (Koop et al. 2008) even if they have yet to put them fully into practice. Some of these though possible would require considerable investment and co-operation to implement practically. None the less interest and investment in Blockchain solutions for healthcare. The following examples are early commercial initiatives where Blockchain technologies have been applied in healthcare.

Patientory is a company, founded in 2016 in Atlanta, which offers end users integrated management of their medical records via an eponymous mobile application. The infrastructure supporting the overall environment is based around the Ethereum framework. As well as allowing app users to develop an individual profile for their health data, users are able to connect to care providers and they are also encouraged to interact with others who have similar health conditions or concerns using social media features. The system is HIPPA compliant and clearly, security has been a critical feature to be addressed during the development phase (Figs. 1.10 and 1.11).

1.7 Summary

Having previously explored the principles and features of Blockchain systems, including a focus on the security characteristics, we looked at some of the problems particular to health care that Blockchain may look to address. We also considered

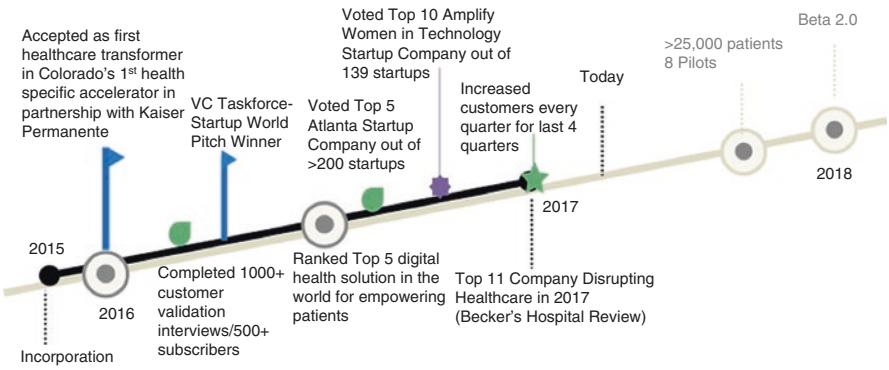

Fig. 1.10 Roadmap indicates development of Start-up from inception to Beta release Patientory (2017)

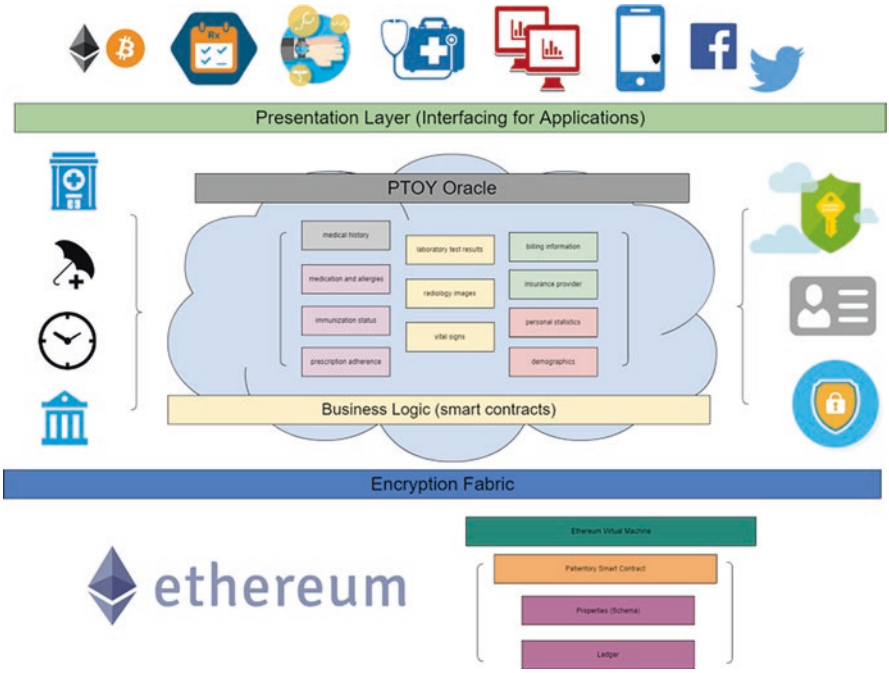

Fig. 1.11 Architectural schematic illustrating integration of Ethereum platfrorm and encryption Patientory (2017)

the conceptual features of these systems apply in problem solving as well as a number of frameworks that have been practically applied to create new healthcare platforms. The implementation described by Nakamoto (2009) was made available via an open source licence and as the potential for its use beyond Bitcoin was recognised several parties created their own implementation platforms and frameworks. Though many were used as the basis for new Crypto-currencies that proliferated over the next decade others were focused on providing a general purpose model that could be applied to business problems more generally. In our first section, we provided an overview of the components that comprise a system based on Blockchain and their fundamental characteristics. That the Blockchain model for the management of data and transactions has potential application in Healthcare Information Systems (HIS) is fairly self-evident. The designs proposed for more effective and integrated HIS pose problems that Blockchain systems could readily solve. That said though, clearly, they are not of themselves sufficient, though perhaps in certain areas they may be considered necessary, or at least an effective and available solution.

The aspirations for HIS have been well mapped and the challenges of adoption have been explored. Some of the issues involve the inertia around sensitive mission critical data. Others are related to investment and support. None the less, as sources

of patient data grow richer and more diverse it is every more tempting to securely integrate systems that exist, and create overall strategic advantages for new approaches of connecting healthcare focused organisations and their supply chains. The introduction of Blockchain technologies may well represent a significant step on the road to the maturity of technology in HIS, supporting their more widespread adoption. In our future work, we shall examine a few of the platforms currently being used to implement systems for healthcare, looking at their background features and variety before exploring early systems in this area.

References

Achour Mostéfaoui MR (2001) Leader-based consensus. Parallel Process Lett 11(1):95–107

Alevtina Dubovitskaya ZX (2018) Secure and trustable electronic medical records sharing using blockchain. In: AMIA annual symposium proceedings. AMIA, Bethesda, pp 650–659

Alhadhrami Z, Alghfeli S, Alghfeli M, Abedlla JA, Shuaib K (2017) Introducing blockchains for healthcare. In: International conference on electrical and computing technologies and applications (ICECTA). IEEE, Piscataway, pp 1–4

Ana Reyna CM (2018) On blockchain and its integration with IoT. Challenges and opportunities. Futur Gener Comp Syst 88:173–190

Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S, Murthy C, Nguyen B, Sethi M, Singh G, Smith K, Sorniotti A, Stathakopoulou C, Vukolić M, Cocco SW, Yellick J (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference. ACM, Porto, pp 30:1–30:15

Apostolaki M, Vanbever L, Zohar A (2017) Hijacking bitcoin: routing attacks on cryptocurrencies. In: Symposium on security and privacy, IEEE, pp 375–392

Ariel Ekblaw AA (2016) A case study for Blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In: 2nd international conference on open & big data. IEEE

Asolo B (2018) Proof of importance explained. Retrieved from https://www.mycryptopedia.com/proof-of-importance/

Atzei N, Bartoletti M, Cimoli T (2017) A survey of attacks on Ethereum smart contracts SoK. In: Proceedings of the 6th international conference on principles of security and trust – volume 10204, ACM, pp 164–186

Tama BA, Kweka BJ, Park Y, Rhee K-H (2017) A critical review of blockchain and its current applications. In: International conference on electrical engineering and computer science (ICECOS). IEEE, Palembang, pp 109–113

Cermeno JS (2016) Blockchain in financial services: regulatory landscape and future challenges for its commercial application. BBVA

Chang J (2018, Oct) Blockchain: the immutable ledger of transparency in healthcare technology. Retrieved from sidebench: http://sidebench.com/blockchain-healthcare-technology/

Chen L, Xu L, Shah N, Gao Z, Lu Y, Shi W (2017) On security analysis of proof-of-elapsed-time (PoET). In: Stabilization, safety, and security of distributed systems. Springer, Cham, pp 282–297

Delegated Proof-of-Stake Consensus (2018, Oct 23). Retrieved from bitshares: https://bitshares.org/technology/delegated-proof-of-stake-consensus/

El-Yafouri R, Klieb L (2014) Electronic medical records adoption and use: understanding the barriers and the levels of adoption for physicians in the USA. IEEE 16th international conference on e-Health networking, applications and services (Healthcom) 2014 pp 506–512

Eyal I, Sirer EG (2018) Majority is not enough: bitcoin mining is vulnerable. ACM Commun 61:95–102
Angeletti F, Ioannis Chatzigiannakis, Vitaletti A (2017) The role of blockchain and IoT in recruiting participants for digital clinical trials. In: 25th International conference on software, telecommunications and computer networks (SoftCOM). IEEE, Split, pp 1–5
Wang F-Y, Yuan Y, Rong C, Zhang JJ (2018) Parallel blockchain: an architecture for CPSS-based smart societies. IEEE Trans Comput Soc Syst 5(2):303–310
Gervais A, Wust K, Glykantzis V, Ritzdorf H, Capkun S, Karame GO (2016) On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, Vienna, pp 3–16
Hyperledger (2018) An introduction to Hyperledger Retrieved from https://www.hyperledger.org/wpcontent/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf
Saranummi N (2009) Keynote: personal health record and value-based healthcare 2009. 9th international conference on information technology and applications in biomedicine, 1–4, 2009
Sukhwani H, Martinez JM, Trivedi KS, Chang X, Rindos A (2017) Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In: 36th symposium on reliable distributed systems (SRDS). IEEE, Hong Kong, pp 253–255
Herlihy M (2017) Blockchains and the future of distributed computing. In: Proceedings of the ACM symposium on principles of distributed computing. ACM, Washington, DC, pp 155–155
Irwin PR (2017) Tracking digital footprints: anonymity within the bitcoin system. J Money Laundering Contro 20:172–189
Ko J, Lu C, Srivastava M, Stankovic J, Terzis A, Welsh M (2010) Wireless sensor networks for healthcare. Proc IEEE 98:1947–1960
Jayachandran P (2017, May 31) The difference between public and private blockchain. Retrieved from Blockchain Unleashed: IBM Blockchain Blog: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
Koop E, Mosher R, Kun L, Geiling J, Grigg E, Long S, Macedonia C, Merrell R, Satava R, Rosen J (2008) Future delivery of health care: cybercare. IEEE Eng Med Biol Mag 27(6):29–38. https://doi.org/10.1109/MEMB.2008.929888
Judmayer A, Stifter N, Krombholz K, Weippl E, Bertino E, Sandhu R (2017) Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms. Morgan & Claypool, San Rafael
Juels A, Kosba A, Shi E (2016) The ring of gyges: investigating the future of criminal smart contracts. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, pp 283–295
Kao SH (2018) The static analysis of WannaCry ransomware. In: 20th international conference on advanced communication technology (ICACT). IEEE, Korea, p 1
Lamport L, Pease M, Shostak R (1982) The byzantine generals problem. ACM Trans Program Lang Syst 4:382–401
Lima C (2018) Blockchain-GDPR privacy by design: how decentralized blockchain internet will comply with GDPR data privacy. IEEE
Liskov MC (1999) Practical byzantine fault tolerance. In: Proceedings of the third symposium on operating systems design and implementation. ACM, New Orleans
Mayo KP (2016) A blockchain-based approach to health information exchange networks. Semantic Scholar
Mettler M (2016) Blockchain Technology in Healthcare: the revolution starts here. In: 18th international conference on e-health networking, applications and services. IEEE
Patientory Inc (2017) Retrieved from https://medium.com/@patientory/healthcare-re-engineered-and-powered-bypatientory-ff667b86066 (On November 2018)
Rifi N, Rachkidi E, Agoulmine N, Taher NC (2017) Towards using blockchain technology for eHealth data access management. In: 2017 fourth international conference on advances in biomedical engineering (ICABME). IEEE, Beirut, pp 1–4
Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system

Oguzhan Ersoy ZR (2017) Transaction propagation on permissionless blockchains: incentive and routing mechanisms. In: Crypto valley conference on blockchain technology. CoRR

Ongaro D, Ousterhout J (2014) In search of an understandable consensus algorithm. In: Proceedings of the 2014 USENIX conference on USENIX annual technical conference. ACM, Philadelphia, pp 305–320

Vimalachandran P, Wang H, Zhang Y, Heyward B, Whittaker F (2016) Ensuring data integrity in electronic health records: a quality health care implication. In: International conference on orange technologies (ICOT). IEEE, Melbourne, pp 20–27

Piekarska HH (2017) Introduction to security and privacy on the blockchain. In: European symposium on security and privacy workshops (EuroS&PW). IEEE, Paris, pp 1–3

Proof of Authority Chains (2017) Retrieved from https:// github.com/paritytech/parity/wiki/Proof-of-Authority-Chains

Quenetain SD (2017, Oct 23) Delegated proof of stake: the crypto-democracy. Retrieved from Blockchain Expert: https://www.blockchains-expert.com/en/delegated-proof-of-stake-the-crypto-democracy-2/

Bush RA, Kuelbs C, Ryu J, Jiang W, Chiang G (2017) Structured data entry in the electronic medical record: perspectives of pediatric specialty physicians and surgeons. J Med Syst 41(5):75

Ryan Henry AH (2018) Blockchain access privacy: challenges and directions. IEEE Comput Rel Soc

Scheuermann FT (2016) Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun Surv Tutorials 18(3):2084–2123

Spiegelman IA (2016) Solidus: an incentive-compatible cryptocurrency based on permissionless byzantine consensus. CoRR

Kabene SM, Orchard C, Howard J M, Soriano MA, Leduc R (2006) The importance of human resources management in health care: a global context. Hum Resour Health 4:1478–4491

Ross SE, Lin C-T (2003) The effects of promoting patient access to medical records: a review. J Am Med Inform Assoc 10:129–138

Steward J (2017) BGP hijacking for cryptocurrency profit. Retrieved from Secureworks: https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit

Tian H, Zhang Y, Xing C, Yan S (2017) SGXKernel: a library operating system optimized for intel SGX. In: Proceedings of the computing frontiers conference. ACM, New York, pp 35–44

Swan M (2015) Blockchain: blueprint for a new economy 1st ISBN 1491920491 9781491920497. O'Reilly Media, Inc

Tosh DK (2017) Security implications of Blockchain cloud with analysis of block withholding attack. In: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing. ACM, Madrid, pp 458–467

Wen WW (2018) A survey on consensus mechanisms and mining management in blockchain networks. CoRR

Gordon WJ, Catalini C (2018) Blockchain Technology for Healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J:224–230

Xiaoqi Li PJ (2017) A survey on the security of blockchain systems. Futur Gener Comput Syst

Liu Y, Liu X, Tang C, Wang J, Zhang L (2018) Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin. IEEE Access 6:23261–23270

Wood G (2014) Ethereum: a secure decentralised generalised transaction ledger. Retrieved from https://gavwood.com/paper.pdf

Yi XL (2018) A new blind ECDSA scheme for bitcoin transaction anonymity. IACR Cryptology ePrint Archive, p 660

Zonyin Shae JJ (2018) Transform blockchain into distributed parallel computing architecture for precision medicine. In: 38th international conference on distributed computing systems. IEEE, Vienna, pp 1290–1299

Chapter 2
Digital Transformation of Healthcare

Hamid Jahankhani and Stefan Kendzierskyj

Abstract The digital transformation needs to go a lot further to provide a seamless but secure and protected data interchange where a multitude of beneficial impacts can be gained such as longitudinal medical data, interoperability, secure patient centric generated data and its use cases, to name a few. Positioned with the increasing threat of data breaches, the healthcare sector has started to make deeper inroads into the beneficial uses of blockchain as the mechanism to provide immutability, audit trail, security and protect the privacy of data to ensure a better way forwards for healthcare transformation. This chapter aims to discuss the impact of digital transformation on the healthcare industry.

Keywords Digital transformation · Interoperability · Blockchain · IoMT · Data breaches · Cyber-attacks · Patient centric data · Electronic health records · Health information exchange

2.1 Introduction

The healthcare industry has undergone a transformation, as other industries, with the move from paper based methods to electronic and technology moving more from on-premise to cloud based servers with some levels of integration to other systems. But looking further into the current setup and future needs, it is clear a much more strategic digital transformation needs to happen for a number of reasons that all support and benefit each other's case. This expeditious progression in technology is leading towards more precision based medicine with better patient outcomes at point-of-care. This helps both healthcare professionals and patients to arrive at more efficient and quicker diagnosis. Technology is assisting this movement forwards be it in smart wearable devices, IoMT, etc., but a transformation is needed to see more widespread interoperability between the silos and disparate

H. Jahankhani (✉) · S. Kendzierskyj
London Campus, Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk; Stefan.Kendzierskyj@northumbria.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_2

systems. An individual patient's medical record still sits in an insular system with no full archive of the longitudinal medical history. Also, even though it is well documented that the healthcare industry is under cyber-attack and processes/solutions are continually deployed to mitigate the attacks, it still has not lessened the fact that data is widescale breached. As all technology progresses at fast rate of knots then some form of methodology is needed to ring-fence the security aspects, keep integrity but equally provide transparency of data.

Blockchain appears to be the driving mechanism to offer a secure framework to operate under and enables the possibility to provide this needed interoperability and help progress the transformation in a more integrated nature. The themes associated with transformation can all benefit from this programme of enhancement leading to possibilities to make better use of artificial intelligence and machine learning for more precision based medicine and better delivered patient outcomes.

2.2 Defining the Driving Factors of Blockchain in Healthcare

The focus of this section discusses the advocacy of blockchain in healthcare and for a number of important reasons that stand independently of each other, but collectively create a strong purpose to solve legacy and more recent issues, some causing more serious effects. Transparency and security of data are key drivers that blockchain can provide and take care of the corruption, fraud, misconduct that are discussed in Chap. 3 in how clinical trials are conducted. Closely linked, are improving patient privacy and having a more patient centric outlook for a longitudinal medical history that solves interoperability problems.

Figure 2.1 presents the healthcare landscape and starts with current issues and working counter clockwise to the blockchain mechanism.

The above mapping explains the current issues with the disparate silos of data that offer no linkage or ease of data access to patients, health providers and other organisations. Although held in silos this does not offer any confidence in privacy and security of patient data since there may be inadequate layers to offer correct authenticated access. There are a lot of benefits to hold the medical records in what is known as longitudinal data giving patients and healthcare providers a complete medical history. Also, with all this longitudinal medical data held in a secure method such as blockchain gives rise to great opportunities of analytics, with the consent of parties involved. Consent can be authenticated via blockchain. These analytics can offer a greater insight into health issues and better ways to offer more efficient clinical paths and form a validated health information exchange that takes care of interoperability issues.

Alongside longitudinal medical data are other important considerations regarding clinical research data and the process/current methods deployed from setting up trials, ensuring correct stages of informed consent are captured, to the reporting in the trials and post marketing of drugs. Issues arise in a number of stages with evidence in how trials are setup, non-conformance of consent and the dangers of

Fig. 2.1 Mind map of all concepts connected to the healthcare landscape

selective reporting, bias and misconduct which leads to much more serious implications explained in later sections. Blockchain can play a significant part in all parts of clinical research processes.

The advancement of smart wearables and Internet of Medical Things (IoMT) has meant much more accurate data can be captured seamlessly as sensors update cloud systems automatically. There is a huge increase in data expected with the billions of medical devices set to occur over the next few years. More data presents some concerns over storage with the cost implications but equally over the security of the data. Again, with some application to blockchain there can reside a more secure method to authenticate access to the data to only those with permissions that were allowed. This will give more clarity and privacy comfort to patients knowing that authentication is the layer of protection to their sensitive medical data.

As the Fig. 2.1 map illustrates that there is a very alarming factor indicating the rise of cyber attacks in the healthcare section and their sophistication. It's a known fact that the healthcare industry suffers the highest level of cyber-attacks. These attacks result in a multitude of issues from ransomware and data breaches that lead to identity theft and victimisation. Some attacks can be devasting and after effects

not fully understood since patients will not likely be aware of any criminalisation of medical data post attack from the breached data. Clearly, the reasons for some undertaking the attacks are financial gain from selling of the breached data at high values in comparison to other data such as credit card information to obtaining ransomware payments and further spiralling effects of identity theft. But hacktivism is also on the rise where financial gain is not the motive and more born out of a desire to install chaos or state sponsored attacks designed to destabilise economies or political turmoil. Exposure to the increased cyber-attacks in healthcare is a serious issue, not just for the healthcare organisation but also to the individual, since none can determine what damage can be achieved with breached data in the hands of criminals. It is a driving factor to ensure a method is cultivated to protect and secure such as blockchain.

The following other sections in this Chapter covers areas of healthcare transformation such as IoT, smart wearables, devices, etc., that enhance aspects of precision medicine and patient outcomes but create the additional concerns with more data and the way it is currently. More depth is given to the interoperability that blockchain provides and higher levels of protection for privacy of data than the current methods of Trusted Third Party. Figure 2.2 displays some of the central themes of healthcare transformation.

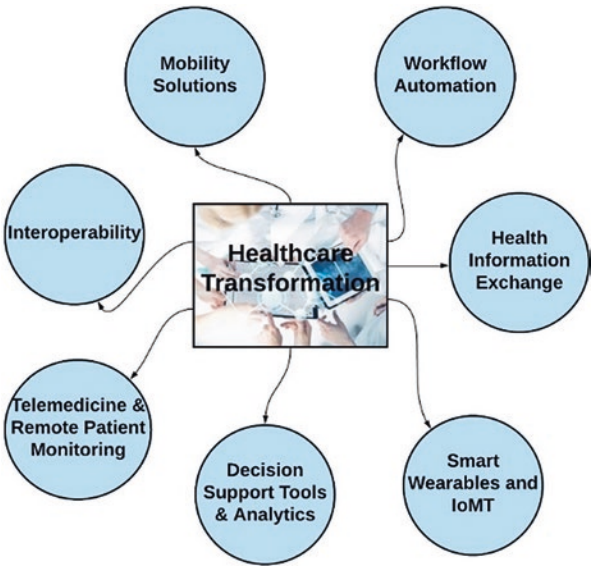

Fig. 2.2 Healthcare transformation drivers

2.3 Digital Transformation of Healthcare Records

All the population in any given territory, at points of their life, touch with healthcare records. There has to a place where all the patient's medical history and clinical data is stored. The obvious key data is what makes our identity unique, be it data of birth, social security number, and so on. It also contains all the diagnosis, medications, allergies, immunizations, laboratory test results. So, a mixture of personal and highly sensitive information. It is clear why medical records are intrinsic to the operational side of healthcare as without access to a record many functions would cease e.g. an operation due to take place needs have the medical record reviewed first. The records will contain extremely sensitive information that will have direct correlation to how they should receive treatment and diagnosis, Dubovitskaya et al. (2017). The records are also shared between many parties that needs give input/opinion as to arrive at best outcomes.

Personal and sensitive information makes the value of a healthcare record be worth a much higher premium on the deep web. This is due to personal identity information being something one cannot just cancel as would happen with a stolen credit card. The criminalisation value also increases in terms of its re-use life cycle or longevity, so the more times it can be re-sold or help to purchase medications, setup other criminal ventures, etc. So, the digitalisation of records has made it easier to re-use since when cyber-hackers attack they can access many records quickly, remotely and in a format that is easily transferable to the deep web or other criminal exchange sites. This was not the case or that easy with manual paper based records and would have been a laborious task for determined criminals.

In 2008, there were only less than 10% of medical records being stored in electronic format (see Fig. 2.3 and adoption of EHR records, ONC 2016).

With the obvious drawbacks of paper-based records, electronic healthcare records (EHR) increased to a point where practically all are kept in this format.

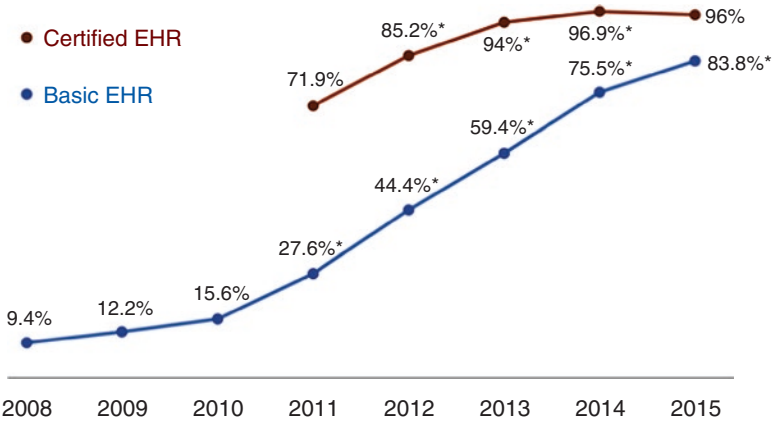

Fig. 2.3 Adoption of EHR records. (ONC 2016)

Whilst all acknowledge that paper-based records are difficult to share, the electronic format has largely been a similar issue and remained in silo providers and consequently this conveys an interoperability obstacle. This disparate updating of electronic medical records makes this difficult to track and keep up to date since they are held in silos and require multiple consents. All medical stakeholders need access and there is a case for the patient to also have assurances to access a longitudinal medical history. The transformation from paper to electronic was a necessary step and certainly the digital format allows a number of benefits in storage and ease of access. The issue lies in the interoperability and authentication as explained by recent organisations undertaking reports and analysis. Centralizing records is not the question or task but there is a question mark over its security when centralised as explained in later sections. Patients have concerns now in how the EHR is maintained with so many recent highlighted cyber breaches and this has impacted on their reluctance to divulge all information on the record.

In 2015, a published report by the Office of the National Coordinator for Health Information Technology (ONC) laid out the *Shared Nationwide Interoperability Roadmap* which presents a 10-year roadmap for interoperability, ONC (2015). In summary, 16 key areas were highlighted to find better ways to improve authorization/access, longitudinal health data, identity, etc., to name a few. As well as interoperability, this sensitive data would benefit all if it could be shared with a range of providers such as healthcare institutions, pharmaceutical industry, insurance companies, research establishments, gathering and securing of IoMT smart/wearable data, etc. But essentially the consideration is to put the patient first and give them the control and permission to allow access. From a patient perspective, giving them control through permissions is safer for allowing sensitive data to be accessed and clinical researchers have more benefits to gain permissions to a pool of data; whereas currently there are concerns in the way data is held in the centralised manner.

This has been the reason why there is great hope and consensus to create data access through blockchain architecture which contains the properties to be immutable, auditable, scalable, and ensure privacy and security are respected. As Dubovistskaya et al. (2017) note that it was relying on centralised entities storing sensitive data and controlling permissions (i.e. the patient had no control) that meant a single point of failure was an issue and the breakdown of any interoperability taking place. Also, why this discussion covers healthcare data breaches/ransomware as it's a significant added factor to give weight to the blockchain debate in terms of enforcing a better method of security.

Engelhardt (2017) in the review *'Hitching Healthcare to the Chain'* makes four concise points that summarise why healthcare needs balanced patient care with privacy/access, completeness of information, cost and by putting the patient at the centre of all in terms of data control allows them to be 'active agents in their own care'.

2.4 Privacy of Data and Interoperability

Data privacy has become more complicated as the increase of the Internet usage and digital/electronic data became a normal way to interface with holding records. Hence, why this has led to more recent need to control who has access to the data and regulated frameworks, such as GDPR. Since this publication has a central theme of securing data, then there are a few worthwhile factors to mention on how to treat the data depending on the healthcare requirements in the concept of blockchain. There are ways in which data could interact with blockchain, be it off-chain and on-chain data storage. Depending on its healthcare use case may be how data can be stored, if for example as off-chain in data lakes with blockchain acting as the authentication mechanism.

Essentially, for privacy permissions, there are three ways to store the data:

- **Unencrypted data** – all those on the chain, such as a public chain, can read all data
- **Encrypted data** – participants must use their private key to access the data
- **Hashed data** – this is the authorisation link that is the immutable digital record and timestamp and directs to where data is secured off-chain.

Sensitivity and who should access are the primary questions to help determine type of blockchain and how the data should be treated. Particularly in the healthcare industry, to comply with regulatory complications and the size of data (for example large data files such as imaging data) it is mostly likely to suit as off-chain deployment; Engelhardt (2017). In some cases, the data is being stored in data lakes, so an ecosystem is created with blockchain controlling as the hashed authentication permissions and pointing to the off-chain data lake. Linn and Koo (2016) explains that transactions in the block contain the user's unique identifier, the encrypted link to the health record and transaction timestamp. There can be certain metadata included within the transaction. Regarding the data lake, any information located here is encrypted and so protects only those authorised to access and security and privacy are respected.

See Fig. 2.4 for an example concept on the interoperability of healthcare data and how this ecosystem can facilitate a health data interchange in a secure way and protect privacy. In a later Sect. (2.4), *Is Healthcare Ready for Blockchain*, there are a number of successful pilots/live systems deployed that has given confidence to pursue further blockchain methods in healthcare.

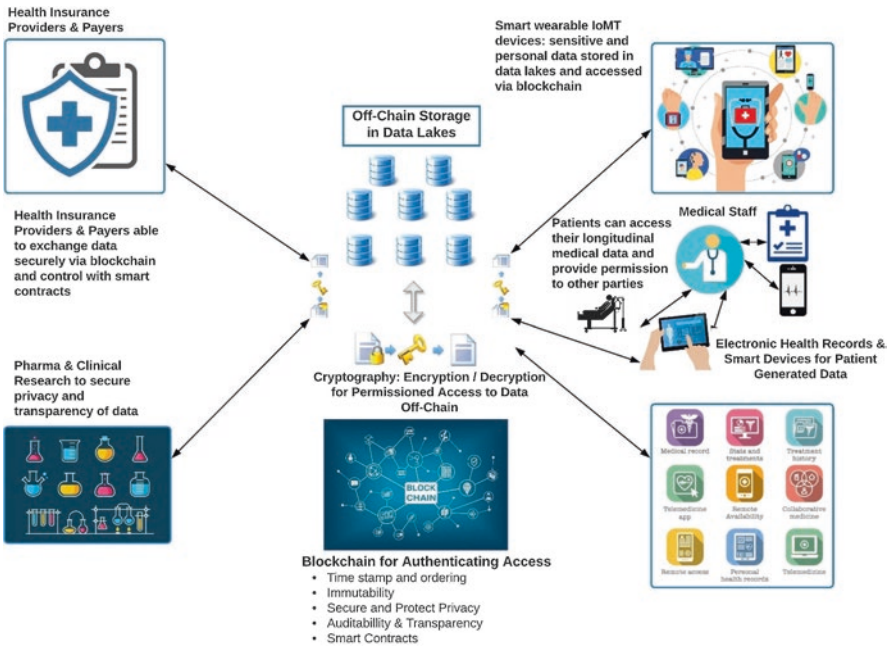

Fig. 2.4 Example of Blockchain ecosystem demonstrating interoperability and health data interchange

2.4.1 Interoperability

If privacy is a key component to a patient's security and how that data is authenticated through blockchain, then so too is the interoperability and how to overcome the disparate silos of data that presents to aim for the concept of longitudinal medical history. It is not just to satisfy the purposes of ease of access to medical history, but this is what is needed to also facilitate and keep up with the technological advances being made in precision based medicine. So, it is a fundamental aspect as part of healthcare transformation.

Interoperability covers the capability to allow a seamless interchange of data across different information systems and different software applications. Although operating systems and cloud based architecture have allowed a lot of flexibility it stops at the point where data cannot reach outside its silo unless organised in a requested way for particular information or setting up some form of API (Application Programming Interface) which means a method or pre-set protocols and programming. Although an interchange of information occurs, it is restricted in its requests, security and certainly a patient has no control over it. Plus, there is an expense, for example, to handle a requested transfer of patient information from one institution to another. If the expense was approved, then it too must satisfy the legal and regulatory side of things which likely has to have some stages of approval to send and add

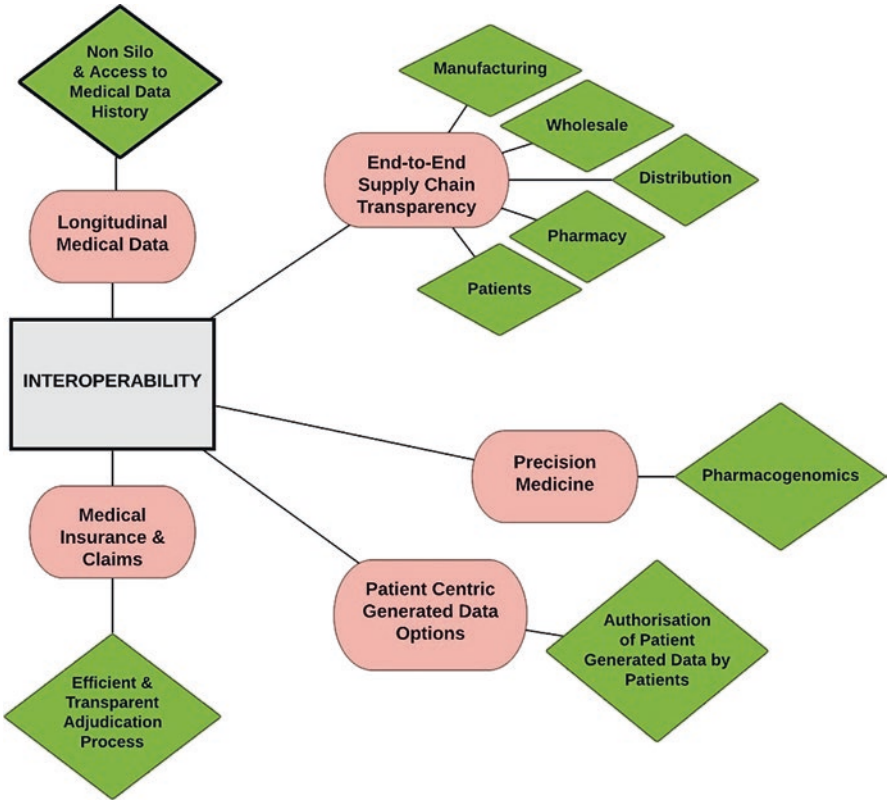

Fig. 2.5 Example of Blockchain ecosystem demonstrating interoperability and health data interchange

to delays and expense in time spent by various parties. This is exactly how blockchain can sit in the layer as the facilitator to all requests and be done through an automated but secure process. The requests could come from any permissioned entity/person that requires the information. As the blockchain authenticates the enquiry the transfer can all be tracked, timestamped in an immutable manner and work as smart contracts basis. This could be a pharmaceutical company requesting data sets across agreed patients to help develop drugs, medical claims could be settled faster, manufacturers trying to develop precision based medicine, etc. The list can be exhaustive and refer to Fig. 2.5 for how interoperability facilitates this and main theme areas of interest.

Perhaps, also a useful driver to transformational change is that, with regards to all the existing systems/databases, they do not need to be changed and can be enhanced and supported into an integration to blockchain architecture that is put in place. In some ways this gives the expression commonly used as requiring a 'single version of the truth' and certainly blockchain can offer that.

2.5 Pushing the Barriers of EHR Access

Currently there are many obstacles for allowing transfer of electronic healthcare records, if considering not just different providers, but also inter country requests as these likely have to satisfy country's legal regulations. These barriers create the difficulties for even a patient requesting their own medical data and there is a general unwillingness for providers to allow it or suggest a high expense to facilitate. Working in tandem to the difficulty to release records is also the concern a patient has in how secure their medical data is, so sometimes data from a patient is withheld due to sensitivity they feel could make then vulnerable should data be 'leaked' in an unauthorised way (it would be hard to track down due to no immutable process).

Blockchain can eliminate these barriers, allow the secure interchange of data to occur in a tracked and authenticated fashion and allow patients to trust the privacy blockchain provides (so perhaps be more transparent in what they advise their medical providers). There are already specific projects to transform how EHR can be better placed in a decentralised system such as blockchain. For example, Labchain is run by DDQ a company legally approved by the Dutch government to run a permissioned blockchain to allow digitally transferring blood values instead of the current system of using postal mail to exchange values, Labchain (2018). These would be blood analysis results that can be exchanged between hospitals and is secure as the data is not stored on the blockchain and is off-chain. This is used as authentication by way of hash values and is the digital fingerprint and immutability that blockchain can offer.

2.6 Smart Wearables and Data Capture

The possibilities and coming transformations within healthcare for using the Internet of Things (IoT) and Internet of Medical Things (IoMT) offers huge potential with remote monitoring and obtaining data from medical sensors on the body that report data seamlessly to cloud systems. Under older methods, biometric details would need to be physically captured or extracted from patients and written up as recorded information alongside the medical record and stored in a silo method. With the transformation of device capability and huge growth in the healthcare industry gives way to a more accurate and reliable method to record vital signs, skin temperature, body weight, heart rates, blood sugar levels, sleep patterns, calorie measurements, medication intake and effects, etc. There are also a whole range of fitness devices that offer metrics and analysis and offer a unique footprint for digital forensics explained in later chapters and shown in Fig. 2.6 as to types of devices and information exchange.

There are many benefits to improve patient outcomes, help conduct research and capture data in clinical trials. Rifi et al. (2017) observe these benefits and acknowledge the data sharing will improve the communication between patients and

Fig. 2.6 Smart wearable devices and interaction with patients and data storage off-chain

healthcare professionals, but also make aware that the security needs to be taken care of and blockchain is a solution to help provide this.

A robust infrastructure must be in place to protect and secure data; Liang et al. (2017) discusses the concept of data sharing and incorporating smart wearables into this design and running this over blockchain. Rather than just support the data in conventional cloud based systems in an uncoordinated or unconnected way this could be better addressed by using blockchain as the underlying architecture to control permissions, security and authentication. Whenever the patient generates health data it can then be seamlessly uploaded to the blockchain. It offers the quality of immutability and time-stamping, so for example in the case of clinical trials it's of importance to capture valid and correct data from smart wearables, otherwise it will be difficult for researchers to correlate and measure. Also, looking at it from the perspective of a patient it provides that protection and security layer to the personable and sensitive information a patient would be concerned if breached into places where identity theft and victimisation are the currency of criminals. As explained later in this chapter there are a few innovative live deployments where patients can make use of their data accumulated from their medical interactions. For example,

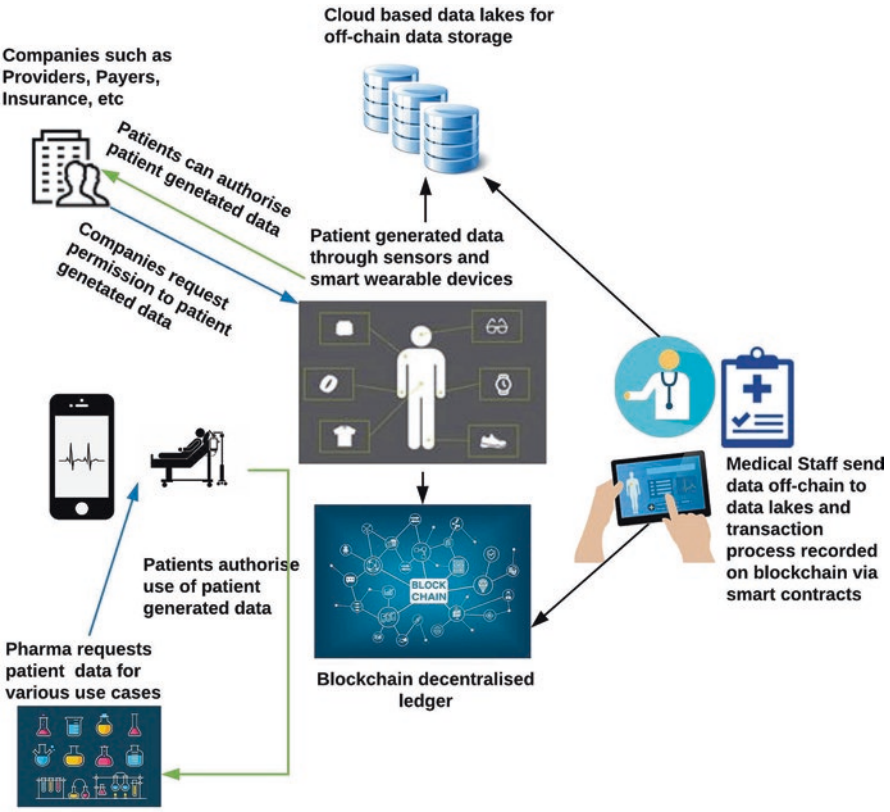

Fig. 2.7 Patient Centric Personal Health Data Sharing

either selling or donating biometric data to pharmaceutical industry. What was once a model where the patient was the last to know on contents of their data (or what was held on them) or be able to access data puts them in a position of control in this patient centric model. It ties very closely in with interoperability regarding data and its access points.

The idea of patient centric generated data, where the patient is at the centre of how their data is utilised, can be seen in Fig. 2.7. It gives a concept flow of the patient being in control and experience a better range of outputs than current architectures allow.

Looking specifically inside the world of clinical research, accuracy and transparency are key indicators to help measure effectiveness in trials. Zevala (2017) adds weight to the reasons why smart wearables are helpful for improving accuracy in clinical trials with data being collected in between visits instead of manual processes and relying on memory of patients. This also takes care of data becoming corrupted and can also alert researchers to any non-compliance or safety issues to the patient. Also, as the data is automatically collated this offers flexibility to the

patient and not impact on their time regarding reporting/recording. Bresnick (2016) reports on a survey by the Association of Clinical Research Organisations (ACRO) that there is high intensity to support IoT/IoMT due to the benefits talked about for precision medicine, but there must be security and privacy of the data. It's becoming clear why support is growing for blockchain and evidenced in surveys discussed in later sections of this research.

However, with this potential explosive increase in data also leads to more higher risks to security and privacy if not properly addressed. More and more data will be gathered and be a signature identity to the patient and create more unique biometrics.

2.7 Patient Centric Data Ownership

It has been mentioned that by sharing electronic health data across multiple organisations it can potentially save billions in cost, Monegain (2013). Research was undertaken by Premier Quest Alliance across 333 hospitals, that are members of the Alliance group, and analysis mentions by sharing the data, 92,000 lives were saved and with revenue savings of just over $9 billion over 4.5 years. Some key results of central-line associated blood stream infections reducing by 59 per cent and pressure ulcers by 64 per cent. If extrapolated nationwide, then 950,000 lives could be saved and savings of $93 billion. Saving lives is a key driver of healthcare services and blockchain can allow the discussion to be easier as it takes care of the more difficult questions on how to manage security and data sharing.

However, there are other reasons outside the saving lives and interoperability savings and revolves around healthcare data being a wealth of intelligence and by sharing this data it can improve the quality of services and innovations to make systems smarter and target precision medicine; Yue et al. (2016). With data currently scattered in silo mode in many different provider systems this makes the task of strategically looking at healthcare data in a smart way almost impossible. Many providers would be concerned on breaking the privacy parameters to patients if by sharing data in conventional ways. But equally and also worrying is that it is not reliable to leave responsibilities to Trusted Third Parties (TTP) where a single point of failure can be attacked, and data breached.

The innovative approach is to allow the patient to sit in the centre of all, have a concept of real-time monitoring of their health journey and essentially be in control. Having a patient centric driven model opens to other dimensions and use cases. Simply put, there would be a range and variety of stakeholders interested to mine the data available, with of course permission granted by patients. Research industry and other organisations will be keen to access this wealth of data to re-purpose to a number of initiatives that may be precision based medicine or unlock a number of new in-roads to solving diseases with smarter interventions. The data, if permissioned and released to industry, across millions of users can be anonymised and further protect patients since the core data is what is significant. Also, as mentioned

in the previous section, combining electronic medical data with smart data that has guaranteed accuracy (since it is recorded by sensors) again gives the healthcare industry huge confidence. Artificial Intelligence (AI) can also play a factor to help mine and analyse the data to better predict outcomes and correlations. There can be a Machine Learning aspect to 'train' these systems to intelligently predict and proactively offer intelligent insights for better decision making processes.

2.8 Other Blockchain Health Transformation Benefits

Whilst the above sections focus more on the blockchain tangible benefits of transformation in a sense of improving health, targeting precision medicine and patient outcomes, utilising the wealth of data intelligence etc., there are other benefits that can also equally play a strong factor for consideration and explained in the following.

2.8.1 Claims Adjudication

Currently there are many complex methods and processes to adjust and approve payment to claims made. There are estimations that 10% of healthcare costs are fraudulent. Das (2017) gives indication that in the US in 2016, Medicare fraud has caused $30 million in losses which could mostly be around non-performed services or excessive billing. By trusting the data shared, having easier data interchange process and automating the process and provide an immutable and auditable chain through smart contracts, can give a more transparent vision of the 'single version of the truth'. There should also be cost savings for applying more efficiency to the process in terms of facilitating payments more quickly and less communication required to do that. Many believe that there is scope to eliminate third parties such as clearing houses, third-part administrators, etc. There is a further interesting concept that ties into patient centric data and smart wearables and that is the possibility or real-time adjustments to premiums. If data from smart wearables is automated to smart contracts held on blockchain, then it may be possible to incentivise patients to better lifestyle as premiums can automatically re-adjust according to health risks and better well-being, etc., from data that is analysed. Presently if attempted in a conventional way then the method would be more static and require a lot of human intervention for applying a re-issued premium and how to audit it in a way that is trusted. If pursued through a blockchain method, then it will be more dynamic and responsive to the patient and its interactions and full audit trail given.

Blockchain can help manage better the high overhead healthcare administration costs that are inefficient with issues of duplication of requests. For example, some studies have been completed that indicate large amounts of budget are wasted in paperwork trails that are connected with insurance and billing claims and have

concerns over transparency on price; Jiwani et al. (2014). It makes sense that blockchain can help transform the processing side of healthcare administration as its would be configured to eliminate the duplicate processes and automate transactions and use smart contracts methodology to reconcile and audit all.

2.8.2 Drug Traceability and Issues in the Supply Chain

The issues around counterfeit drugs and its authenticity can have detrimental impacts for those connected along the supply chain to the patient. Deception and fraud lie amongst drug origin, expiry, compound mixtures that may be contaminated or wrong ingredients that impact effectiveness, wrong dosage, and the list can go on. There should be some secure method to manage all from raw materials to active pharmaceutical ingredient (API), to manufacturing, formulation, packaging and distribution. Where the supply chain is so sensitive to these external pressures there should be a positive momentum towards adopting blockchain as the layer to give the traceability, immutability, time-stamping through its smart contract process.

According to some research undertaken by the World Health Organisation there is evidence to suggest 10% of drugs worldwide are counterfeit and that dramatically increases in developing countries to 30%; Mettler (2016). Counterfeit drugs hold no boundaries and cross from supplement type to more treatment type drugs for disorders (e.g. cardio-vascular). They can have impure qualities, high or low dosages and if the patient relies on the active ingredients to work for health preservation then it becomes more high risk and dangerous to the patient. When blockchain is used, everything is time-stamped and recorded on the chain as to the production date, location and its product component origins. Ownership, in case of transfer to other parties is also transparent. Anything that is out of the chain is not verified and can be treated as forged until evidence is given as to the parameters set (or rules applied to smart contracts). The objectives to control and reduce counterfeit drugs could be achieved as well as potentially saving lives through controlling ineffective drugs that contaminate the supply chain.

Figure 2.8 explains how blockchain can be the mechanism to secure data from any tampering and help deter counterfeit drugs from entering the supply chain or the myriad of other issues discussed earlier in this section.

2.9 Is the Healthcare Industry Ready for Blockchain?

To gain confidence and global consensus (as well as prove the creditable research with evidential backed models that work) there should be blockchain pilots undertaken for analysis. In this section there are some leading examples of live deployment of blockchain within the healthcare industry. Each live deployment addresses

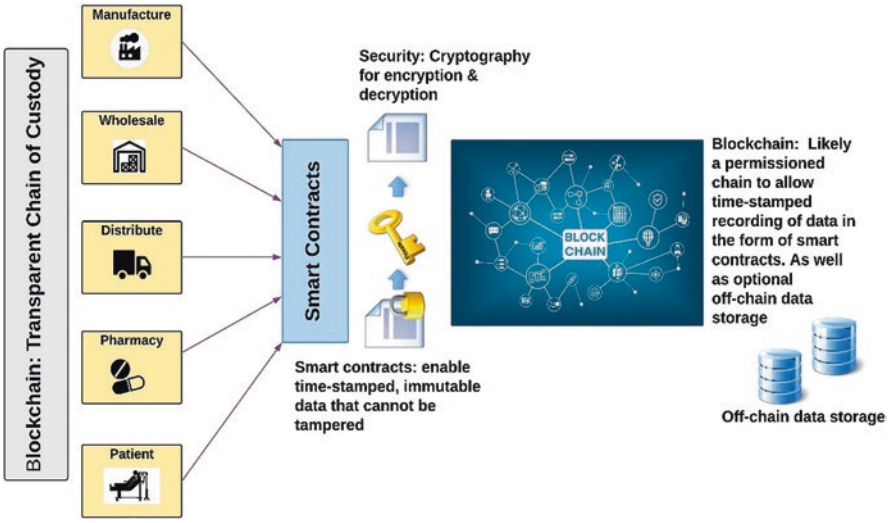

Fig. 2.8 Blockchain and the transparent chain of custody

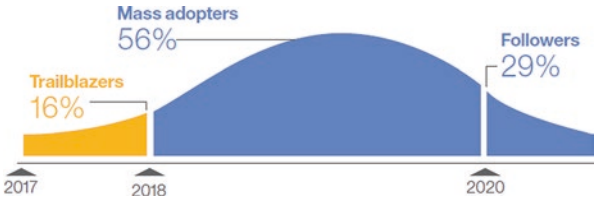

Fig. 2.9 Confidence with early adopters. (IBM Institute of Business value 2016)

issues such as interoperability, transparency, privacy, health data interchange, claims adjudication, drug traceability and supply chain integrity, to name a few.

Blockchain applications to the healthcare industry are version 3.0 which has evolved from blockchain version 1.0 for cryptocurrency and smart contracts deployment as version 2.0.

A recent survey (IBM Institute for Business Value 2016) of 200 healthcare executives (a mix of payers and providers across 16 countries) found that 16% were expecting to deploy a blockchain solution for healthcare soon. The survey holds a much higher percentage than other sectors of banking/finance and commerce which have been longer established in blockchain methodology than in healthcare. Figure 2.9 describes these early adopters as 'Trailblazers' and other Healthcare Institutions and a timeline of how the healthcare industry will react to adoption.

The IBM survey (Fig. 2.10) describes the friction areas around inaccessible information (the interoperability and security/privacy concerns on data) that both leading Trailblazers and other Healthcare Institutions mostly agree on. Also, they agree with the top three impact areas being **Clinical Trial Records**, **Medical Health Records** and **Regulatory Compliance**. The findings of the survey match well with the thrust of this research in the sense of although there is demand for open access

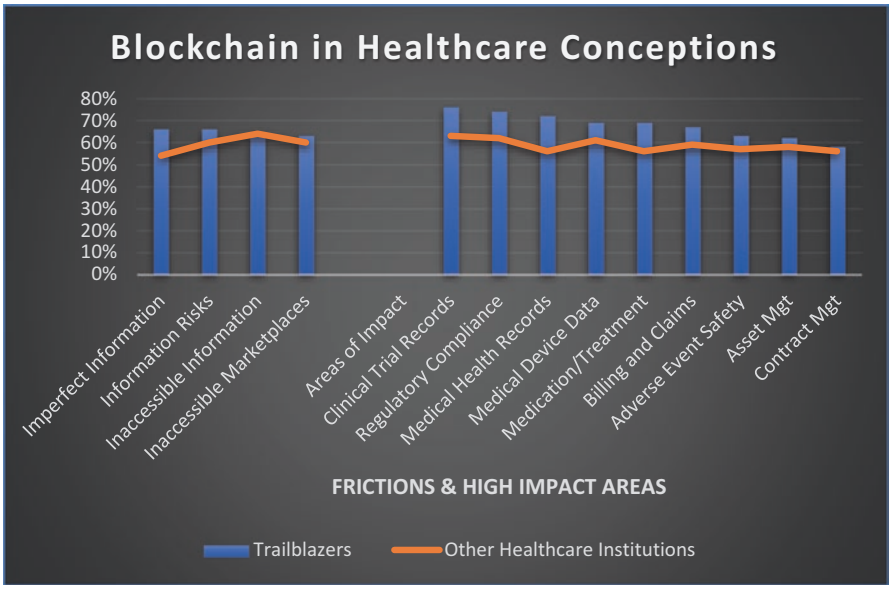

Fig. 2.10 Survey of 200 Healthcare executives; source a mix two data sets. (IBM Institute of Business Value 2016)

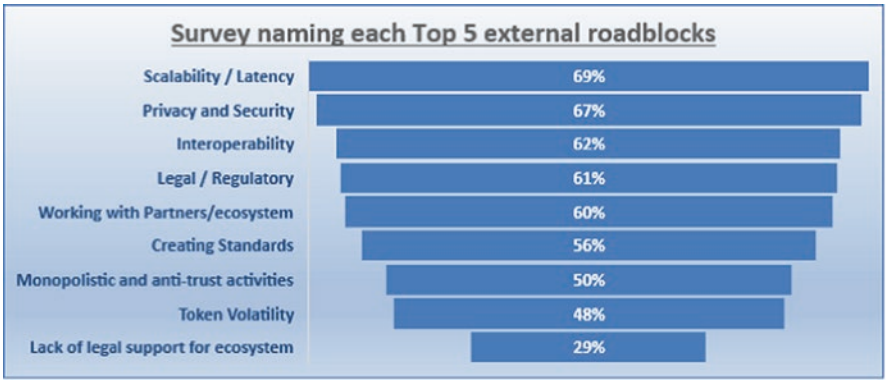

Fig. 2.11 Survey of 558 respondents proficient with blockchain in healthcare. (Cognizant 2017)

of trials data they agree that there is mistrust and data is hard to obtain/share where permissioned.

In Fig. 2.11, data was extracted to show a global survey of 558 respondents carried out by Cognizant (2017) and displays a similar outlook with regards to issues of privacy, security, interoperability and regulatory. The respondents were mostly considered proficient with blockchain and the survey asked respondents what they thought the top five external roadblocks would be.

The IBM Institute for Business Value (2016) survey has interesting points regarding *outcome switching* in clinical trials and survey comments match the research undertaken that data reported could be selective and should have greater transparency and sharing, which is explored further in Chap. 3. If the argument for withholding data was not to expose this data to competitors before public exposure, then blockchain would enable recording in real-time, be protected on blockchain through permissions and with the timestamp have an immutability so that it can't be denied.

To help validate the research and understand why interest in blockchain is growing, it is worth reviewing some blockchain healthcare initiatives that cover resolving a range of typical healthcare issues and explained as follows.

MedRec This was developed by MIT researchers (Azaria et al. 2016) and implemented in the Beth Israel Deaconess Medical Center (a teaching hospital of Harvard Medical School) to handle EHRs making use of existing blockchain technology and Ethereum smart contracts. Azaria et al. (2016) quote that it 'gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites'. This is one of the objectives, enforcing the rationale to use blockchain; to improve the interoperability, data sharing, transparency, and biomedical and outcomes research and benefit access to secure longitudinal research data, Angraal et al. (2017). The method is storing not the actual health record but signature of the record on the blockchain and this assures immutability and gives the patient control of access to the record and for those patients that may not want to control their data they may have the option to delegate these responsibilities; Halamka et al. (2017). Data is entered by the physician through the MedRec Provider App where stored data is accessed via a hashed link. The Ethereum blockchain controls the permissions and the patient has rights to download at any time as the blockchain authenticates valid privileges.

Guardtime In 2011, Estonia collaborated with a company called *Guardtime (*a Netherlands based company which conducts a blockchain architecture), to secure public and internal records and then after this initial success, in 2016, secured one million health records of Estonian citizens using its Keyless Signature Infrastructure (KSI); Mettler (2016). This innovation was a way to help solve the challenge to increase clinical health data exchange and interoperability and so improve transparency of the data. Estonia's embrace of blockchain technology has made it a country where 100% of its medical records are online in a secure and private method. The success of Estonia has given confidence to other regions such as in the UAE and a major healthcare provider there.

Gem Health Gem, a Californian based company partnered with Philips, created a blockchain healthcare ecosystem called the Gem Health Network and is a platform that sits on top of blockchain architecture and can easily deploy distributed applications, Ark Invest Research (2016). The aim was to connect all disparate arms of healthcare and with the patient at the centre as in control and have this community of patients, providers and industry all connected in a health data exchange, rather

than medical data in silo's, insurers claims on silo's, etc. As it's a permissioned blockchain it can control who can access sensitive information and ensures anonymity (patient information can't be linked to a patient in an event of a data breach).

Healthbank Based in Switzerland, the *healthbank* mantra is "my data, my choice, my *healthbank*", Nichol (2016). The data control is left to the user (hence the quote explains the meaning) and can even chose to provide data for medical research and perhaps receive financial compensation and if the patient data is of significant value they may be rewarded at a higher than normal rate, Mettler (2016). In this way *healthbank* becomes a patient driven system and blockchain is being further investigated to ensure fast, secure and authenticated access to patient data. This is a good example of ways to look at improving transparency and security in the clinical research world.

Pokitdok An API platform-as-a-service allowing users to interact with over 700 trading partners and use identity management to validate the partner transactions involved. This can help facilitate what was once data held in silos and now having seamless interaction. For example, near instant billing and insurance claim resolution, Engelhardt (2017).

Patientory A start-up that believed there was a need for more collaboration between providers and patients to allow more connectivity and transmit data securely using blockchain technology. They also developed a mobile healthcare app to help patients keep a track on their medical history, bills, pharmacy medications, insurance and so on, Slabodkin (2017). Interestingly patients can also connect with other patients for similar health problems.

Modum Founded in 2016 and designed to help improve the pharmaceutical for supply chain monitoring. Traceability and compliance are difficult in current scenarios and blockchain helps cut down on the paper trail and provide a more tamper proof system that is auditable along all its journey. This is particularly specific in the pharmaceutical industry where in some regulation compliance it is essential that deviations are reported in temperature, light conditions, humidity, etc., as IoT sensors monitor the temperature of the products and sensor data and is transferred to the blockchain. A smart contract is initiated thereafter (this is the integrity and immutability the system offers) and the data recordings are compared what is measured against the compliance requirement. Should a deviation occur then a notification is released to the parties required to know, Schumacher (2017).

iSolve The Advanced Digital Ledger Technology is a solution by iSolve that manages the life cycle of drug development and drug supply chain in the biopharma and healthcare industry by using blockchain as the mechanism to track, audit and record all logistical movement of medications. Data sharing and transparency are key components to the system. There is a need to have meticulous tracking due to counterfeit and fraudulent drugs and medications. This issue is highlighted more in regions

where regulation and legal frameworks are not mature or right controls and monitoring. Blockchain can handle the life cycle from development to distribution so even something simple like expiry dates can be driven with accuracy and negate the chances of fraudulent relabelling of changing of dates; Engelhardt (2017). iSolve also manages the acquisition of IP assets, can raise funding and advance drug development through Smart Market where information is held in a secure method and is trackable, immutable and visible as a marketplace to investors and service providers.

Medicalchain A distributed ledger that allows permissioned based blockchain to securely store health and patient records and the user to give permissions to healthcare professionals (these could be doctors, pharmacists, hospitals and laboratories) for access to their personal medical data. The transactions are recorded/audited in a transparent manner, but privacy of the patient is of key importance. This takes care of interoperability issues and the scenario of fragmented healthcare services. If information could be more integrated then it may help lessen medical errors as some research undertaken by McMains (2016) at the John Hopkins Hospital in the US concludes that medical errors are the third leading reason for deaths (in the US). This may be due to the uncoordinated healthcare approach of silo data.

BurstIQ Blockchain enabled for securely handling person-centric data, as an authenticated and permissioned interchange, connecting any data from any source. The model allows researchers, businesses and individuals to connect and share data. Individuals can decide if and when to share, sell or even donate their data; accessed through their HealthWallet. This could cover electronic medical data and other such as diagnostic, behavioural, fitness, pharmaceutical, smart data, etc.

2.10 Conclusions

The healthcare industry is no stranger to undergoing transformation of its paper and manual processes to more digital and electronic methods and associated data workflows. As technology has advanced, so too has the delivery of more precision based medicine and the Internet of Medical Things (IoMT) has opened up an abundance of many smart sensors and devices culminating in large collation of data and behaviours that can help determine better outcomes at point of care. But although beneficial with the digitalisation of medical records these are still stored in many disparate silos and healthcare is now suffering the most cyber-attacks resulting in significant data breach losses and identity theft than any other sector. Blockchain presents itself to be a fit for purpose solution to a wide range of legacy issues that have dominated the healthcare industry. These legacy issues have tended to provide the patient weaker perspectives and offer risks that may have wide and far reaching consequences. As medical science evolves, then so too must the mechanism and tools that support how all the data is protected and handled.

References

Angraal et al (2017) Blockchain technology: applications in healthcare. Circ: Cardiovasc Qual Outcomes 1–4. Available at: https://doi.org/10.1161/CIRCOUTCOMES.117.003800. Accessed 20 Oct 2018

Ark Invest Research (2016) How blockchain can enhance EHR operability. Available at: http://research.ark-invest.com/blockchain-and-healthcare. Accessed 20 Oct 2018

Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: using blockchain for medical data access and permission management. In: 2nd International conference on Open and Big Data (OBD), Vienna, pp 25–30. Available at: https://doi.org/10.1109/OBD.2016.11. Accessed 20 Oct 2018

Bresnick J (2016) How will internet of things devices impact precision medicine. HealthIT Analytics. [Online]. Available at: https://healthitanalytics.com/news/how-will-internet-of-things-devices-impact-precision-medicine. Accessed 20 Oct 2018

Cognizant (2017) Healthcare: blockchain's curative potential for healthcare efficiency and quality. [Online]. Available at: https://www.cognizant.com/whitepapers/healthcare-blockchains-curative-potential-for-healthcare-efficiency-and-quality-codex2995.pdf. Accessed 20 Oct 2018

Das R (2017) Does blockchain have a place in healthcare? Forbes. [Online]. Available at: https://www.forbes.com/sites/reenitadas/2017/05/08/does-blockchain-have-a-place-in-healthcare/#42a2eeba1c31. Accessed 20 Oct 2018

Dubovistskaya A et al. (2017) Secure and trustable electronic medical records sharing using blockchain. In: AMIA 2017 annual symposium proceedings. [Online]. Available at: https://arxiv.org/abs/1709.06528. Accessed 21 April 2018

Engelhardt M (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innova Manage Rev 7(10):22–34. Available at: https://doi.org/10.22215/timreview/1111. Accessed 20 Oct 2018

Halamka J et al (2017) The potential for blockchain to transform electronic health records. [Online] Available at: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records. Accessed 20 Oct 2018

IBM Institute for Business Value. (2016) Healthcare rallies for blockchains: keeping patients at the center. [Online]. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03790USEN. Accessed 31 May 2018

Jiwani A, et al. (2014) Billing and insurance-related administrative costs in United States' health care: synthesis of micro-costing evidence. BMC Health Serv Res 14: 556. [Online]. Available at:https://doi.org/10.1186/s12913-014-0556-7. Accessed 20 Oct 2014

Labchain (2018.) Available at: https://www.labchain.nl/. Accessed 20 Oct 2018

Liang X et al. (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: IEEE 28th annual international symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, pp 1–5. Available at: https://doi.org/10.1109/PIMRC.2017.8292361. Accessed 20 Oct 2018

Linn L, Koo M (2016) Blockchain for health data and its potential use in health IT and health care related research. [Online]. Available at: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf. Accessed 20 Oct 2018

McMains V (2016) John Hopkins study suggests medical errors are third-leading cause of death in U.S. John Hopkins University. [Online]. Available at: https://hub.jhu.edu/2016/05/03/medical-errors-third-leading-cause-of-death/. Accessed 20 Oct 2018

Mettler M (2016) Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th international conference on e-health networking, applications and services (Healthcom), Munich, pp 1–3. Available at: https://doi.org/10.1109/HealthCom.2016.7749510. Accessed 20 Oct 2018

Monegain B (2013) Data-sharing initiative reduces deaths. Healthcare IT News. Available at: https://www.healthcareitnews.com/news/data-sharing-initiative-reduces-deaths. Accessed 20 Oct 2018

Nichol, P. (2016) Blockchain applications for healthcare. [Online] Available at: http://www.cio.com/article/3042603/innovation/blockchain-applications-for-healthcare.html. Accessed 20 Oct 2018

ONC (2015) Connecting health and care for the nation: a shared nationwide interoperability roadmap. [Online]. Available at: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf. Accessed 20 Oct 2018

ONC (2016) Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008–2015. [Online]. Available at: https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php. Accessed 22 Oct 2018

Rifi Net al (2017) Towards using blockchain technology for eHealth data access management. In Fourth International Conference on Advances in Biomedical Engineering (ICABME), Beirut, pp. 1–4. Available at: https://doi.org/10.1109/ICABME.2017.8167555. Accessed 6 May 2018

Schumacher A (2017) Blockchain & Healthcare. 2017 Strategy Guide for the Pharmaceutical Industry, Insurers & Healthcare Providers. [Online]. Available at: https://www.researchgate.net/publication/317936859_Blockchain_Healthcare_-_2017_Strategy_Guide. Accessed 20 Oct 2018

Slabodkin G (2017) Blockchain remains a work in progress for use in healthcare. Health Data Manag. [Online]. Available at: 2017. ProQuest, https://search.proquest.com/docview/1914536464?accountid=12860. Accessed 20 Oct 2018

Yue X et al (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10):1–8. [Online]. Available at: https://doi.org/10.1007/s10916-016-0574-6. Accessed 20 Oct 2018

Zevala C (2017) How IoT is improving the accuracy of clinical research. IoT Evolution. [Online]. Available at: http://www.iotevolutionworld.com/m2m/articles/431211-how-iot-improving-accuracy-clinical-research.htm. Accessed 20 Oct 2018

Chapter 3
Healthcare Patient and Clinical Research

Stefan Kendzierskyj and Hamid Jahankhani

Abstract Clinical trials and research are a very involved and often lengthy process with formalities and regulations that should be adhered to. There are questions over the transparency of clinical research data from the start of the initial process of registration, informed consent, clinical outcomes and to where approval is given by post marketing and publication. These impacts suggested have manifested itself in the form of fraud, misconduct, selective reporting, bias and consequently had other effects to those taking approved drugs; some resulting in fatalities. Access to research data has also been difficult to obtain from those involved in the clinical trials such as patients and even researchers whom would be interested in the post marketing phase and pharmaceutical analysis. Evidence is presented with data extracted from credible sources that highlight the concerns in registration, informed consent and clinical research outcomes and how they are reported with recent example of how opioids misuse has ended up as a serious issue as a consequence of non-transparency. This Chapter suggests a theoretical model to propose how blockchain could present a more transparent and secure method to tackle the issues mentioned, with utilising blockchain as the mechanism/framework for clinical research institutions, regulation and non-regulation bodies, pharmaceutical organisations, drug manufacturers/suppliers and patients.

Keywords Clinical research · Clinical trials · Clinical outcomes · Fraud and misconduct · Selective reporting · Bias · Blockchain · Data integrity · Traceability · Smart wearables · Cyber-attacks · Data breaches · Opioids misuse

S. Kendzierskyj · H. Jahankhani (✉)
London Campus, Northumbria University, London, UK
e-mail: Stefan.Kendzierskyj@northumbria.ac.uk; Hamid.jahankhani@northumbria.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_3

3.1 Introduction

Over recent years it has become clearer from research and studies undertaken that there are issues with data from clinical trials being made more transparently available; from the start of the process with registration and informed consent through to publication outcomes and drug administration. Fraud and misconduct are also reported alongside privacy of patient data concerns and the integrity of the whole process. At all points of the journey's process, it highlights suggestions or requests to improve transparency and security as explained in parts of this chapter. There has also been great technological advancement in using smart medical wearables to gather data more accurately during trials, rather than more mechanical methods of patients filling in forms when requested or next visits to the clinics. But with the advantages of valuable data comes the risk of data integrity and complexities of digital forensics. Blockchain offers a more beneficial method to seamlessly record data.

What is discussed in this Chapter is a theoretical model using blockchain as the mechanism to secure and support all processes through the data journey. This will give a more guaranteed method to provide data (which may be currently withheld) back to clinical researchers and also present data access to patients whom in some cases currently consent and undertake trials but never then gain access to results or insights of the study that they made valuable contributions to. But worryingly, there is a lot of data that is not published and studies that do not have significant results remain to be not included and may imply bias in the outcomes, Proehl and Hoyt (2017). There is also a more serious side of transparency in the full sets of raw data being available from drugs being prescribed as well as analysis on how in many cases data in the setup of the Protocol of a Trial is not matching to the clinical trial outcomes. This misalignment in outcomes can have an impact on patients from less to severe, such as fatality.

3.2 Transparency of Clinical Research/Trials and Drug Traceability

Interoperability and longitudinal data are beneficial to patients and providers, as mentioned in earlier sections and enhance both the privacy and security if run on architectures such as blockchain. However, there is also significant potential for companies involved in research to enter a new era of discovery to help better understand disease interactions, and if that data was made easily available to researchers, then the benefits would be huge; Engelhardt (2017). The access to this abundance of data is not the issue; it's often the transparency, security and privacy of that data that is the problem and blocked by many obstacles, ethics, etc. But with blockchain this will offer the patient a way to 'permission' data to be shared anonymously; with the patient being at the centre, authorising access to clinical researchers or industry.

Engelhardt (2017) makes an interesting point that not only do patients want this control, but they want their data to be useful and for researchers the value of blockchain is the immutability of the data, meaning the data is trusted not to change. This is a crucial concept in the research world that data can become more trusted.

If legacy issues are analysed it's easy to see that clinical trials are subject to many errors and fraud that undermine the whole process and can invalidate the research undertaken. Benchoufi and Ravaud (2017) specify that reproducibility is an issue (misconduct and fraud) and ideally it would be better to equip research communities with secure data sharing and a way to guarantee privacy, perhaps using blockchain. Benchoufi and Ravaud (2017) go on to solidify their case for blockchain because it 'allows for tracking, sharing and caring for data' and can be a better step towards transparency and improving trust in the research community. The research is specific on blockchain application to benefiting clinical research and worth noting the positive aspects and why to consider as follows:

- **Chronological order** – tracking can take place in the correct event order to apply a time order logic
- **Data integrity** – data falsification is as close as possible to being eliminated along with issues of embellishing
- **Traceability** – with the timestamp, a copy of the transaction is kept across the nodes ensuring no tampering of the data and provide credibility.

See Fig. 3.1 as per Benchoufi and Ravaud (2017) proposed model for explanations of the complex stages and flows of diverse data and applied metadata so keeping the data 'true' but confidential on blockchain. Smart contracts can be deployed in certain stages as that validates all previous steps.

3.3 Theoretical Model Using Blockchain to Secure Data in Clinical Research Trials

Tackling the issues of the transparency and security of healthcare data has been a difficult problem to resolve. However, with the recent advancement in blockchain application (some examples were given in the previous chapter) it now provides a tool or mechanism to support the data journey all the way, providing the benefits of blockchain.

Figure 3.2 proposes a trustless blockchain framework between clinical research institutions, regulation and non-regulation bodies, the pharmaceutical industry, drug manufacturers/suppliers and more importantly the patients.

The type of blockchain suggested could be Ethereum; since it already has significant use in healthcare applications, and speed and efficiency are known quantities in terms of transaction and processing time. But equally for future research or pilots it can be flexible to other types of blockchain. It will also be a permissioned framework, since users would need to be invited to access information where authentication

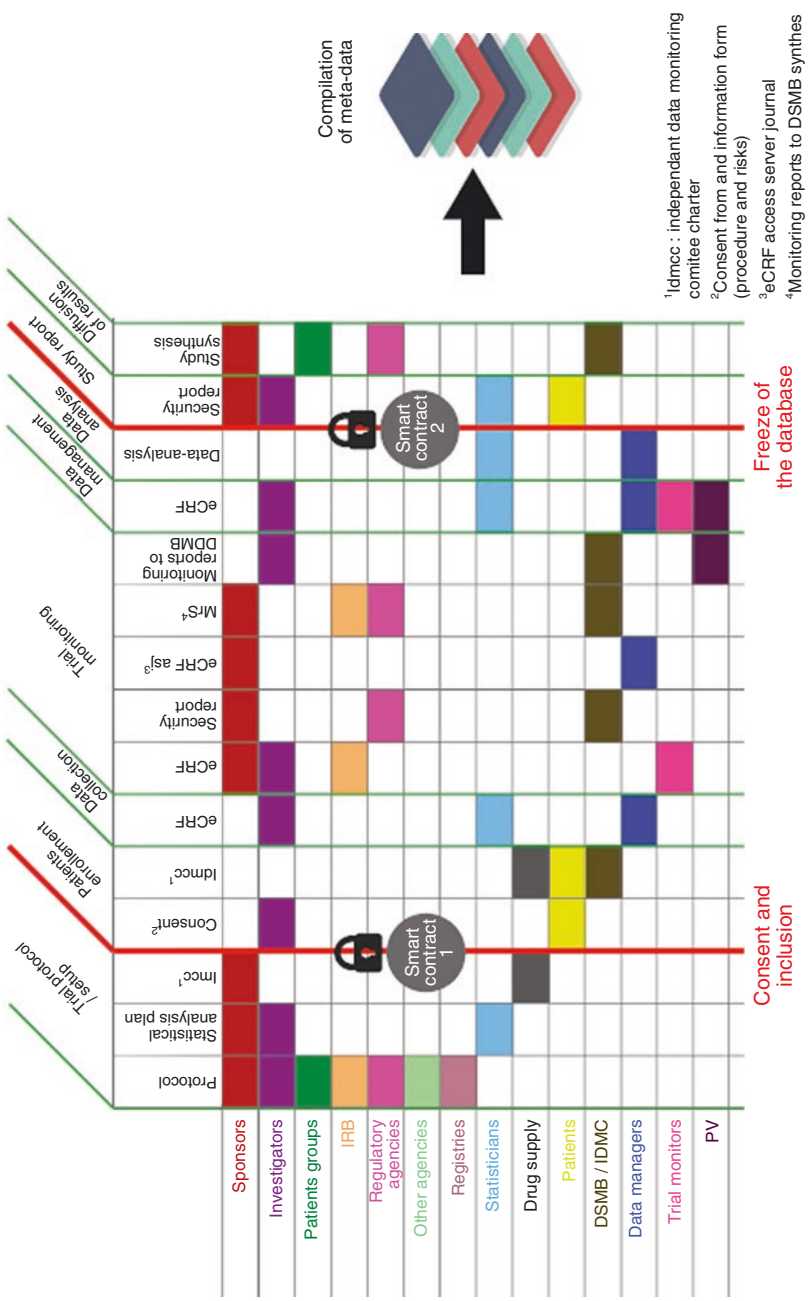

Fig. 3.1 Clinical trial data supported by benefits of blockchain. (Benchoufi and Ravaud 2017)

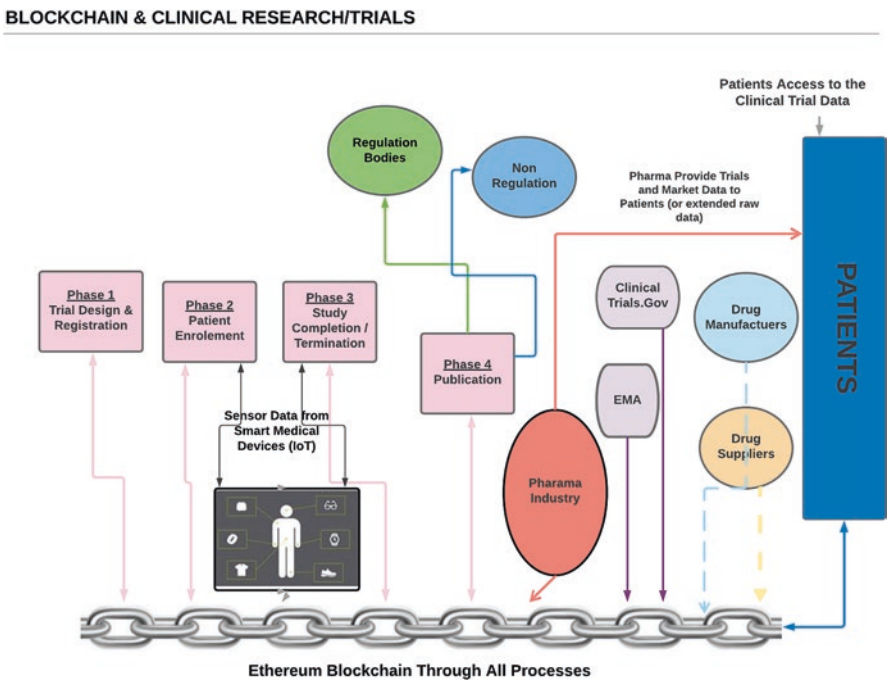

Fig. 3.2 Theoretical model using blockchain mechanism to strengthen the clinical research processes

is given (and not a permissonless public method, such as bitcoin). Ethereum also has the benefits of smart contracts as shown in the model presented by Benchoufi and Ravaud (2017) discussed earlier, where an immutable timestamp and time ordering can be achieved. Data can be stored off-chain (due to patient sensitivity and possible data size) but permissioned and authenticated via the Ethereum blockchain.

3.4 Using Blockchain for Tackling the Issues

To explain the theoretical blockchain model, this section describes the clinical data journey and how blockchain supports more transparency and strengthens the privacy of clinical and patient data. Blockchain can be the layer through the whole clinical trial journey and be used to verify, validate and sanity check all transactions and interactions that are recorded, and time stamped in a way that delivers integrity. There are many parts to the chain that can be subject to any of the issues discussed.

3.5 Clinical Trials & Research Phases

Clinical research is a very important process to facilitate new medications and improve patient outcomes and procedures that can accommodate a better way of life for many people. Clinical research is necessary to assess how treatments will work with patients, if they can be judged to be safe and lead the way to prevention based medicine. The process to undertake the research is known as trials and formulates the testing operation.

Great trust is placed in the process but at many points along the journey it is subject to data not truly being represented and a fraction of the research found in published reports, Song et al. (2010). Figure 3.3 shows the path of data and a mechanism to provide a way of immutability, from the start with the clinical phases to the provision of important feedback from the market to clinical researchers and patients who undertook the trials. The clinical trial data regarding study purposes, patient consents, registration information can all be stored on the blockchain through smart contracts giving a time ordering stamp. If any revision changes occur to the trial,

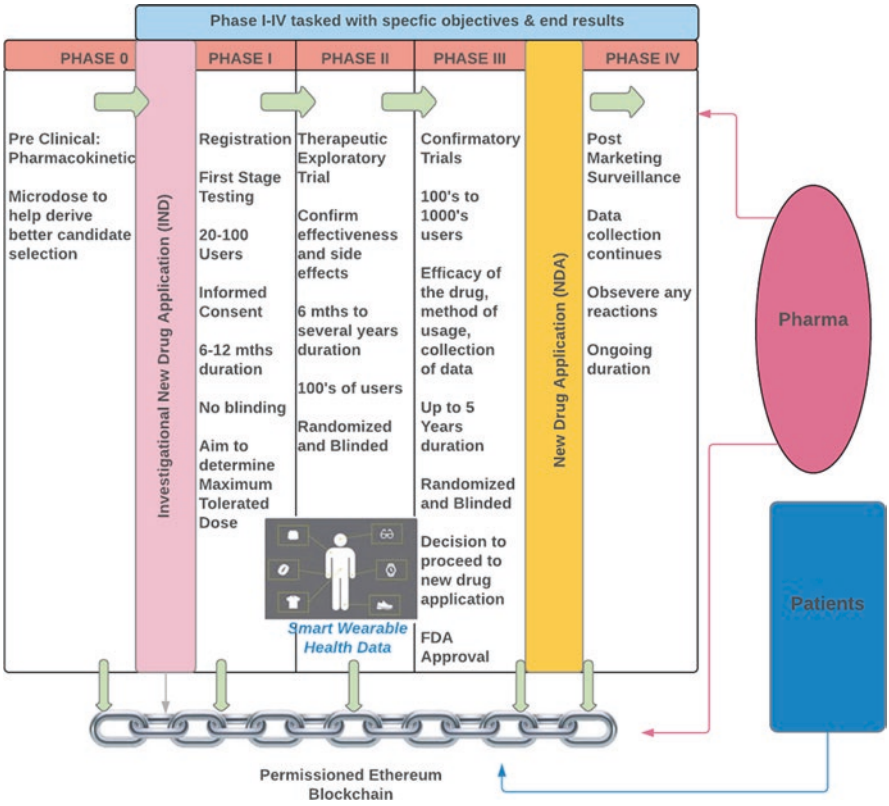

Fig. 3.3 Blockchain enhancing the privacy of data through the clinical phases

then the patient needs to give consent and it is recorded in the same fashion. This is an important aspect explained later in the data analysis in later sections as changes in any trial method could have an impact to the patient and they should have given consent to proceed on any new significant amendment. It can be seen in the data analysis given from the raw data collated in the wide gap in outcomes reported compared to the original Protocol setups.

There are many examples of where in Phase III trials, data remains unpublished after studies are completed and this can remain so for several to many years: such as gabapentin, paroxetine, pregabalin, oseltamivir and zanamivir and with oseltamivir (Tamiflu as its more known name) resulting in worldwide healthcare misdirection, Ramírez (2013). This could be avoided if data capture was an essential requirement and all data, including non-successful trials, were secured onto the blockchain model. The issue of data being cherry picked or reported selectively has a detrimental effect for researchers, physicians and patients themselves.

3.5.1 Clinical Trial Phases

As mentioned already, clinical trials compose of a number of phases all of which follows a protocol that has an intervention to arrive at understanding the safety, effectiveness/performance, safety and how the dosage would best work. Some trials can be randomised where participants are randomly selected to be given the approved treatment that is up to date or a drug that is under development. The trials are normally blinded, in essence this means the physician is not aware of which participants receive treatment. This is done to protect the integrity of the trial, so study teams are not biased or leant to one direction if they know, for example, which participant is taking the placebo treatment. Usually the trials can be conducted when all information collated on the quality of the nonclinical safety has adequately passed approvals (this can be a committee type approval).

3.5.1.1 Clinical Phase Stages

To help understand the detailed stages of clinical trials this section details a breakdown of different processes within the stages (refer also to Table 3.1). Knowing the stages can help better position why perhaps blockchain can play a significant factor to protect in each phase the multiple data points that are captured and audit trail will be more transparent. In later sections multiple issues are presented due to the current structure clinical trials operates in.

Table 3.1 Different processes within the stages of clinical trials

Types of trials	Description
Treatment	Allow testing of new synthesis of drugs or therapy approaches
Prevention	Methods to assess in preventing those that never had the particular disease or prevent return of the disease. Depending on approach will depend on including medicines, vaccines, vitamins, minerals or lifestyle changes
Diagnostic	Used to evolve better tests or procedures for diagnosing types of disease and may include those with signs or symptoms of disease/condition
Screening	To help with early detection screening is useful to help better detect signs
Quality of life	Looks at ways or methods to advance the comfort for those with chronic illnesses

3.5.1.2 Design Considerations of a Trial

It might seem detailed for a publication such as this to go into depth in clinical trial design. However, it is connected to what is delivered in the clinical outcomes as they should match to the objectives set out as part of the design and ratified in the Protocol that is approved to proceed as trial. This is evident as causing issues when analysed in later sections in this Chapter.

Objective of Trial These are what you would expect in terms of the medical questions that need answering (e.g. number of subjects, duration, etc.) but more importantly the objectives most likely are more than one and need segregating into Primary and Secondary objectives. Every trial should have primary clinical research question(s) that is not vague but is thought through after much deliberation to arrive at a particular hypothesis that can be tested according to National Center for Biotechnology Information (2018). Secondary questions are usually constructed to support primary questions.

Patient Selection To target the patient population, asset of eligibility criteria needs to be positioned as enrolment of patients can then be more specifically addressed. To set the right selection process a set of inclusion and exclusion criteria is created. In simple terms to be eligible for the trial a patient must meet all the inclusion criteria.

Control Selection It is an FDA requirement to have well controlled trials so that unbiased or non-selective evaluation of the effectiveness and safety of the drugs is carried out. If bias and selective reporting becomes part of the delivery, then a cascade of issues can arrive in Phase IV (post marketing).

Randomisation This process is derived before the intervention begins where the study participants are randomly allocated to receive one or other alternative treatments that form part of the study. Some participants receive the study treatment while others receive the standard treatment or a placebo. This is done to eliminate

any bias and allows blinding of the identity of the treatments to participants, assessors and other. Randomisation itself is subject to variations (simple, restricted, stratified and adaptive).

Blinding Also, known as masking depending on organisations where various groups involved with the trial are withheld information, such as patients, healthcare providers or researchers. This is fundamental part of the process to again protect bias from happening and there are a number of variations such as open, single, double and triple blind. Below Fig. 3.4 shows typical blinding process and procedure.

3.5.1.3 Description of Process in the Phases

Phase 0 (Pre-Clinical Trials) This phase is used to help derive a better candidate selection for the full trial by applying to a small select number of participants (or animal study) and provide a microdose. Usually before any testing in humans can begin, it should have had extensive laboratory research performed to arrive at some rational drug design, look at synthesis and purification before proceeding to animal testing. It helps rank the best pharmacokinetic (PK) pharmacodynamic (PD) parameters to decide how to take forwards the development. This can make sure to limit chances of adverse effects.

IND (Investigational New Drug) If Phase 0 is successful and passed successful testing, the FDA (Food and Drug Administration) is given the testing data and requests FDA approval (the IND application). If approved, a formal written protocol

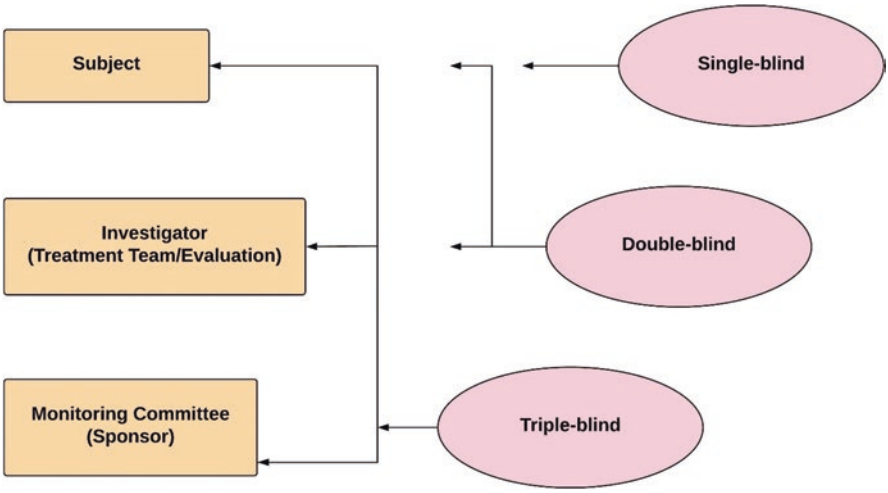

Fig. 3.4 Blinding process in clinical trials

is created, and human testing may commence. The IND application would consist of preclinical data, composition and source of drug information, chemical and manufacturing information, proposed clinical plans and protocol and ethical committee clearance.

Phase I Ensures it adheres to the Declaration of Helsinki and ICH GCP (International Conference on Harmonisation). Informed consent is required, approval by regulatory body and Protocol approved by Ethics Committee. First stage of testing in humans and designed to test safety, PD and PK of the drug and tolerance levels. There is no blind study at this stage. The aim of the trial is to assess the maximum tolerated dose (MTD) of the new treatment. The number of participants can vary from 20 to 100 and a duration of 6–12 months.

Phase II Usually a therapeutic exploratory trial, which are controlled clinical studies, to confirm the efficacy, observe safety issues/side effects and can be tested in patients that may have the disease the treatment is designed to target. Testing can be randomised, single blind (comparison with standard drugs and participants do not know if they have received placebo or standard drug) or double blind (compared with placebo standard drug and physicians and participants do not know which group received placebo or experimental drug). A duration of 6 months to several years and approximately 20–300 patients.

Phase III Designed as a therapeutic confirmatory trial testing the efficacy of the drug against existing therapy, determine optimal dosage schedules (usually termed Therapeutic Confirmatory types). A large scale randomised, controlled and blinded trial on 100's to up to 3000 patients and designed to confirm that the preliminary evidence amassed in Phase II is safe to administer in the way designed and intended recipients of the new drug. Timeline is up to 5 years and because of this can be expensive, difficult to run and therefore collation of data is important to validate all. At the end of Phase III, a decision is made as to either proceed to file for a NDA or terminate.

NDA (New Drug Application) This is the formal proposal for approval to making a new drug for sale and the NDA contains all the necessary data from preclinical to Phase III.

FDA Approval There is a process for the FDA to review and may take 2–3 years. The evidence to sway approval should be that the drug is safe and effective, benefits are more heavily weighted and proposed labelling is correct.

Marketing Permission The drug will undergo a marketing phase.

Phase IV (Post Marketing Phase) The drug is out in the market and studies continue on data collation, analyse any adverse effects/reactions and if harmful effects are found the drug can be no longer sold or restricted. The phase may also involve

safety monitoring, called Pharmacovigilance and any support such as technical. Further evaluations are undertaken on cost/benefit analysis (Pharmacoeconomics).

3.6 Smart Wearable Health Devices in Clinical Trials

Some years before the invention of smart wearable devices the data collection was a manual process and could be managed by interviewing the users involved in the trial. This may not achieve the most accurate results, since it's based on experience and memory and subject to bias in the patient's interpretation. There is also the question of privacy and security of how these data records are kept.

More advanced development of smart health wearable devices (IoMT) has taken out the unpredictability of capturing accurate data or having to plug devices to download to computers. These devices can come in a multitude of types and use cases ranging from activity trackers, pacemakers, monitoring, etc. Data can be transmitted in real time to researchers without any additional practical requirements from those participating in the trials. Data is captured seamlessly, uploaded and synchronised to cloud and blockchain acting as the authentication piece. All associated data on the patient can be stored and connected in a timestamp ordering manner on the blockchain and connected to patient healthcare records. This gives complete accuracy as chronological ordering and can be adhered to several smart contracts as milestone points in trials. It also takes care of the silo issues of containing data in separate locations which comes with the problem of cyber security breach risks; interoperability is a key aspect here. Liang et al. (2017) explain a similar process in their presentation of integrating blockchain with healthcare wearables.

One of the other concerns that blockchain can remedy is a way to store and protect the huge growth anticipated in healthcare wearables and its associated data coming from Wireless Body Area Networks (WBAN). This concern, as mentioned previously regarding healthcare being a primary target for cyber hackers and data breach. If alternative mechanisms such as blockchain are not considered, then there is a greater risk of more data being breached through the increase in attack surface with the volumes of heath wearable data now also considered a target for cyber-attackers. The patient is the most vulnerable in this current cycle with no control, access or understanding of where the data is kept or even if the breach has happened, although GDPR is designed to at least give notification within 72 h of breach occurrence; however, this does not help the patient if security was not taken care of. Wearable technology is a significant evidence addition to the trial process and blockchain is the underlying support to all parts of the trial chain.

3.7 Publication and Post Marketing Effects and Issues

When it comes to Phase IV, post marketing, it is a very crucial stage of the phase. Hopefully if all has been carried out diligently in Phase 1–3 and all data collated (whether positive or negative) then when the drugs are available in the market it will not have any adverse and unexpected effects or results. However, as explained in more detail later in this Chapter, if processes are not followed and data is not collected in correct manner there are a spiral of issues that can cascade from serious, such as fatalities, downwards. This can be a lot to do with the way reports are presented and distort the information given for evaluation or approval. In the true sense there should not be any 'bad' information as even negative results are valuable to all associated in the trials process.

Publication bias, cherry picking, and selective reporting are issues in the current trials process. The annual spend by pharmaceutical industry on clinical trials is circa 90 billion USD and as example of the scale of activity, Roche and Novartis in April 2013 declared activity in 1000 clinical trials, Public Eye (2013). A lot is at stake for these companies and why there is public pressure for a method to increase higher transparency to ensure that evidence-based processes avoid the affliction the clinical research industry suffers in the form of selective publishing that can distort the clinical outcomes by obscuring relevant data to researchers and patients, Ross et al. (2012). There appears to be a lack of accountability, marketing involvement and practise of seeding trials, particularly in industry sponsored trials. As Ross et al. (2012) outline in their research that seeding trials does not inform on all objectives to patients and researchers and effects patients from making fully informed consent decisions. In this Chapter included are some examples of litigations undertaken on pharmaceutical companies who have placed cherry picking, misconduct and fraud as a part of the clinical trial process in order to achieve hidden objectives and highly unethical practices that go largely unreported.

The blockchain model proposed would handle every part of the research process including any published effects and feedback from the market place, so researchers can gain extended understanding to align on new or other trials. This can be said for any unpublished data and seems a reasonable request to allow all data to be accessible.

3.8 Regulation/Non-regulation and Pharmaceutical Behaviours

The role of regulatory bodies, such as in the UK the Medicines and Healthcare products Regulatory Agency (MHRA), takes care on approval of regulating medicines, medical devices and associated equipment with its main aim to safeguard public health. There are many international regulatory bodies around the world and they often collaborate with each other e.g., Food and Drug Administration (FDA).

In the case of, for example, MHRA they would issue a licence (marketing authorisation) to allow issue of medicines for treatment once full assessment has been undertaken by an evaluation team of experts. Testing of the drugs is the process through clinical trials and will have had to meet strict criteria.

However, even with an approval process undertaken with regulatory bodies there looks to be a number of issues. John Castellani, of PhRMA (Pharmaceutical Research and Manufacturers of America) was quoted to give opinion that if regulators viewed all trials data behind closed doors then it would be good enough, Goldacre (2013). But this implies a mistrust, no chances to review all sets of data in a transparent manner and in more direct terms, which Goldacre (2013) makes good point on, is that the serious implications to patients with exposure to drugs that may be more harmful or of no effect at all. In certain cases, regulatory bodies have not identified the data inconsistencies that previous independent parties have seen. It would benefit all if whole data sets, including raw data which can be thousands of pages long, were authenticated through blockchain so many independent eyes from all parts of the process can validate and test the theories as does in normal world of academic science.

Whilst it appears pharmaceutical companies look to present data in a selective way there are some in the industry that are looking to offer a more transparent access to all trial raw data sets. GlaxoSmithKline signed up to AllTrials (started in 2013 as advocating open access on all trials research) with an open declaration of transparency; AllTrials (2013). This can only benefit patients and allow then access and protect privacy through blockchain.

3.9 Drug Manufacturers and Suppliers

Since this research presents a holistic solution for all parts of the trials process with blockchain as the model to encourage transparency and protect privacy, then it is also good that blockchain can also offer a secure method for drug traceability. It is mostly about strong chain of custody in the manufacturing and supply of drugs to a patient and blockchain heralds itself as the answer to the issue where things have gone wrong and acts as the block to fake drugs entering the supply chain. As it stands counterfeit drugs are estimated to be at 50% in low income countries with a global market range of $200 billion (DrugPatentWatch 2017). As well as counterfeit drugs being a failure to treat the patient, it may also kill/harm the patient. Blockchain will create the place where the ecosystem of a supply chain would interact and record all transactions without being able to tamper the records. The result is a transparent method to secure the chain of custody and data.

3.10 Patients and Clinical Researchers

Perhaps the most important part and central to all the transparency and privacy of the data theme are patients and researchers. As it currently stands along the clinical research data flow explained in earlier sections, if some information is excluded or selectively positioned for the reasons mentioned then the most impact is conveyed to the patient and researchers. There seems a trust given by patients to the clinical research providers that their information gained from trials will help advance medical outcomes. This trust is extended down the line with regulatory bodies to approve to release to the public and the pharmaceutical industry to share the full clinical data sets. Consenting in this trial process usually to a patient means being exposed more understanding of the results. It is stated in the Declaration of Helsinki that participants should be advised of the results. However, the placement of this trust looks in many cases to misguided as many participants/patients are not given access to results or further understanding; Logvinov (2014). In the previous Chapter (Digital Transformation of Healthcare) patient centric data was discussed and the benefits to place patients in the centre of all activities. This clearly makes a more transparent model in terms of clinical trials as the patient can be more directly engaged and also learn more on the trial they undertook, and any other data sets outside their own. They can also understand further from pharmaceutical companies what the wider effects or analysis are after Phase IV when the drugs are publicly available.

Researchers have the issue of not accessing all data impacts in the post marketing phase that pharmaceuticals may chose or not chose to report, and so science may develop in a direction that is either stifled or led in alternative routes. Patients have no control over their data and where and what is held. If blockchain can facilitate as a mechanism to safely share data, then there are more opportunities available to researchers than just curing the interoperability issue. A network of patients, scientists, researchers, clinicians, etc., could actively share data across the board to help advance research in a more dynamic fashion. If all the data is recorded and audited and permissions given to access, then potentially this can go a long way to resolve selective reporting. Intervention data exaggerated, misconstrued or negative results hidden are causing the effects mentioned later in this Chapter.

3.11 Clinical Trials Processes

The clinical trials data flow and its associations with interoperability, privacy and security of the healthcare data makes a very captivating model to analyse. The purpose of the next few sections is to review the following:

- Survey data from leading industry organisations taking a global perspective regarding if blockchain is ready for adoption to healthcare initiatives.
- Analyse some key data points in the clinical trials process, which are Trial Registration, Informed Consent, Trial Outcomes and healthcare cyber security

breaches. This helps determine, with other evidence found in previous sections and in critical discussion later in this Chapter, that there is a real need to look at a mechanism to support transparency, security and privacy of healthcare data and will help validate the urgency of this need.

3.12 Clinical Registration Analysis

It is difficult to assess globally how many trials go unregistered and unpublished and is thought-provoking to imagine that to some extent there is a lot of wastage of expenditure and any knowledge that could have been gained and shared with other researchers or groups. Prayle et al. (2012) took an in-depth review of registered and interventional clinical trials and discovered that only 22% of trials that were mandatory to post results actually did. It raises the question of how monitoring is taking place. Also, another interesting fact is that 40% of industry sponsored trials reported their results compared to 9% in non -industry sponsored trials.

Whilst the outcomes of clinical trials are clearly measurable factors and issues revolving around are explained in this Chapter, it's also recognised that a lot can be said for the accuracy in how clinical data is registered and over the years the quality has been noted as being poor, Viergever et al. (2014). The analysis compared a previous 2009 study by Viergever and Ghersi (2011) against a 400 randomised records sample in 2013 (taken from 23,046 interventional trials) on registration data, interventions and outcome. The analysis showed increasing trial registration/quality issues and needed improvement. Half of industry funded trials did not input the primary contact name and in non-industry funded trials it was nearer to 95%. Contact information appears to be removed by those undertaking trials when the study is completed or for some reason stopped. Other issues show retrospective registration, which can cast bias to results. There are driving factors of registration in the form of legal, regulatory, ethics, funding policies, etc., and as Viergever et al. (2014) point out that even though there are these important considerations, some trials still go on to be unregistered. In the assessment they also found that the primary outcome was only reported in 66% of registered trials and other details such as medication dosage., etc. was reported in 70% of registered trials, Viergever and Ghersi (2011). It seems from the research that besides just increasing the percentage of trials registered, if some enforceable measures for quality assurance could also be considered (this would be how to record/capture data and look at what controls to enhance the process).

The irregularity of the method and way registration is undertaken adds to the publication bias explained later in this section and a further look into why is it that there are some organisations that require registration but do not enforce it; or as best practice than mandatory. An interesting quantitative and qualitative analysis was undertaken by Wager et al. (2013) and reviewed a random sample of 200 journals from a list of 3512 journals.

The quantitative study shows:

– 142 journals require no registration (71%)
– 55 require registration (28%)
– 3 were encouraged to register (2%)

It's interesting to also understand the qualitative study Wager et al. (2013) did where interviews with 15 editors of a selection of 31 journals were undertaken to understand reasons trial registration was not required and as follows the main points:

– Competition; in the way of concerns of failing to rival journals who are not themselves imposing process of registration
– Primary papers; perhaps as a smaller or mid-level journal not requiring submitting papers
– Lack of clinical trials papers; in case some organisations might not publish many clinical trials to formalise registration
– Small trials; if the trial was a small research project there were feelings that registration would probably be not a necessary factor
– Effectiveness of registration; doubts whether negative trials would be published, even if registered
– Developing regions; trial registration in emerging countries may not have enforced registration so requesting requiring this for papers may create issues if there is no registration in the country or origin.

Table 3.2 from Wager et al. (2013) shows over a period of time (including their sample selection) of analysing different random journals that requiring to register is more or less of same percentage. This could be an additional ingredient to publication bias and adding to the problem in a cumulative way.

3.13 Informed Consent and Privacy

Informed consent sits well with the flow of data with regards to this research and transparency. The role of participants is strategically important to the clinical trials study process and therefore should have assurances on the ethics, respect privacy, inform participants on any changes and generally involve them at all points. Hence transparency is the key theme here. There is a process that should be followed from the first agreement/consent to ongoing periodic checking with participants that they still bear willingness to continue. Where it can be of issue, in terms of transparency and privacy, is when new information comes to light and a new consent form should be agreed. This is especially important if, for example, to highlight new side-effects.

There are current issues in informed consent. As example, a FDA report into 57 clinical trials found that over 53% failed to protect the participant interests and issues in the process of informed consent; Seife (2015). Ethical safeguards are in place with reference to the Declaration of Helsinki as per World Medical Association (2018) so at least the guidance and operational framework is there. But it needs a

Table 3.2 Comparison over the years of 'required registration'. (Wager et al. 2013)

			Source	Registration		
Study	Search date	Journals		No in sample	Required	Encouraged
Matarese	2008	Italian; UK	Medline; Medline	76; 76	0; 21 (28)	—; —
Meerpohl	2010	Paediatric	*Journal Citation Report*	69	11 (16)	5 (7)
Meerpohl	2011	Open access paediatric	*Directory of Open Access Journals*	41	9 (22)	4 (10)
Krleza-Jeric	2009	WAME members	WAME membership list	102	35 (34)	—
Kunath	2011	Urology	*Journal Citation Report*	55	18 (33)	2 (4)
Wager	2012	Random sample	Cochrane CENTRAL database	200	55 (28)	3 (2)

diligent approach from clinical organisations and as per this research, a model that can be applied onto blockchain to secure all stages of consent; that is all notifications of checking to proceed, any new trial protocol amendments, etc. If applied as a smart contract, then privacy is respected and data capture of any event time-stamped in order.

3.14 Clinical Outcomes Data Analysis

Clinical outcomes are the measuring tool to determine the baseline objective that patients will undergo to assess the drug efficacy and treatment process and success ratios. In the case of clinical trials, before commencement a Protocol/Registry is designed that lists the parameters i.e. types of participants, procedures, medications, duration, outcomes, etc. It's expected to conform to CONSORT (Consolidated Standards of Reporting Trials) which gives a minimum check list specification to aid transparent reporting. It's of high importance since this is the central piece to the whole chain of events. If poorly documented or inadequate validation against the outcomes is given, or worse if selective reporting is applied leading to misconduct and fraud, then potential impacts are cascaded to patients, from minimal issues to loss of life. Therefore, the data analysis in this part of the data flow in clinical trials looks to be essential in what is captured, reported and possible effects (these can only be validated from patient use in post marketing of which seems sufficient and growing in evidence and explained in later section).

3.15 Global Aspect of Clinical Trials

If the number of trials/studies enrolled in ClinicalTrials.gov (the largest of clinical trials database run by US National Library of Medicine) is currently, as of May 30, 2018, at 274,416 then the sample selection of data analysed in this section presents a worrying concern on the current state of affairs; (ClinicalTrials.gov 2018). See Table 3.3 for the global percentage breakdown, Fig. 3.5 for the perspective growth of Trials over time and Trials results posted in Fig. 3.6.

It is also worth understanding the breakup of types of studies undertaken and what results are posted on ClinicalTrials.gov as in Table 3.4:

3.16 Clinical Outcomes Data Concerns

Given the prospect that there is a potentially large amount of data that could be reviewed and extracted; for the purposes of assessment for this research a smaller subset is reviewed and validated with original Protocols and its delivered outcomes. It suggests a more extensive study can be undertaken outside of this research for larger data sets and analysis to see if there is a more substantial problem than envisaged.

COMPare (CEBM Outcome Monitoring Project) is an organisation that monitors clinical trials and has a mantra to alert on misreported outcomes and are monitoring the top 5 medical journals (The Lancet, Annals of Internal Medicine, JAMA, BMJ and NEJM). They analyse the trial protocol/registry entry (as per CONSORT) and any outcomes that are switched are reported and letters sent to editors to notify; COMPare Trials Project (2016). It's important to measure against the protocol set, so to avoid a false positive by random chance. When the trial is complete there should be a match to see where reported outcomes are different from pre-trial. It should be declared and explained so unbiased representation is given.

The following Fig. 3.7 shows high level report created from the raw data as per site COMPare Trials Project (2016). It's a quantitative analysis from period October 2015 to January 2016 undertaken by coders who audited, checked and advise the pre-specified outcomes. Also, if it was reported and if new outcomes were added.

Table 3.3 Number of global registered studies. (ClinicalTrials.gov 2018)

Region	Percentage of Registered Studies
Non-U.S. only	130,418 (48%)
U.S. only	96,663 (35%)
Both U.S. and non-U.S.	14,845 (5%)
Not provided	32,490 (12%)
Total	**274,416 (100%)**

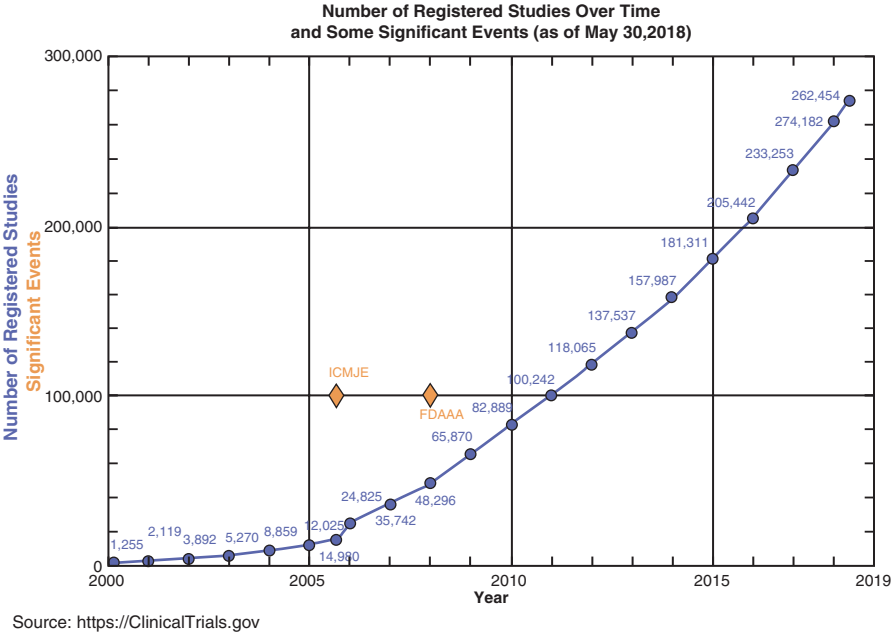

Fig. 3.5 ClinicalTrials first posting since 2000. (ClinicalTrials.gov 2018)

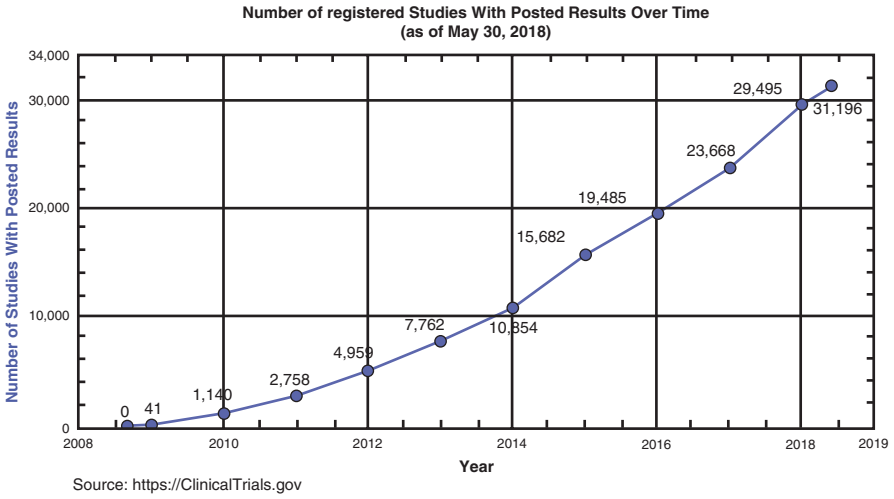

Fig. 3.6 Number of registered studies with results posted. (ClinicalTrials.gov 2018)

Table 3.4 Types of registered studies. (ClinicalTrials.gov 2018)

Study and intervention type (as of May 30, 2018)		Number of registered studies and percentage of total	Number of studies with posted results and percentage of total
Total		274,416	31,217
Interventional		218,243 (80%)	29,376 (94%)
Type of intervention	Drug or biologic	128,004	23,415
	Behavioural, other	67,229	5207
	Surgical procedure	23,245	1610
	Device	26,870	3643
Observational		54,919 (20%)	1841 (6%)
Expanded access		481	N/A

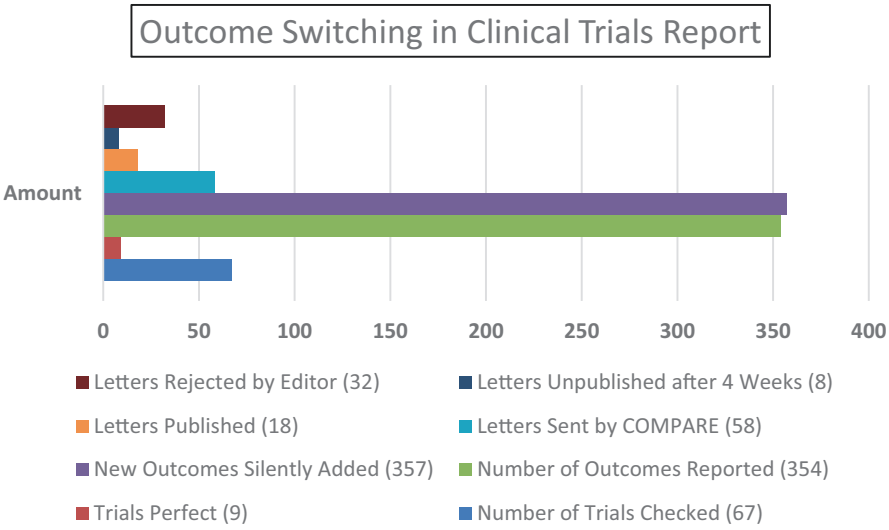

Fig. 3.7 Outcome switching in clinical trials report. (Data sourced from COMPare Trials Project 2016)

Full sets of raw data can be located at the COMPare Trials Project (2016) and links to the full assessment sheet for each trial to ensure transparency of the analysis.

Figure 3.8 shows 67 trials were reviewed from October 2015 to January 2016. Only 9 Trials were found to be perfectly correct whilst it was found 354 outcomes were not reported. However, noted were 357 new outcomes that had been silently added. COMPare have followed up by sending 58 letters of which 18 letters were published. If a mean average is calculated it only presents each trial as reporting 58.2% of its outcomes from original specification. The average of silently added

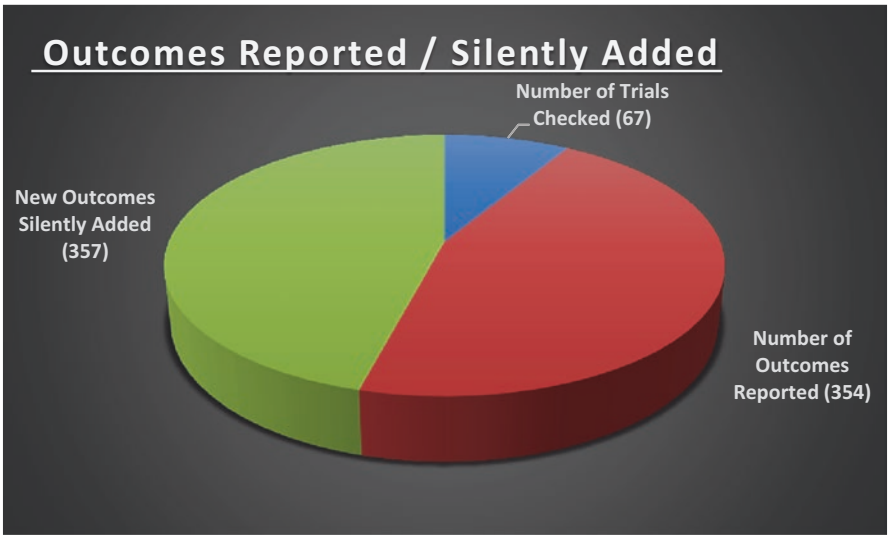

Fig. 3.8 Trials outcomes reported vs trials outcomes silently added. (Data sourced from COMPare Trials Project 2016)

outcomes is 5.3. COMPare is currently assessing this first set of findings as an academic submission but provides useful deliberation and concern for this research regarding transparency, security and privacy of data. It also suggests more work in this area and a more transparent method of monitoring the Protocol and outcomes delivered; blockchain could assist in this deliberation by using smart contracts making review easier over a period of time.

Table 3.5 shows a slice of the COMPare Trials Project (2016) of 67 Trials reviewed which are showing the pre-portion of pre-specified outcomes as correct, which should show 100% and the new undeclared non-prespecified outcomes that were added and for a correctly reported paper that should be zero. Table 3.6 describes the higher undeclared non-prespecified outcomes and a snapshot of the top sample of data taken from a full data set.

3.17 Research Misconduct, Fraud and Selective Reporting Impacts

Fraud, misconduct and selective reporting all have negative and serious impacts, but it is worth distinguishing the difference to understand what the drivers are. It may be assumed fraud and misconduct could be classified as being the same activities and definitions, when in fact there are clear differences. According to Gupta (2013) fraud has some form of deliberate action whilst misconduct may be a case of a

Table 3.5 Correctly added pre-specified incomes. (COMPare Trials Project 2016)

Journal	Trial title	Trial published	Prespecified outcomes reported	Undeclared non-prespecified outcomes reported
BMJ	Liraglutide in people treated for type 2 diabetes with multiple daily insulin injections: randomised clinical trial (MDI Liraglutide trial)	28/10/2015	19/19 (100%)	0
JAMA	Effect of vericiguat, a soluble guanylate cyclase stimulator, on natriuretic peptide levels in patients with worsening chronic heart failure and reduced ejection fraction: the SOCRATES-REDUCED randomized trial	08/11/2015	2/2 (100%)	0
JAMA	Naproxen with cyclobenzaprine, oxycodone/acetaminophen, or placebo for treating acute low Back pain	20/10/2015	1/1 (100%)	0
Lancet	Safety, efficacy, and immunogenicity of VGX-3100, a therapeutic synthetic DNA vaccine targeting human papillomavirus 16 and 18 E6 and E7 proteins for cervical intraepithelial neoplasia 2/3: a randomised, double-blind, placebo-controlled phase 2b trial	21/11/2015	2/2 (100%)	0
NEJM	A randomized trial of progesterone in women with recurrent miscarriages	26/11/2015	9/9 (100%)	0
NEJM	A study in older subjects to evaluate the safety and ability of andexanet alfa to reverse the anticoagulation effect of apixaban or rivaroxiban	09/11/2015	20/20 (100%)	0
Lancet	Skin antisepsis with chlorhexidine–alcohol versus povidone iodine–alcohol, with and without skin scrubbing, for prevention of intravascular-catheter-related infection (CLEAN): an open-label, multicentre, randomised, controlled, two-by-two factorial trial	21/11/2015	7/8 (87.5%)	0
Lancet	Extended pre-exposure prophylaxis with lopinavir–ritonavir versus lamivudine to prevent HIV-1 transmission through breastfeeding up to 50 weeks in infants in Africa (ANRS 12174): a randomised controlled trial	18/11/2015	3/5 (60%	0
NEJM	Nivolumab versus docetaxel in advanced nonsquamous non–small-cell lung cancer	22/10/2015	3/5 (60%)	0
NEJM	Sofosbuvir and velpatasvir for HCV in patients with decompensated cirrhosis	16/11/2015	5/9 (55.6%)	0

(continued)

Table 3.5 (continued)

Journal	Trial title	Trial published	Prespecified outcomes reported	Undeclared non-prespecified outcomes reported
NEJM	A phase 3 randomized trial of nicotinamide for skin-Cancer chemoprevention	22/10/2015	5/11 (45.5%)	0
NEJM	Cabozantinib versus everolimus in advanced renal-cell carcinoma	05/11/2015	4/16 (25%)	0

Table 3.6 Analysis of higher undeclared non-prespecified outcomes. (COMPare Trials Project 2016)

Journal	Trial title	Trial published	Prespecified outcomes reported	Undeclared non-prespecified outcomes reported
Lancet	An internet-delivered handwashing intervention to modify influenza-like illness and respiratory infection transmission (PRIMIT): a primary care randomised trial	24/10/2015	0/12 (0%)	17
Lancet	Immediate delivery compared with expectant management after preterm pre-labour rupture of the membranes close to term (PPROMT trial): a randomised controlled trial	09/11/2015	17/35 (48.6%)	17
Lancet	A randomized, open-label, multi-center, active-controlled, parallel group study to determine the efficacy and safety of the REG1 anticoagulation system compared to bivalirudin in patients undergoing percutaneous coronary intervention	04/11/2015	1/1 (100%)	21
BMJ	Stepped care for depression and anxiety in visually impaired older adults: multicentre randomised controlled trial	23/11/2015	0/8 (0%)	22
Lancet	Neurodevelopmental outcome at 2 years of age after GA or awake-regional anaesthesia in infancy	04/11/2015	0/3 (0%)	26

failure to follow structured and well established protocols. Fraud has the intentional and planned actions to cause deception for personal gain by fabricating research data and misleading reporting of the results. With misconduct it may not be intentional actions or more a case of poor management to follow structure and processes that in set in place. The Medical Research Council makes clear its statement in its code on fraud and misconduct and has clear distinction on deliberate, dangerous and

negligent actions that deviate from accepted practices and protocols. This will not include honest errors and mistakes, and even poor research that has not the intention to deceive.

3.17.1 Types of Fraud and Misconduct in Clinical Research

Fabrication New data sets and records may be created. One area of the clinical research workflow that may be prone to this deception is at the various stages of Informed Consent, mostly in Informed Consent forms. Here data could be fabricated if some amends to the trials were made, then to imply consent was acknowledged by the patient.

Falsification Data is altered in any records so deliberately implying a different version of outcomes or perhaps hiding negative data.

Plagiarism Other person's work/ideas may be taken and acknowledged as one's own work.

Deception The intentional obscuration or inclusion of data that may create a bias or lead to selectively represent misleading directions.

The motivations to any of the above can be due to a number of reasons, some for personal gain and others for professional ambitions or just inadequate disciplines to ensure that the protocols and procedures are diligently followed taking in consideration Medical Research Council codes of conduct and the overall importance of accuracy. If any of the above consequences suffer the actions of the types of fraud and misconduct, then it can have a myriad of effects and some examples explored in later examples.

An interesting report method by Seife (2015) looked at 57 published clinical trials (due to redactions many trials were not identifiable and hence only the 57 were selected) from 600 clinical trials and identified several issues. The chart analysis below (Fig. 3.9) summaries the research results, Seife (2015) and based on data it shows that 22 trials were falsified; 14 trials had issues with adverse events reporting; 42 trials had protocol violations; 35 trials had inadequate/inaccurate record keeping; 30 trials had a failure to protect patient safety and issues with the Informed Consent process; and 20 trials where violations were there but not categorized. Only 3 publications of a total of 78 publications that were outputs of the trials disclosed a picture of violations or malpractice in the trials. In others there were no expressions of these concerns and types of violations explained which presents a picture that the publications had successful trial process with no concerns.

This lack of transparency with the quantitative data examples gives validated reasons to look at blockchain as the framework to control all and ensure a better way

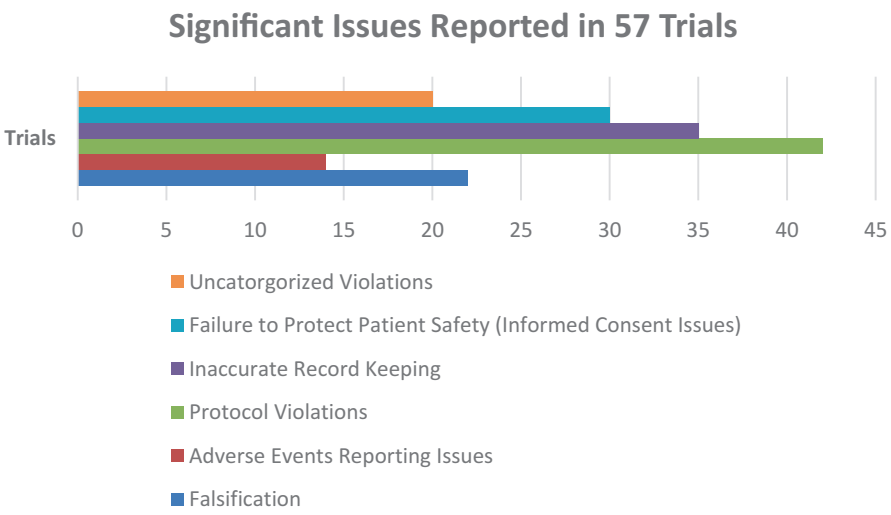

Fig. 3.9 57 Trials selected showing significant issues. (Data sourced from Seife 2015)

to modulate the data. However, the interesting aspect to these results is more than just the clear violations, inaccuracies, falsifications, etc., but more the fact of the range of potential impacts to patients. The research that was produced by Seife (2015) shines a torch on a few case studies and where, for example, falsification of laboratory results of chemotherapy regimens resulted in the researcher falsifying the lab results; this obscured the facts that the patient had impaired liver/kidney functions and was exposed to the first dose which was fatal. The researcher was found criminally negligent (a custodial sentence applied) yet no details of this appeared in the peer-reviewed content that tie-in to the chemotherapy trials the patient was deceased from.

The concerning aspect is how many trials are there where the data/outcomes are misconstrued or covered up; be it for the gain in the market edge, competitor pressure or in one's belief that showing only 'interesting' selective data is acceptable and only worth recording. The smart contracts feature of blockchain would allow a clear and transparent model to base all data and archived in a time stamp method with time ordering so bolstering integrity to the whole process. This should capture most aspects including all raw data, so situations such as the case described above can be transparently analysed by all those permissioned on the blockchain. This can ensure even the negative results or some results that do not match the positioned post marketing effects are kept in compliance and sanity checked by those unbiased and qualified to assess. Hopefully, the effects of a transparent model will lessen the occurrences of falsification, fraud, deception, etc. and more adherence to medical ethics and greater integrity.

3.17.2 Publishing Clinical Trial Data – Noncompliance

The previous sections go into a deep dive of the various stages of processes and the potential failure points. Another area to consider is the completed clinical trial publishing aspect which leaves a question mark on its conformity and compliance to publish the data. The previous sections covered where the data may be cherry picked or selectively reported, etc., but this question is more about the time to publish from completing the trial. Some cross-sectional analysis has been undertaken by Ross et al. (2012) and who reviewed compliance with FDAAA (FDA Amendment Act of 2007) on funded trials by National Institutes of Health (NIH). The analysis concluded that 46% of 635 registered and completed trials had published the results in peer-reviewed journals within 30 months of trial completion. The target is aimed at 1 year so 30 months is a long way from this target date recommended by FDAAA. Another fact is after 5 years one third of completed trials are still unpublished. This lack of diligence to publish can suggest publication bias but more importantly does not factor in consumer safety.

More analysis by Bourgeois et al. (2010) talks about observing 546 drug trials registered in ClinicalTrials.gov and discovered 66% had published their trials but again late on delivering publication and not within the requested publishing window. Just 32% of industry-funded trials had their results published within 24 months of completed trial. A larger review shows more gross noncompliance, undertaken by Zarin et al. (2011) of 79,143 records in ClinicalTrial.gov recorded that 52% of registered/completed trials had published within 2 years. There is a common theme across the analysis undertaken that noncompliance adds to the dangers and issues created when drugs are publicly available. There may be significant issues that could be stopped before widely being distributed if data was shared much earlier and transparently. Also, if perhaps other groups of researchers had access to these published results then it might add reflection to their study that would allow a change of tact or repeating unnecessarily what may not have worked first time or potentially causing harm to participants. Goldacre (2013) makes stronger comments that the number of clinical trials ignoring FDAAA requirements is more like 60–90%. It is suggested this might be due to publication rules being more relaxed with having to prove clinical trial registration.

It's clear that compliance falls short in the process as per cross-sectional studies undertaken by those mentioned in previous sections and is not in sync with FDAAA requirements. The suggestion is full disclosure and transparency on the results would provide an invaluable resource to clinicians and researchers to understand the risks/fundamental points of new drugs regarding safety and efficacy, Logvinov (2014).

There is some concern mentioned in other reports of allowing full disclosure but looks to be more a case of how something should be packaged and presented for consumption by the pubic and all. Logvinov (2014) mentions that dumping huge volumes of data into a database may not be helpful to consumers. But this can be more effectively managed via authentication on blockchain by giving permissions

to all or certain parts of data (but at least the whole data sets are there for usage). It makes sense that participants can discuss results with providers/investigators. It will also support and help the general cause of clinical research enrolment and ensure there is still interesting to participate. If blockchain can help facilitate a closer relationship between investigators and participants, then they may feel more consulted and empowered with information they receive. Pharmaceutical organisations have argued that divulging all can be a risk to their intellectual property and erode a competitive edge (especially in emerging markets that may reproduce very similar drugs on the back of the pharmaceutical bulk of research work. It is a difficult balance but likely the more important angle will sit in public health and safety than preservation of intellectual property and commercial aspects. But the Trade-Related Aspects of Intellectual Property Rights (TRIPS) does offer a protection clause (Article 39, para 3) to pharmaceutical in their right to protect opening up undisclosed data unless a threat to public health, Logvinov (2014).

3.18 Cyber Risks to Clinical Healthcare Data

Under the current methods that healthcare data is stored in presents a serious risk to the CIA triangle (Confidentiality, Integrity and availability). It is of major concern and connected to the clinical research flow of data as whilst there are substantial benefits to all in the advancement of healthcare technology; be it wearables, machinery, drugs to assist better and more targeted healthcare, etc., it also means the data will exponentially increase and needs to be a more sophisticated method to protect healthcare data. Also, it requires clearer transparency to protect the worst effects of data breach for any patient of identity theft and possible victimisation that normally follows. Fig. 3.10 below highlights this widescale breach of data across industries but clearly demonstrates that healthcare has the highest levels of attacks.

Gemalto is an organisation that collates and aggregates worldwide data breaches in various industries and proactively monitor this through the *Breachlevelindex.com*. The report is useful as is also backed by where the weblink data source originated from and so can be validated as high quality, quantitative data. It makes measurement of the data in terms of data records lost/stolen, type of breach, source of breach and filtered into the industry sectors. Gemalto apply a scoring system to value the risk factor of the breach. So, a scoring measurement of the risk impact is as follows:

- 1–2.9 (minimal)
- 3–4.9 (moderate)
- 5–6.9 (critical)
- 7–8.9 (severe)
- 9–10 (catastrophic)

When analysing the healthcare industry, the data makes interesting discoveries. In 2017, there was a 27.3% increase in records breached compared to the year of

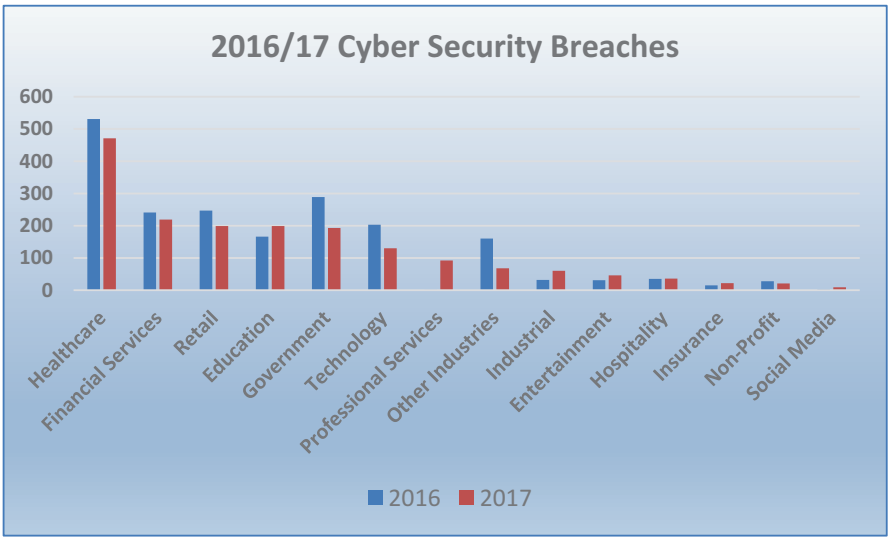

Fig. 3.10 Cyber security breaches 2017 industry comparison. (Data sourced from Breachlevelindex.com 2018)

Table 3.7 Breakdown of 473 healthcare breaches of 2017. (Breachlevelindex.com 2018)

Source of breach	Breach volume
Malicious outsider	322
Malicious insider	68
Accidental loss	82
Hacktivist	1
Type of breach	**Breach volume**
Identity theft	414
Nuisance	19
Account access	18
Existential data	11
Financial access	8
Financial loss	3

2016 (33,717,772 from 26,467,715 records in 2016). There were 473 organisation healthcare data breach incidents in 2017 (see Table 3.7 for the breakdown of categories) and the full raw data sets extracted from the *Breachlevelindex.com*.

A snapshot of the top 10 incidents can be seen in Table 3.8 where the top incident had a catastrophic breach exposing 26 million records and given a rating risk score of 9.0.

However, it is also worth to analyse and compare where the type of breach and source of breach occurs most. Figs. 3.11 and 3.12 show a dangerous correlation mix

Table 3.8 Top ten healthcare cyber security breaches in 2017. (Breachlevelindex.com 2018)

Rank	Organisation breached	Records breached	Data of breach	Type of breach	Source of breach	Location	Risk score	Weblink to site of data source
13	**National Healthy Service (NHS)**	**26,000,000**	17/03/2017	Identity Theft	Accidental Loss	UK	9	https://www.telegraph.co.uk/news/2017/03/17/security-breach-fears-26-million-nhs-patients/
36	**Commonwealth Health Corportation**	**697,800**	01/03/2017	Identity Theft	Malicious Outsider	USA	8	https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
37	**Airway Oxygen**	**500,000**	18/04/2017	Identity Theft	Malicious Outsider	USA	7.9	http://www.healthcareitnews.com/news/500000-affected-ransomware-attack-home-medical-equipment-supplier
45	**Urology Austin**	**279,663**	27/02/2017	Identity Theft	Malicious Outsider	USA	7.9	http://www.kxan.com/news/local/austin/ransomware-attack-on-urology-austin-gets-patient-information/994849601
46	**Women's Healthcare Group of Pennsylvania**	**300,000**	01/01/2017	Identity Theft	Malicious Outsider	USA	7.7	https://www.nbcphiladelphia.com/news/local/Womens-Health-Care-Group-Pennsylvania-Hackers-Medical-Information-Stolen-Data-Breach-436635983.html
66	**Med Center Health**	**160,000**	19/03/2017	Identity Theft	Malicious Outsider	USA	7.4	http://www.wbko.com/content/news/Med-Center-Health-416769003.html
72	**HealthNow Networks**	**918,000**	10/04/2017	Identity Theft	Accidental Loss	USA	7.3	https://www.hipaajournal.com/918000-patients-sensitive-information-exposed-online-8762/
74	**Pacific Alliance Medical Center**	**266,123**	14/06/2017	Identity Theft	Malicious Outsider	USA	7.3	https://www.hipaajournal.com/pacific-alliance-medical-center-announces-ransomware-attack-8925/
75	**Retina-X and Flexispy**	**130,000**	12/04/2017	Identity Theft	Malicious Outsider	USA	7.3	https://motherboard.vice.com/en_us/article/53vkba/a-week-later-hacked-spyware-vendors-havent-warned-their-130000-customers
79	**Arkansas Oral & Facial Surgery Center**	**128,000**	26/07/2017	Financial Loss	Malicious Outsider	USA	7.2	https://www.tripwire.com/state-of-security/latest-security-news/oral-surgery-center-notifies-128k-patients-ransomware-attack/

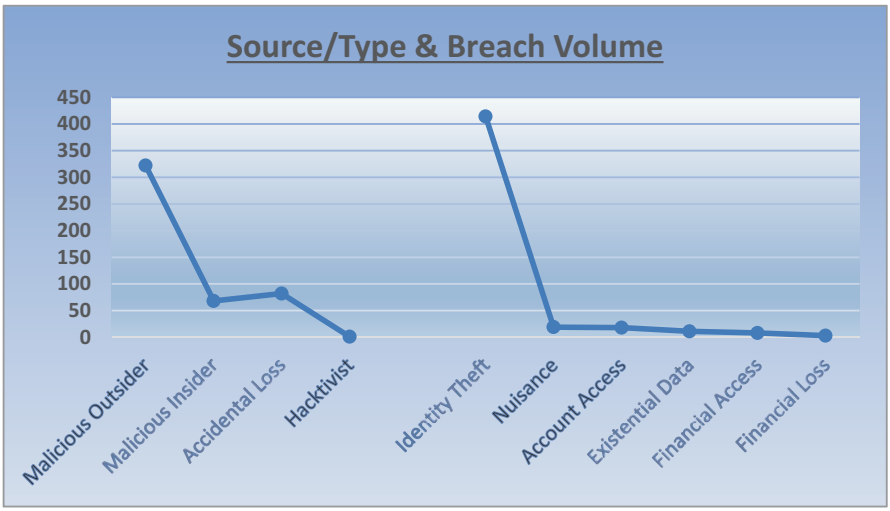

Fig. 3.11 Correlation mix of malicious outsider/identity theft. (Breachlevelindex.com 2018)

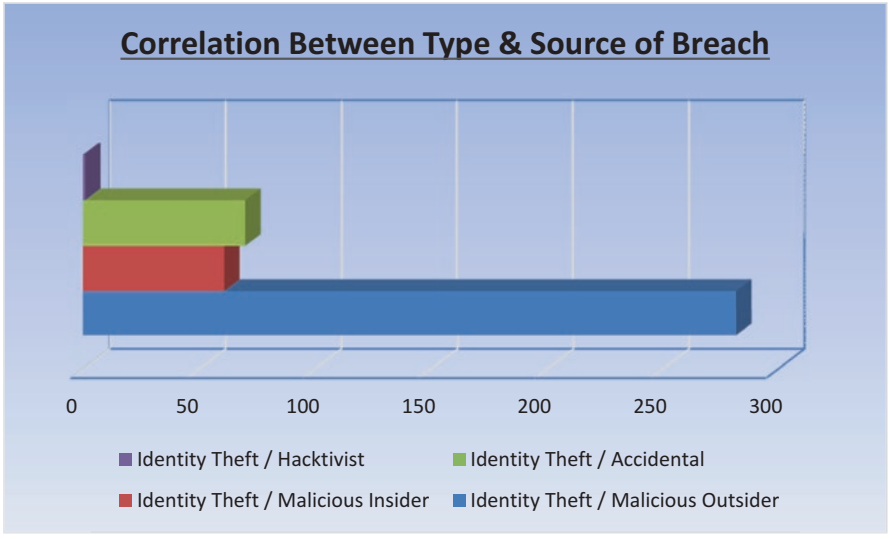

Fig. 3.12 Type and source of breach. (Breachlevelindex.com 2018)

between the worst type of breach (identity theft) and the source of breach as malicious outsider.

It is clear from the quantitative analysis that identity theft is the major objective which correlates with it being a malicious outsider orchestrating the attack. However, other sources of breach such as accidental loss are on the increase so there is likely a requirement of ongoing training programmes, better defences, etc. Whilst that is a necessity, there should be a more direct mechanism to help protect the patient when records are breached and therefore makes a strong case for blockchain application. The identity theft is the major concern since it is a well-known fact on why malicious attackers chose the healthcare industry as next section will explain.

3.19 Case Studies: Marketing Ineffective/Dangerous Drugs – Opioids Study, Breast Cancer Screening – Interoperability Study, etc

3.19.1 Opioids Misuse

Continuing with the theme of patients being at the most vulnerable position is perhaps interesting to look at the prescription opioids scandal; as this highlights the whole question on how drugs are passed through into the market with positive/selective reporting and publication. Prescriptive opioid effectiveness has been reported in the BMJ as having a very high failure rate of over 90%; Moore et al. (2013). In the report, the opioid oxycodone has a failure rate of 100% and quoted as less useful than a placebo. This appeal through the published report, to regulators such as MHRA and large pharmaceutical companies, was done to try and generate an outlook to transparency but so far did not make any impact. Whilst drugs being ineffective is not helpful to solving patient pain, the problem lies in many reports of drugs being harmful to patients, causing addiction and even fatal outcomes. There are numerous risk factors associated with Opioid use and there can't be too many positive outcomes if risk is shown to lead to hospitalisation, criminality and mortality.

Perhaps the more recent and well-known case of Purdue Pharma, that manufactures the OxyContin painkiller, is valid to demonstrate the non-transparent and misconducted way a drug was brought to market and has been associated with causing 200,000 deaths in the US whilst making £26 billion; Cohen (2018a, b). Lawsuits and litigations are the natural response but the accusations of deception in the marketing process, place serious doubts on the current system of how data and information is accessed and regulated; Bellon (2018). Figure 3.13, through the Cohen (2018a, b) report, shows the extent in the UK of how the addiction and opioid admission is growing in the UK, a worrying aspect as it follows a path already taken in the US with the UK as the largest consumer of painkillers in Europe. Prescriptions are surging (£263 million spent annually in England, Cohen 2018a, b) and the

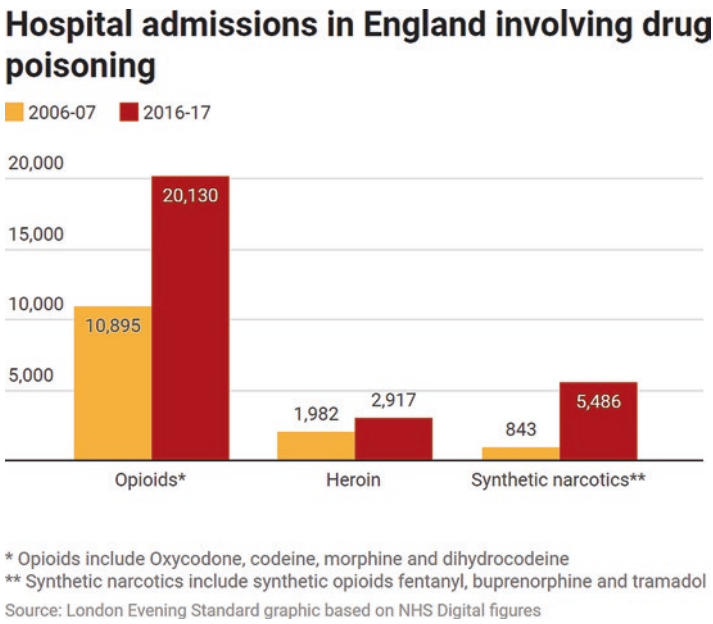

Fig. 3.13 The growth of opioid admissions. (Cohen 2018a, b)

effects are starting to become more published as opioid fatalities increase to 2038 in 2016 attributed to opioid abuse; Hurley (2017). Figure 3.14 shows the rise in opioid deaths and useful as a graphic to understand in relation to growth over the two time periods.

There are many real-life cases of effects to patients who started off with a prescribed opioid drug from their GP for pain relief for medical injuries with all beginning in good stead but then the patient having to increase to higher dosage amounts and eventually becoming a drug addict and purchasing higher quantities illegally. The destruction caused can be anything from major impacts to work, home, family and even fatality; a story that is similar to Philip Hopwood in damage to all these things but fortunately not his life; Cohen (2018a, b).

With a history of over 200,000 deaths in the US and seemingly aggressively growing in the UK there are question marks over regulators like MHRA and Big Pharma companies. There have been both quantitative and qualitative data analysed previously which can bring sense to proposing a validated model such as blockchain as to the many good reasons explained throughout this publication. However, just as important as looking at the effects of selective reporting, bias and misconduct is the importance of transparency so that ethics and trust can be held in more confidence. There's almost an inborn trust most patients have in taking advice from the medical profession in prescription of drugs but as shown in the example of opioids it can potentially cause a reverse of all good intentions, from criminalising an individual

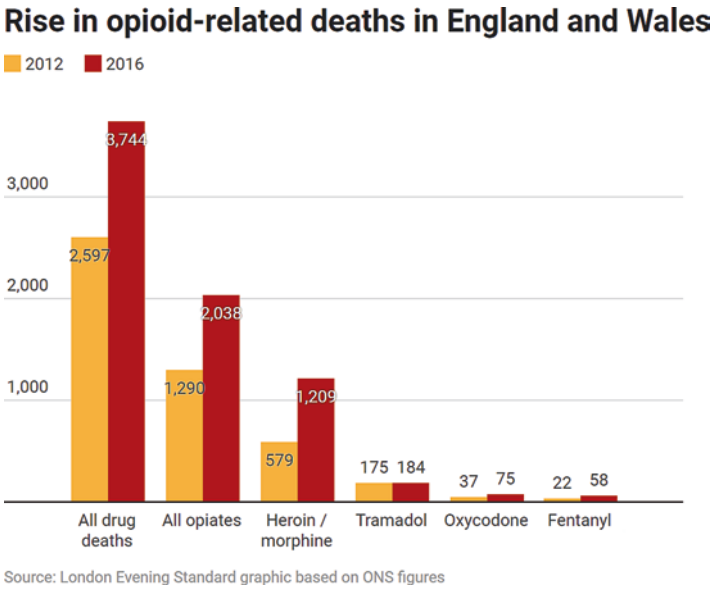

Fig. 3.14 The rise in opioid deaths according to ONS. (Cohen 2018a, b)

into illegal drug purchase to losing one's life. The inborn trust now needs a more validated model as proposed in this research that although is trustless, is the purpose to make this more transparent since no single entity has total control and can be selective in its approach. The patient is put in the centre of control and at least has the knowledge to make more informed decisions.

3.19.2 Breast Cancer Screening – Interoperability Study

Another example is of how perhaps blockchain could have helped avoid IT mishaps due to interoperability issues where a technical issue that dated to 2009, was only picked up in 2018. There appears a question mark in this case of how 450,000 women missed being sent breast screening check-up letters and resulted with up to 270 women dying, Matthews-King (2018).

The IT glitch affected only women aged between 68 and 71 as screening occurs every 3 years for women aged 50–70 years old. The glitch was picked up when the national screening IT system underwent an upgrade and discovered that women involved in a particular study (AgeX trial managed by Oxford University) were not receiving final screening at the 70 age mark. When a much wider review was launched it discovered a similar situation replicated in other parts of England. The problem looks to be the length of time before the glitch was picked up (almost 10 years).

Whilst errors can happen it may have been a better placed model to secure all healthcare records on blockchain and milestone screening results and next due dates all captured and accessible by patients and all parties that need be involved. Perhaps this could have made the system more transparent and operate in a proactive way.

3.20 Conclusions

The clinical trials theoretical model presented in this research makes an interesting example of how healthcare data can be made more transparent, privacy strengthened and how to make best use of blockchain through its time stamp, time ordering, smart contracts and immutability. It offers the benefits just outlined above but opens up a very serious debate and question on potential harm caused by bias, selective reporting, misconduct and fraud, which currently appears to have many gaps in its clinical process, as the example data analysis leads to suggest. Blockchain can tighten up these processes and offer a balanced framework so confidence is restored and reduce the issues described, as the example provided in the case of opioids abuse. There appears a range of destructive issues to a patient that can lead to fatalities. This alone should help qualify the next steps and additional research be committed to make a more trust worthy framework centred on blockchain. Healthcare looks to need the offering of the tangible benefits of interoperability, longitudinal medical data, more privacy protection against cyber breach/identity theft and more protection of the unforeseen damages caused by not having a method of transparency through the whole process of clinical trials research.

References

AllTrials (2013) GSK statement. [Online]. Available at http://www.alltrials.net/supporters/organisations/gsk-statement/. Accessed 30 May 2018

Bellon T (2018) U.S. state lawsuits against Purdue Pharma over opioid epidemic mount. [Online]. Available at https://www.reuters.com/article/us-usa-opioids-litigation/u-s-state-lawsuits-against-purdue-pharma-over-opioid-epidemic-mount-idUSKCN1IG2WU. Accessed 16 June 2018

Benchoufi M, Ravaud P (2017) Blockchain technology for improving clinical research quality. Trials 18:335. Available at https://doi.org/10.1186/s13063-017-2035-z. Accessed 20 Oct 2018

Bourgeois F, Murthy S, Mandl KD, (2010) Outcome reporting among drug trials registered in ClinicalTrials.gov. Ann Intern Med 153(3):158–166. Available at https://doi.org/10.7326/0003-4819-153-3-201008030-00006. Accessed 20 Oct 2018

ClinicalTrials.gov (2018) Trends, charts and map. [Online]. Available at https://clinicaltrials.gov/ct2/resources/trends. Accessed 1 June 2018

Cohen D (2018a) The opioid timebomb. [Online]. Available at https://opioids.standard.co.uk/#article. Accessed 16 June 2018

Cohen D (2018b) The opioid timebomb: how addiction to painkillers cost me my wife, my children, my home and my £150,000-a-year job. [Online]. Available at https://www.standard.

co.uk/news/uk/the-opioid-timebomb-how-addiction-to-painkillers-cost-me-my-wife-my-children-my-home-and-my-a3791006.html. Accessed 16 June 2018

COMPare Trials Project (2016) Goldacre B, Drysdale H, Powell-Smith A., et al. www.COMPare-trials.org. [Online]. Available at http://compare-trials.org/results. Accessed 1 June 2018

DrugPatentWatch (2017) Can blockchain technology put an end to counterfeit drugs. [Online]. Available at https://medium.com/drugpatentwatch/can-blockchain-technology-put-an-end-to-counterfeit-drugs-c4087e652fe0. Accessed 20 Oct 2018

Engelhardt M (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev 7(10): 22–34. Available at https://doi.org/10.22215/timreview/1111. Accessed 20 Oct 2018

Goldacre B (2013) Are clinical trial data shared sufficiently today? No. BMJ, Br Med J (online) 347: 1–3. Available at https://doi.org/10.1136/bmj.f1880. Accessed 20 Oct 2018

Gupta A (2013) Fraud and misconduct in clinical research: a concern. Perspect Clin Res 4(2). Available at https://doi.org/10.4103/2229-3485.111800. Accessed 20 Oct 2018

Hurley R (2017) Drugs caused record number of deaths in England and Wales in 2016. BMJ, Br Med J 358. [Online]. Available at https://search.proquest.com/docview/1925754408?accountid=12860. https://doi.org/10.1136/bmj.j3750. Accessed 16 June 2018

Liang X, et al (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), Montreal, QC, pp 1–5. Available at https://doi.org/10.1109/PIMRC.2017.8292361. Accessed 20 Oct 2018

Logvinov V (2014) Clinical trials transparency and the trial and experimental studies transparency (TEST) act. Contemp Clin Trials 37(2): 219–224. Available at https://doi.org/10.1016/j.cct.2014.01.001. Accessed 20 Oct 2018

Matthews-King A (2018) Breast cancer screening: 450,000 women missed out on checkup invitations due to IT error, Jeremy Hunt admits. [Online]. Available at https://www.independent.co.uk/news/health/jeremy-hunt-breast-cancer-screening-inquiry-nhs-women-invitations-missing-a8332446.html. Accessed 18 June 2018

Moore A et al (2013) Expect analgesic failure; pursue analgesic success. BMJ, Br Med J (Online) 346. Available at https://search.proquest.com/docview/1945757929?accountid=12860. https://doi.org/10.1136/bmj.f2690. Accessed 16 June 2018

National Center for Biotechnology Information (2018) [Online]. Available at https://www.ncbi.nlm.nih.gov/. Accessed 20 Oct 2018

Prayle A, Hurley M, Smyth A (2012) Compliance with mandatory reporting of clinical trial results on ClinicalTrials.gov: cross sectional study. BMJ, Br Med J 344. [Online]. Available at https://doi.org/10.1136/bmj.d7373. Accessed 20 Oct 2018

Proehl J, Hoyt S (2017) Integrity and transparency in reporting clinical trials. Adv Emerg Nurs J 39(1): 1–2. Available at https://doi.org/10.1016/j.jen.2017.01.009. Accessed 20 Oct 2018

Public Eye (2013) Clinical trials. [Online]. Available at https://www.publiceye.ch/en/topics-background/health/clinical-trials/. Accessed 20 Oct 2018

Ramírez J (2013) Lack of transparency in clinical trials: a call for action. Colomb Méd, CM 44(4): 243–246. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4002000/. Accessed 20 Oct 2018

Ross J, Gross C, Krumholz H (2012) Promoting transparency in pharmaceutical industry-sponsored research. Am J Public Health 102(1): 72–80 Available at https://doi.org/10.2105/AJPH.2011.300187. Accessed 20 Oct 2018

Seife C (2015) Research misconduct identified by the US Food and Drug Administration. [Online]. Available at https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2109855?alert=article. Accessed 10 June 2018

Song F, et al (2010) Dissemination and publication of research findings: an updated review of related basics. Health Technol Assess 14(8). Available at https://doi.org/10.3310/hta1480. Accessed 20 Oct 2018

Viergever RF, Ghersi D (2011) The quality of registration of clinical trials. PLoS One 6(2). Available at http://dx.plos.org/10.1371/journal.pone.0014701. Accessed 10 June 2018

Viergever R, Karam G, Reis A, Ghersi D (2014) The quality of registration of clinical trials: still a problem. PLoS One 9(1): 1–12. Available at https://doi.org/10.1371/journal.pone.0084727. Accessed 20 Oct 2018

Wager E et al (2013) Hardly worth the effort? Medical journals' policies and their editors' and publishers' views on trial registration and publication bias: quantitative and qualitative study. BMJ 347: f524. Available at https://doi.org/10.1136/bmj.f5248. Accessed 10 June 2018

Zarin D et al (2011) The ClinicalTrials.gov results database—update and key issues. N Engl J Med 3;364(9): 852–860. Available at https://doi.org/10.1056/NEJMsa1012065. Accessed 20 Oct 2018

Chapter 4
Information Security Governance, Technology, Processes and People: Compliance and Organisational Readiness

Berta Pappenheim da Silva, Alonso Jose da Silva II, and Josefine Ehlers Davidsen

Abstract Compliance and an increasing level of cyber maturity form crucial part of corporate defence systems and are the basis of any well-functioning cyber security programme. As the scope of compliance widens with the maturity of the organisation, the human element needs to be addressed as well. Cyber maturity assessments, red teaming and capture the flag exercises help simulate the threat vectors tactics, tools and procedures, give defenders an insight into the enemy motives and help mitigate technical exposure. However, most of these exercises are being delivered with an exclusive aim to achieve technical learning and address incidents on a technical vulnerability level. This chapter looks at how can organisations – having achieved the necessary compliance and governance standards – understand and address human behaviour as cyber security threat. These can be team member's individual blind-spots and glitches in high-risk team dynamics, which are, if ineffective, are considered system vulnerabilities. When these risk behaviours have been identified and addressed with targeted interventions and training, organisations will be able to mitigate the human risk directly, just as they would patch their on-line systems or scan their networks.

Keywords Corporate defence systems · Cyber resilience · Electronic patient health information · Red teaming · Risk behaviours · PHI · Cyber maturity assessment · NISTGDPR · Cyber-attack · Cyber Range · Wargaming · Cyberpsychology

B. Pappenheim da Silva (✉) · A. J. da Silva II · J. E. Davidsen
The CyberFish Cyberpsychology Solutions, London, UK
e-mail: bps@thecyberfish.com

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_4

4.1 Introduction

As part of the UK Government's work to make the UK a world-leading nation in cyber resilience, British organisations receive unparalleled support to implement common baseline of measures to help ensure the fundamental resilience of organisations to cyber threats. Electronic patient health information (PHI) is a very attractive target for on-line threats: sensitive data loss is a crucial challenge for any health and social care organisation.

The wealth of data available on healthcare networks and the potential impact of data inaccessibility makes the industry very attractive to cyber criminals and nation states alike. Furthermore, as PHI are often handled and shared with a wide scope of personnel and supply chain, the risk of an accidental breach is consequently increased. To minimise these risks, healthcare providers need to maintain a robust information security governance, for instance have tried-and-tested incident response plans in place should a breach occur.

Organisations should develop an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents should be recorded regardless of the need to report them. Organisations should have communication plans in the event of an incident which includes notifying the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable. In the event of an incident that involves a personal data breach Departments should comply with any legal obligation to report the breach to the Information Commissioner's Office.

Security governance, implemented controls, the exposure, motivations and attack vectors will be always driven by the industry sector. Other governing factors are of course the size, level of complexity and the maturity of the organisation at the point in time when implementing the systems and the strategy the organization is aligned with. The cost of implementation will vary according to the scope of the project and the complexity to ensuring that the resources required are proportionate and sustainable to use.

All governance documents – the very building blocks of any cyber security programme – generally address how the organisation will cover the three most important areas:

1. processes: the set of rules and responsibilities controlling the organisation's operating functions
2. people: who operate the functions and the requirements revolving around them,
3. technology: used to identify threats, protect data, detect intrusion, respond any incidents and restore systems.

The intended internal controls represent a mix of the three elements and getting the three things right and in place is key to good governance.

A good starting point is the delivery of a cyber maturity assessment especially with a view to getting senior visibility and sponsorship within the organisation. Choosing the right framework will depend on the size of the organisation, the complexity of their system requirements and also personal bias of their cyber security

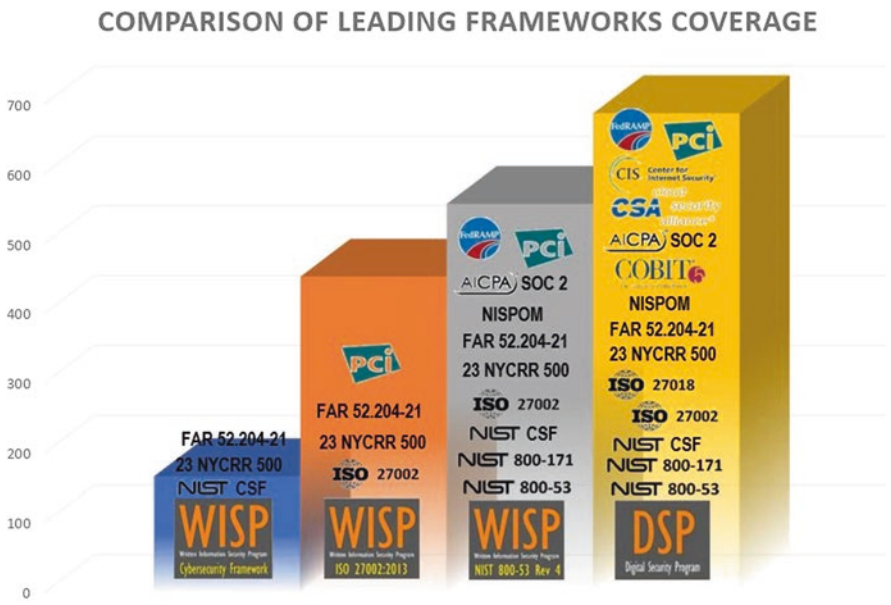

Fig. 4.1 Cyber Security Frameworks, Complianceforge 2018

leadership as to which framework they feel most at ease and have previous experience working with (Fig. 4.1).

As seen from the above, the fourteen (14) domains of ISO 27002 security controls are spread between the twenty-six (26) families of NIST 800-53 rev4 security controls. ISO 27002 is fundamentally a subset of NIST 800-53.

The NIST Cybersecurity Framework (NIST CSF) takes parts of ISO 27002 and parts of NIST 800-53, but is not inclusive of both. As such the NIST CSF is recommended for smaller companies that will be able to pick a best practice framework to align their operations with: where ISO 27002 and NIST 800-53 will be better suited for larger companies or those that have unique compliance requirements, such as healthcare organisations. Unfortunately, common requirements such as the Payment Card Industry Data Security Standard (PCI DSS) are more comprehensive than the NIST CSF, so an organisation would need to use parts of ISO 27002 or NIST 800-53 to meet PCI DSS as a framework (Fig. 4.2).

What is discussed in this Chapter is in essence, however, the way an institution can progress from compliance to organisational readiness – be it a specific operation or business function – reliant on timely and accurate information, the protection of sensitive data, networks or communications systems, with a scope to operating in cyberspace. Technology, processes and people are all critical to the success and credibility of any organization's cyber posture, be them a commercial entity, government agency or a combination. However, many organizations never evaluate and exercise their cyber maturity their actual capabilities and business processes to determine if those processes, people and technology components will satisfy operations during hostile circumstances. In this chapter we will explore how organiza-

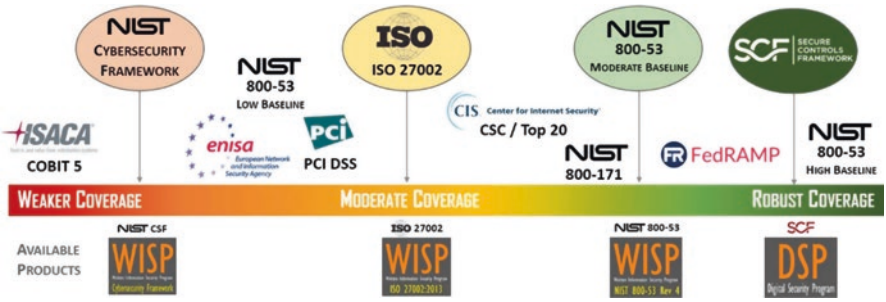

Fig. 4.2 NIST or ISO?

tions may use various scenarios in order to assessing effects on critical systems and data that will have an impact on the operation.

4.2 Compliance Standards in Healthcare

When choosing an enterprise risk management framework and assessment methodology, an organisation should ensure it fits their purposes. Risks applicable to multiple business rules can be controls driven or efficiency driven ensuring on-going management of efficiency and risk monitoring. The design, maintenance and modification of an industry specific repository of business rules and process objectives should result in an easily manageable system, where the assessment and monitoring of specific business process controls and design are kept on an available, operational level.

According to the UK Government's Minimum Cyber Security Standard, the starting principle for any organisation in establishing their cyber security governance is that "there shall be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services". Implementing and demonstrating best practice through internationally recognised frameworks such as the Cyber Essentials Programme as well as compliance with the General Data Protection Regulation (GDPR) are the basic requirements to build network and information security on within the healthcare sector. Additional security measures and incident reporting obligations for operators of essential services (OES) in critical national infrastructure (CNI), including healthcare providers are detailed in the NIS Directive (Network and Information Systems Regulations 2018). Adherence to compliance frameworks and maintaining standards are an important milestone in creating trust within the healthcare supply chain ecosystem to award and get contracts.

Organisations need to define the right approach they intend to take to maintain the required standards for each or all of the above readiness frameworks.

Departments shall know and record all sensitive information they hold or process, the reasons why they hold or process that information, where the information is being held, which computer systems or services process it and what are the impacts of its loss, compromise or disclosure. The right documentation, action plans and other written policies need to be designed to ensure the above requirements.

Organisations should ensure that the resources they intend to deploy to maintain the above systems are available on the long term. Adherence to internal regulations needs to be ensured by regular audits. As compliance has to be maintained on a long term basis, the right number of appropriately experienced staff need to be allocated to the projects, who can be mobilised quickly and made available to support the project in case of incidents. The organisation needs to ensure that individuals who are in charge will be project-managed effectively whilst enabling them to add value by bringing in innovation with their proposed approach to regulatory compliance.

In terms of financing compliance initiatives, one does not fit all. According to Deloitte's GDPR Benchmarking Survey (2018), 39% of organisations surveyed spent less than €100,000 on GDPR compliance, whilst 15% reported spending more than €5 million. There was no correlation found between the organisation's size and the budgets assigned to GDPR compliance, nor have the surveyors identified any trends in different industry segments. Furthermore, there was a considerable variation found in the compliance/privacy headcount with 45% of respondents having a dedicated privacy function (Data Protection Officer or DPO) and 32% managing privacy jointly with another function and 23% with no formal privacy function at all (ibid).

The GDPR contains some new challenges that were not covered by earlier legislation and as such organisations found it increasingly challenging to adopt their internal compliance policies prior to the 25th of May 2018, which is when the GDPR came into force. Ensuring that personal data is stored in a way that subjects are informed and their consent is unambiguously recorded was the main challenge, alongside with the records of processing activities.

Organisations of all sizes need to make sure they comply with data protection regulations, small and micro companies are no exception to the rule. The CyberFish Company have trained 100 small businesses in the London Borough of Tower Hamlets in early 2018 to new privacy regulations in a "GDPR 101" training.

These sessions were held with the objective of helping local startups and micro business owners deal with the 'how' of the implementation of GDPR compliance. During these training sessions it was found that people paid more attention to infographics rather than slides where information was presented to them in a text only format.

A particularly effective training was delivered for a small recruitment company that was directly involved in healthcare recruitment services, where handling and storing of sensitive data was even more relevant. The easier to relate to the material the more enjoyable people found the training and the more questions they had due to personal reflection on the content (Fig. 4.3).

4.3 Maturity Assessments: Wargaming and Threat Intelligence Sharing to Improve Sectoral Cyber Resilience

When undertaking readiness assessments, developing action plans and written tailored template/toolkit materials organisations are expected to take full account of existing and planned NCSC arrangements for cyber incident response, existing

Fig. 4.3 Examples of The CyberFish Company's infographics based training slides for a small recruitment firm

sectoral resilience arrangements, the recently published draft UK National Resilience Standard for Cyber, and regulatory requirements in respect of reporting to NIS Competent Authorities and the Information Commissioner.

A single cohesive end-to-end management solution is essential for effective response to accelerating threats. Organisations however must be able to prevent, pinpoint and address security threats in a cost efficient and timely manner. Compliance is maintained by steering the course intended to improving the visibility of requirements, implementing protective controls and establishing continuous monitoring.

Requirements are updated based on a careful obtaining of threat intelligence information using defence models such as the 'cyber kill chain' (Lockheed Martin) and via the sharing of expertise feeding into an array of short-term, high impact information on current attack vectors and new indicators of compromise to form the threat landscape that will be the bases of any cyber defense. This continuous work needs to drive improvements and ultimately, the ability to respond to, and mitigate, the impact of cyber incidents as part of wider resilience and business continuity planning (Fig. 4.4).

Part of this work is identifying any key strengths and areas for development in existing or planned arrangements to respond to a range of types and levels of severity of cyber threats as part of a regular cyber maturity assessment.

The scope of any maturity assessment should include all internal governance, structures, processes and policies in respect of cyber capabilities and cyber threat intelligence, the outcomes of regular vulnerability assessments and red teaming exercises and how these relate to wider operational resilience arrangements.

Assessments should include consideration of the clarity of roles and procedures to be adopted in the event of different types and severity of cyber-attack at the IT/technical/cyber, legal, HR, communications, senior management and other levels of the organisation (or external providers).

Additionally, assessments should take into consideration of the culture of the organisation. One good example is exercising cyber incident that helps executives avoid mistakes made by their peers. Simulations show where investment in risk mitigation will give the best return, for corporate resilience and breach recovery.

Simulating a major breach is the best way to help leaders internalize the business nature of the cyber threat. Just 90 min invested in rehearsing a major breach can also transform a Board's appreciation of IT security. Intense simulations show executives how they will be personally responsible for leading business recovery after a breach. Leaders can only avoid mistakes made by other organisations if they have rehearsed how to do so.

In the healthcare sector, reporting and notification of significant public sector cyber incidents to central coordinating bodies, regulatory bodies and other key partners is required, as well as coordinating and communicating with them thereafter is necessary.

As an industry, by receiving, sharing and acting upon cyber threat intelligence helps keep the entire supply chain and ecosystem more efficient as new cyber vulnerabilities and attack vectors arise daily. As an example when a healthcare com-

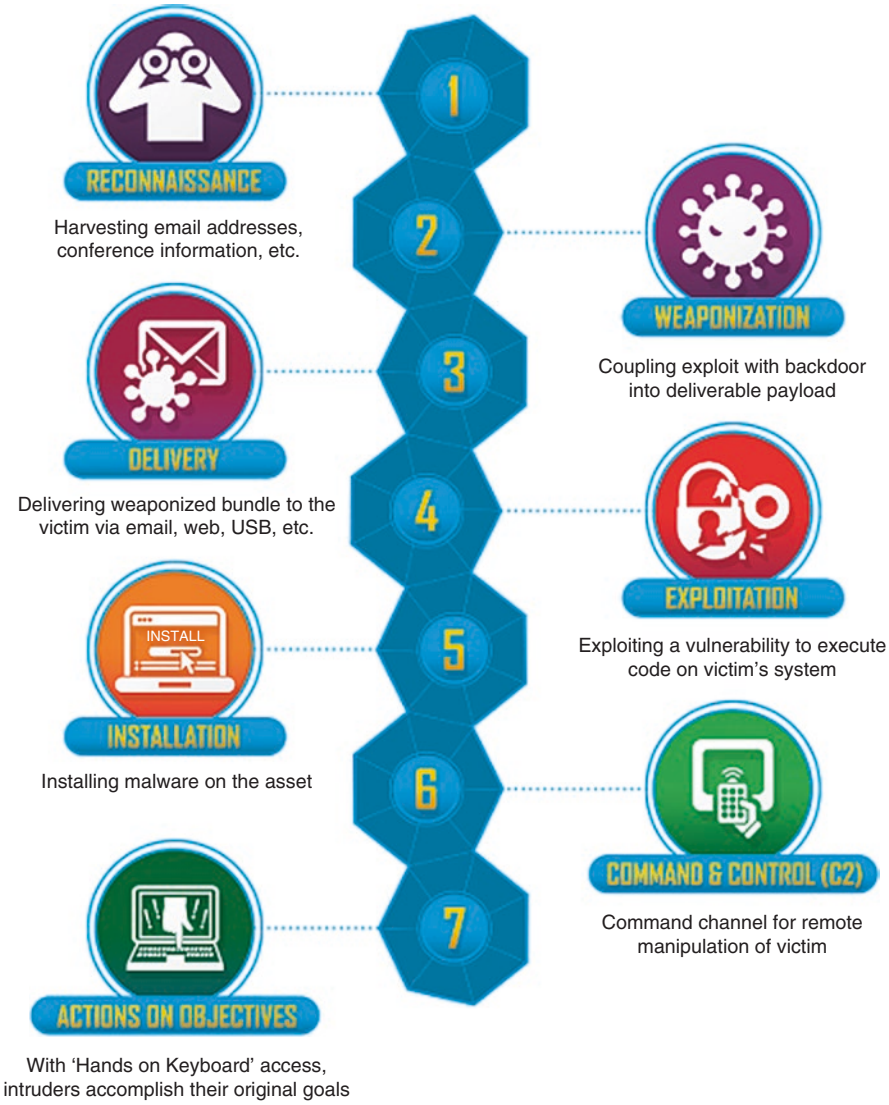

Fig. 4.4 The Lockheed Martin supply kill chain

pany updates its systems or makes an acquisition or brings on a new supplier the risk increases when hackers find this out and threat information is not shared, this exposes the new company in the supply chain to targeted attacks such as social engineering campaigns that can target the business.

The analysis and threat intelligence sharing can also be used to develop relevant scenarios for any wargaming exercises and also facilitates a discussion between business and security managers about which risks and types of information assets

are most important, what are the 'crown jewels' of the organisation. It is crucial to be aware, on a day to day basis, who would want to compromise these information assets, and what the implications of an attack could be with regard to loss of sensitive data, intellectual property, loss of reputation, business disruption, or fraud. Similarly this is true to the mechanisms for accessing up to date advice and guidance on incident management across the healthcare sector.

By sharing threat intelligence information within the sector it becomes possible to learning lessons in the wake of cyber incidents of other organisations.

As part of these readiness assessments, organisations should consider the benefits of exercising, in a prioritised and compartmentalised manner, the most important and/or most immature parts of organisational systems.

On the basis of those readiness assessments, the delivery of individual action plans for each organisation needs to be adopted and implemented, this will help demonstrably improve organisational readiness to respond to and recover from cyber-attacks, including improved arrangements for interacting with wider sectoral, local, regional and national response and resilience arrangements.

4.4 Process Focus

When designing policies and processes regard should be had to authoritative UK and international sources of advice and guidance on cyber incident management and threat intelligence sharing, such as CREST, NIST, ENISA and FIRST.

Processes must include clear, practical implementation steps, resource requirements and ongoing operation must also be identified, and tailored appropriately based on the individual organisation's circumstances. Alignment with individual organisations needs to be in line with improving the cross- sector coherence of incident response arrangements.

Process audits should, where possible, work from existing common taxonomies (refined and improved as appropriate) to allow for further collaboration and coordination. Organisations should consider how these arrangements effectively constitute the incident management and threat intelligence sharing "ecosystem" within which individual health sector organisations operate, and will provide important context for work.

On the basis of assessments, a range of weighted recommendations and options for improvement needs to be drawn up. This should be presented in the form of action plans with different options identified depending on resource availability, timescales and levels of ambition based on business unit and system priorities. Organisations should continuously support on-going work to address the issues identified in the assessment and, when adopted and implemented, help demonstrably improve sectoral, local, regional and national arrangements for responding to and recovering from cyber-attacks.

A key part of the weighted recommendations and options should be consideration of potential options for innovation to help improve the efficiency and effec-

tiveness of sectoral, local, regional and national incident response arrangements while reducing burdens. Organisations should be expected to gather views from discussions with central coordinating bodies and sector specific organisations about what the ideal arrangements would look like for cyber incident management and identify realistic short, medium and long term options for moving towards those arrangements.

Management must take the lead on the development of any tailored written materials required by organisations as part of the initial implementation of the action plans. This may, for example, include (but not be limited to) the drafting and supply of:

– Written documents setting out clear governance, structures, policies and processes for responding to cyber incidents, including sharing, receiving and acting upon cyber threat intelligence as part of the wider sector, and interacting with wider sectoral, local, regional, UK arrangements.
– Playbooks for technical teams to use in wargaming exercises in order to respond to cyber incidents of different types and levels of severity; and
– Scenarios for exercising that are appropriate to the size and sector, potentially as part of a strategic plan and recommended series of exercises linked to any improvement work (i.e. testing improvements identified), proportionate to previously identified resources.

A set of written template materials as part of a toolkit can ideally be freely disseminated across the healthcare sector or supply chain for use by individual organisations to improve their own cyber incident management and threat intelligence sharing arrangements.

It is vital that the sectoral cooperation will result in lessons learned through working with individual organisations and the central coordinating bodies. These structures and networks can then be used to develop materials and threat information that will drive sustainable improvements throughout the healthcare sector.

Organisations' cyber incident readiness materials may, for example, include:

- cyber incident readiness self-assessments and improvement action plans (e.g. by developing a matrix that different units can use to assess their maturity levels, appropriate to different system complexities)
- template governance, structures, policies and processes for responding to cyber incidents, including procedures for sharing, receiving and acting upon cyber threat intelligence
- template playbooks for technical teams to use in order to respond to cyber incidents of different types and levels of severity
- template scenarios for exercising that can be used to test and improve incident management arrangements, potentially as part of a template strategic improvement plan

Consideration of the need to tailor these templates and the contents of the toolkit so that they can be used by organisations of different sizes (e.g. small, medium,

large) is key. Internal policies should also take account of, and offer support to, the early-stage plans to improve cross-public sector sharing of cyber incident management expertise referenced under the recommendations discussed.

4.5 People

4.5.1 Onboarding, Identity and Access Management

According to the Government's Minimum Cyber Security Standard, organisations should ensure that users are given the minimum access to sensitive information or key operational services necessary for their role. All access shall be removed when individuals leave their role or the organisation. Periodic reviews should also take place to ensure appropriate access is maintained.

Onboarding users should start with making determinations prior to the user reporting for job duty. All staff involved in the delivery of the services should be cleared by internal security to use the systems and understand and follow the principles of data protection. On-boarding processes must happen either before, or soon after, a new employee is allowed on the network. These processes need to be highly automated, interconnected, and tied together in a logical sequence. The result is then increased user productivity and decreased managerial burden and lower overall costs.

Vetting employees to the Baseline Personnel Security Standard (BPSS) process is deemed necessary in the health sector when the nature of data accessed requires security procedures to be carried out prior to an individual taking up any works.

Employee vetting must be completed before access to buildings, information and systems will be permitted. In some cases, where individuals are recruited overseas, it may not be practicable to meet the BPSS fully. In these instances the decision should rest with the organisation's guidelines. Verification of identity and right to work should be a pre-requisite that must be provided in all cases.

Access to sensitive information and services should only be provided to authorised, known and individually referenced users or systems. Users and systems should always be identified and authenticated prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service, devices need to be authenticated and authorised for access. The ability to quickly provision, modify, and deprovision user accounts is the fundamental goal of standing up a movers-leavers identity lifecycle management program.

Organizations in the healthcare sector often collect a rich set of authoritative identity data and connect to systems that control network access like Active Directory (AD). With controlled workflows, organizations can quickly automate the provisioning and deprovisioning of user accounts. At the highest level, identity management systems are typically composed of three major elements: users, sys-

tems/applications, and policies. Policies define how the users interact with the different systems and applications.

Identity Management is a discipline that "enables the right individuals to access the right resources at the right times and for the right reasons" (Gartner IT Glossary). Most identity and access management (IAM) products provide a variety of methods for implementing the policies to control access to organizational resources, with varying terminology being used to describe these methods. However, all forms of access control can ultimately be mapped back to one of four classic models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC), and Attribute-based Access Control (ABAC).

Users with wide ranging or extensive system privilege should not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing. Multi-factor authentication is recommended to be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi-factor authentication should also be used for access to enterprise level social media accounts. Passwords for highly privileged system accounts, social media accounts and infrastructure components should be be changed from default values and should not be easy to guess. Passwords which would on their own grant extensive system access, should have high complexity.

4.5.2 User Awareness Training

Ideally user awareness training is done in a small group size to allow people reflect on learnings and to be able to ask questions from a cyber security expert. Specific training materials need to be created reflecting on the organisation's compliance framework, processes and priorities. In a study undertaken by The CyberFish Company mapping the current cyber security training landscape, between July and August 2018 a total of 50 interviews were undertaken from various industries. Overall, a large majority, 85% of respondents agreed that mentoring frameworks are considered an effective tool for mitigating individual risk factors associated with cyber security exposure. When asked about innovative projects corporate cyber security teams work alongside the HR teams, most companies cited routine training (27%), specific cyber security training (24%), business continuity exercises (20%), specialist recruitment (12%), performance appraisals (12%) and other areas such as specific neurodiversity related projects. According to The CyberFish data, the most popular way to improve employees' cyber security awareness was computer based training. This was reported as an existing practice by 59% of organisations. 39% of organisations base their cyber security awareness updates on regular and industry specific threat intelligence updates and feeds. 16% have OSINT monitoring

techniques in place for their senior executives and the same percentage provide targeted training or coaching to senior leadership team members in the subject of cyber security best practice. 36% of companies included cyber security awareness training during new employees' on-boarding activities. 30% gave out some kind of cyber security/privacy kit to their employees including privacy filters, webcam covers and other gadgets. 23% did regular phishing tests and 14% delivered regular incident response simulation exercises. 7% of companies surveyed had clear competency based assessment techniques in place for recruitment and development purposes in the cyber security team. 5% of organisations involved their HR team members in their incident simulation exercises. 4% of organisations surveyed had a neurodiversity policy in place. 6% of the organisations surveyed did not use any of the above practices. In terms of the budget for 2019, 36% plans to invest in CBT, but a large percentage, 32% will pursue more targeted training, specifically, 1:1 coaching solutions with a cyber security expert. 35% of the organisations surveyed plans to increase the spend on industry specific threat intel feeds and updates, while 19% reported they will invest in phishing simulation exercises. 14% wants to focus on wargaming and incident simulation and a further 6% plans to involve a behavioural expert in this process. 19% will deliver a human risk audit and 11% aims to develop a neurodiversity policy. Apparently, the GDPR hype was to subside by 2019 as only 1% mentioned future investment in this area.

4.5.2.1 Leadership and C-Suite

In a survey by PWC, cyber security threats ranked as one of the highest concerns for CEO's and when surveyed, 40% prioritised cyber security as the highest threat to the company. However, CEO's are famously busy and not likely to click through computer based bleak training slides in order to learn about how to counter cyber security threats, understand how malware works and set up stellar passwords. Breaching a C-suite executive is primary target for cyber criminals, hacktivist operations but even nation state actors. Therefore, raising their awareness and instilling responsible digital behaviours are key in reducing the likelihood of successful attacks targeting these executives. By a quicker cycle of identifying breaches and taking the warning signs seriously can help containing attacks successfully. Non-technical members of the management team may struggle to understand cyber security jargon and therefore their education risks to remain superficial. Engaging them in an incident response setting is crucial in order to help them understand their own role in responding to a crisis. Without any wargaming experience they may also likely delay the process of identifying a data breach and containing the incident as it might not be straightforward to them to instantly pick up problems that could point to a cyber security incident.

The following infographics have been designed by The CyberFish for non-technical audiences to raise their cyber awareness (Figs. 4.5 and 4.6).

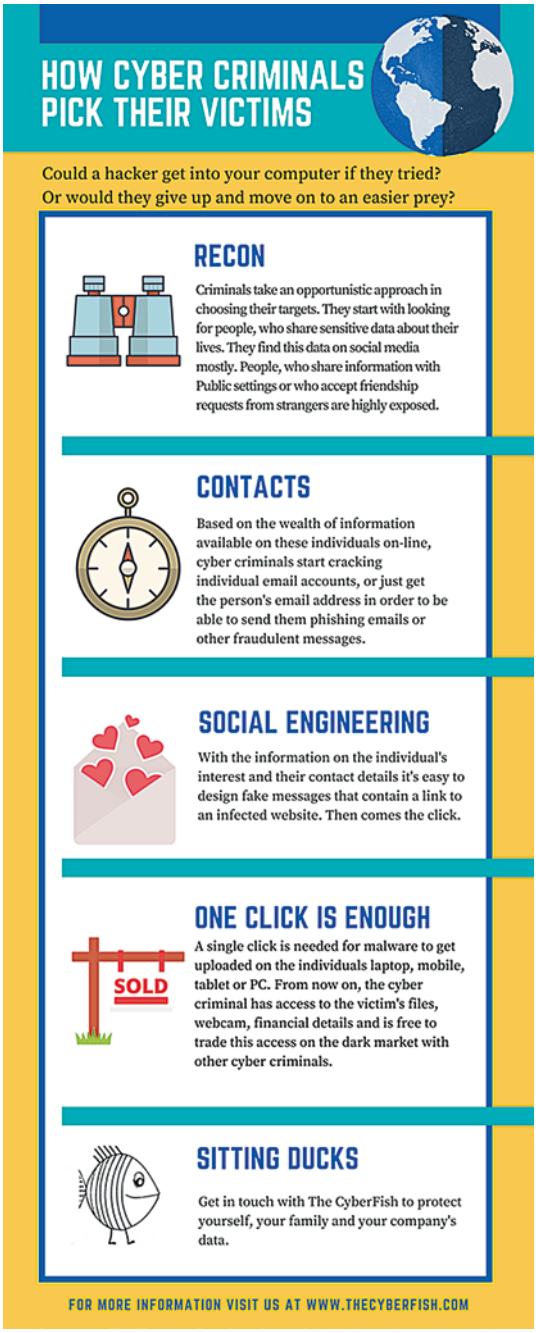

Fig. 4.5 Infographics to raise awareness of cyber threats

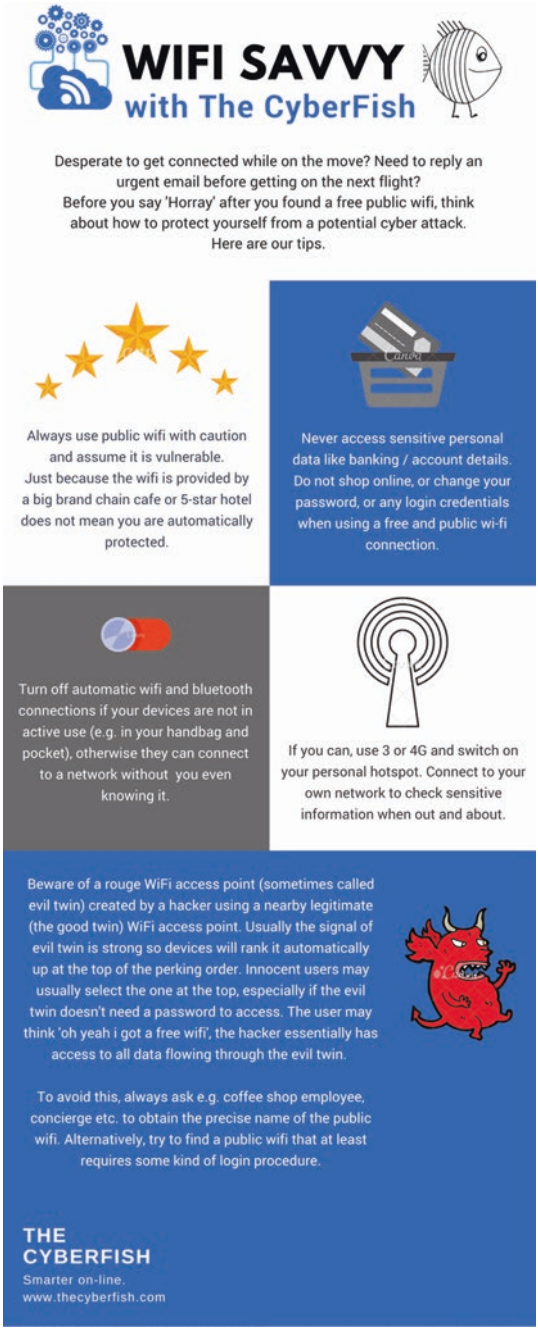

Fig. 4.6 Infographics for cyber hygiene best practices

4.6 Incident Response Team Readiness Exercises -Red Teaming. From Compliance to Readiness

The MOD defines red teaming as 'the art of applying structured critical thinking and culturally sensitised alternative thinking from a variety of perspectives, to challenge assumptions and fully explore alternative outcomes, in order to reduce risks and increase opportunities' (MOD 2010).

As the complexity and connectivity of an information system and the associated risk for this system increase, organizations must establish procedures for reacting to any incidents affecting their information systems.

A cyber range is a controlled electronic computing environment with systems, networks, services, and users generally isolated from a live network. Such a range has a defined baseline that could be physical or virtual with one or more instances configured for a specific wargame scenario. A range can provide access to participants without depending on the participants' ability to provide their own equipment. A cyber range can offer an excellent means to demonstrate desirable and undesirable features of an IT environment to a training audience.. It can allow leadership to ask difficult "what if" questions, discover where improvements might be needed, or confirm the existing architecture, procedures, or training are adequate.

However, a range may have the drawback of creating unrealistic or artificial settings to which the training audience would not normally have access. As an example, if participants who do not host their own email services are expected to run an email server during the exercise in the range, this can create additional training challenges that may hinder the exercise. This highlights the need to know the training audience (Fig. 4.7).

Apparently however, wargaming and capture the flag exercises are being delivered with an aim to achieve technical learning and address incidents on a vulnerability level rather than a decision making level.

Dedicated trainings are delivered in specific infrastructures such as cyber labs that focus on individual work especially within the right range of digital domain. Other than technical skills however, incident response requires some social skills as well. Making decisions based on sound judgment, involving team members when necessary, escalating issues following the necessary analysis and in a timely manner, communicating in a factual and clear way with both technical and non-technical stakeholders are skills that need to be practiced and honed day to day.

Frequent, non-crisis interaction simulating near real scenarios between various stakeholders involved in protecting the organisation's infrastructure will enhance real world response capabilities. Established relationships facilitate rapid information sharing among team members and must include relationships across sectors, with suppliers, with vendors and with incident response organisations.

Convincing others and managing stress, thinking outside the box and finding the right solutions to problems when the time is pressured need to be part of the development process that every member of the Cyber Incident Response Team needs to be comfortable with.

ID	Objective
01	Determine the effectiveness of the cyber education provided to the training audience prior to the start of the exercise
02	Assess effectiveness of the organization's/exercise's incident reporting and analysis guides for remedying deficiencies
03	Assess ability of the training audience to detect and properly react to hostile activity during the exercise
04	Assess the organization's capability to determine operational impacts of cyber attacks and implement proper recovery procedures for the exercise
05	Determine the success of scenario planning and execution between the ECG, RT, and training audience
06	Understand the implications of losing trust in IT systems and capture the work-arounds for such losses
07	Expose and correct weaknesses in cyber security systems
08	Expose and correct weaknesses in cyber operations policies and procedures
09	Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment
10	Determine if the injects meet the objectives of the training
11	Enhance cyber awareness, readiness, and coordination
12	Develop contingency plans for surviving the loss of some or all IT systems

Fig. 4.7 Objectives for wargaming, MITRE, Cyber Exercise Playbook 2014

Organisations increasingly report delivering incident response maturity assessment exercises based within the client's bespoke threat environment using their threat intelligence information not only to strengthen business continuity planning and incident response capabilities, but also to develop the critical skills and competencies needed across the cyber security team.

These simulations contribute to the soft skills development of individuals within technical teams as individuals are given opportunities to test their reactions and team dynamics in a safe environment and experiment with different approaches working together.

In a recent voluntary wargame exercise hosted by Bank of England (BoE), up to 40 firms were invited to take part in a day-long exercise with the Treasury, FCA and UK Finance. The aim to identify any weaknesses in the responses of financial institutions to major cyber-attacks, as well as helping authorities and firms identify improvements to their collective response arrangements and incidence response strategy at corporate level.

BoE states that it's "important to test the ability of firms and organisations to communicate with each other during such an attack" (The Guardian, 9 Nov 2018).

As such, wargaming with a focus on team dynamics and individual behaviours ultimately leads individuals in teams through a transformation from an individual 'make or break' penetration tester mindset to a well-functioning response team culture that can successfully function in high stress environments.

Challenge	Impact	Resolution
Participants have varying levels of training and education about cyber security.	This will create confusion about the goals and activities associated with the cyber scenario.	Ensure that cyber injects match the skills and capacity of the training audience while adequately demonstrating cyberspace threats.
Participants have only a minimal understanding of the concepts of defense in depth, internal security, spearphishing, and other malicious activities.	The exercise participants will not have a common baseline of terminology and experience to on which to base reactions to exercise injects.	Provide a threat briefing to the PNs to increase understanding of spearphishing, malicious logic, attack Tactics, Techniques, and Procedures (TTPs) and defense TTPs.
Participants rely too heavily on what a tool "tells" them versus what the data actually means because they lack an understanding of what is taking place on the network.	The training audience may not respond appropriately to the injects due to a lack of awareness and ability to correlate events occurring on a network or system.	Mentor the training audience on understanding how their enterprise works, what alerts mean, and what tools/data are available to determine actuality of reported events (commercial, military, or other courses already exist).

Fig. 4.8 Cyber Exercise maturity level considerations, MITRE (ibid)

Organisations increasingly report delivering incident response maturity assessment exercises based within the client's bespoke threat environment using their threat intelligence information not only to strengthen business continuity planning and incident response capabilities, but also to develop the critical skills and competencies needed across the cyber security team (Fig. 4.8).

These simulations contribute to the soft skills development of individuals within technical teams as individuals are given opportunities to test their reactions and team dynamics in a safe environment and experiment with different approaches working together. As such, wargaming with a focus on team dynamics and individual behaviours ultimately leads individuals in teams through a transformation from an individual 'make or break' penetration tester mindset to a well-functioning response team culture that can successfully function in high stress environments (Fig. 4.9).

Observation during the exercise is key to a successful training experience. Observers with various focus areas (such as technical, leadership, content, communication) can identify difficulties in how the participants respond to the exercise scenarios. By doing so they offer suggestions for adjustments afterwards the exercise execution, and support deconfliction between real world and exercise injects.

Observation forms completed throughout the course of the exercise help retell the story of what actually took place. These observations not only capture the detailed responses to injects during execution and allow modification of the exercise direction during execution, but also provide lessons learned after the exercise.

The hotwash should occur on site while events remain fresh in the participants' memories, and should involve all who participated in the exercise. This provides immediate feedback and serves as a good forum for senior leaders to discover the key successes or focus areas for future exercises. The hotwash session should be led

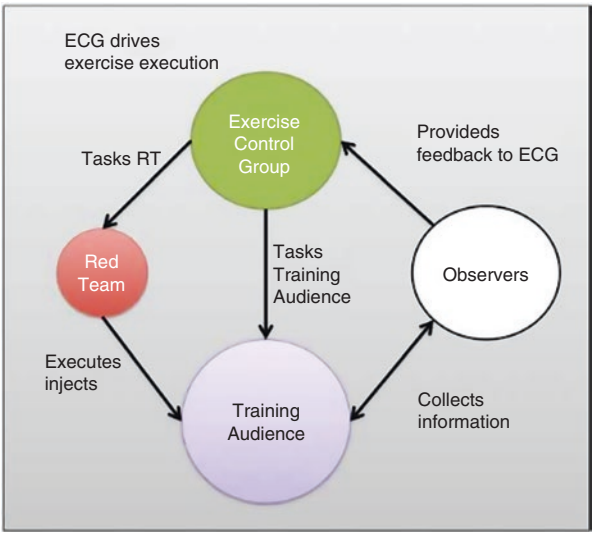

Fig. 4.9 Exercise information flow (MITRE) ibid

by a moderator and consist of a focused discussion on what worked well, what must improve, and what the organization should consider for the next exercise. Additionally, the moderator should distribute a survey consisting of a series of yes/no questions about aspects of the exercise and free-form fields to capture feedback.

Wargaming different scenarios provide the opportunity to discover an organization's deficiencies within a controlled environment. Organization leadership must then create remediation plans and follow up on deficiencies identified during the exercise. Conversely, exercises can also emphasise teamwork elements that proved effective (Cyber Storm Final Report 2016).

4.7 How Our Private Digital Exposure Can Permeate Corporate Systems

Despite that the younger generations have grown up with the internet, touch-screens and hyper-connectivity, awareness on data-protection and protecting our personal information have not become even a rudimentary part of general education or conversations in our private homes. This is a good example of how little an integral part of our daily lives the matter of protecting data still is and how human behaviour is a relevant risk with regard to protecting crucial infrastructure and protecting the human right to privacy. Information security awareness can be a crucial tool in overcoming weaknesses of human behaviour and unintentional harm to institutions, businesses and individuals. Our hypothesis is that an element that must be integrated into this awareness training, is the learnings of Daniel Kahneman's

behavioural economics, including the well-known and recognised difference in system 1 and system 2 thinking. In "Thinking Fast and Slow" from 2013 Daniel Kahneman describes in depth how our brains deal with decision making, and why we often cannot trust our first impulses.

System 1 thinking is the one we use when solving tasks, we are familiar with, in a familiar setting. In this system, our decision-making is on 'autopilot'. The pathways in the brain are shorter when applying this system, so by utilizing system 1 thinking our brain consume less energy – which from a psychological evolutionary perspective is desirable. Further, in this system of thinking, our assumptions and biases are not challenged, as this would take the analytical aspect of system 2 thinking. System 1 thinking is extremely valuable to us, as it allows us to navigate in our daily lives, without having to question everything we meet on our way.

Have you ever experienced going to work, and when you arrive, you barely remember the trip you just had, either on your bike or in your car? When you tie your shoes in the morning, sit behind the wheel in your car and walk into the elevator at your office, turn on your computer and type in your password you are relying on your system 1. It is behaviours you have done so many times, that these actions have become an integral part of your daily whereabouts. Have you then tried to explain to someone how you tie your shoes in the morning? It will not be as simple as just doing it. When a skill or knowledge becomes integrated into the deeper layers of your brain, it can become a challenge to approach these in a critical way. The brain prefers to save the energy, and not rebuild the structure of information and knowledge of the world that it has acquired.

System 2 takes more effort. It is a system that activates more areas of the brain and takes for you to focus your attention on a specific matter or task. It is active if you are writing a paper, learning a new language and when you are solving a complex challenge or identifying sophisticated phishing emails. System 2 is both required when learning a new skill and attaining new knowledge, but is also crucial when we are having a lookout for information security risks.

If you wish to solve a problem, you first need to acknowledge the existence of that problem. Being aware of and understanding the nature of system 1 and system 2 thinking, will make us more capable of realising when system 1 thinking makes up a risk rather than being an efficient decision-making process.

4.7.1 Why System 1 and 2 Thinking Are Fundamental When Increasing Security Awareness

Your behaviour in a well-known environment and situation is more likely to be rational, than when you are under pressure – be it a deadline coming up, a massive pile of emails you have to respond to, you are having challenging times in your private life or being victim of a spear phishing attack.

If a challenge you are facing is of interest to you and is within the realm of a topic you already have a basic understanding of, the stress hormones released by your brain over shorter periods of time, can sharpen our focus and make you highly capable of problem solving. If the challenge is of too great a magnitude, if the pressure is too intense and if you have been working in a stressful environment for a longer period of time, we are more likely to resolve to decision 1 thinking and the our behaviour will be more driven by the structures in our brains that we have in common with other animals – the so-called reptile brain. This is the part of the brain that has a less refined set of opportunities but can take actions either towards fight, flight or freeze.

This means that you could be capable of solving a complex issue, when you are well-rested, have had enough to eat and are being challenged in a way that is meaningful to you. But what happens when you have been working to solve a problem relentlessly over the past 5 h, did not have time for a break or to eat and the problem keeps spinning out of control. This is the moment where your best intentions and strong capabilities can be jeopardized by 'freezing' and not being able to move forward or 'fighting' where you could consider anyone around you as a potential enemy.

4.7.2 Team Dynamics in Cybersecurity

This brings us to the crucial role of looking at the team dynamics when we wish to increase cybersecurity capabilities in the organisation. In a simplistic scenario, imagine that the 7 members of an IT-department are extremely knowledgeable in their respective fields – but one of the people in the team is showing behaviour of bullying and is creating an atmosphere of nervousness and poor communication. The team members no longer ask each other for support when there is a task they cannot finish on their own, and openly sharing doubt about tasks has become an opening for the bully to display the person as incompetent. In one scenario, management can see that the quality of the results on the team is decreasing and after having involved HR, ends up letting go of the person responsible for the toxic behaviour. The atmosphere changes dramatically and the psychological safety make it much more likely that the team members ask for help and learn from each other. In another scenario, the management team finds that the knowledge of the "bully" is too valuable to let the person go, and no more is being done about it. The atmosphere on the team stays saturated with nervousness and each person sealing of their challenges to minimise the risk of being put on display.

In both of these scenarios the responsibility for the toxic atmosphere is ascribed to the person who is showing destructive behaviour. But what if this person is really being uncomfortable because he feels he left out because of being the latest arrival on an already consolidated team, and it is the communication style of two of the colleagues that remind him of being undermined for his smarts in high school. This triggers a fight-response in him, which then impacts the team.

Imagine the impact of these dynamics when they get information that an insider in the business has been sharing sensitive personal information of senior managers with a third party, and the team has to quickly identify which data has been shared, how and which immediate precautions should be taken.

To be able to positively identify the issues of the group, it is not sufficient to look at the skills and behaviour of each person. We must assess the group dynamic to get a full grasp of existing blind-spots and risk-behaviour. By doing so, it will be possible to work in a targeted manner.

4.7.3 Human Vulnerabilities

957 data security incidents were reported to the Information Commissioner's Officer (ICO) in Q4 2017/18. Causes are categorised as acts of negligence, such as data sent to the wrong recipient, loss of paperwork, failure to use bcc when sending e-mail. Individuals cope with stressful situations in a different way then they function in their everyday environment. We have seen countless examples of incidents reported by media where corporate teams cracked under pressure to realize: an adequate technical response alone is not enough to manage a crisis.

Cyberpsychology is an emergent new field that is continually amassing research in the field of how human behaviour changes in a digital environment. Application of cyberpsychology and organisational psychology principles are required by every organisation to be able to successfully mitigate human risk in their cyber security defences. Nevertheless, corporate cyber security awareness training solutions are only beginning to map and mitigate the what the human component of cyber security risk constitutes at an organisations. Incident response simulations focus exclusively on technical learnings.

Can we trace the incidence of making a specific error: such as clicking on the wrong link, sending the e-mail to the wrong people, or using the same password on every platform back to personality traits? Can an organisation's digital risk can be increased because of certain behaviours people in mission critical roles may have? And if so, what can we do to prompt the right responses to strengthen the organisation's cyber defences?

The cyber security industry needs to apply principles from this emerging new science of understanding how behaviour changes on-line (Aiken 2016). If we aim to understand the effects of the ever increasing digital exposure on human behaviour we have to look at these behavioural changes from a cyber security perspective. How can an organisation improve its defences by fortifying their human firewall in a targeted way? Can incident response teams improve their performance by understanding how members react in stressful environments and cope with complex challenges?

Within incident response specifically, one way to uncover behavioural blind-spots and behaviour that increase vulnerability to cyber-attacks, is by putting people in a scenario that will resemble the challenges of an actual attack or breach. If you

ask a person how they react under pressure, it is highly unlikely that they will give you a correct answer.

There is of course the influence of social desirability when answering a question about your own behaviour, but we also need to consider the impact of internalised biases. It is very common that we overestimate our own capabilities compared to others, and expect that we would behave in a rational, morally and ethically desirable way.

Our behavioural reactions to stress – or "derailers" as they are also called – are as individual as we are. But certainly, there are also patterns related to our personality. These personality-related behaviours are most certainly overlooked in current offerings in digital hygiene. Or at least it is still a niche. Wargaming sessions that look into the individual risk exposure and also team dynamics are a starting point in the analysis of which behaviours are more common with respective types of personality. This is an effective tool for mitigating risk-behaviour and targeting the relevant areas of development.

Instead we can place ourselves into simulation reflecting the real experience of pressure, risk and complexity. We might be consciously aware that it is an exercise, but just like your brain will accustom to you wearing virtual reality glasses within 120 milliseconds, your unconscious brain will react to a simulation rather alike to a real emergency-situation.

Capturing, analysing and assessing the behaviour shown in a wargaming simulation exercise gives organisations valuable insights that methods like interviews or anonymous questionnaires will not be able to match in validity.

One example of a situation that was unexpected by the individual himself, played out in a recent wargaming simulation exercise with 10 participants. The task was clearly defined by the beginning of the exercise and the rules for solving the tasks were also both described on paper and read out to the participants. One of the rules was that each participant would be responsible for capturing the agreed plan on paper, as each individual could be picked out and have their paper utilised for assessing the technical and strategic capabilities of the team.

One team member did not capture the agreed plan on paper. We do not know the reason why – It could be that he thought that the rest of the team members capturing the plan would suffice, despite having been informed otherwise. Maybe he felt the rules did not apply to him. Maybe he was not paying attention when the text was being read out. The next question would be, why none of his team members made him aware of the potential consequences of not writing the plan in his notes. When the exercise was finished, each team member would roll a dice. The participant who did not write down the agreed upon plan, rolled a six, which decided on him being chosen to submit the official response of his team. His not having written down the plan resulted in his team losing that part of the simulation.

What unfolded afterwards was rather significant. From being one of the most verbal participants on the team, the participant who was directly or indirectly responsible for the team not getting a crucial point, became silent during the next exercise. He would take notes notoriously, mostly look down. As he started engaging with the group again, the first five times he did so, was with a joke. It took

another 15–20 min until the participant was fully engaged with the team. It is of course relevant to look into the learnings for this individual. What were the reasons for his lack of compliance with the given rules? Was he distracted, or did he feel that he did not have to comply? Was it his way of stepping into a role as an informal leader and delegating the responsibility? What would this type of setback have meant if it was not a simulation exercise? Then we have the influence from the team. Why did no one ask him to follow the rules? Could they have him less stressed by more actively inviting him back into the conversation after the mistake? Were they even interested in doing so?

Our hypothesis is that the elements described above, that represent behavioural risk in an incident response, could not be captured in an interview or questionnaire, and could not be anticipated in a formal incident response plan or in a cyber security framework paperwork. Assessing behaviour in a simulation that enfolds under pressure and with the presence of others offers a unique insight and a valid understanding of blind-spots and high-risk behaviour of individuals and teams.

When these blind spots and behaviours have been identified and addressed, organisations will be able to target these directly, just as organisations would patch their systems or scan their exposure. At the end of the day, these individual blind spots are glaring system vulnerabilities. They can expose the organisation to a threat just as any unpatched system would. Organisations need to recognise that the transition to cyber psychology-driven human risk assessment represents a cultural shift for organisations and will bring along new challenges for implementation.

References

Aiken M (2016) The cyber effect. Spiegel & Grau, New York

Bank of England stages day of war games to combat cyber-attacks (2018) The Guardian. (Online). Available at https://www.theguardian.com/business/2018/nov/09/bank-of-england-stages-war-games-combat-cyber-attacks-data-breaches. Accessed 11 Nov 2018

Cyber Exercise Playbook (2014) The Mitre Corporation. (Online). Available at: https://www.pdffiller.com/211594986-pr_14-3929-cyber-exercise-playbookpdf-Cyber-Exercise-Playbook-Mitre-Corporation-mitre-Various-Fillable-Forms. Accessed 31 Oct 2018

Cyber Storm Final Report (2016) US Homeland Security. (Online). Available at https://www.dhs.gov/publication/cyber-storm-final-reports. Accessed 06 Nov 2018

Deloitte's GDPR Benchmarking Survey (2018) Deloitte. [Online]. Available at https://www2.deloitte.com/global/en/pages/risk/articles/deloitte-gdpr-benchmarking-survey-the-time-is-now.html. Accessed 07 Nov 2018

IT Glossary. Gartner. (Online). Available at https://blogs.gartner.com/it-glossary/identity-and-access-management-iam/. Accessed 07 Nov 2018

Minimum Cyber Security Standard (2018) UK Government. [Online]. Available at https://www.gov.uk/government/publications/the-minimum-cyber-security-standard. Accessed 07 Nov 2018

MOD (2010) The development, concepts and doctrine centre (DCDC), Red teaming guide, 2010 Accessed https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf

NIST 800-53 vs ISO 27002 vs NIST Cybersecurity Framework? (2018) Complianceforge. [Online]. Available at https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002.html. Accessed 07 Nov 2018

The Global State of Information Security® Survey (2018). PWC (Online). Available at https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html. Accessed 31 Oct 2018

Chapter 5
Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime

Jaime Ibarra, Hamid Jahankhani, and Stefan Kendzierskyj

Abstract Cybercrime has reached to a level that any cyber-attack can cause great levels of extortion. With the support of technology, healthcare organisations have been able to enhance medical treatment assuring better solutions to improve life-style of people. Likewise, criminals are attracted to the information allocated within hospital and clinics regardless of physical or digital storage. Electronic Health Records (EHR) are the most important asset in healthcare and criminals are aware of their value in the black market, including the dark web. This paper analyses the impact of cyber-attacks to healthcare organisations including methods used by criminals to enhance their anonymity, and the value of healthcare data nowadays. It studies blockchain, The Onion Router (TOR) and other common tools to ensure security and privacy while navigating through the internet and the reason why cybercriminals take advantage of the dark web to sell stolen information from hospitals in order to get higher financial gain. It also looks at the levels of extortion that is caused to organisations and how people are compromised.

Keywords Cybercrime · Cyber attack · Electronic health records · EHR · TOR · Blockchain · Virtual private network · Proxy · Anonymity · Extortion · Dark net · Black market · Personal identifiable information · PII · Internet of things · Cloud computing · Deep web · Dark web · Attacker · Clinical trial · Medical treatment · Endpoint security · Network security · Ransomware · Information theft · Denial-of-service · Cryptomalware · Cryptocurrency · Cryptomining · Track covering · Encryption

J. Ibarra · H. Jahankhani (✉) · S. Kendzierskyj
London Campus, Northumbria University, London, UK
e-mail: jaime.jimenez@northumbria.ac.uk; hamid.jahankhani@northumbria.ac.uk; Stefan.Kendzierskyj@northumbria.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_5

5.1 Introduction

A cyber-attack is a daily risk that organisations must deal with, which involves financial, organisational, technological and reputational threats causing damage and/or disrupting services. The world is facing an era where most of criminal performance and activities are being executed through the internet and organisations are struggling to find out the most optimal solution to protect the cyber security of their infrastructure along with their most critical assets. Technology is located everywhere and it provides a great support in businesses where data has become the most important asset due to the sensitivity of the information trusted by customers, partners and regulatory officers. On the other hand, implementation of Information and Communication Technology (ICT) infrastructures has allowed cyber criminals to perform malicious actions, where the scope is currently speculated as limitless along with all the infinite opportunities to break into computer systems and machines without authorisation.

The healthcare sector has adopted sophisticated network infrastructures and allowed to integrate machines into their systems. This term is known as Cyber-Physical Systems (CPS) and enhances the performance of medical treatments offering better lifestyle options to patients. Thanks to the Internet of Things (IoT), cloud computing, along with other cutting-edge technologies such as Artificial Intelligence (AI), Machine Learning (ML), Data Science, Bio-telemetry, Virtual Reality (VR), the medical sector has shown a noticeable evolution reaching to the point of using nanotechnology to perform highly complex and dedicated surgeries. In addition of these advancements, the implementation of Electronic Health Records (EHR) systems has contributed to hospitals, clinics including trials and research to have immediate access to information regarding patients. This includes people that can reach to this information from any device that has access to a network with internet connectivity, thanks to the deployment of wireless networks such as Wi-Fi. Nowadays, it is possible to monitor in real-time health, the conditions of patients without having a doctor or nurse watching over the person 24/7 thanks to the deployment of portable and wearable devices giving the nomination of Wearable Body Area Networks (WBAN). These networks transmit information regarding the condition of a patient to cloud environments, processing tons of data every second and where possible, sending notifications to general practitioners or specialists in case of any abnormal behaviour. The design, configuration and deployment of electronic devices has changed the landscape of healthcare compared to traditional paperwork, which involved lots of time spent at the hospital taking basic tests such as blood tests, heartbeat, blood pressure, etc. Likewise, it has attracted organised cybercrime to perform cyber-attacks directed to healthcare organisations causing great chaos and compromising the lives of people, reaching to a point when a doctor is submitted to superlative amounts of stress because it is their responsibility to make life-or-death decisions when systems are disrupted during a delicate process such as a surgery. This can compromise forever the condition of a patient. Cyber criminals are keen to obtain greater and ambitious financial gain regardless of the organisation,

prestige and security posture they are likely adopting or have in place. Criminals understand that money nowadays is in healthcare and they would do whatever it takes to obtain the desired money, even if that implies to extort people. Attacks suffered such as WannaCry ransomware to England NHS in 2017, or the hacktivist group Orangeworm performing cyber espionage through healthcare systems (i.e., x-ray machines) demonstrate that healthcare organisations must address their budgets to cyber security solutions including awareness training in order to protect information trusted by patients and their partners. EHRs possess basically all the life history from a person and if this ends up in the hands of criminals it may possibly imply blackmailing for a lifetime, destroying the reputation of a compromised person or in worst scenarios, planned terrorist attacks attempted against the life of the victim. Cyber-attacks to healthcare are increasing and the level of extortion caused to people is growing as well, therefore the high demand of security professionals and preparation of future generations to protect data in this interconnected world needs to keep up with this growth. Organised crime is taking advantage of selling health records in the dark web considering the wealth of information available, including the history of the person, leading to social engineering attacks without scope (Illmer 2018). The dark web is known for not presenting boundaries or controls but for making the best place for organised crime to work at free will. Even though it is possible to access it through The Onion Router (TOR), attackers are using this network to remain anonymous when attacking the organisation due to its strong mechanisms to remain hidden throughout the internet, making it difficult to investigators to trace them back. However, TOR presents vulnerabilities and attackers are looking at other ways to assure anonymity, considering other options such as blockchain technologies along with other tools such as Virtual Private Networks (VPN) and Proxy routing. In addition, blockchain is currently very popular and attackers are inserting malware into highly sophisticated computers to perform cryptomining due to the benefits of solving as many math puzzles as possible to be considered as the main node between peers.

This chapter analyses the value of healthcare records in the black market, detailing the parameters it presents and why it attracts so much to cyber criminals to steal it along with the future extortion that can cause issues for either organisations and people in general. Moreover, it explains how cyber criminals are taking advantage of the dark net in order to get higher financial gain. This is because the dark web is used not just to sell stolen information, it allows to connect between malicious hackers, trade information about potential targets and limitless applications beyond our imagination. The rest is divided as it follows: Sect. 5.2 explains the value of EHRs for the black market, Sect. 5.3 explains the usage of EHRs for clinical trials and research, Sect. 5.4 details the most common cyber extortion attacks and its impact to the healthcare. Sect. 5.5 analyses blockchain, along with TOR and other common tools used to accomplish anonymity. Finally, Sect. 5.6 concludes this chapter with some further research suggestions.

5.2 Electronic Health Records and Their Value to the Black Market: A Rare Commodity to the Organised Cyber Crime

Healthcare organisations are facing a digitalisation era where their main assets such as health records from patients, machines used for medical purposes are being connected to the internet. The deployment of electronic personal health record (ePHR) systems is providing health consumers greater accessibility and a better control over their information. It consists on the migration from medical provider-centred to patient-centred, which if this system is associated with the recently implemented European GDPR (Ducato 2016), provides users a better control of their personal identifiable information (PII). Unfortunately, current healthcare providers are struggling to implement appropriate security solutions to protect their assets due to business digitalisation, and often rely on hardcopy medical records. Therefore, these organisations must identify as soon as possible and determine suitable security controls to reduce impact given by security breaches compromising the information from patients.

Electronic health records (EHR) are offering greater benefits and a significant productivity increase, compared to traditional paper-based systems, and which 83% of regular hospitals are adopting these solutions. Likewise, 96% of hospitals providing critical and customised services are acquiring these systems focusing on the benefit of their patients. However, the digitalisation of these organisations is one of the inefficiencies according to Forbes (Yao 2018) and therefore, EHRs are more susceptible to hacking and theft. Likewise, that other information such as credit cards, bank details, etc., have attracted attackers for its theft, the question now is how much are patient lives worth to hackers?

Hackers are using more sophisticated methodologies in order to insert malicious software into machines for information theft, unauthorized disclosure and extort their victims to acquire financial incomings (Casteel 2018). For instance, the ransomware attack that caused damage to England NHS produced costs of almost £92 million. As shown in the research from Catarinucci et al. (2015) and Rushanan et al. (2014), the processing of Personal Health Information (PHI) tends to be collected in real-time with telemedicine devices connected to IoT networks (i.e. Wearable Body Area Networks WBAN, wireless sensor networks WSN, biotelemetry systems), easing the procedures from General Practitioners (GPs), making fast decisions, and avoiding unnecessary appointments with patients.

In 2017 Deloitte, one of the nominated "big four" organisations, has claimed four large technological innovations that could lead to the speculated hospital of the future. The mentioned technologies are the following (also see Fig. 5.1):

- Usage of blockchain networks to accomplish data privacy and anonymity. It is supposed to offer information only for patients and the capable personnel involved in a certain medical procedure.
- Virtual reality technologies, especially aimed to orthopaedic rehab procedures, making it easier and friendly to patients who are getting recovered from complex and sensitive surgeries that compromised the mobility and motor of his/her body

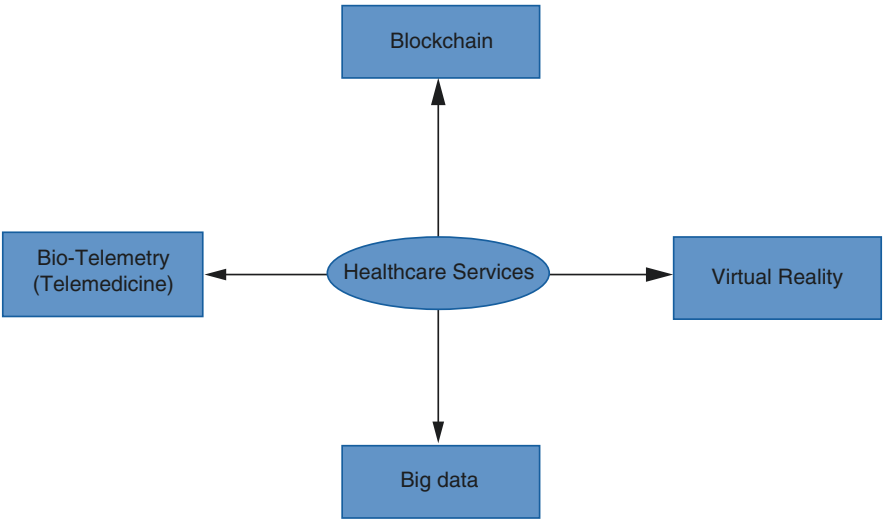

Fig. 5.1 Four innovative technologies for the hospital of the future

(e.g., microdiscectomy performed on the spine given by a herniated disc), experiencing memorable situations and motivating the patient.
- Usage of data science for higher data processing, aimed to medicine and treatment prescriptions at faster responses.
- Bio-telemetry systems, used for patients who require to be monitored in real-time, even when the doctor is not present.

The increased demand on the Internet of Things (IoT), along with cloud computing systems allowed organisations to offer services to users to monitor in real time their health in order to make faster decisions and improve their lifestyle (Islam et al. 2015). The more information users are storing on customised services, the more exposure they are providing to their PII, attracting hackers to exploit other footprinting sources to achieve the data thefts they are looking for (Mendelson 2017). In addition, IoT-based devices and applications are being criticised for not showing the process of data collection and processing. Furthermore, in most of the cases, it does not contain the correspondent consent from its users. Moreover, it is predicted to grow to an estimated amount of 163.2 billion IoT devices within health purposes, highlighting the challenge of data collection through IoT devices without the user being aware of potential issues or threats, (Whitmore et al. 2015), leading to questions such as: Is the data collected disclosed to authorized users as the provider claims? Is the data being used for the only intended purposes? (O'Connor et al. 2017)

In addition to IoT, cloud services are providing a significant support to healthcare organisations (Shu and Jahankhani 2017) as per Fig. 5.2 and it provides structure in the following:

- Higher savings on data storage because of the availability of hiring Software as a Service (SaaS) cloud systems.

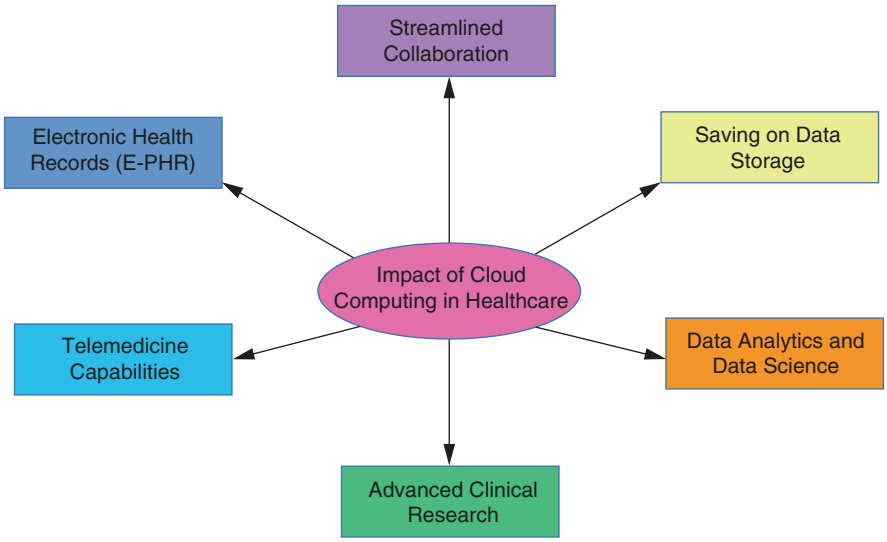

Fig. 5.2 Impact of cloud computing on healthcare

- Data science used to process and analyse millions of data processed throughout the network.
- Advanced clinical research, used for clinical trials, where results are stored from tests, behaviour of new medicines tested on patients including secondary effects of medicines and measures suggested to enhance capabilities of new medicines and treatments.
- Telemedicine capabilities, thanks to the usage of wearable devices, Wearable Body Area Networks (WBAN) and Machine to Machine (M2M) communications for complex procedures applied in modern medicine.
- Streamlined collaboration
- Electronic Health Records in order to manage them, along with the healthcare systems being used.

EHRs offer a significant wealth of information, attracting hackers to exploit and steal. It contains information such as:

- Demographic information.
- Full names, which are the same as encountered on personal IDs, driver licenses, passports.
- Address history, including places where the patient lived before.
- Work history, including former work places where the patient provided services to previous organisations.
- Names, ages, contact details from relatives, which can belong to parents, siblings, life partners or any representative the patient trusts. The health provider contacts this person in case the patient faces an emergency.
- Financial information, including bank details, credit/debit cards.

- Social Security Number (National Insurance Number in the UK)
- Medical history, which contains sensitive information. It includes details of previous medical appointments along with details from doctors and nurses. Moreover, it has critical information such as allergy details, surgeries the patient was submitted, results from medical diagnosis such as x-rays, electromagnetic resonance, etc. The appointments listed include diagnosis, prescriptions, treatments and dates for the next medical control organised in a chronological manner.

As shown beyond just data, EHRs contains precise details of the victim's life. Once a health provider is subjected to a security breach compromising patient records, customers who suffered from the breach can likely get exposed to extortion by way of blackmail that can continue for a considerable time or even a lifetime. Furthermore, if EHRs contain additional information such as cancer diagnoses, sexually transmitted diseases, psychological conditions established (i.e., asperger syndrome, autism, depression, alcoholic), the victim can be exposed to public embarrassment or political assassination depending on the goals of hackers.

One of the greatest challenges that has overshadowed the web's benefit is the risk associated to our data privacy, security and rights. This is now becoming such an issue that the founder of the web Sir Berners-Lee (Sky News 2018) through the world wide web foundation and the recent web summit in Lisbon has launched the charter for the web: a Magna Carta of digital rights. Speaking from the Web Summit, Berners-Lee said: *"The web is at a crucial point. More than half the world's population remains offline, and the rate of new people getting connected is slowing. Those of us who are online are seeing our rights and freedoms threatened. We need a new Contract for the Web, with clear and tough responsibilities for those who have the power to make it better. I hope more people will join us to build the web we want."*

The report, "The Case for the Web", as part of web foundation campaign, has outlined the key action needed to confront risks on data privacy and more importantly the centralisation of power online among a small group of companies. The report highlights that living in the connected world with billions of people in countries where there is no comprehensive law on personal data protection, would particularly leave societies vulnerable to increasingly common incidents involving breaches of personal data. This is ever more important when dealing with Health.

The ordeal for a patient in discovering that their identity is available for criminals to gain benefit from, because of the healthcare institution having been breached by a malicious attacker, is extremely concerning. The large scale WannaCry ransomware attack of 2017 highlights the dangers of large scale data breach which no one really knows how far and wide the identity theft will appear or manifest itself. On the deep web, the value of the medical data is said to be ten times that of stolen credit card numbers, (Francis 2018) and if big data sets are available they can go for large sums of money. So, the attraction to attack the healthcare industry is clearly one motivated by its value on the deep web. There likely is a much larger adverse effect from those that suffered from identity theft and the criminal victimisation because of the data breach and a deep violation of the patient's privacy (Stofko 2018). The loss of data surrounding identity is of course a problem but so too can be sensitive medical history and therefore the impact is far deeper and greater than losing credit card

details. Well, at least with GDPR in place data breach notification must be announced within 72 h or penalty consequences will be delivered. Consequences are worse, as unlike a stolen credit card which can be cancelled and therefore if discovered in time by the victim they can at least deploy damage limitation strategies (Shu and Jahankhani 2017). But medical records hold valuable data points that map a person's identity and can't be changed and give the attacker time to work out how to plan the best outcome from stolen data.

Various quantitative and qualitative analysis research demonstrate a few reasons for healthcare to consider alternative mechanisms such as blockchain (Paterson 2018). Whilst blockchain is a technical tool to aid and support a better method than currently deployed, the driving forces are enhancing privacy of data and securing a better transparency of data that ultimately should help achieve towards the goal of protecting the patient. One can argue in favour of blockchain if just a single aspect can show the benefits such as interoperability.

After some research done on the dark web site WallStreet Market (see Fig. 5.3), at the left of the picture, cards are worth between $15 and $22, while at the right side it is seen that social security numbers are worth $3. However, considering the details that EHRs have, it could be worth hundreds, or thousands of dollars given by all the details they present and the unlimited scope of malicious actions that attackers can perform, derived by accessing this information.

Looking back in 2015 (Seleman 2018), past security breaches to health providers compromised the information of 100 million personal health records (PHRs), and it involved the investment of millions of dollars to remediate their systems. In addition, healthcare organisations heavily regulated themselves had to afford the payment of penalties of $380 per PHR stolen. In 2016, it was reported 450 security breaches from health providers compromising 27 million of PHRs, which over 65% of the notified incidents were given by insider threats. In 2017, Marsh-Microsoft Cyber Perception elaborated a survey between July and August and from their results, 27% belonged to healthcare organisations who were victims of cyber-attacks in the past 12 months, which was more than financial institutions (20%), and almost twice compared to Information and Communication Technology industries (14%).

Over the last years, the impact from cyberattacks has overcome boundaries and no region in the world is completely immune to incidents in the cyber space. As seen in the information above, human lives are critical as well as its sensitive information it holds, making the healthcare market the perfect target for organised cybercrime. Ransomware attacks such as WannaCry and NotPetya had an extended scope affecting the health and insurance service. Another aspect of great concern are places which have poor security maturity and may take from five to ten times longer to detect an intrusion compared to global counterparts. Cybercrime organisations should be viewed in many ways as other kinds of organised crime or businesses, and there they run the operational structure in a similar way; where there are those in charge giving orders, but instead of traditional personnel, they utilise knowledge from their geeks they employed and highly specialised experts who look for and exploit vulnerabilities in the code of commonly used programs (Yip et al. 2017). Therefore, cybercrime is a global industry and is becoming a big business in the dark web. Figure 5.4 shows a snapshot of recent attacks in the healthcare industry,

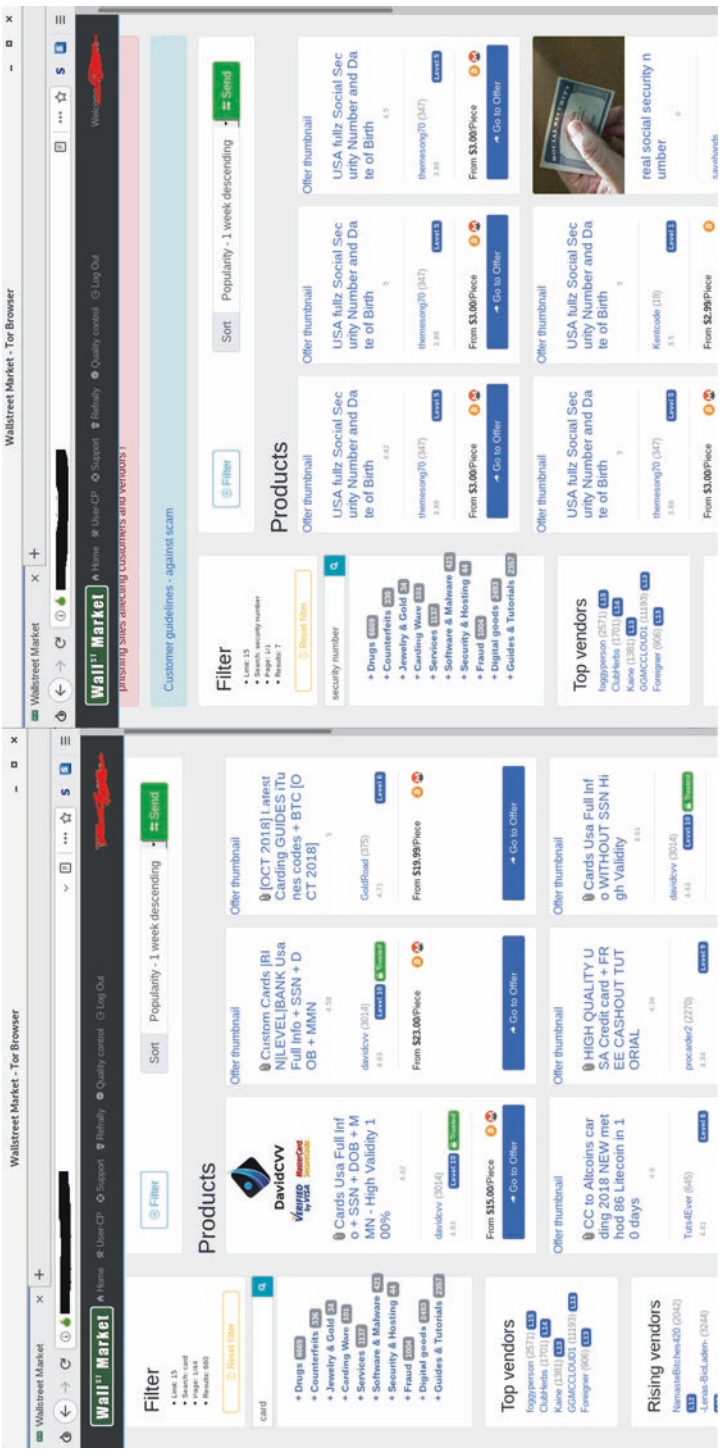

Fig. 5.3 Prices of credit cards (left) and social security numbers (right) at Wall Street Market Darknet Site

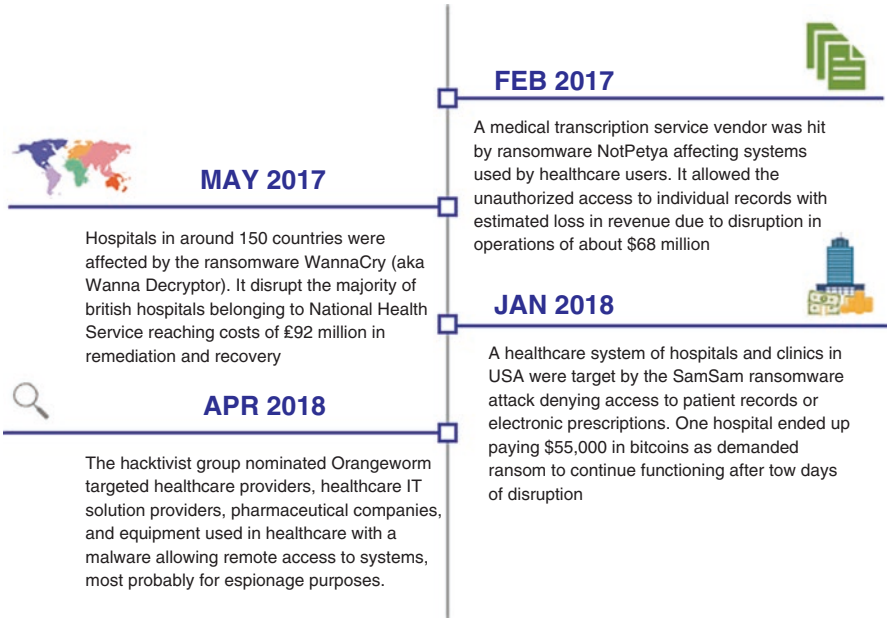

Fig. 5.4 Time line of latest extortion-based cyber attacks to healthcare sector

such as in January of 2018 with the injection of the SamSam ransomware, or in April a hacktivist group named Orangeworm remotely accessed equipment and systems for possible espionage purposes (Wyman 2018).

Criminals use cryptocurrency for various reasons. The main ones are because of the anonymity it offers and also for the purpose of avoiding the payment of taxes at their respective countries requirements and rates, especially within the EMEA region. In addition, along with cryptocurrency incoming, cyber criminals are developing malware to execute cryptomining on the background of infected hosts. Considering that next the generation of healthcare providers will use technologies such as blockchain for data privacy, virtual reality, internet of things connecting dedicated machinery to private networks increasing productivity and supporting on delicate procedures such as surgeries, and data science for the processing of higher amounts of traffic, then it demands the purchasing of sophisticated computers. Assets in the healthcare market are showing higher value and attackers are looking for new tactics and methods in order to accomplish their malicious goals creating extortion on organisations, taking advantage of the fact that shutting down systems within hospitals and clinics creates high pressure on employees, doctors, etc., because they have to make life-or-death decisions.

Cybercrime does not present boundaries, and they are always keen to find new skilled people in order to join their cause. Over the last years, it has been appreciated how social media is ruling on time consumption for end users, allowing them to build contact networks, connect with other people and share stories by uploading pictures, sharing files and trading information. Nowadays, social media is being

commonly used within businesses and healthcare organisations and so are not the exception. On the other side, the usage of these platforms allows attackers to steal information and the trading of compromised data. It takes just some minutes to create fake profiles to avoid detection of unusual behaviour under these infrastructures, using it as cybernetic campaigns to attract people in order to join for their cause (Leukfeldt et al. 2016). Hacktivists groups tend to upload confidential information threatening the integrity and reputation of organisations causing damage and extorting their internal employees. In some countries, included the UK, the healthcare sector is considered as Critical National Infrastructure (CNI), along with vital services such as electricity, water and transportation, making it an attractive target for malicious hackers with great desire of generating chaos. In addition, the business of cybercrime allows to share information between members regarding potential targets using social media and websites allocated within the dark net. It is possible to find reports and journals mentioning how businesses are investing in network and endpoint security in the majority of companies rather than training people to avoid and to respond to a cyber-attack executed by criminals. In fact, besides using social media to elaborate the proper reconnaissance addressed to the potential target, it can be used for scamming, searching exposed personal data belonging to careless people.

Organisations are facing a daily battle within the cyber space, where businesses are defending their assets to protect data trusted by customers. Meanwhile, cybercrime is developing new methodologies in order to steal this information regardless of their motivation. The healthcare industry is facing an era where technology is providing a great contribution to deliver cutting-edge solutions regarding medical treatment, providing a better lifestyle for patients. Therefore, it is important for this market to understand the value of their physical and digital assets in order to apply the most optimal security measures and reduce the risk impact given from organised crime.

Cyber criminals are relying on the growth that the dark web is presenting because of the lack of control, which governments have been struggling to shut down these illegal websites for years. In fact, 4% of the entire internet is the World Wide Web (WWW) commonly known by all end users. Meanwhile, the rest is known as the deep web while a part of this belongs to the dark net, which cannot be found with traditional search engines such as Google. Besides, the dark net offers strong layers of anonymity allowing attackers to be untraceable. The dark web in only accessible using dedicated software that could be either The Onion Router (TOR) or Invisible Internet Project (I^2P). All web pages encountered on the dark net are not controlled by law enforcement therefore, cyber criminals are performing unscrupulous actions taking advantage that users take the risk and navigate through the dark net in order to purchase items which can be currently forbidden to be prescribed.

As seen, cyber criminals are taking great advantage of the lack of governance and control over the dark net, letting them exploit and sell the information stolen on healthcare organisations, medicines that are not legally commercialised on common pharmacies. EHRs from patients can be found on the cyber black market at higher prices and can contain information that cannot be found on other organisations. This is because, users trust their data to these organisations considering the fact that

healthcare services are free in most of countries and in wealthy and highly developed countries they count with highly sophisticated equipment at their disposal.

5.3 Electronic Health Records for Clinical Trials and Research

In healthcare, the development of medicines takes time in order to be finally elaborated and authorized by international committees to be prescribed by doctors. It follows a complex process called clinical trial, which consists in the development, testing, follow-up, improvement and distribution of medicines addressed to human patients. Before starting the process, the trials must be performed with animals and recruits groups of people to evaluate the behaviour of their immune systems, looking for secondary effects of medicines developed. In addition, all this information is recorded in patients' health records and research databases, where attackers find it attractive as well. This is because, they can take competitive advantage to sell in the black market these medicines until they get officially authorized by medical federations for its commercial aspects (Ctu.mrc.ac.uk. 2018). Medical treatment and medicine prescription has been involved in debate for years, specifically pointing out that the consumption of drugs can provide a great improvement on lifestyle; however, because of the way drugs have been processed, distributed and consumed by people, it created a great controversy and medical federations made the decision to forbid the drug consumption. In some countries, it is allowed the consumption of drugs, for example a few months ago Uruguay declared as legal to consume marijuana and once the law has been implemented, it went out of stock immediately in just 2 days in what was expected to last for a month.

Clinical trials are divided in the main phases which are detailed below (nhs.uk. 2018):

- **Phase I** is aimed to measure the safety of new treatments. It assesses the side effects of the treatment, and it involves small groups of people, which are commonly in healthy conditions. For instance, it is examined whether the treatment makes changes on patient such as blood pressure raised, causing any sickness, etc.
- **Phase II** is applied to greater groups of people. It is addressed for patients who are under the required symptoms for which the treatment is being aimed. Researchers analyse whether the submitted treatment is safe and the effects under the required condition.
- **Phase III** involves even greater number of people who are selected randomly to receive the treatment in order to analyse the behaviour of the new treatment. This phase takes longer compared to Phase I and II because the treatment has a different reaction on every patient.
- **Phase IV** is performed once the medicine has been approved by regulatory authorities. It carries out the information of the medicine's effect on people from different countries, ethnicities and evaluates side effects of the medicine related to long term usage.

Clinical trials and research can receive volunteer people, and some clinics hire people in order to test the effects and effectiveness of the new treatment deployed. However, it demands an extended amount of time to analyse the behaviour of the treatment in people. In addition, this process is supposed to be transparent for patients, meaning that only researchers have the knowledge of all the patients submitted to clinical trials, while patients are not aware whether anyone has volunteered to try the effects of the medicine (Weng et al. 2014). One of the great benefits of clinical trials is that patients involved in this process are the first ones experimenting the effectiveness of the treatment, which offers higher possibilities of enhancing their lifestyle before it becomes available for the general public. A negative consequence is when the patient, by accident, uncovers that they are allergic to one of the components of the medicine, making researchers immediately suspend the trial with the person and review the group.

The main outcomes of the results obtained from clinical trials are to prevent illnesses testing vaccines, detect or diagnose illnesses, perform blood tests on patients, treat illnesses by testing existing or new medicines, and analyse psychological support and help people to control their symptoms (De Moor et al. 2015). All this information is allocated under their health records which are managed by the information systems implemented in hospitals and clinics. Cyber criminals are keen to gain access to this information in order to develop their medicines and sell it on the black market before it becomes available to the public or in the worst case scenario, the treatment and its commercialisation gets rejected by authorities (O'Flaherty 2018). Furthermore, having gained this sensitive information allows the black market the opportunity to hire those that don't object to being involved with criminals and perform terrorist acts. For instance, a patient who possess diabetes, who has enemies, can be murdered just by providing him the wrong order in a restaurant causing an immediate heart attack or effects of that intent.

As seen, the ePHR robbery has increased in popularity within the organised crime and the dark net because it leads to numerous social engineering attacks that can extort victims, get financial gain from them along with healthcare organisations involved or in the worst case scenario to perform a terrorist attack, compromising the life of a victim(s). The dark web is the home for cyber criminals and they are keen to get this information in order to plan future attacks. The number of acts that can be performed getting this information is limitless and it can likely be achieved for long term extortion purposes.

5.4 Crypto-Viral Extortion Attacks and Its Impact on Healthcare

Healthcare organisations are prone to three kinds of cyber-attacks that can cause huge amounts of extortion to their employees because of the fact that disrupting systems or compromising the security of their patients leads them to make crucial decisions that compromise their health. The cyber-attacks mentioned are:

- **Denial of Service/Distributed Denial of Service (DoS/DDoS)** – Consists in the degradation of the performance from computer systems and machinery used in healthcare, which are connected within a corporate network. Currently there are machines connected to computers which insert the information and allocate it along with EHR from patients accelerating the process of the organisation. This attack can also disrupt completely the functionality of computers and hosts within the network, and there are artefacts performing processes such as x-ray, magnetic resonance, fridges to maintain blood texture, health monitoring devices including the personal wearable, (Snell 2018). The distributed attack is done useing botnets, a network of infected computers allowing attackers to flood target computers with huge amounts of traffic, saturating resources from the target such as CPU, RAM memory, stack memory on network devices. For instance, stopping the functionality of a monitoring device while performing a surgery, can cause high stress/pressure on doctors because they could likely struggle on the next steps due to the exposure the patient is being submitted to and cause irreversible damage or disease; therefore the decisions made by doctors during delicate processes are extremely crucial.
- **Ransomware –** This attack has seen a significant increase in popularity for the benefits attackers are receiving from injecting this malicious software in healthcare organisations. This malware can either lock the access to computer systems or encrypt critical files within hosts. In other words, attacks are kidnapping data processing systems or devices and the only way users can retrieve their systems back is by paying the demanded ransom. Some victims of ransomware did not pay the demanded amount of money because they strongly believed that although the payment is sent it does not guarantee attackers will reset systems to their last version. The best countermeasure at the moment to remediate this cyber-attack is the availability of backup systems in off-line sites because ransomware has gotten more sophisticated and are looking to destroy backup servers to assure victims pay the demanded ransom and obtain financial incomings for this cyber extortion technique.
- **Information Theft –** Cyber criminals are always looking for new information that organisations provide, and nowadays healthcare providers are storing plenty of valuable information, which is increasing steadily in the black market. Healthcare organisations are the ones in the market who possess tons of sensitive information and being stolen by attackers causes damage to the reputation of the organisation; but it also exposes patients to potential harm. As analysed beyond, unauthorized access to personal data leads to cyber criminal to perform further limitless cyber-attacks with all the gathered information. It can be something as simple as blackmailing patients for a lifetime, or something more harmful such as identity theft given by selling this information in the black market. The scope for damaging people and organisations thanks to data theft is absolutely limitless.

Analysing the mentioned threats from an organisational standpoint, All roles within healthcare services have an important impact in terms of protecting sensitive data, which is trusted by patients and doctors as well. It is likely that its IT infrastructure is not well safeguarded due to a limited budget. Nevertheless, personnel

must count with suitable training not just for the accomplishment of the goals of the organisation. It also has to be done in order to apply suitable preventive cybersecurity measurements to protect the information and prevent incidents that could stop medicine procedures, this is because there is the possibility that an incident of high magnitude can cause irreversible damage.

In addition, to strengthen the anonymity of criminals, they are abusing the usage of cryptocurrency, with special mention to Bitcoin, a blockchain technology that provides anonymity and because this system is based on trust and does not have a centralized authority, it is speculated as uncontrolled as well. The next section will describe how cyber criminals take advantage of tools such as TOR and blockchain technologies to accomplish anonymity during the execution of cyber-attacks.

5.5 Analysis of Blockchain Technologies, the Onion Router, and Other Tools Used for Anonymity During the Execution of a Cyber Attack

(a) Blockchain

Blockchain is a very intriguing new technology that started gaining popularity for cryptomining purposes. With the increased rate in cryptocurrencies such as Bitcoin, Ethereum, etc., people started to do research about how the business works and the benefits of doing cryptomining. It promises great enhanced features in terms of security and data privacy that could transform not only the FinTech market, but other industries too. Other sectors such as Retail, E-commerce, Internet of Things, Smart Energy and Healthcare are investing deeply in research and deployment of applications adopting the optimised usage of blockchain technologies.

Blockchain is a distributed system, secure, peer-to-peer (P2P) environment that works on the principle of trust, sharing and the mutual calculation of transactions. In addition, if is a fault tolerant system, does not count with a centralised application managing the network. Moreover, following Fig. 5.3 it has strong cryptographic algorithms, using block-based cryptography. Every transaction is submitted to a hashing procedure, normally SHA-256 for Bitcoin transactions. There are cryptographic schemes, exactly Elliptical Curve Digital Signature Algorithm (ECDSA), used to sign a hash digest from the previous block (N-1). This digest is used to calculate the hash digest of the current block (N). In addition, each block contains the Merkle tree root hash to keep the information of all transactions executed in the network. In the blockchain network, each header contains a nonce, timestamp, value of previous hashes done, gas limit, the difficulty along with other parameters including meta-data making difference between the different existent blockchains (see Fig. 5.5).

To achieve the trust between peers, it uses several mathematical algorithms, depending on the type of blockchain. This technology offers security and transpar-

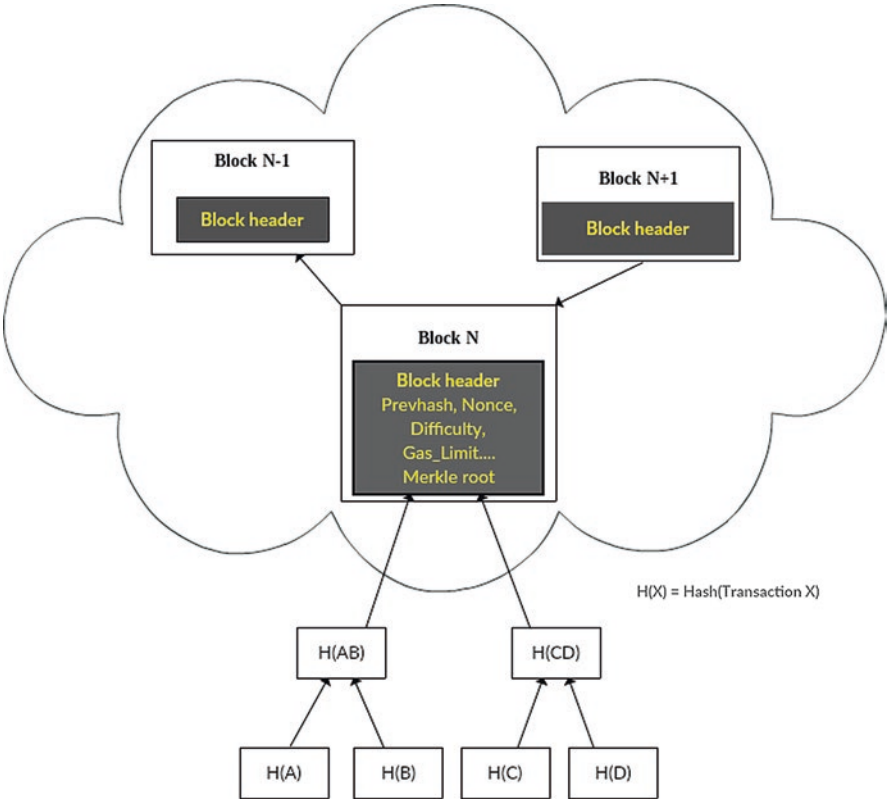

Fig. 5.5 Blockchain structure

ency of transactions, privacy, availability, immutability; however, because it does not have a central authority; this P2P network can be speculated as uncontrolled.

The most popular blockchain technologies used for cryptomining are Bitcoin, Ethereum, Monero and a commercial-based one named Hyperledger, developed firstly by the Linux Foundation developing the partnership between industries by advancing blockchains. Hyperledger received the contribution of great companies such as IBM, Monax, Soramitsu and Intel. One of the newest features hyperledger presents is that peers are divided into two separated runtimes with three different roles: endorser, committer and consenter, offering independent scalability.

As seen, lots of organisations are keen to create services and enhance their current portfolios using the blockchain as an innovative solution and on the other hand, the huge amounts of data being processed throughout the network and thus, polluted payloads or data misuse are great concerns that require some actions to resolve. The TOR network leveraged the blockchain to assess some unusual behaviours. For instance, the blockchain can be used by cyber criminals to deliver malware by inserting malicious payloads to deploy encryption using public key cryptography and selling the private key to decrypt the content and abuse this technology feature. In

addition, blockchain can be exploited to deliver malicious payloads to users dedicated to cryptomining such as ransomware. And nowadays, cryptomalware has increased in popularity inserting malicious payloads into systems used for cryptomining, abusing the resources of computers especially in bitcoin systems, because of its functionality. Computers with mining applications are solving as much mathematical puzzles as possible consuming the CPU and GPU if computers count with graphics card. This is called in Bitcoin, Proof-of-Work (PoW). It requires 51% of all the math puzzles solved for the peer to get control of the node and therefore, better rewards for the connected peer. Cryptomalware is used to create botnets and perform mining at the background abusing the resources of the infected user and supporting cyber criminals to solve more puzzles, take control of the node and get higher rewards. Great potential targets prone to cryptomalware attacks are gaming computers, supercomputers, highly sophisticated servers, in healthcare equipment and devices connected to networks used for medical purposes (Moubarak 2017). In addition, a great concern of blockchain networks will mostly lead to several ways of mechanisms behaving in an unusual manner because of the potential expansion of blockchain networks that are uncontrolled. Another area of misuse in healthcare systems, is allowing the blockchain network to perform as Command and Control Servers to the infected bots in order to receive additional instructions or malicious payloads.

(b) The Onion Router (TOR)

The Onion Routing (TOR) system, is a common network that assures anonymity for TCP-based applications (web browsing, remote shell, instant messaging), along with stream isolation for location-hidden services. This network consists of approximately 12,000 routers, divided in several layers, which each router has specific roles depending on the level of confidentiality given by the network. TOR is a distributed system that forwards client requests using encryption techniques from the source to the last node before arriving to the server (see Fig. 5.4). Firstly, the TOR clients start looking for its registered nodes on the internet analysing within their databases, which are considered as trusted and redundant authority systems in charge of listing to all the nodes on the TOR network. This system works on a circuit based network which downloads the information of related nodes setting a circuit, which requires a minimum of 3 nodes on the established routing table during the connection between client and server.

Encryption is the main feature to achieve anonymity under this network. Comparing this system with common sites, the WWW nowadays employs encryption protocols such as SSL (Secure Sockets Layer) to protect client data or other content within the packet payload as it traverses throughout the internet. In case of TOR networks, once the connection is established between client and server, each node within the network hides the pair of keys for encryption and decryption respectively. Moreover, each node assigns a different IP address of the server and client allowing complete anonymity during the session built. Hence, every node does not have knowledge about the routing table, they only send/receive the encryption and decryption keys, whilst the client/server send/receive the information in plaintext. Furthermore, to prevent data tampering during the established session from anony-

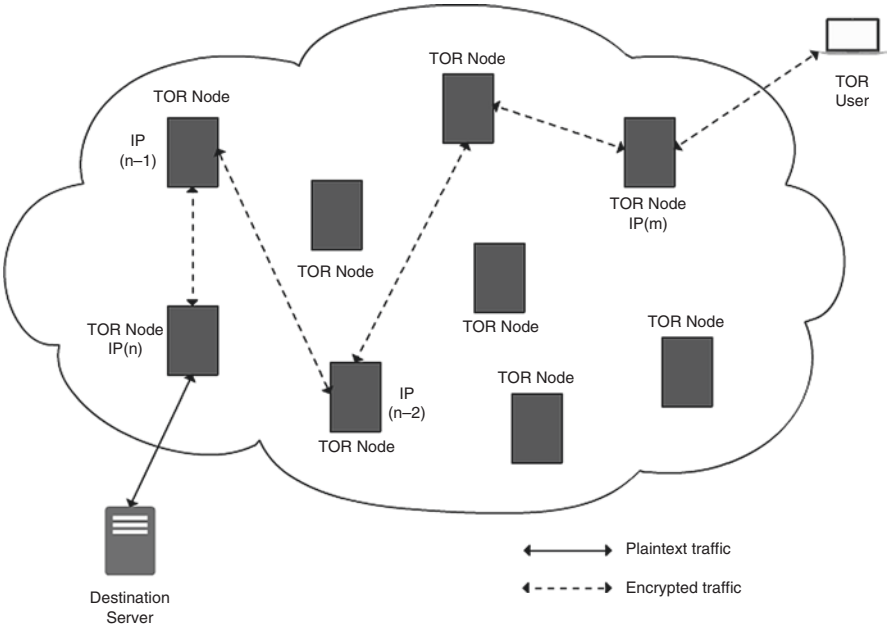

Fig. 5.6 Simplified overview of TOR network

mous clients including eavesdropping, the same process is done for additional requests but using different chain relay nodes. Therefore, each session has a unique circuit built and route within the network (see Fig. 5.6).

Cyber criminals are taking great advantage of the TOR network because a non-negligible part of it is managed in a obscure manner by the TOR foundation. Moreover, most of the bridge router locations are still unknown, and considering the features that this network gives, it makes forensic investigators struggle tracing back the location of these authors who performed cyber-attacks. It is speculated that cyber criminals are under the dark net as refugees of the Internet, taking advantage of freedom and exploiting the benefits of being anonymous while navigating throughout the internet.

(c) Other Common Tools

Even though the TOR network is secure and private, it does not guarantee the expected 100% security, and cyber criminals are aware of this feature. In fact, it is possible to review reported vulnerabilities on the website www.cvedetails.com on the Torproject. For instance, the vulnerability CVE-2017-16,541 reported on 4th of November of 2017 detailed that an unpatched version of TOR below 7.0.9 in devices using MacOS and Linux allows attackers to bypass the anonymity feature and discover the IP address of the client. Considering this feature, cyber criminals are keen to deploy stronger track covering mechanisms, so forensic investigators would

struggle to locate the people and devices involved in an cyber-attack extorting the intended victims.

An extra capability added during a cyber-attack is the configuration of proxy routing services within the machines involved in the cyber-attack. A proxy is a service which acts as a bridge connection between client and server. When the client is sending a request to establish a new session with the server, in the packet the IP address of the proxy server is shown instead of the end user, allowing it to hide their location. In addition, it is possible to change the port during a TCP session between client and server (see Fig. 5.7). A common freeware tool and available on the market is the usage of a packaged nominated **Proxychains**, which allows the attacking host to navigate through the number of proxies configured hiding the IP address of the client. This service is available by default in the penetration testing distribution **Kali Linux**, used commonly by ethical hackers and pen testers. It allows to configure the number of proxies the request must be transmitted through prior to reaching the destination. For instance, if the service is configured with four proxy IP addresses, the packet header will be submitted to a change of sender IP address, four times before reaching the receiver.

In addition to the usage of proxy routing, cyber criminals are always keen to hide the information allocated within the payloads of a transmitted packet. One of the best options is the usage of a Virtual Private Network (VPN), which creates a tunnel during an established session, and all the information navigating throughout it, is submitted to strong encryption techniques. Therefore, joining the usage of proxy routing, a VPN, along with configuring the machine to navigate through TOR network, it would end in a complex network shown in Fig. 5.8.

When performing a cyber-attack, criminals are considering two important factors, how much worth is to perform the specific attack to a particular target, along with time consumption. Even though the configuration of proxies, implementation of VPNs and navigating through TOR means significant delays in the connection established between the attacker and the target, the importance of hiding is vital for

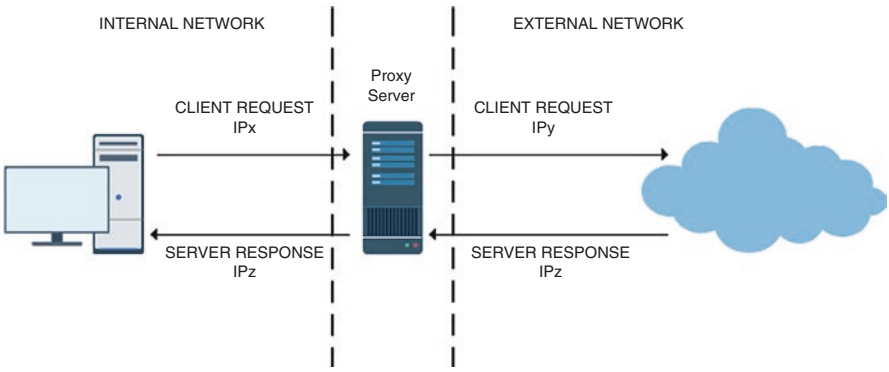

Fig. 5.7 Performance of a proxy to assure anonymity

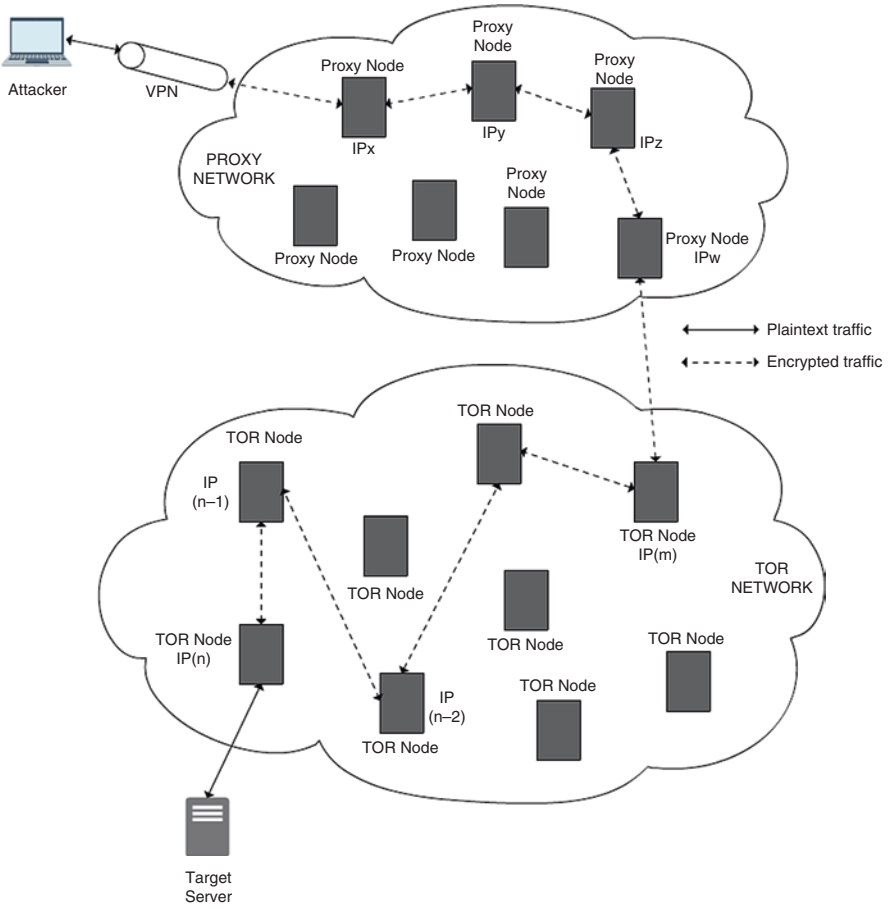

Fig. 5.8 Possible network used by cyber criminals to assure enhanced anonymity during a cyber attack

criminals during an attack to take advantage of the rewards obtained. The delay caused by this pattern can be measured considering the following information:

- Consider the delay caused by encrypting and decrypting the information that is transmitted throughout the VPN
- Delays caused by transmitting packets through different proxies including the delay caused by replacing the IP address
- The delay caused by the usage of TOR network, finding available nodes. Considering that it is required a minimum of 3 nodes as mentioned beyond creating the circuit. In addition, the connection between each node replaces the IP address and includes encryption during the communication.

Even though the session between attacking host(s) and target(s) has been affected by the delays applied due to the features mentioned above, it can take years for

cyber investigators to deter the pattern of the attack, taxonomies followed by hackers and uncover their identities. When tracing back the unauthorized system it is important to follow IP addresses from the sender to find the original location; however, applying the mentioned techniques could likely lead investigators to fall under a limitless mesh that could lead them to abort the investigation.

5.6 Conclusion and Further Research

It has been analysed that cyber criminals are keen to accomplish their purposes no matter what it takes for them to achieve or who can be affected. They are basically financially driven or with the intention to create chaos within organisations, critical infrastructures and with greater chances of generating nation-state alerts. The healthcare sector is totally prone to the most dangerous cyber-attacks because of the information they manage along with the great responsibility of assuring that patients remain alive even when systems get severely disrupted. Even though it is possible to trade stolen information by using social media platforms such as Facebook or Twitter, criminals are keen to keep using the dark web thanks to the limitless scope that an uncontrolled network can provide. In addition, cryptocurrency mining is gaining popularity and criminals are inserting malware into robust machines and stealing resources following the behaviour of a Denial-of-Service (DoS) attack. Likewise, TOR assures anonymity, blockchain offers same features; however, none of them offers 100% anonymity because of vulnerabilities from their systems or the possible extraction of metadata, providing valuable information for forensic investigators. Therefore, despite increasing the time response because of hiding the IP addresses through proxy routing and encrypting data due to VPN, it enhances the anonymity and increases the possibility of remaining hidden when performing a cyber-attack throughout the internet. Although healthcare organisations are spending lots of money in network and endpoint security, it will not stop the organised crime businesses to keep looking for different methods in order to perform data theft or any other malicious activity that could extort from people, to hire skilled people and join their cause. It is important to point out the protection of EHR in health organisations, and the impact of stealing it, enables it to reach to different attack taxonomies, paths, methods and especially diverse social engineering threats due to the sensitivity of the information stolen. For further research it is suggested the application of the anonymity mechanisms, mentioned in this Chapter, be tested in virtual environments to extract precise data of the strength of the security and privacy they claim to assure. In addition, it is recommended to keep navigating through the dark web to discover whether criminals are keen to acquire different assets from organisations to alert the market before suffering a legitimate data breach; the dark net evolves as well as the common internet and it is necessary to keep eye on what cyber criminals are up to. However, it is recommended to take the necessary security measures to ensure privacy while browsing through the dark web. TOR is a good tool to navigate through but to enhance the anonymity hiring a VPN service

and configuring proxies to hide the original IP address is suggested as well because of the flaws that web applications show frequently. Likewise, healthcare organisations must invest in research for strong security mechanisms because of taking responsibility of patients lives and it must be recommended for higher budgets aimed to the cyber security of these organisations and the appropriate measures to ensure confidentiality, integrity and availability of 99.999% system uptime; as expected with implementing ICT infrastructures. With the awakening of cutting-edge technologies supporting enhanced medical treatment, it is required to further investigate in terms of security to ensure business continuity and higher levels of reliability in this interconnected world. People must not get surprised that in other countries around the world that likely they would consider healthcare as part of critical infrastructure, following the example like the UK for instance, and therefore the requirement of regulatory compliance and research on technological areas such as IoT must be addressed to this sector in terms of cyber security.

References

Casteel K (2018) The DOJ wants to stop drug sales on the dark web, but that's a tough task. [online] FiveThirtyEight. Available at: https://fivethirtyeight.com/features/the-doj-wants-to-stop-drug-sales-on-the-dark-web-but-thats-a-tough-task/. Accessed 13 Nov 2018

Catarinucci L, De Donno D, Mainetti L, Palano L, Patrono L, Stefanizzi ML, Tarricone L (2015) An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J 2(6):515–526

Ctu.mrc.ac.uk (2018) What is a clinical trial?. [online] Available at: http://www.ctu.mrc.ac.uk/about_clinical_trials/what_is_a_clinical_trial/. Accessed 22 Nov 2018

De Moor G, Sundgren M, Kalra D, Schmidt A, Dugas M, Claerhout B, Karakoyun T, Ohmann C, Lastic PY, Ammour N, Kush R (2015) Using electronic health records for clinical research: the case of the EHR4CR project. J Biomed Inform 53:162–173

Ducato R (2016) Cloud computing for s-health and the data protection challenge: getting ready for the general data protection regulation. In: Smart cities conference (ISC2), 2016 IEEE International, IEEE, pp 1–4

Francis R (2018) Healthcare records for sale on dark web. [online] CSO Online. Available at: https://www.csoonline.com/article/3189869/data-breach/healthcare-records-for-sale-on-dark-web.html. Accessed 13 Nov 2018

Illmer A (2018) Social media: a cybercrime hunting ground. [online] BBC News. Available at: https://www.bbc.co.uk/news/business-36854285. Accessed 23 Nov 2018

Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS (2015) The internet of things for health care: a comprehensive survey. IEEE Access 3:678–708

Leukfeldt ER, Kleemans ER, Stol WP (2016) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. Br J Criminol 57(3):704–722

Mendelson D (2017) Legal protections for personal health information in the age of big data – a proposal for regulatory framework. Ethics Med Public Health 3(1):37–55

Moubarak J, Filiol E, Chamoun M (2017, October) Comparative analysis of blockchain technologies and TOR network: two faces of the same reality? In: Cyber security in networking conference (CSNet), 2017 1st. IEEE, pp 1–9

nhs.uk (2018) Clinical trials. [online] Available at: https://www.nhs.uk/conditions/clinical-trials/. Accessed 22 Nov 2018

O'Connor Y, Rowan W, Lynch L, Heavin C (2017) Privacy by design: informed consent and internet of things for smart health. Procedia Comput Sci 113:653–658

O'Flaherty K (2018) Why cyber-criminals are attacking healthcare – and how to stop them. [online] Forbes. Available at: https://www.forbes.com/sites/kateoflahertyuk/2018/10/05/why-cyber-criminals-are-attacking-healthcare-and-how-to-stop-them/#167d8e507f69. Accessed 23 Nov 2018

Paterson A (2018) How cybercriminals are using blockchain to their advantage|SecurityWeek.Com. [online] Securityweek.com. Available at: https://www.securityweek.com/how-cyber-criminals-are-using-blockchain-their-advantage. Accessed 13 Nov 2018

Rushanan M, Rubin AD, Kune DF, Swanson CM (2014, May) SoK: security and privacy in implantable medical devices and body area networks. In: Security and privacy (SP), 2014 IEEE symposium on. IEEE, pp 524–539

Seleman M (2018) Ransomware ravages healthcare: cryptoviral extortion in the healthcare sector

Shu IN, Jahankhani H (2017) The impact of the new European General Data Protection Regulation (GDPR) on the information governance toolkit in health and social care with special reference to primary care in England. In: Cybersecurity and cyberforensics conference (CCC), IEEE, pp 31–37

Sky News (2018) Web creator sir Tim Berners-Lee: I see a revolution. Starting right now. [online] Available at: https://news.sky.com/story/web-creator-sir-tim-berners-lee-i-see-a-revolution-starting-right-now-11559034. Accessed 24 Nov 2018

Snell E (2018) How healthcare organizations can reduce cyber extortion risk. [online] HealthITSecurity. Available at: https://healthitsecurity.com/news/how-healthcare-organizations-can-reduce-cyber-extortion-risk. Accessed 13 Nov 2018

Stofko L (2018). How are the deep web and dark web affecting healthcare today? [online] CIO. Available at: https://www.cio.com/article/3228253/internet/how-are-the-deep-web-and-dark-web-affecting-healthcare-today.html. Accessed 13 Nov 2018

Weng C, Li Y, Ryan P, Zhang Y, Liu F, Gao J, Bigger JT, Hripcsak G (2014) A distribution-based method for assessing the differences between clinical trial target populations and patient populations in electronic health records. Appl Clin Inform 5(2):463

Whitmore A, Agarwal A, Da Xu L (2015) The internet of things – a survey of topics and trends. Inf Syst Front 17(2):261–274

Wyman O (2018) [online] Oliverwyman.com. Available at: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/july/holding-healthcare-to-ransom-industry.pdf. Accessed 13 Nov 2018

Yao M (2018) Your electronic medical records could be worth $1000 to hackers. [online] Forbes. Available at: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#778f241c50cf. Accessed 13 Nov 2018

Yip M, Webber C, Shadbolt N (2017) Trust among cybercriminals? Carding forums, uncertainty and implications for policing. In: Policing cybercrime. Routledge, London, pp 108–131

Chapter 6
The Transparency of Big Data, Data Harvesting and Digital Twins

Stefan Kendzierskyj, Hamid Jahankhani, Arshad Jamal, and Jaime Ibarra Jimenez

Abstract Computer storage and cloud computing has become more powerful with multiple algorithms running complex data analysis looking at intelligence trends, user behaviour, profiling and ways to make use of these outputs. Added with the artificial intelligence (AI) interaction has meant a new and dynamic method to create models forging analysis to be more clinical, proficient and continually seeking more improvement with the self-learning and intelligent programming of machine learning (ML). In the healthcare sector there is deep interest in collecting, curating the data and making the best use of silo'd data through methods such as blockchain. This can then lead to a multitude of innovations such as precision based medicine, targeting individual variability in genes, their environment, etc. It also means that big data analytics in healthcare is evolving into providing these insights from very large data sets and improving outcomes while reducing costs and inefficiencies. However, there also are some ethical impacts in the process of Digital Twins which can lead to segmentation and discrimination. Or perhaps the data that is automatically collected from healthcare sensors in IoMT and what type of governance are they scrutinized to. It is clear that data is the most important asset of not just an organisation but also to the individual and why the General Data Protection Regulation (GDPR) has taken an important stance in data protection by design and default, that all organisations needs to follow. This chapter aims to highlight some of the concerns.

Keywords Data Harvesting · Digital Twin · Big data · Transparency · eHealth · Healthcare · Social media

S. Kendzierskyj · H. Jahankhani (✉) · A. Jamal · J. I. Jimenez
London Campus, Northumbria University, London, UK
e-mail: Stefan.Kendzierskyj@northumbria.ac.uk; hamid.jahankhani@northumbria.ac.uk; arshad.Jamal@northumbria.ac.uk; jaime.jimenez@northumbria.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_6

6.1 Introduction

The term Big Data has been around since the 1990s and describes the large volume, veracity and variety of data – structured, semi- structured or unstructured and may be too large to be handled by traditional databases, software technologies and methodologies. Approximately 80% of the data being processed daily today is unstructured where the data can come in any shape or form, so not containing a set record format. Examples of these can be documents, digital pictures, social media feeds, etc. Structured data is therefore arranged with data fields side-by-side in fixed lengths and contains a sequence of attributes and spreadsheets are a good example of this.

Due to some of the advances in processing power, storage, speed, types of devices, etc., has meant the quantity of data produced every day is at 2.5 quintillion bytes and with IoT accelerating will have a direct effect to more large data volume increase; Marr (2018). In the last 2 years 90% of the data in the world today was generated. IDC did some research for predictions by 2025 and some staggering numbers given as globally, by then, will be generating 163 zettabytes of data a year (1 zettabyte is equivalent to 1 trillion gigabytes), Cave (2017) and that is ten times the amount of data as currently is being created. Other IDC research ties in with the IoT explosion as mentioning the average connected person will interact with smart devices approximately 4800 times a day which equates to every 18 sec there is an interaction, Cave (2017). This points to a lot of behavioural analytics being generated on individuals and there are concern over this and its use cases from these analytics.

The primary goals of Big Data analytics are to help businesses unravel their data to make more evidenced based business decisions that can be critical. Ng et al. (2015) indicated that as the volume and variety of healthcare related data continues to grow, the analysis and use of this data will increasingly depend on the ability to appropriately collect, curate and integrate disparate data from many different sources. This means that Big Data analytics in healthcare is evolving into providing insight from very large data sets and improving outcomes while reducing costs.

Looking through past years and the advancement in data mining technology it's clear that many organisations have made monetary and time investments into how to format metadata requirements and curate data and apply what is priority, etc. To remain competitive business executives needed to adopt the new technologies and techniques emerging due to Big Data. But as Big Data has become high profile for companies, and this could be competition, kudos, technological advancement, etc., there hasn't been much done in the way of protecting the rights of the individual who owns the content of the data and what can be done to the data especially around the area of consent and this has led to a lot of people being concerned about how their data is accessed, what purposes, identity leakage and so on. These concerns, plus increasing data breaches, laid the foundation process for GDPR as it puts emphasis on organisations to proactively secure data and gain the consent of individuals before processing can commence and apply a lifecycle approach to data protection by design and default.

6.2 Big Data and Healthcare Impact

Data has and is still regarded as the most important asset of any organisation. Early adopters such as organisations like Google, Apple and Facebook have taken advantage of what data has to offer over the years especially when there was a realisation of what potential it holds around data mining which added value to the companies. Healthcare is a sector that can benefit from the use case of Big Data as it is a complex industry with many moving parts and with patients at the heart of it. Better health profiles and predictive modelling can be created to give much more precision based medicine with high rates of success in diagnosis, treatment and prevention. It is clear that patients need benefit from these better and improved outcomes and one way to do this is by having records and information digitalised in a way that can be easily analysed for any patterns, trends and preventative analysis. The predictive modelling tackles the complicated understanding around the biology of a disease so Big Data plays a part to aggregate lots of data components. As can patient health tracking on various vital health statistics through smart device and IoT. Characteristics can be monitored seamlessly and without relying on any patient memory call-back as all data is captured and automatically updated to cloud based systems. This does present another complex issue of data security and proposals of other methods such as blockchain can be introduced. Another benefit to having this type of patient tracking is keeping patients out of hospital since they can be monitored remotely in this way and this increase in analytics can have more positive behavioural effects on the patients as they figure out and interpret the importance of the smart wearable technology.

Fundamentally, the advent of the age of Big Data poses opportunities and challenges for industry. Previously unavailable formats of data can now be saved, retrieved and processed (but curation comes at a cost as to know what priority should be saved). Essentially data is being generated in a growing number of ways and therefore the use of traditional transaction databases have been supplemented by multimedia content, social media, and countless types of sensors. Big Data use is increasing rapidly, in that the world is changing and becoming an ever more digital space – compared to a few years ago, and today a lot is managed and shared online. The data that has been collected from smartphones, computers, devices, social media platforms such as Twitter, Facebook, Instagram, is then subsequently analysed, transmitted and reports driven on this data. Many observations are already drawn that this is only just the beginning; the evidence is overwhelming that this will increase, and data will be collected on just about everything. If data is compared to what was collected since the beginning of time up until the end of 2000; it will be significantly less than what is now collected in a minute (Marr 2018). Likely it is impossible to stop this journey of data accumulation since so much of the world is not connected and automatically analysed with sophisticated, artificial intelligence and machine learning algorithms.

6.2.1 Data Harvesting and Mining

A huge amount of data and wealth of information is regularly generated about our lives with or without knowing. A digital footprint is established that stays forever and mostly cannot be erased. Whilst individuals think on obvious places such as credit card, banking, purchases, social interactions etc., that builds this picture of preferences and routines, there is the aspect of data mining that is going on in the background that is more cause for concern. Forrester undertook research and output of a report in 2014, *Big Data's Big Meaning for Marketing*, and some highlights discussed by Kramer (2015) with regards to personal data protection, financial liabilities and ethical dilemmas. Methods of protecting individual's identity may not go far enough in the case of identity protection in the data mining process. Forrester outlines how Netflix released data after believing it had anonymised the data, but University of Texas researchers were able to identity Netflix users for anonymous reviews, but by knowing some parameters such as movies rented then it was possible to reverse-engineer the data and find out all viewing history; Pepitone (2010).

Whilst many would be in favour of healthcare providers mining data to ensure best placed precision based healthcare, where data mining is used to predict health needs; it might still have questions raised. This sounds good but could raise ethical questions on privacy invasion. An example of Carolinas Healthcare System who manages 900 care centres and purchase data collected from credit card purchases, store loyalty programs, etc., to allow identification of high-risk patients in attempts to intervene prevention on any health issues developing, Kramer (2015). This identification by medical practitioners would enable gaining insight into patients' lifestyles and habits. A risk score is used so doctors can see flagged up issues. The data is collected from credit card purchases, store loyalty programs, and other public records. In theory, medical practitioners can learn more about their patients—and their patients' lifestyles—from their shopping habits than from brief, or sometimes nonexistent, consultations. Although the data doesn't yet identify individual purchases, it does provide a risk score doctors can use to highlight potential problems. The issue could become a more trust based issue between medical providers and patients if the data mining intrudes into the privacy and questions even healthy patients about their habits and digital footprints they leave. Or it may not take too long before insurance companies also start to review this mined data and risk score and that influences the service a patient receives, or worst case is refused if deemed too high a risk.

Or perhaps the case of Target, a retail organisation, that through a number of factors was able to identify and assign shoppers with a pregnancy prediction score (due to the array of 25 products when analysed together) and estimate a birth delivery due date to a small window. It allowed Target to provide coupons to the specific stages of pregnancy and highlighted a case of a dad who discovered his teen daughter was pregnant because Target mined her purchased data and sent her ads for baby products, Hill (2012).

6.2.2 Social Media Data Misuse

The widespread success of online social networking sites (OSNS) such as Facebook is a tempting resource for businesses engaged in electronic commerce.

Using personal information, willingly shared between online friends' networks, OSNS appear to be a natural extension of current advertising strategies such as word-of-mouth and viral marketing. However, the use of OSNS data for business marketing purposes has provoked outrage amongst social network users and highlighted issues over privacy. Within such environments, OSNS users disclose information that would be potentially rich sources of data mining for commercial organisations because it includes information that can personally identify an individual in rich detail (Krishnamurthy and Wills 2010). Such 'personally rich' information includes attributes such as name, location (city), telephone numbers, email addresses, photos, interests and purchases etc. This rich online social network data together with electronic word-of-mouth (eWOM) communications of OSNS users represents a tempting resource for viral and word-of-mouth marketing unlike other online and offline data which has to be prepared before systematically explored for patterns of use meaningful to commercial organisations (Kohavi et al. 2002; Zhang et al. 2011). A qualitative investigation of 861 blog comments from 715 individual online users were collected during the launch of Beacon, an unsuccessful third party marketing initiative by Facebook. Results show that business integrity, transparency of data use, user control, automatic disclosure and data leakage were key privacy concerns posing significant challenges to using business analytics in online social networks. However, attempts to leverage personal information and eWOM communications for commercial gain have provoked outrage amongst OSNS users because of privacy concerns. Privacy concerns of online social network users include use of personal information by unknown others for potential harmful purposes (e.g. by sexual predators), use and selling of personal information without notice and consent, access of personal information by unwanted audiences (Young and Quan-Haase 2009), involuntary disclosure of personal information, damaged reputation because of rumours and gossips, unwanted contact and harassment or stalking, third party use of personal information, and identity theft (Boyd and Ellison 2008). Consequently, privacy concerns challenge the classic thinking outlined by Kohavi and Provost (2010) that online (social) environments are particularly suitable domains for data mining because of the rich and large volume of data publicly available. Rather, issues of privacy concerns have emerged that overshadow the commercial potential of OSNS data (Hoadley et al. 2010) and highlight the boundaries of acceptance and use of business analytics in social networks. Privacy concerns have emerged as a critical factor determining the willingness, or not, of internet users to divulge personal information to online companies. Many studies have used 'privacy concern' construct to understand privacy in online contexts. Therefore 'privacy concern' has become a central construct to study privacy in information systems research. Likewise, it is a useful construct for business analyt-

ics because it provides theoretical guidance in defining and measuring privacy-related issues in the context of mining social network data for business marketing.

Facebook's personalised marketing tool "Beacon" was initially withdrawn by the Facebook due to users' backlash because of privacy concerns and ultimately shut down due to settlement of a lawsuit of $9.5 million. What should have been a successful innovation, however, was damaged and ultimately withdrawn because the nature and form of privacy concerns in OSNS was poorly understood.

6.3 Digital Twins in Healthcare: Transparency, Ethical Implications and Security Concerns

The term "Digital Twin" is an emerging engineering paradigm, which can occur in healthcare data-driven practices such as delivering personalized 3D printing as prosthesis for a surgery or dedicated manufacturing pieces for building or vehicle maintenance purposes, as examples. On the other hand, it involves conceptual and ethical implications, but what is really the concept of "Digital Twin"? It basically means the connection between the physical and digital world; the ability to visualise in computers, mobile devices or even in holographic projections what we are accustomed to watch daily. Looking back years ago, the film IronMan, and those scenarios where Tony Stark was able to manipulate and visualise the design of the new chemical element required in order to stop poisoning his body from using palladium for his arc reactor.

The Digital Twin takes the concept of Cyber-Physical Systems (CPS) to a higher level. This is because within an organisation, their assets can get digitalised (i.e., artefacts, devices, processes) and people can understand their behaviour, extract data in real-time in a 24/7 basis because of the implemented sensors across the asset, measuring physical values (e.g., voltage, pressure, amount of sugar). It requires to take advantage of Big Data analytics along with cloud computing systems in order to process tons of data in just seconds, making probabilistic approaches, math algorithms and establishing best options based on the calculations made. With all these features, organisations can make decisions and assess their results firstly over the digitalised assets extracting pros and cons, along with their associated risks prior to its implementation in the physical environment. This term stands for a paradigm, where individual physical assets are paired with digital models reflecting its status in a dynamic manner. The concept of Digital Twin has been applied by NASA for the development and monitoring of aerospace vehicles in order to last longer and tolerate extreme conditions compared to the Earth.

Modern engineering has provided a great support for the evolution of medicine. The establishment of mathematical models of patients, processing tons of "biodata" leading it to precise and effective medical interventions. Nowadays we count with supercomputers able to read molecular data making it possible to build personalised models, complemented by a continuous health and lifestyle tracking, resulting pos-

sibly in the "digital" representation of a patient – a "virtual patient". Therefore, the Digital Twin is an instrument showing the impact analysis of cutting-edge engineering solutions on core topics within healthcare such as health, disease, preventative care, and enhancement. It is claimed that many technical universities are training and preparing students in clinical technology, whilst doctors are working alongside with engineers from a wide range of backgrounds to enhance the functionality of modern medicine. Engineering standpoint and innovation drives a debate regarding human enhancement such as replacing broken parts of the body using 3D printed implants, arguing the possible; to enhance the human body with new capabilities. For instance, neural implants used for visual prosthetics addressed to blind people; however, it can lead towards capabilities that can get likely assessed beyond what is speculated as "normal" human sight providing access to parts that are considered normally inaccessible under the electromagnetic spectrum. The idea of digitalising molecular and physiological structure of people in order to deter whether the person is in healthy condition, estimate potential disease based on daily monitoring, measuring physical values such as heartbeat, blood pressure, sugar levels, etc., in order to elaborate the adequate medical prescription. In fact, it has been proven the efficacy of an approach done to pick the most appropriate drug for cancer treatment besides chemotherapy.

The concept of Digital Twin is used in industry to monitor the performance of artefacts and pieces of machinery in order to perform preventative maintenance. In fact, digitalisation of individual artefacts is simple because it is based on the instrumentation of electronic sensors placed across the artefact and besides, artefacts have an unique shape after its manufacturing, making easier the instrumentation. In healthcare otherwise, the human structure is more complex because of the constant molecular and physiological changes throughout their lives, making it complex to extract precise molecular data even though it is available the usage of wearable devices for medical purposes. Unfortunately, Digital Twin is still far from real and currently modern engineering approaches have reached digital models of genetic, biochemical, physiological and behavioural features of individuals. Therefore, the concept of Digital Twin offers a reliable instrument addressed to the impact analysis in healthcare because the usage of probabilistic models of individuals for customised medicines supports the engineering of a healthy condition and the advantage of big data to represent either a person or artefact.

To implement the concept of Digital Twin, it is necessary to differentiate heterogeneity when acquiring data over one's life time because in medicine the declaration of "healthy" or "normal" is done based on a population after clinical trials or following a pattern based on international medical committees. With the "digitalisation" of patients nonetheless, it must be required therefore a sharper statistical model in order to deter the declaration of normal or healthy status, and likewise of disease status and susceptibilities. An approach of Digital Twin in healthcare should rely on a detailed status of a healthy individual rather than basing it on diseased status records. In medicine, the declaration of healthy can reach to the state of "symptomless illness" and the biodata processed using probabilistic and statistical models within the concept of Digital Twin can allow doctors to infer the possibility

of developing diseases. However, the engineering prototype coming along with Digital Twins brings into debate within medicine the optimal declaration of healthy – normal – status, carrying the question whether certain human features should be optimised or enhanced. Therefore, it is essential for decision making in healthcare to have the distinction between therapy, preventative care and enhancement, depending the condition of the patient.

The main purposes of enhancement in modern engineering actions are addressed to either restoring the functionality of a system or its modification. Digital Twins change the stereotype of existing engineering thanks to the elevated transparency of the status and performance of an artefact including the centrality of each one. Compared to medicine for instance the individual approach will impact the differentiation between therapy and enhancement because the declaration of normal or healthy status is often based on group or population statistics. However, with the concept of Digital Twin, individualisation is essential for its optimal functionality in healthcare. In addition, establishing an accurate digital model of a person would not be based on instrumentation for better decisions during healthcare interventions, but will also be part of the patient's identity. Digital Twins may therefore make doctors to review again what therapy should be considered when deploying personalised medicine. Digital Twins implies moral issues as well. For instance, depending on whether medical interventions are considered as daily treatment, therapy or enhancement, it can lead to different conclusions depending on what extent, which conditions and the public costs covered by the healthcare system.

Digital Twins brings great features and a significant contribution for the deployment of the hospital of future, because it can give a detailed account of molecular, physiological, phenotypic and lifestyle of people. It is considered currently an interesting conceptual tool which is worth to understand the technological trend in medicine along with a reflection on its future implementation, thereby the need of understanding the categories of health, disease and enhancement. Whilst the processing of data involves several biological aspects, along with behavioural data involving personality, manners, stress levels and also lifestyle of patients such as diet regimes, whether the patient does exercise, smoking, alcohol, etc. However, it is worth the analysis of some possible ethical and social implications of this trend. It is mandatory to understand that currently human beings are already using enhancement techniques. For instance, people can improve their lifestyle by performing exercise, a customised diet to increase muscular mass or stamina. The introduction of wearable devices and Wearable Body Area Networks (WBAN) allows real-time monitoring in a 24/7 manner delivering full-time support to the person in order to make fast decisions. A better lifestyle obtained by training and diet schemes might have the same results as the enhancements obtained by pharmaceutical treatment. Other arguments that could likely occur is the fear that human enhancement technologies might lead to people separation, having a disruptive effect on the current democracy, or the higher payments to afford this service as well because personalised medicine will increase the cost at individual level compared to traditional treatment.

In addition, Digital Twins can support the industry in the deployment of 3D printed organs used for prosthesis implementations such as replacing bones which are part of the spine given by a herniated disc or a heart transplant with the data extracted from the characteristics of the human being. A research from Lee Cronin from the University of Glasgow has demonstrated that chemical synthesis is possible using 3d printers in order to produce drugs to improve their lifestyle. The features mentioned bring concerns in terms of data privacy because the processing of tons of data measured in real-time along with the extraction of information from Electronic Patient Health Records (ePHR) and the data processed from wearable devices, makes the healthcare market prone to data theft and tampering. For instance, the modification of data while printing pills in order to synthesise illegal drugs such as cannabis or marijuana even though in some countries is considered legal. Data theft under a Digital Twin would lead to dedicated terrorist attacks terminating the life of the person by following different social engineering attacks. Therefore, there is importance of the need for strong governance frameworks and mechanisms addressed to ensure transparency on how Digital Twins are being used ensuring data privacy, integrity and availability, along with the protection of humans' rights and distribution of benefits given by the population's personal biological information.

6.4 Conclusions

Industry 4.0 (the fourth industrial revolution) sees the fast moving advances of the Internet of Things (IoT), big data, artificial intelligence (AI), more interaction in cyber-physical systems (CPS) and scalable cloud computing. Predictions by Gartner of more than 20 billion devices connected to IoT by 2020 are well understood, but more importantly will mean a huge volume of data will be generated.

Effects of data breaches, identity theft are widely known to take place in healthcare, but the more concerning impacts are how the data analysis or data harvesting are being utilised with numerous recent examples such as Cambridge Analytica, Google DeepMind App project with the NHS, and so on. Whilst it is understood big data analysis is needed and progressive to the requirements of Industry 4.0 there should, in tandem, be sanity checks on how the governance is developed on these more innovative technologies and their impacts studied.

References

Boyd D, Ellison NB (2008) Social network sites: definition, history, and scholarship. J Comput-Mediat Commun 13:210–230

Cave A (2017) What will we do when the world's data hits 163 Zettabytes in 2025? Forbes. Available at: https://www.forbes.com/sites/andrewcave/2017/04/13/what-will-we-do-when-the-worlds-data-hits-163-zettabytes-in-2025/#25ed8bc9349a. Accessed 10 Nov 2018

Hill K (2012) How target figured out a teen girl was pregnant before her father did. Forbes. Available at: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4ee09e726668. Accessed 11 Nov 2018

Hoadley MC, Xu H, Lee J, Rosson MB (2010) Privacy as information access and illusory control: the case of the facebook news feed privacy outcry. Electron Commer Res Appl (Special Issue on Social Networks and Web 2.0), 9(1):50–60

Kohavi R, Provost F (2010) Applications of data mining to electronic commerce. Data Mining and Knowledge Discovery, 5(1/2), 2001. Retrieved on September 15, 2010, from http://robotics.stanford.edu/~ronnyk/ecommerce-dm/editorial.pdf

Kohavi R, Rothleder NJ, Simoudis E (2002) Emerging trends in business analytics. Commun ACM 45(8):45–48

Kramer S (2015) The big risks of big data mining. V3B. Available at: https://v3b.com/2015/06/the-big-risks-of-big-data-mining/. Accessed 11 Nov 2018

Krishnamurthy B, Wills EC (2010) On the leakage of personally identifiable information via online social networks. SIGCOMM Comput Commun Rev 40(1):112–117

Marr B (2018) 'how much data do we create every day? The mind-blowing stats everyone should read'. Forbes. Available at: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2a7b7b3760ba. Accessed 10 Nov 2018

Ng K, Kakkanatt C, Benigno M, Thompson C, Jackson M, Cahan A, Zhu X, Zhang P, Huang P (2015) Curating and integrating data from multiple sources to support healthcare analytics. Stud Health Technol Inform 216:1056

Pepitone J (2010) 5 Data breaches: From embarrassing to deadly. CNN Money. Available at: https://money.cnn.com/galleries/2010/technology/1012/gallery.5_data_breaches/index.html. Accessed 11 Nov 2018

Young AL, Quan-Haase A (2009) Information revelation and internet privacy concerns on social network sites: a case study of Facebook, ACM

Zhang M, Jansen BJ, Chowdhury A (2011) Business engagement on Twitter: a path analysis. Electron Mark 21:161–175

Chapter 7
Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger

Haider Al-Khateeb, Gregory Epiphaniou, and Herbert Daly

Abstract Blockchain technology can be incorporated into new systems to facilitate modern Digital Forensics and Incident Response (DFIR). For example, it is widely acknowledged that the Internet-of-Things (IoT) has introduced complexity to the cyberspace, however, incident responders should also realise the advantages presented by these new "Digital Witnesses" (DW) to support their investigation. Logs generated by IoT devices can help in the process of event reconstruction, but their integrity -and therefore admissibility- can be achieved only if a Chain-of-Custody (CoC) is maintained within the wider context of an on-going digital investigation. Likewise, the transition to electronic documentation improves data availability, legibility, the utility of notes, and therefore enhances the communication between stakeholders. However, without a proof of validity, these data could be falsified. For example, in an application area such as eHealth, there is a requirement to maintain various existing (and new) rules and regulations concerning authorship, auditing, and the integrity of medical records. Lacking data control could lead to system abuse, fraud and severe compromise of service quality. These concerns can be resolved by implementing an online CoC. In this paper, we discuss the value and means of utilising Blockchain in modern systems to support DFIR. we demonstrate the value of Blockchain to improve the implementation of Digital Forensic Models and discuss why law enforcement and incident responders need to understand Blockchain technology. Furthermore, the admissibility of a Digital Evidence to a Court of Law requires chronological documentation. Hence, we discuss how the CoC can be sustained based on a distributed ledger. Finally, we provide a practical scenario related to eHealth to demonstrate the value of this approach to introduce forensic readiness to computer systems and enable better Police interventions.

H. Al-Khateeb (✉) · G. Epiphaniou · H. Daly
University of Wolverhampton, Wolverhampton, UK
e-mail: H.Al-Khateeb@wlv.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_7

Keywords Digital investigation · Forensic readiness · Incident response · Digital witness · Decentralised computing · Liability attribution · eHealth · Data integrity · Digital evidence

7.1 Introduction

Digital Forensics has disseminated to cover the wide variety of technologies we utilise, in an era where connected devices (IoT) are forecasted to be around 30 Billion (Navarro-Ortiz et al. 2018). Digital Forensics is a prominent and inevitable part of an Incident Response plan covering electronic data and an established skill area in the cyber security industry. Examples of legal recognition in the United States goes back to 2006 when courts adopted new rules for civil procedures to acknowledge digital information as an acceptable form of evidence and implemented a mandatory system, namely electronic discovery (eDiscovery) to establish the grounds for this new branch of forensic science (Navarro-Ortiz et al. 2018). In present days, one approach in which the National Cyber Security Centre (NCSC) in the UK addresses the vision of the UK Cyber Security Strategy 2016–21, "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world", is by certifying Bachelor and Master's degrees where Digital Forensics is a clearly defined path alongside few other well-established titles such as cybersecurity, information security, and computer network and Internet security.

The main purpose of Digital Forensics is to perform technical investigations within the boundaries of the legal system in response to criminal activities that involve electronic devices. The objective is to support or reject a hypothesis related to a criminal or civil case. Disputes between commercial parties could also be the reason for performing eDiscovery within this context. Forensically sound tools (sound; vetted and tested thoroughly) are utilised by trained investigators to collect, analyse and reconstruct events and actions to help to explain what happened in support of a prosecution (Daryabar et al. 2017). Technical investigators are referred to as Expert Witnesses, and they become responsible to produce a conclusion that is admissible to a Court of Law.

The scope of digital investigations continues to increase. Building an effective team requires specialist skills in areas such as computer and mobile phones, onsite (crime scene) investigations, call data records, search orders, forensic readiness planning, data recovery, and audio-visual forensics. Non-electronic data is within the scope as well considering the highly integrated cyber-physical ecosystem we interact with. For instance, a digital currency such as Bitcoin can be saved offline as part of a paper-wallet. This approach is attractive for users who aren't tech-savvy, to enable offline money exchange, or to keep Bitcoin addresses safe against online attacks on the long-term. Therefore, a forensic investigator would be expected to seize this offline storage medium in cases associated with money laundering or illegal dark web trading. A Bitcoin paper-wallet is usually designed with elements of physical security; a folded design to resist shoulder-surfing. Additionally, tamper-resistant measures such as anti-candling hologram stickers are used which shows

that offline analysis techniques could become one of the required skillsets for the team. Another example to demonstrate the extended scope of modern digital investigations to involve body scanning is the emerging practice of microchip implants. In 2018, thousands of people in Sweden have inserted microchips into their hands for identity check; to access their office at work, gym, and pass through train gates (Pollitt 2010).

This paper discusses the utilisation of Blockchain for modern DFIR. The need for a tamper-proof series of timestamps could be traced back to the 1990s while the first conceptualisation of the technology was described in a white paper authored by Satoshi Nakamoto (a fictional name) in 2008 (Nakamoto 2008) to enable distributed Bitcoin transactions. The Blockchain is formed of a basic list of records, namely blocks, which are linked using cryptographic algorithms. The solid connection and continuity of blocks prevent the modification of existing data blocks and any written content will, therefore, be verifiable and permanently accessible. This has triggered a lot of interest from various industries such as banking and energy, while other proposals were presented to support governance models (Mengelkamp et al. 2018; Cocco et al. 2017). Consortiums have been established and private research labs opened to investigate potential models that could help to cut the middle-man (which is cost-effective) and automate processes for businesses back-end systems (Johng et al. 2018). Furthermore, the distributed nature of the technology removes any single-point-of-failure and provides the mean to hold participating parties accountable for their records because each recorded transaction will be witnessed by all connected nodes and only an enormous amount of computing power can override their data. Possible in theory but non-practical; attacking the network becomes harder when more self-motivated devices become part of the distributed system. The need for provenance tracking goes beyond the financial and supply chain markets as it is also a very critical requirement for forensic investigations. Tracking the origin and movement of case-related data (e.g. seized items) is challenging as it is subject to human error, theft and counterfeiting. A recent example from Iceland showed that poor work practices have been reported as the reason for the disappearance and untreacability of seized assets following a Police raid (Daryabar et al. 2017).

Records on the Blockchain are virtual and representatives of any seized item, therefore suitable to support the creation of a CoC compared to a paper-based solution that can be destroyed or a central system that can be vulnerable to Denial-of-Service (DoS) and less resistance to integrity attacks. To elaborate, once a physical or electronic item is seized, a virtual token is created to act as a certificate of authenticity for that item at that specific time. Thereafter, a new virtual token is created to openly evident changes to that item during transport or alteration. Other metadata can also be supported which allows the CoC to include other useful information.

In the remaining part of this chapter, the reason why law enforcement investigators should understand and utilise Blockchain technology is discussed in Sect. 7.2, how Blockchain technology can improve the implementation of digital investigation models is discussed in Sect. 7.3, and how a Chain-of-Custody (CoC) can be maintained with Blockchain is demonstrated in Sect. 7.4. Then, Sect. 7.5 presents a

case study related to eHealth to demonstrate the value of this approach to introduce forensic readiness to computer systems and enable better Police interventions. Sect. 7.6 discusses Digital Witnesses (DW). Finally, we conclude our chapter in Sect. 7.7.

7.2 Why Police Digital Investigators Need to Understand Blockchain Technology

7.2.1 To Maintain Compliance with Digital Investigation Principles

Law enforcement agencies perform digital investigations to reconstruct events from the past in support of on-going cases. However, not all investigations can be prosecuted due to reasons not limited to the nature of the incident but also the validity and integrity of the investigation process itself, this is where Blockchain technology becomes useful. The technology can help compliance with guidelines. In the US, the Department of Homeland Security, US Secret Service has published Best Practices for Seizing Electronic Evidence as a pocket guide for first responders (U.S. Department of Homeland Security – United States Secret Service 2015). In the UK, the Association of Chief Police Officers (ACPO) has agreed to a set of guidelines to be adopted by Police Forces in England, Wales & North Ireland. Non-compliance can be a reason to invalidate the integrity of the investigation. The principles listed in the ACPO Good Practice Guide for Digital Evidence (Williams 2012) are:

Principle 1: "No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court".

Principle 2: "In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions".

Principle 3: "An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result".

Principle 4: "The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to".

These principles, especially Principle 3, is clearly enforcing a verifiable audit trail on the investigation process. Blockchain-based Digital Investigation Models can help to achieve that as discussed in Sects. 7.3 and 7.4.

7.2.2 To Facilitate Multijurisdictional Investigations

The cyberspace is cross borders. Therefore, multijurisdictional investigations are routinely pursued by law enforcement agencies around the world. As such, there are various frameworks and models addressing miscellaneous technologies (e.g. IoT), case studies, crime scene scenarios and local laws. This complexity is an obstacle as it is resource consuming and introduces many legal challenges. Additionally, there are International Organization for Standardization (ISO) standards such as the ISO/IEC 27037 to comply with as well. It provides guidelines for the identification, collection, acquisition and preservation of Digital Evidence while another standard namely the ISO/IEC 27043 provides guidelines based on idealised models for common incident investigation principles and processes. A key enabler for multijurisdictional investigations is the utilisation of a collaborative environment and a permission-based model to share evidence. Hence, the possible value of a Permissioned Distributed Ledger System (Permissioned Blockchain) for law enforcement.

7.2.3 To Have More Witnesses

While some crimes are reported or supported by a witness accepted by a Court of Law, others are hearsay and might not be as valuable to support a prosecution unless we have means to trace records back to their originator. In the cyberspace, the concept of DW has been introduced. Despite many challenges and complexities introduced by the IoT paradigm, it has also empowered digital investigations with new DWs. This can be an IoT device capable of preserving and sharing data (Digital Evidence) with other connected devices or the cloud. Collaboration between IoT devices is at the core of this approach and Blockchain is a key facilitator to establish a trusted CoC.

Accepting devices to act as a DW requires specific properties. For example, anti-tampering behaviour, binding credentials, binding delegation, and accepted procedures as discussed in (Nieto et al. 2016). The “anti-tampering behaviour” property means that an IoT device should have a solid security feature such as an embedded Trusted Computing Hardware to periodically verify its integrity. The device should invalidate its own eligibility to be a DW in cases of malfunctioning or failures of integrity checks. Blockchain-based models are being developed to trace the status of these devices and securely record relevant values as part of a digital CoC.

7.2.4 To Support Victims with Blockchain-Based Forensic-Enabled Devices

Victims of cybercrime are usually keen to construct and maintain Digital Evidence to support their assertion. They will, therefore, be interested in forensic-enabled solutions as part of their cyber safety. For instance, victims of cyberstalking (al-Khateeb et al. 2017) cannot predict the time or means they will be targeted and would adopt forensic-enabled software and hardware to preserve Digital Evidence. Captured information can be used to report and escalate the incident with the Police and increase the chances of acquiring evidence that is admissible to a Court of Law. Furthermore, victims should not have to be tech-savvy while digital investigators are expected to utilise the opportunity presented by Blockchain forensic-enabled devices to support the case towards suitable prosecution.

7.2.5 To Investigate Technology Misuse

Digital investigations cover any electronic data including the many current and future Blockchain-based implementations. Cryptocurrency (e.g. Bitcoin) transactions are recorded on a Blockchain making the technology a topic of interest because cryptocurrencies are widely used in the Dark Web, subject to money laundering, tax evasion, and price manipulation. In 2018, the Federal Bureau of Investigation (FBI) reportedly "has 130 cases tied to cryptocurrencies", according to Supervisory Special Agent Kyle Armstrong, speaking at the Crypto Evolved conference in New York.

7.2.6 To Develop New Solutions in Response to Emerging Digital Forensics Challenges

Digital investigators work in the field with hands-on experience. They are in a good position to provide the required feedback based on existing challenges. A good understanding of what technology can offer helps practitioners to contribute towards deploying new solutions. For example, the following classifies the widely reported challenges facing digital investigations:

Technical Challenges Represented by the evolvement of new devices (e.g. IoT) to address, new models (e.g. Cloud Computing) to understand and prepare for, and increased volume of data to preserve and analyse (e.g. Big Data).

Legal, Regulatory and Procedural Challenges We need to develop the means to facilitate national and cross borders investigations while adhering to local laws.

Likewise, incident response within a specific company is governed by corporate policy and procedures. Moreover, many standards and models are introduced while compliance is complex and varies between stakeholders.

Social Challenges For example, problems that victims of cybercrime face when considering a voluntary hand over of their personal digital devices to preserve Digital Evidence. This has a clear impact on their privacy as well as losing access to their own personal assets.

7.3 How Blockchain Technology Can Improve the Deployment of Digital Investigation Models

7.3.1 Introducing Digital Investigation Models

There are several published investigation models and they all attempt to elaborate on the steps to be taken by the forensic team. For example, to define the principles, tasks and responsibilities to maintain the integrity of the preserved evidence. They aim to achieve this without contradicting any local jurisdictional laws and regulations, the team would, therefore, exercise with care to maintain compliance with the prevailing jurisdictional requirements. Digital forensics is all about the process, it is a recognised scientific methodology and should be designed to provide the ability to verify all reported conclusions (or process output). The initiation stage is usually triggered by a reported incident. In its simplest form, an investigation model could consist of: acquisition, analysis and reporting. However, the complexity of the cyberspace attracted various revisions. In an early paper (Navarro-Ortiz et al. 2018), four stages were suggested namely "acquisition", "identification", "evaluation", and "admission as evidence". In knowledge management terms, data is usually captured from a seized media within a physical context, processed for evaluation within a logical context, and finally submitted as evidence within a legal context. This model was then amended in 2001 as part of the first Digital Forensic Research Workshop (DFRWS) (Pollitt 2010) to six stages starting with an "identification" phase to detect incidents as part of proactive monitoring or auditing to trigger the forensics process. A "preservation" phase where procedures for case management are introduced to maintain the integrity of evidence collection. The "collection" phase where data is extracted from the crime scene for further processing at a consequent stage called the "examination" phase. Captured data is then "analysed" to locate and recover hidden artefacts and report any incriminating evidence. Finally, a concluded evidence statement is reported as part of a "presentation" phase.

The IT security catalogue from ISO includes standards focusing on electronic discovery (eDiscovery) namely ISO/IEC 27050-1:2016, ISO/IEC 27050-3:2017, and ISO/IEC 27050-2:2018. Overall, they aim to locate and preserve pertinent Electronically Stored Information (ESI) including data by any stakeholder involved

in the investigation. The ISO/IEC 27050-1:2016 defines key concepts within seven main stages very similar to the those developed by the DFRWS model starting with "identification", "preservation", and "collection". The consequent steps and their details have then been developed as: "procession", "review", "analysis", and finally ESI "production". Other relevant standards such as the ISO/IEC 27037 are also covered to describe related activities and needed interactions. ISO/IEC 27050-3:2017 provides a code of practice for eDiscovery and practical measures covering the duration of the ESI lifecycle from the initial creation to the final disposition. Finally, the ISO/IEC 27050-2:2018 supports the eDiscovery process with guidance for governance and management. While all documents are written to be used by both technical and non-technical personnel, this standard aims at senior management levels within a company including those with requirements for regulatory and industry standards. It helps to advise on how to select and maintain ownership of risks related to eDiscovery. This usually involves developing as well as implementing the required policies in order to achieve internal and external compliance.

The DFRWS framework and ISO/IEC 27050 have been designed as general-purpose frameworks for ESI, the investigators must follow up revisions aimed at coping with advancement in technology or to meet the requirements of specific case studies. For instance, (Daryabar et al. 2017) argued that tailoring of existing models is required; the study developed a domain-specific cyber forensic investigation model for higher education institutes in which a policy was incorporated to address the capabilities and nature of this environment. Another study (Ma 2018) redefined the investigation phases as "classes", while actions within each class were defined as associated "elements". The authors then utilised Coloured Petri Net (CPN) modelling to represent the overall process. Furthermore, discussions in this area of research went beyond introducing a comprehensive or tailored framework to introducing loop-back activities were revisions were encouraged during the digital investigation life-cycle to confirm actions and achieve better reliability (Nakamoto 2008).

7.3.2 Integrating Blockchain Technology for Digital Investigation Models

To address the question of how Blockchain technology can help to achieve the aims of existing digital investigation models, we should consider a generic framework such as the DFRWS framework and the ISO/IEC 27050 standards. Figure 7.1 demonstrates the framework while incorporating knowledge management terms (Navarro-Ortiz et al. 2018) to discuss the integration of Blockchain technology.

The "identification" phase incorporates several actions including -but not limited to- incident detection, resolving file signatures, profile detection, anomaly detection, system monitoring, complains, and audit analysis. These actions are key enablers for the forensics process because there can be no case to investigate if no

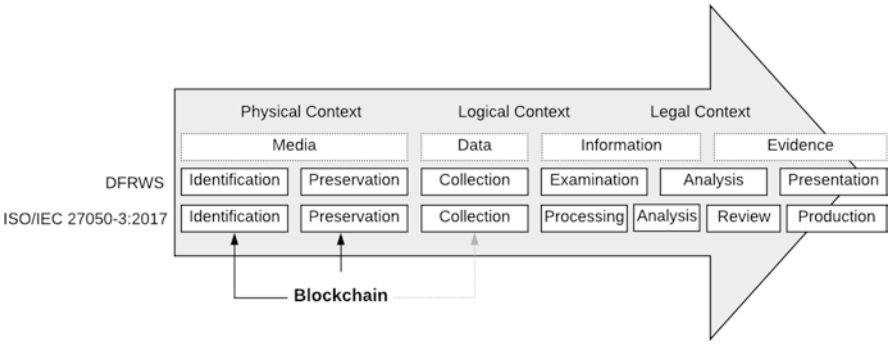

Fig. 7.1 The role of Blockchain as part of the wider digital investigation process can be realised by automating the "identification" and "preservation" phases

event was reported. While these actions seem to be contained within a physical context, at first sight, they are practically required to address all the legal requirements to satisfy a Court of Law in the case of a crime which is usually finalised during the "presentation" stage. Traditionally, this early logging of events will only be hashed during the data "preservation" phase following the creation of a forensic image, because systems -by default- are not forensic-friendly. However, Blockchain-based systems could introduce an automated implementation were all events are logged as part of a growing list of records (blocks). Each block contains a cryptographic hash of the previous block in addition to a timestamp. Hence, systems will be -by design- forensic-enabled. Both the "identification" and "preservation" phases are concerned with the media to be captured. The media in this context can contain an artefact of interest whether it is network traffic, volatile memory, physical storage or other forms of electronic data.

The "preservation" phase traditionally covers forensic imaging to create an identical electronic copy of the original, this image is then hashed. This is when a CoC is introduced and maintained per the ACPO guidelines. However, the introduction of Blockchain at an earlier phase provides opportunities such as:

Data Availability Records can be backed up and stored in several places, their integrity can always be verified separately -when needed- relying on the Blockchain.

Continuous Fraud Detection and Forensic Readiness The Blockchain can be used to automate processes, it introduces forensic readiness to systems, and several copies of the Blockchain exist in remote locations which reduced the risk of deletion.

Efficiency The maintenance of data integrity will not be time-consuming for the investigators.

Reliability Since records are already hashed as part of a trust-worthy automated process establishing a chain of blocks, there will be no risk to the investigation

related to the miscalculation of hashes. Traditionally, hashes are calculated several times when the crime scene is inspected.

Therefore, the "collection" phase in which forensically sound software and hardware tools are utilised can start immediately. As part of this phase, case-relevant artefacts and data remnants are extracted in preparation for the additional examination. Hence, the value of integrating Blockchain technology in digital investigation models can be seen in the automation of the "identification" and "preservation" phases, and to a degree, in the "collection" phase if the system is designed to store some of its critical data (e.g. identifiers) in the Blockchain directly. While Blockchain technology is not meant for data storage due to computational complexities, it is theoretically possible to store data on a Blockchain. These early phases in the investigation model are the core part to facilitate evidence presentation within the expected legal requirement which leads to the final legally-binding case decision.

To integrate the technology, one of the three high-level types of Blockchain implementations should be considered. A public Blockchain is shared in the wild (Internet) with no access restriction which means that any participant can send a transaction or act as a validator on a voluntary basis. The benefit of this approach (as seen with Bitcoin and Ethereum) is the existing evidence of popularity due to the included economic incentive given to volunteering participants. Another benefit is the devices ability to join and exit at any given time within predefined rules, this can be useful to provide integrity checks for a wide range of IoT devices acting as DWs without requiring infrastructure cost; there is no need for the vendors to maintain data centres or pay for system and network administrators. On the other hand, private Blockchains require registration and approval, a participant must first be invited by the network administrators, but transactions are relatively faster than public Blockchain networks. The key benefit of this approach would be the ability to maintain a CoC without exposing data to the public Internet, and the ability to know the identities of all participants. A hybrid approach is also possible with a consortium Blockchain in which several companies practising control, it is therefore permissioned and semi-decentralised. With regards to Digital Forensic Models, all the three types of Blockchain implementations can contribute to the creation of a digital CoC. Cryptography can be used to secure sensitive data sent to a public Blockchain making it a feasible option. Identifying a participating device from the network is not always required because the CoC starts from the device itself (DW) and is therefore known and linked to the Blockchain, not the other way around as demonstrated in Fig. 7.2. Furthermore, as the Blockchain technology is emerging, some argues that any non-public Blockchain implementation could suffer the fate of the Intranets in the 1990s when companies built their private capabilities within their perimeters. Then, Intranets became less popular with the advent of web-based services such as the Software-as-a-Service (SaaS) products.

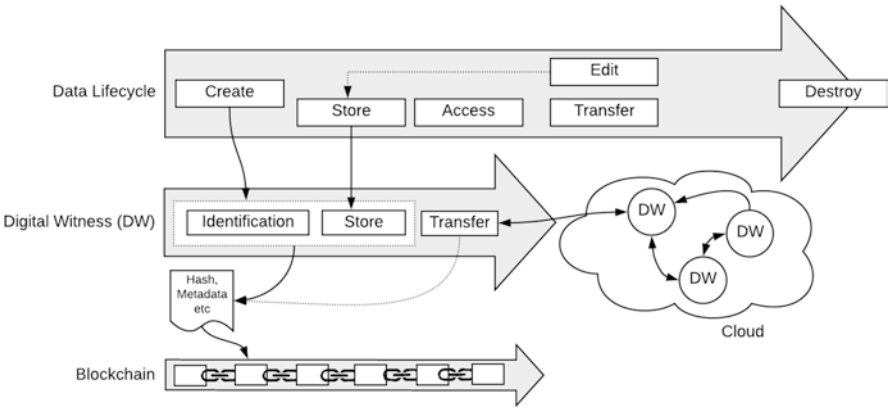

Fig. 7.2 The role of DW is to identify and preserve data. Data can be stored on the device or transferred to other devices (Hearsay DW) in the cloud. The Blockchain is utilised to initiate the Digital Chain-of-Custody (CoC) as early as when the data is created

Table 7.1 Excerpt sample worksheet from "Appendix: Resources" of the fundamental computer investigation guide for windows by microsoft corporation

Evidence description /number	Acquisition date	Acquisition location	Acquisition method	Acquired from	Acquired from (signature)	Storage location
	Transfer date	Transferred to (location)	Transfer reason	Now in custody of	Now in custody of (signature)	Storage location
Additional notes						

7.4 Towards a Blockchain-Based Digital Forensic Chain-of-Custody

Like fingerprints and DNA, the value of Digital Evidence in a crime scene. However, it is more fragile and easily lost if the investigators do not follow suitable precautions. In law, CoC documentation provides the required admissibility and proof of validity. Table 7.1 shows an excerpted sample from a worksheet designed to log the relevant details when investigating a computer, this CoC Log Documentation was developed and published by Microsoft as part of their Fundamental Computer Investigation Guide for Windows.

CoC logs vary in their design, they can be very detailed as a mean to remind investigators of all the required details to think about and write down. Others, however, are more adaptable to the real needs of the crime scene by requesting fundamental details valid for all cases while amending a space for additional notes. An example for the several questions to think about at the crime scene:

– Was the seized object intentionally hidden?
– Was the seized computer connected to a kill switch?

These questions are not valid for all scenarios but can be very critical crime scene notes and should be documented to support the investigation at a later stage. Therefore, a well-designed CoC log allows enough space and incorporates guidelines to enforce good systematic practice. A CoC within a legal context is defined as the sequence of documented actions performed during forensic investigations. This covers all the stages of the adopted investigation model from acquisition and seizure to the presentation of findings. Traditionally, the CoC is based on a paper trail. However, with the emergence of the alternative -digital- mediums the term "paper trail" could also describe other methods to maintain an audit. That said, a more inclusive term would be "audit trail". Overall, a CoC form serves the following functions:

- Identifies the evidence.
- Identifies who has handled the evidence
- Describe actions performed, or to be performed, on the evidence: control, transfer, analysis and disposition.
- Lists dates and times the evidence was handled.

The authenticity of each record in the CoC has a significant value to the investigation as it could be used to convict a suspect to a specific crime. Contamination of seized files would raise suspicions that certain events were fraudulently planted and would, therefore, disqualify the evidence. A CoC could also link a physical object (e.g. a memory disk) to an individual. In cases where the defendant claims no prior link to the seized object being investigated, the CoC is utilised by the prosecution to demonstrate that the object was in the possession of the defendant at the time of seizure. As a general role, the CoC must document every action and every evidence transfer between persons from -and as early as- evidence acquisition. It must be verifiable that no other persons could have altered -or accessed- that evidence. Therefore, to restrict access, the recommendation is to keep the number of transfers as low as possible.

The CoC is how the accountable law-enforcement officer is identified during the lifetime of the investigation. Several officers could take part due to separation of duties, hence a crime scene investigator will be named on the CoC to have the physical custody of the seized evidence, while other identifiable officers can be named afterword on succeeding transactions in chronological order. The required transactions metadata include timestamps and the signature of officers involved at each step, while examples of other metadata include the name of the law-enforcement agency, case number, date of receipt, date of report, in addition to a detailed descriptive list of related seized items with their serial numbers, make and models. Traditionally, this information is written as part of a "Bag and Tag" practice directly on the bag containing the evidence.

When the investigators are dealing with electronic evidence extracted from a live environment such as connected servers, or powered machines, the CoC plays a critical role to document actions. The known Locard exchange principle, also known as

Locard's theory, states that any contact between items will cause an exchange. In the digital realm, this translates into any contact between computers, a computer and a storage device or utilising an input device which includes moving the mouse to click on the screen. However, in the context of a live environment, there are many important artefacts residing in the computer's Physical Memory including but not limited to user credentials, running processes, DDLs, encryption keys, files, open sockets and Registry Keyes. Physical Memory is stored on RAM chips lined up in built-in notches on the motherboard. Therefore, the evidence acquisition stage is when a "Memory Dump" (byte-to-byte copy of the volatile memory) is taken at the crime scene before attempting to shutting down the device's operating system. The process of memory acquisition could mean running a command on the system to capture and store memory to a connected storage device, and while this conflicts with *Principle 1* of the ACPO guidelines as discussed earlier in Sect. 7.2.1, this requirement is addressed by *Principle 2* given that each action is fully and rationally documented with a satisfactory explanation on the CoC.

A digital CoC replaces the paper-based approach, it describes an electronic documentation of this process. Digital CoC can be convenient but more vulnerable to integrity attacks (data alteration), which puts the whole investigation at risk. The solution we discuss in this paper focuses on the utilisation of Blockchain to enable trust, integrity, authenticity, traceability, and verifiability. The attributes and components of a Digital CoC are described and discussed below:

A Distributed Ledger CoC records are distributed to a decentralised computing network system incorporating multiple sources or nodes to store and retrieve these records when needed.

Linked-Blocks To amend the Blockchain with a new CoC record to the ledger, it must include one reference signature (hash) from the previous record in the Blockchain. This way, all records have pointers to other records and are linked in a chronological order. If data in any block is changed (e.g. due to system failure or integrity attack), the hash (as a unique representation of the record) will also change resulting in a mismatch with the recorded reference hash in the consent block. This would break the chain and the overall system would, therefore, reject any altered block.

Network Nodes These are the participating computers. They form and support the distributed environment and perform the mining process to add or verify transactions.

Transactions A transaction in this use case is the process of adding a new CoC record. Adding a new transaction to a distributed interlinked ledger means that copies of the new record will be synchronised with the whole network. This global update indicates the system has no single-point-of-failure, which is an effective countermeasure against availability attacks.

The above can be used to define the Blockchain-based Digital CoC as a distributed ledger formed of blocks of electronically hashed evidence records that are linked together to establish a chain. Evidence records in this context relate to the process of handling acquired crime scene evidence from the time it is seized or collected until the time it is presented to a Court of Law. Nonetheless, the architecture of a Blockchain-based CoC whether for a standard implementation or to enable a CoC for DWs (more discussion in Sect. 7.5) will consist of the following main components:

Evidence Storage This is where the evidence is stored. Requirements could vary because physical evidence entails a special storage facility to avoid data alteration, while the options for electronic data could include the Cloud as a solution.

Digital CoC Enabled through the Blockchain as discussed earlier.

The Interface This component is responsible for enabling communications between all the users. It incorporates access control and evidence management; creating a new record, evidence state verification, and disposal of evidence.

7.5 Blockchain for Forensic-Enabled Electronic Systems: A Case Study in eHealth

Digital systems such as electronic documentation and reporting tools offer the healthcare sector both quality and the required utility to facilitate communication between permissioned stakeholders. Examples of regular stakeholders include healthcare providers, auditors, patients but also incident responders when an investigation is triggered. However, utilising technology without following appropriate guidelines raises serious concerns related to data integrity and compliance with local laws and regulations (Staats et al. 2017). Without measures to enforce documentation integrity and completeness, records cannot be trusted to provide a realistic reflection of the patient condition. There are also several legal issues since this type of data affects the patients' safety and quality of healthcare which leaves the organisation accountable for medical errors (Moffatt-Bruce et al. 2016).

Nonetheless, there are other reasons to extend the requirement beyond maintaining data integrity for the records separately. A CoC is a more appropriate means to create a verifiable series of events in the form of a story to support DFIR. A practical example showing the benefit of establishing a CoC can be demonstrated with Disease Management Programmes (DMP). Over the last two decades, several DMPs have been implemented worldwide in response to the escalating burden of chronic conditions. The implementation of DMPs was an attempt to improve the

quality of care for selected chronic conditions that are influenced by lifestyle and behaviour change (Alhaboby et al. 2018). These programs came in different designs and evaluation techniques to deliver a variety of interventions tailored to pre-defined case studies. DMPs can be delivered through a web-based disease management solution. However, studies show evidence that people with long-term conditions and disabilities are frequently labelled as vulnerable, and commonly victimised online. While those victimised patients require instrumental support via DMPs to understand their conditions and empower them to manage their own treatment in everyday life, additional short and long-term consequences related to cyber-victimisation could intensify existing psychological and health complications. For instance, 'distress' as a commonly reported impact of cyber-victimisation could theoretically lead to neurohormonal changes in the blood, increasing cortisol, catecholamine and insulin secretion resulting in increased blood glucose, heartbeat, blood pressure, urination and other changes (Alhaboby et al. 2016). Preserving an admissible evidence for the above requires a connected Forensic-enabled system to be in place. This would then help patients to request help, provide sufficient information to what they go through, and support a legal action to mitigate against cyber-victimisation. A summary of threats and opportunities for this case study would therefore be:

1. Non-adherence to self-management planning is a major instability factor, while DMPs and Online Coaching Programmes are cornerstones to support the stability of long-term self-management for people with long-term conditions.
2. Likewise, we argue the inverse correlation on stability between the impact of cyber-victimisation versus the ability to forensically document all submitted data for such incidents.

The benefit of developing forensic-enabled DMPs introduces many opportunities; Firstly, it gives the victims, or a third-party acting on their behalf, the advantage of supporting a legal action against an attacker to address the source of the problem (Alhaboby et al. 2018). A recent study (al-Khateeb et al. 2017) provides evidence that that victims of cyberstalking accept the idea of third-party intervention as a response to threats. The study also shows that victims seek help from the independent anti-cyberstalking organisations and the Police. In law, preserved incriminating material (e.g. breaking the Protection from Harassment Act 1997 in the UK) supported by a documented incident log in the form of a CoC can be admissible to a Court of Law. Secondly, this information could be sufficient to reduce the time required to recover the identity of the attacker. Thirdly, the evidence could be utilised to support the victim's eligibility for extended instrumental support from national health services. Finally, this level of automation in the documentation process offers an opportunity to implement more accurate methods to assess the risk associated with victimisation attacks.

7.6 Blockchain to Enable Digital Witnesses

7.6.1 Exploiting the Widespread of IoT Devices

The Internet of Things (IoT) is the interconnected network of standard devices such as laptops and smartphones, and non-standard devices such as moving vehicles, software applications, connected fridges (all home appliances), and virtually any connected object. A significant part of this phenomenon is focusing on consumer applications. Smart Homes, as an example, raises many legitimate concerns related to data privacy (Risteska Stojkoska and Trivodaliev 2017) but as the technology emerges further it covers more aspects of our daily living. Our cyber-physical interactions can also be captures by IoT sensors within a connected car, a plane, or via a mobile phone, or digital watch. There are IoT applications to support agriculture, transportation, healthcare, environment and energy management. Holistic frameworks are being proposed (Risteska Stojkoska and Trivodaliev 2017) to incorporate the components of various IoT architectures within a single management model. This type of research towards extending the interoperability (Wan et al. 2014) between IoT devices could be utilised to facilitate further collaboration, in our case, to collaborate on providing event-related evidence within their sensing capabilities.

7.6.2 The Role of a Witness

Rather than discussing the challenges introduced by IoT, in this section, we look at an opportunity provided by this complicated network of devices to facilitate potential witnesses for DFIR. In law, the role of a witness is fundamental, and testimony is a form of evidence obtained from a witness who makes a statement to declare a fact (Smith and Bace 2002). A witness claims to have direct knowledge or information related to the case being considered in court. Witness testimony can be oral or written and is accepted after an oath. Additionally, having an incident witnessed by more than one person increases the validity and assertion that it was a true event. Furthermore, when the witness uses one of their senses (e.g. seeing, hearing, smelling) then they are called “eyewitness”, this is in contrary to hearsay, which is to testify that the information was perceived indirectly. For example, it could have been written or said by someone else. Technology could also be utilised, and it is important to note that the use of science and technology by means of an instrument (e.g. microphone) to aid the perception of a human sense is acceptable and is not considered hearsay. At times, the information could initially be captured by an instrument (e.g. recorded in a log by a computer system), in this case, an independent Expert Witness must analyse this electronic data to present the evidence to a Court of Law. In the case of IoT, we argue that IoT devices can act as DWs to provide affirmation towards events related to a crime scene within their sensing

capabilities (Nieto et al. 2016). However, a CoC must be maintained for any data generated by these IoT devices to be admissible, and further work in this area is required to standardise the requirements to be met before an IoT device can qualify for the role of a DW.

7.6.3 IoT Devices as Digital Witnesses

The data lifecycle is the sequence of phases data go through from the initial creation until it is finally deleted (Abuosba 2015). Data can be generated from a manual human entry, collected from an external source or captured from the environment (signal reception or sensor data). Through this journey, data could be edited to recreate new data units, or viewed and archived. Data transfer occurs when data units are copied across communication channels. Data, including data remnants, can be used as Digital Evidence and is therefore very important to the digital investigation process if put within the right context for analysis. In the case of forensic acquisition at a crime scene, data, and the medium storing the data are covered by the "identification" and "preservation" stages of the eDiscovery process as demonstrated in Fig. 7.1. The earlier discussion also covered how Blockchain can be utilised to preserve data at these two stages. Therefore, for an IoT device to comply with this process it should first be able to identify records of interest, to log this data (for short or long term), and to transfer the logs to the network system as demonstrated in Fig. 7.2.

Some IoT devices are supported by a data storage facility. For example, CCTV (Closed-circuit Television) are usually configured to stream their recordings or store them locally. However, IoT sensors and actuators require support from additional resources to process and store data. Other applications such as Connected Cars (CC) could include cameras, low-powered sensors and internal storage, but a CC system would still transfer data to the network as an attempt to avoid Denial-of-Service (DoS) attacks or because the internal storage cannot cope with the rate at which new data is generated in the long run. In Fig. 7.3, we show that a DW should have the ability to process and log newly captured data to a Blockchain, but it does not have to store data for a long time, instead, a DW could pass it through to a cloud-based network. A forensic investigator could then acquire a copy from what we call a "Hearsay DW" device. Integrity and authenticity checks can be performed using the hashes and metadata submitted to the Blockchain as part of a digital CoC.

Additionally, IoT devices which are not resource-constraint could provide many other artefacts to contribute to the value or the admissibility of the Digital Evidence as explained below.

Device-Related Identifiers Capturing values such as Device ID, Build No and Kernel version helps to identify the device from which the evidence was captured.

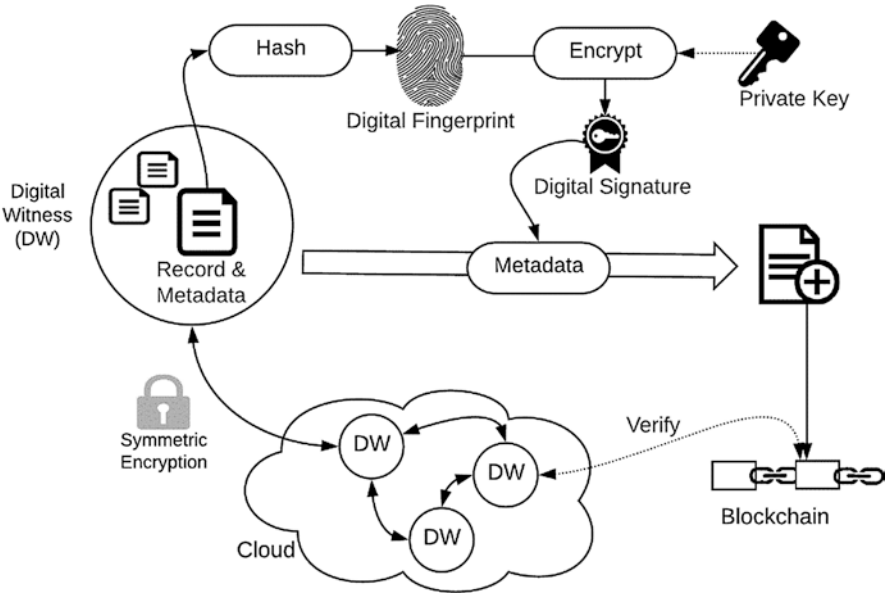

Fig. 7.3 In a DW scenario, data can be identified, signed and sent to one or several Hearsay DW for backup. The cloud can be utilised to facilitate data availability. Metadata is signed by the IoT device private Key to maintaining authenticity

Location Indicators GPS coordinates, connected Wi-Fi and Network Operator data can be invaluable to recover the location of an incident captured by a nearby DW.

Time-Related File system timestamps show the time when each file was created, accessed and modified.

Security Indicators Devices should be designed to self-report any integrity check concerns related to their internal workings of the DW itself. This can be the outcome of misconfiguration or a Malware infection (Irshad et al. 2018).

Integrity Checks Captured data must be hashed to maintain the integrity of the file at the time of acquisition or submission. Multiple hashes are recommended to avoid errors within this process. Examples of hash functions currently used include MD5, SHA-1, SHA-512 and SHA-256.

The Digital Evidence in traditional cases is documented by a qualified Digital Investigator. This is a typical admissibility requirement included within guidelines such as the principles published by the Association of Chief Police Officers (ACPO) in the UK. Therefore, for forensic readiness to be maintained, the software should automate the process of data acquisition with reference to these principles, and the software code should go through a review process to meet the reliability requirement with reference to standards (e.g. the Daubert standard).

7.7 Conclusions

Blockchain has shown its potential to support computer systems with a tamper-proof series of timestamps making it a suitable facilitator to establish a strong digitalised Chain-of-Custody (CoC). The distributed nature of the technology makes it resistant to various cyber-attacks against the availability and integrity of its data. These advantages are most suitable for DFIR to develop new approaches in the fight against cybercrime. We have explored and discussed various implementations making Blockchain very useful to digital investigators. Additionally, we have reviewed how the digital investigation and eDiscovery models have emerged over time, this was important to demonstrate how Blockchain could effectively support an innovative deployment for the "identification" and "preservation" phases of this process. Thereafter, the concept of Digital Witnesses (DWs) was introduced to show how we can exploit IoT devices to automate the identification and preservation of Digital Evidence. The aim was to cover incidents as they happen from several angels (this would depend on the number and nature of available DWs). To qualify as DW, IoT devices should have solid security features such as an embedded Trusted Computing Hardware to periodically verify its integrity.

In conclusion, IoT extends the Internet beyond standard devices to include appliances we have at home, vehicles we use to travel, and wearable devices such as watches and digital trackers. This introduces various challenges on top of which is privacy implications. However, privacy and DFIR are two confronting disciplines. Therefore, in this work, we look at the opportunities provided by the increasing number of IoT devices. Particularly, we looked at a new approach where a Blockchain-based Chain-of-Custody can be established at the same time pre-identified data (data of interest) is generated by an IoT device. The data of interest can be about the device itself, other IoT devices or the environment around. This will provide a new level of forensic readiness. That said, more work is needed in this area to cover topics including but not limited to data governance, standardisation of DW admissibility, and the trade-off between DW and user privacy.

References

Abuosba K (2015) Formalizing big data processing lifecycles: acquisition, serialization, aggregation, analysis, mining, knowledge representation, and information dissemination. 2015 international conference and workshop on computing and communication (IEMCON), pp 1–4. https://doi.org/10.1109/IEMCON.2015.7344533

Alhaboby ZA, Al-Khateeb HM, Barnes J, Short E (2016) The language is disgusting and they refer to my disability: the cyberharassment of disabled people. Disabil Soc 31(8):1138–1143. https://doi.org/10.1080/09687599.2016.1235313

Alhaboby ZA, Alhaboby D, Al-Khateeb HM, Epiphaniou G, Ismail DKB, Jahankhani H, Pillai P (2018) Understanding the cyber-victimisation of people with long term conditions and the need for collaborative forensics-enabled disease management programmes. In: Jahankhani H (ed)

Cyber criminology. Advanced sciences and technologies for security applications. Springer, Cham

al-Khateeb HM, Epiphaniou G, Alhaboby ZA, Barnes J, Short E (2017) Cyberstalking: investigating formal intervention and the role of corporate social responsibility. Telematics Inform 34(4):339–349. https://doi.org/10.1016/j.tele.2016.08.016

Cocco L, Pinna A, Marchesi M (2017) Banking on Blockchain: costs savings thanks to the Blockchain technology. Futur Internet 9(3):25

Daryabar F, Dehghantanha A, Choo K-KR (2017) Cloud storage forensics: MEGA as a case study. Aust J Forensic Sci 49(3):344–357. https://doi.org/10.1080/00450618.2016.1153714

Irshad M, Al-Khateeb HM, Mansour A, Ashawa M, Hamisu M (2018) Effective methods to detect metamorphic malware: a systematic review. Int J Electron Secur Digit Forensics 10(2):138–154. https://doi.org/10.1504/ijesdf.2018.090948

Johng H, Kim D, Hill T, Chung L (2018) Using Blockchain to enhance the trustworthiness of business processes: a goal-oriented approach. 2018 IEEE international conference on services computing (SCC), pp 249–252. https://doi.org/10.1109/SCC.2018.00041

Ma A (2018) Thousands of people in Sweden are embedding microchips under their skin to replace ID cards. http://uk.businessinsider.com/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5?r=US&IR=T

Mengelkamp E, Notheisen B, Beer C, Dauer D, Weinhardt C (2018) A Blockchain-based smart grid: towards sustainable local energy markets. Comput Sci Res Dev 33(1):207–214. https://doi.org/10.1007/s00450-017-0360-9

Moffatt-Bruce SD, Ferdinand FD, Fann JI (2016) Patient safety: disclosure of medical errors and risk mitigation. Ann Thorac Surg 102(2):358–362. https://doi.org/10.1016/j.athoracsur.2016.06.033

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Navarro-Ortiz J, Sendra S, Ameigeiras P, Lopez-Soler JM (2018) Integration of LoRaWAN and 4G/5G for the industrial internet of things. IEEE Commun Mag 56(2):60–67. https://doi.org/10.1109/MCOM.2018.1700625

Nieto A, Roman R, Lopez J (2016) Digital witness: safeguarding digital evidence by using secure architectures in personal devices. IEEE Netw 30(6):34–41. https://doi.org/10.1109/MNET.2016.1600087NM

Pollitt M (2010) A history of digital forensics. In: Advances in digital forensics VI. Springer, Berlin/Heidelberg, pp 3–15. https://doi.org/10.1007/978-3-642-15506-2_1

Risteska Stojkoska BL, Trivodaliev KV (2017) A review of internet of things for smart home: challenges and solutions. J Clean Prod 140:1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006

Smith FC, Bace RG (2002) A guide to forensic testimony: the art and practice of presenting testimony as an expert technical witness. Pearson Education

Staats BR, Dai H, Hofmann D, Milkman KL (2017) Motivating process compliance through individual electronic monitoring: an empirical examination of hand hygiene in healthcare. Manag Sci 63(5):1563–1585. https://doi.org/10.1287/mnsc.2015.2400

U.S. Department of Homeland Security – United States Secret Service (2015) Best practices for seizing electronic evidence: a pocket guide for first responders

Wan J, Zou C, Zhou K, Lu R, Li D (2014) IoT sensing framework with inter-cloud computing capability in vehicular networking. Electron Commer Res 14(3):389–416. https://doi.org/10.1007/s10660-014-9147-2

Williams J (2012) ACPO good practice guide for digital evidence. Metropolitan Police Service, Association of chief police officers, GB

Chapter 8
The Standardised Digital Forensic Investigation Process Model (SDFIPM)

Reza Montasari, Richard Hill, Victoria Carpenter, and Amin Hosseinian-Far

Abstract The field of digital forensics still lacks formal process models that courts can employ to determine the reliability of the process followed in a digital investigation. The existing models have often been developed by digital forensic practitioners, based on their own personal experience and on an ad-hoc basis, without attention to the establishment of standardisation within the field. This has prevented the institution of the formal processes that are urgently required. Moreover, as digital forensic investigators often operate within different fields of law enforcement, commerce and incident response, the existing models have often tended to focus on one particular field and have failed to consider all the environments. This has hindered the development of a generic model that can be applied in all the three stated fields of digital forensics. To address these shortcomings, this chapter makes a novel contribution by proposing the Advanced Investigative Process Model (the SDFIPM) for Conducting Digital Forensic Investigations, encompassing the 'middle part' of the digital investigative process, which is formal in that it synthesizes, harmonises and extends the existing models, and which is generic in that it can be applied in the three fields of law enforcement, commerce and incident response.

Keywords Digital forensics · Standardised digital forensic investigation process model · Survey digital crime scene phase · Digital forensics investigation · DFI · DFA · Event reconstruction process · UML · Unified modelling language · Chain of custody · Information flow · Case management

R. Montasari (✉) · R. Hill
Department of Computer Science School of Computing and Engineering,
The University of Huddersfield, Huddersfield, UK
e-mail: R.Montasari@hud.ac.uk; R.Hill@hud.ac.uk

V. Carpenter
Research Development Innovation and Enterprise Services, University of Bedfordshire,
Luton, UK
e-mail: Victoria.Carpenter@beds.ac.uk

A. Hosseinian-Far
Faculty of Business and Law, University of Northampton, Northampton, UK
e-mail: Amin.Hosseinian-Far@northampton.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_8

8.1 Introduction

A digital forensic investigator might discover significant and incriminating evidence, but if they cannot present the evidence in a coherent and understandable way to the lay audience (such as judge and jury), the case may be lost (Sherman 2006; Montasari 2017a). The complexity of tools and methodologies used to perform a digital investigative process requires investigators to be able to explain the process in a manner that a judge and jury can understand it (Kessler 2010). Such tools and methodologies must also adhere to some standards of practice and be accepted by other investigators operating in the field (Kessler 2010; Adams 2012; Armstrong and Armstrong 2010). Nevertheless, the field of digital forensics still lacks both consensus and formal process models that the courts can employ to determine the reliability of the digital evidence presented to them (Kessler 2010; Adams 2012; Armstrong and Armstrong 2010; Montasari 2016a, b, c, d, e, 2017a, b, c, 2018; Montasari et al. 2015; Valjarevic and Venter 2015; Kohn et al. 2013; US-CERT 2012; Agarwal et al. 2011). The absence of agreements associated with DFIPMs has been widely acknowledged also by other researchers (Montasari 2016a, b, 2017b, c, 2018; Montasari et al. 2015; Valjarevic and Venter 2015; Kohn et al. 2013; Agarwal et al. 2011; Rogers et al. 2006). Zainudin et al. (2011) state that one of the most significant problems encountered by digital forensic investigators is the absence of standardisation in the field of digital forensics.

Casey (2011) argues that the development of a formal process model enables a complete, rigorous investigation, ensures proper evidence handling and reduces the chances of mistakes created by preconceived theories, time pressures, and other potential pitfalls (Casey 2011). Similarly, Valjarevic and Venter (Valjarevic and Venter 2015) state that conducting a digital forensic investigation requires a formalized process model, arguing, "There is currently neither an international standard nor does a global, harmonized DFI process (DFIP) exist". Authors in Montasari et al. (2015) and Valjarevic and Venter (2015) suggest the concept of a widely agreed-upon process model to harmonise the practice of digital forensics. However, despite many calls to bring formalisation to DFIPMs, a solution has not yet been provided (Montasari 2016a, b, d, 2017b, 2018; Montasari et al. 2015; Valjarevic and Venter 2015; Kohn et al. 2013; Cohen 2012). Many researchers acknowledge the limited progress, if any, in defining and improving a formal digital forensic process since the DFRWS held in 2001 (Montasari 2016a, b; Montasari et al. 2015; Agarwal et al. 2011; Trcek et al. 2010; Cohen 2011; Nance et al. 2009).

The existing models have often been developed by digital forensic investigators (DFIs) based on their own personal experience on an ad hoc basis without consideration to establish standardisation within the field (Valjarevic and Venter 2015). This has prevented the establishment of formal processes that are urgently needed by courts of law (Montasari 2016a; Montasari et al. 2015). In many cases, DFIs employ ad hoc tools (Agarwal et al. 2011; Bulbul et al. 2013; Grobler et al. 2010; Ieong 2006; Stanfield 2009) to carry out digital investigations. Therefore, many researchers are increasingly calling for scientific approaches and formal methods

for describing the digital investigation processes (Cohen 2012; Carlton and Worthley 2009; Garfinkel et al. 2009; Pollitt 2008; Leigland and Krings 2004). Furthermore, the existing models often tend to focus on one area of digital forensics and neglect the other areas. This has hindered the development of a generic model that can be applied in both law enforcement and corporate investigations (Montasari 2016a, b, 2018). The adoption of ad-hoc approaches in developing previous models has led to a variety of process models with conflicting stages, activities and terminology, which in turn has prevented the establishment of the formal processes urgently needed by courts and investigators alike (Montasari et al. 2015; Agarwal et al. 2011).

8.1.1 Research Problem and Contributions

The foregoing considerations lead to the following research problem:

> *There does not exist a comprehensive model encompassing the entire digital investigative process that is formal, such that it can assist a court of law in determining the reliability of the investigative process followed, and that is generic, in that it can be applied in the different fields of law enforcement, commerce and incident response.*

Therefore, the SDFIPM was designed and developed as the middle part (i.e. the Investigative Processes Class) of a larger, comprehensive model, the Comprehensive Digital Forensic Investigation Process Model for Digital Forensic Practice, presented in (Montasari 2016a), in order to contribute towards addressing the aforementioned short-comings. The SDFIPM is formal in that it synthesises, harmonises and extends the existing models, and is generic in that it can be applied in the three fields of law enforcement, commerce and incident response. Moreover, we also propose a set of overriding principles included in the model that DFIs will need to employ during the investigative process in order to maximise the chances of the admissibility of digital evidence in a court of law. By implementing the SDFIPM and its Overriding Principles, this model will be of a great value to both DFIs and courts of law alike.

Note that in the context of this research study, the term ‘formal’ is not equivalent to the same term employed in the domains of Mathematics and Computer Science, in which the word ‘formal’ is used to refer to a set of strings of symbols that might be constrained by rules that are specific to it. In contrast, for the purposes of this study, the term ‘formal’ has been employed to refer to the UML Activity Diagrams, scientific methods, standards of practice, consistency, structure, agreed-upon components and terminology, harmonisation, and the unified approach that have been brought to the proposed model, the SDFIPM.

8.1.2 Authors' Note

Prior to the design and development of the CDFIPM (Montasari 2016a), of which the SDFIPM is the middle part of, all the prominent digital forensic investigation process models (DFIPMs) presented to date were critically reviewed. These models were then assessed against three different sets of assessment criteria, including: the Daubert Test (Farrell 1993) Five-Point Requirement, Carrier and Spafford (Carrier and Spafford 2003) Five-Point Requirement and Beebe and Clark (Beebe and Clark 2005) Four-Point Requirement. The aim of this critical review was to gain an in-depth insight into these models and identify which could contribute to our proposed model. Since law enforcement, commerce and incident response were the three environments on which this study focused, the existing models within those three domains which most closely met the assessment criteria were considered for their possible contributions to the new model. Such an approach is considered important by other researchers (Kohn et al. 2013; Cohen 2010, 2012) as any model institutionalized through subsequent intellectual discourse and practical use must take into account other researchers' perspectives, approaches and "vernacular".

In order to assess the previous models against the three sets of assessment criteria, each model was given three sets of scores in accordance with the three sets of assessment criteria. Models were scored according to how many of the requirements were met for each particular set of criteria. This method of assessing the previous DFIPMs against 'three' different criteria is another novel contribution of this research in the field of digital forensic science. It should be noted that Carrier and Spafford's (2003) five-point requirements have also been used by Beebe and Clark (2005), against which they assess their own model (even though they do not provide scores). Likewise, Adams (2012) uses both Carrier and Spafford's (2003) five-point requirements as well as the Daubert Test's five-point requirements against which he evaluates the previous DFIPMs. However, we have built upon the previous initiatives in five different ways. First, we included Beebe and Clark's (2005) four-point requirements, which to our best knowledge have not been previously used by any other researchers as an assessment method against which the exiting DFIPMs are evaluated. Second, we have approached the review and assessment of the previous models differently. For instance, the scores that we have given each model based on the three sets of assessment criteria might be completely different from those given by Adams (2012) based on the two sets of assessment criteria they have used. Third, contrary to Adams questioning the reliability of the Daubert Test in assessing the previous models, we have demonstrated that the Daubert Test is in fact effective in judging the previous DFIPMs. Fourth, we have analysed the most up-to-date models (in addition to the older ones) up to 2014 including Adam's own model presented both in Adams (2012) and Adams et al. (2014). Fifth, we have assessed our own model, the CDFIPM, the evaluation of which will be presented in an upcoming study, against the three sets of assessment criteria.

The results of our critical review of the previous DFIPMs have been presented in our previous studies such as in (Montasari 2016a, e, 2018; Montasari et al. 2015).

Therefore, since this research chapter builds upon our previous studies, we have borrowed some information in the Introduction and Background Sections of this chapter from those studies, with references being made to those past studies.

8.1.3 Structure of the Chapter

The remainder of the chapter is structured as follows: Sect. 8.2 presents the research background. Section 8.3 presents the literature review while Sect. 8.4 provides the methodology employed to conduct the research presented in this chapter. The proposed model is presented in Sect. 5, followed by the description of the SDFIPM's overriding principles in Sect. 5. Finally, the chapter is concluded in Sect. 6.

8.2 Literature Review

Based upon our notes in the Sect. 8.1.2, this section provides a short summary in relation to our critical review of the previous DFIPMs. As Table 8.1 clearly demonstrates, existing DFIPMs display significant disparities in terms of the number of phases, scope and the specific domains that they have been developed for.

The result of this review revealed a gap that there does not exist a comprehensive model for digital forensic investigations that can be widely accepted by the digital forensic community and courts of the law. The previous models have often been criticised for being too specific (Carrier and Spafford 2003; Reith et al. 2002) too high level (Beebe and Clark 2005), too broad (Rogers et al. 2006), too technical (Venter 2006) and too complex (Selamat et al. 2008). These models are considered to be ad hoc tools as opposed to formal models (Agarwal et al. 2011; Trcek et al. 2010; Cohen 2011, 2012; Bulbul et al. 2013; Beebe and Clark 2005; Reith et al. 2002; Turnbull 2008; Ciardhuáin 2004; Karyda and Mitrou 2007; Baryamureeba and Tushabe 2004).

Presenting the review and assessment of these models is outside the scope of this chapter. The reader, instead, is encouraged to refer to the studies presented in (Montasari 2016a, b, c, e, 2018; Montasari et al. 2015) to consult this review.

As shown in the next table (Table 8.2), assessing the previous models against the Beebe and Clark (2005) criteria reveal that there are five models that meet three of the four criteria, while six and five models fulfil two and one out of the four criteria respectively. There are also three models that meet no criteria, while there is one model to which the assessment criteria are not applicable. Similarly, comparing the previous models against the Carrier and Spafford (2003) criteria reveals that there is one model that fulfils all the five criteria, while there are four other models that meet four of the criteria. There are also four, seven and three models that meet three, two and one out of the five criteria respectively, while there is one model to which the assessment criteria are not applicable. In relation to the Daubert Test (Farrell 1993),

Table 8.1 The comparative summary of the existing DFIPMs

The comparative summary of the DFIPMs																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Readiness				✓	✓		✓	✓				✓							✓	
Deployment				✓			✓	✓											✓	
Policy/ Procedure										✓		✓							✓	
Operational readiness				✓			✓					✓							✓	
Infrastructure readiness				✓			✓					✓							✓	
Incident detection (Awareness)			✓	✓	✓	✓						✓						✓	✓	
Report incident (Notification)				✓	✓	✓		✓		✓				✓					✓	
Assess incident.								✓					✓						✓	
Confirm incident.				✓	✓		✓						✓	✓					✓	
Authorisation				✓	✓	✓	✓			✓		✓	✓	✓			✓	✓	✓	✓
Incident response				✓			✓	✓	✓			✓						✓		
Planning (Approach strategy)			✓			✓		✓		✓	✓	✓	✓	✓			✓	✓	✓	✓

Understand task requirements																				✓
Determine overall picture																				✓
Determine required outcomes																				✓
Determine parameters																				✓
Consider physical constraint																				✓
Consider timing constraint																				✓
Consider data constraint																				✓
Plan logistics																				✓
Create outline plan																	✓			✓
Preparation			✓					✓		✓							✓	✓		
Attend site											✓						✓			✓
Securing the scene			✓					✓									✓			
Address safety issues																	✓			✓

(continued)

Table 8.1 (continued)

The comparative summary of the DFIPMs																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Communication shielding																	✓			
Triage											✓									
Examine user usage profiles											✓									
Examine chronology timeline											✓									
Examine browsing activities									✓		✓									
Case specifics											✓									
Carry out preliminary survey																				✓
Documentation of scene				✓		✓		✓									✓	✓		✓
Update outline plan																	✓			✓
Search				✓	✓	✓	✓	✓		✓							✓		✓	
Survey				✓	✓		✓	✓									✓			
Identification	✓					✓		✓	✓	✓					✓		✓	✓		

Preservation	✓		✓	✓	✓		✓	✓							✓	✓	✓		✓	
Collection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓
Volatile evidence collection									✓			✓					✓			
Non-volatile evidence collection									✓			✓								
Authenticate																			✓	
Seizure								✓											✓	✓
Package																	✓			✓
Transport						✓				✓					✓		✓	✓	✓	✓
Storage						✓				✓					✓		✓	✓	✓	✓
Examination	✓		✓	✓		✓		✓	✓	✓			✓		✓		✓		✓	
Harvest								✓				✓							✓	
Reduce								✓				✓							✓	
Identify				✓															✓	
Classify																			✓	
Organise												✓							✓	
Compare																			✓	
Analysis	✓		✓	✓				✓	✓	✓			✓		✓	✓	✓	✓	✓	
Attribute															✓				✓	
Evaluate																			✓	
Hypothesis						✓													✓	
Interpretation															✓				✓	
Reconstruction				✓	✓		✓	✓				✓			✓				✓	

(continued)

Table 8.1 (continued)

The comparative summary of the DFIPMs																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Reporting		✓		✓				✓	✓			✓		✓			✓			
Presentation	✓		✓	✓	✓	✓	✓	✓		✓			✓		✓	✓	✓	✓	✓	
Proof/Defence						✓		✓		✓										
Decision	✓							✓											✓	
Review				✓	✓		✓	✓									✓		✓	
Dissemination						✓		✓											✓	
Returning Evidence			✓					✓					✓							✓
Digital crime scene investigation				✓	✓		✓	✓												
Physical crime scene investigation				✓	✓		✓											✓	✓	
Documentation				✓	✓	✓	✓	✓					✓					✓	✓	✓
Preserving chain of custody						✓	✓					✓								✓
Preserving digital evidence						✓		✓										✓		
Information flow						✓												✓		
Case management						✓							✓							

Table 8.2 Scores obtained by the previous models based on the three assessment criteria

Models	Scores		
	Beebe and Clark	Carrier and Spafford	Daubert Test
A Framework for Digital Forensic Science (Palmer 2001)	2	2	1
Electronic Crime Scene Investigation: A Guide for First Responders (Ashcroft 2001)	1	2	0
Abstract Digital Forensic Model (Reith et al. 2002)	2	4	1
Integrated Digital Investigation Process (Carrier and Spafford 2003)	3	4	2
Digital Crime Scene Analysis (Rogers 2004)	3	4	2
Enhanced Digital Investigation Process Model (Baryamureeba and Tushabe 2004)	0	1	1
An Extended Model of Cybercrime Investigation (Ciardhuáin 2004)	3	5	3
Hierarchical, Objectives Based Framework for the Digital Investigation Process (Beebe and Clark 2005)	3	3	2
Four Step Forensic Process (Kent et al. 2006)	2	3	0
Computer Forensics Field Triage Process Model (Rogers et al. 2006)	3	4	4
Framework for a Digital Forensic Investigation (Kohn et al. 2006)	2	3	1
A Common Process Model for Incident Response and Computer Forensics (Freiling and Schwittay 2007)	0	2	1
Two Dimensional Evidence Reliability Amplification Process Model (Khatir et al. 2008)	1	1	1
Mapping Process of Digital Forensic Investigation Framework (Selamat et al. 2008)	0	1	1
Digital Forensic Process Model (Cohen 2009)	2	2	1
Generic Computer Forensics Investigation Model (Yusoff et al. 2011)	N/A	N/A	N/A
Systematic Digital Forensic Investigation Model (Agarwal et al. 2011)	1	2	1
Harmonised Digital Forensic Investigation Process Model (Valjarevic and Venter 2012)	1	2	1
Integrated Digital Forensic Process Model (Kohn et al. 2013)	2	2	1
The Advanced Data Acquisition Process Model (Adams et al. 2014)	2	3	2

there are two models that fulfil four and three of the five criteria respectively, while three models meet two of the criteria. There are also twelve and two models that meet one and no criteria respectively, while there is one model to which the assessment criteria are not applicable.

Analysing the results of the Beebe and Clark (2005), Carrier and Spafford (2003) and the Daubert Test (Farrell 1993) criteria applied to each of the models identified those that include the components suggested by the three aforementioned criteria as necessary for a DFIPM. In total, there were eight models that were selected for their

possible contributions to the CDFIPM based on their high scores achieved in relation to meeting the three sets of the assessment criteria.

8.3 Overview of the Investigative Process Model

The SDFIPM, which is considered to be a "class" and the middle part of the larger model CDFIPM (presented in its entirety in our upcoming study, has been designed using a top-down approach in order to enable digital forensic investigators to gain a better insight into its compositional components, namely Processes, Phases, Sub-Phases and Overriding Principles. There are 7 processes contained within the SDFIPM, each of which contains a different number of Phases. Apart the Overriding Principles, i.e. Concurrent Processes, which do not provide lower-level details, the remainder of the Processes provide additional lower layers of details, i.e. Phases and Sub-Phases. The SDFIPM will be initially presented in its abstract level, prior to being refined with more details that make up the model's lowest-level structure. Figure 8.1 represents the first instance of the formal representation of the SDFIPM

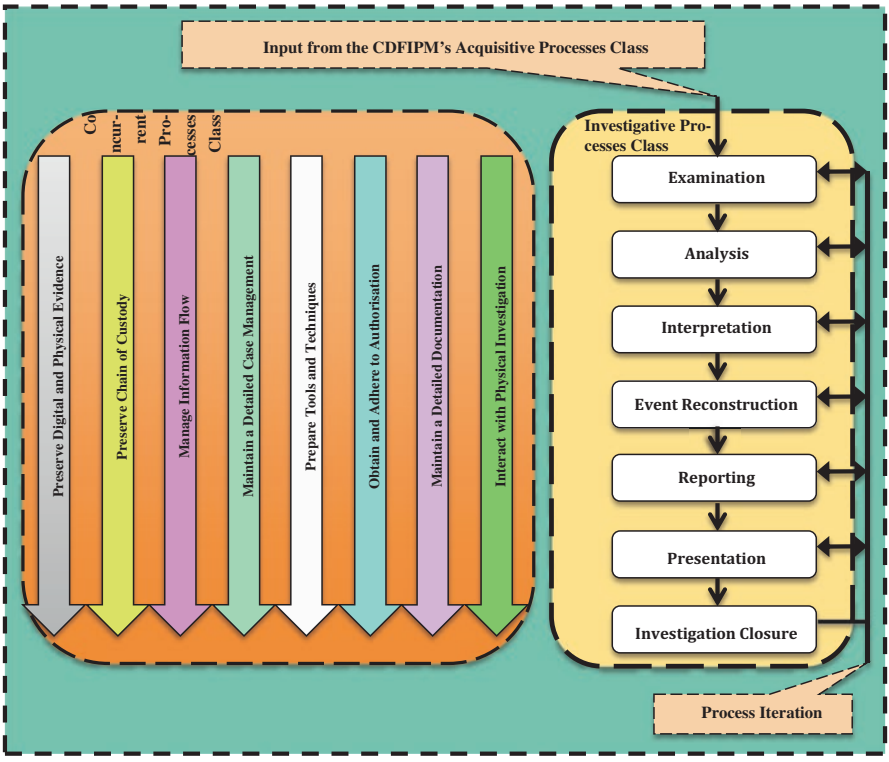

Fig. 8.1 The UML activity diagram of investigative class processes in their abstract level

in its abstract level, containing the first layers of the SDFIPM, namely Processes. Following this abstract representation, each process of the SDFIPM, containing second and third layer details, i.e. Phases and Sub-Phases, will then be represented by a UML Activity Diagram. The combination of all UML Activity Diagrams depicted in Figs. 8.2, 8.3, 8.4, 8.5, 8.6, 8.7 and 8.8 makes up the entire SDFIPM. Each Process will be subsequently discussed under their associated main headings.

8.3.1 Examination Process

The largest amount of investigation time is spent on the Examination Process as well as the Analysis Process (discussed later). During this Process, a large number of techniques need to be used in order to access, find and extract the acquired data representing the potential digital evidence into a human-readable format. Authors of many of the existing DFIPMs such as Carrier and Spafford (2003) state that there should be one single Phase assigned to the Examination and Analysis activities. They argue that these Phases can be confusing as their meaning is only slightly different, and it is common to have two investigators who are referring to the same tasks when they say that they are "analyzing a system" or "examining a system".

This argument is invalid on the basis that the Examination and Analysis stages have different aims and therefore should be assigned two separate Processes. The Examination Phase should involve activities regarding the extraction of potential digital evidence from the acquired data, whereas the Analysis Phase should involve those activities associated with the methodical analysis of digital evidence as well as the construction of the incident. Therefore, in the SDFIPM, the Examination and Analysis have been assigned two separate processes with their own lower-level phases and sub-phase. This approach is supported by Casey (2011), who states "Examination is the process of extracting and viewing information from the evidence and making it available for analysis", whereas "Analysis is the application of the scientific method and critical thinking to address the fundamental questions in an investigation: who, what, where, when, how, and why".

Figure 8.2 represents the UML Activity Diagram of the SDFIPM's Examination Process followed by the description of its lower-level components, i.e. phases and sub-phases.

8.3.1.1 Survey Digital Crime Scene

The Survey Digital Crime Scene Phase has been developed and included in the Examination Process to enable DFAs to find apparent pieces of digital evidence for a particular category of crime in a swift manner, and also to assist them in ascertaining the skill level of the suspect. Determining the suspect's skill level in turn will allow DFAs to decide what examination and analysis techniques are required in the next process of the SDFIPM, the Analysis Process (discussed later). During the

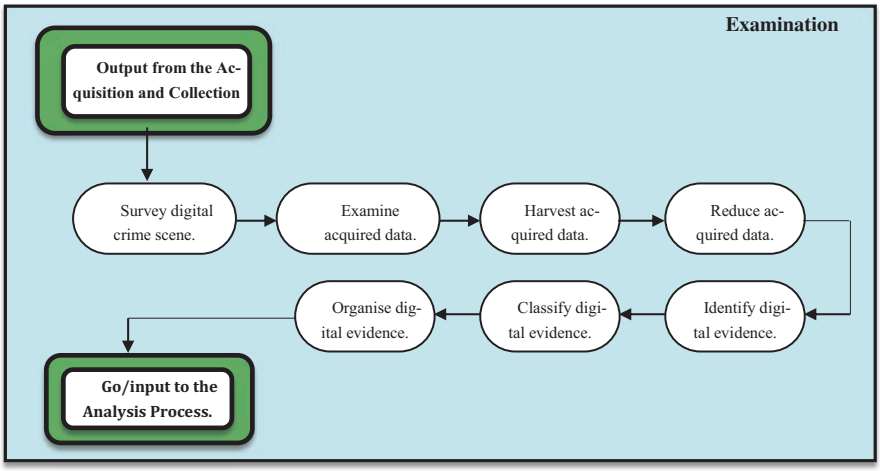

Fig. 8.2 The UML activity diagram of the examination process

Examination Process, the first step that investigators will need to undertake is to survey the digital crime scene to identify and locate potential evidence, possibly within unconventional locations on the system (Montasari and Peltola 2015). It is preferable to carry out the Survey Digital Crime Scene Phase in a DFL as it provides a controlled environment, and the results can be repeated with another copy of the system. To carry out this Phase in a DFL, DFAs must use the image (working copy) of the system acquired from the Acquisition and Collection Process as shown in (Montasari 2017b).

However, in certain circumstances, investigators employing the SDFIPM might be required to perform this phase on a live system to determine whether or not the system should be brought back to a DFL for a full examination and analysis. In such cases, investigators must perform field searches (Montasari 2016a, d) by booting the system into what Carrier and Spafford (2003) call a "trusted environment". In cases where the Survey Digital Crime Scene Phase is to be conducted on a live system, the SDFIPM still requires the investigators to image the system so that any digital evidence could also be acquired in a controlled DFL environment. Whether the Survey Digital Crime Scene Phase is to be carried out on a live system or in a controlled DFL environment, DFAs must adapt their investigative techniques based on the specific category of crime. This is to expedite the subsequent Examination and Analysis activities as there is often a large volume of data to deal with.

For instance, in cases where the computer has been used to store or distribute contraband images, DFAs must in the first place look for graphics with image file extensions and ascertain those that could be relied upon as incriminating evidence. Another example includes server intrusion where investigators should search for apparent signs of a rootkit installation, examine application logs and also search for new configuration files. In other types of investigations such as terrorism where investigators suspect that the system might contain the communication by the sus-

pect, investigators must perform keyword searching to identify any leads related to the investigation. Yet another example derived from (Carrier and Spafford 2003) is when analysing network traffic about an incident; the Survey Digital Crime Scene Phase might analyse traffic for the incident time frame and filter out certain ports and hosts. In other cases, as suggested in (Montasari and Peltola 2015), the investigators should also analyse the "common" and "un-common" locations on the system that might contain artefacts related to the suspect's browsing activities.

8.3.1.2 Examine Acquired Data

Having surveyed the digital crime scene, DFAs will need to perform a detailed examination on the image of the system (working copy) acquired from the Acquisition and Collection Process. See the research paper presented in (Montasari 2017b) for more details. During the Examination Phase, digital evidence needs to be made visible by extracting data into a human-readable form (Montasari 2016a, b; Kohn et al. 2013). DFAs should use the outcome of the Survey Digital Crime Scene Phase to direct their attention towards additional examination types. As an example, they will need to conduct a keyword search once keywords are identified from other evidence. DFAs will also need to extract and process unallocated file system space for deleted files. Moreover, they should examine a low-level timeline of file activity to trace a user's activity.

Since there might be large volumes of data to be examined (Kohn et al. 2013; Ciardhuáin 2004), automated techniques should be employed using tools such as FTK (AccessData 2016) or EnCase (Guidance Software 2016) in order to support the investigators. Furthermore, a large number of techniques might be performed to process the obfuscated data such as deleted or hidden data utilising sound digital forensic methods, as File Allocation tables or disk indexing might be deleted in some investigations. Therefore, this Phase will enable DFAs to ensure that files such as partially deleted files are recognized from the original evidence. During this Phase, DFAs can also reverse engineer suspicious executables and examine encrypted files (Carrier and Spafford 2003). They must also examine all the network packets that were acquired by monitoring software. In certain circumstances, it might be necessary for DFAs to examine the contents of every cluster (physical search) or every file (logical search) (Casey 2011). They will also need to ensure that they employ different search techniques, when appropriate, when preforming this Phase.

8.3.1.3 Harvest Data

After all data including partially discovered files and folders has been made visible in the Examine Acquired Data Phase, data then needs to be harvested by giving a logical structure to the entire data set. During this Phase, the file and folder structure is indexed to provide structure to data which was acquired in the Acquisition and

Collection Process of the CDFIPM. In this phase, raw data will be shown as information, and the partially deleted files which were processed during the Examine Acquired Data Phase will become visible to the degree that they were rendered visible during the Examine Acquired Data Phase. The result of the Harvest Data Phase is the production of a logical structured data set (Kohn et al. 2013) where the extracted raw data has now become structured information (Cohen 2009). Therefore, the harvested information can now be displayed by the original file systems such as FAT or NTFS.

8.3.1.4 Reduce Data

The data examined and analysed in the course of a digital forensic investigation can be very large. Consequently, this data needs to be reduced to expedite the Examination Process. Identifying known elements can enable the investigators to reduce data. Investigators will need to use the metadata and unique identifiers, such as MD5, in order to remove known system files and different other application data (Casey 2011; Beebe and Clark 2005; Cohen 2009). Data that remains will be modified data or data that could be uniquely attributed to the users of a specific computer system. Digital evidence with similar identifying patterns should also be classified based on the types of investigation.

8.3.1.5 Identify, Classify and Organise Digital Evidence

During the Identify Digital Evidence Phase, DFAs must use the known digital evidence data in order to identify the possible incident to be investigated. The outcome of this Phase will be the identification of the potential digital evidence from data that has been examined, harvested and reduced. In the Classify Digital Evidence Phase, DFAs should group together digital evidence with similar identifying pattern based on the types of investigation. This phase will enable the speeding up of the Analysis Process discussed in the next section. During the Organise Digital Evidence Phase, DFAs will need to organise digital evidence in a way so that digital forensic investigation can be accelerated. This can be materialized by focusing on the incident type identified and the data classified. DFAs should restructure digital evidence in order to conduct the identified investigation more appropriately. If similar types of incidents or crimes have taken place in the past and are known to DFAs, they should then use the known classification in order to compare the current digital forensic data (representing potential digital evidence) to the similar past incidents or crimes. At this stage, the Examination Process of the SDFIPM is completed, and its output becomes the input to the Analysis Process, discussed in the following section.

8.3.2 Analysis Process

Based upon the results of the Examination Process, DFAs must now be able to define what the exact characteristics of the incident are and who is to be held accountable for the incident. The aim of the SDFIPM's Analysis Process is to enable the investigators to reconstruct fragments of data based on their significance and to determine a possible root cause of the incident (Montasari 2016a, b; Montasari et al. 2015). The Analysis Process is the most time-consuming stage of the investigative process. Because of the volume, diversity and complexity of data to be analysed in present time digital investigations, the analysis of evidence becomes a challenge. Therefore, DFAs following the SDFIPM should use accredited automated techniques during this Process to complement manual validation techniques in order to expedite this Process.

Figure 8.3 represents the UML Activity Diagram of the SDFIPM's Analysis Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

8.3.2.1 Develop a Hypothesis

Up to this point in the investigation, DFAs have only dealt with what is possibly known from the digital evidence (Montasari et al., 2015). Now, DFAs must be able to formulate a hypothesis of how the incident took place by reconstructing a sequence of events which have resulted in the current state of the system under investigation. In order to develop a hypothesis for the incident or crime, DFAs should base their theory on the followings:

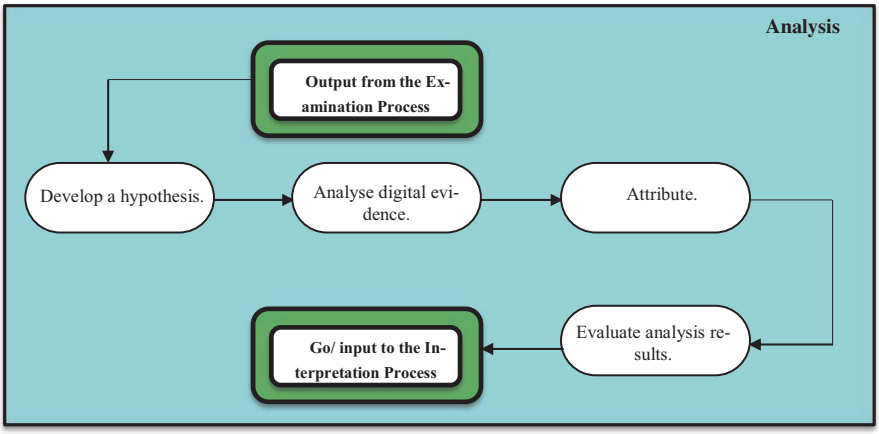

Fig. 8.3 The UML activity diagram of the analysis process

- The assumptions that they have deduced from the phases contained in the Examination Process;
- Digital evidence that they have already organised from the Organise Digital Evidence Phase contained in the Examination Process; and
- The documentation of the crime scene that they have maintained.

8.3.2.2 Analyse Digital Evidence

After DFAs have formulated the hypothesis, they will need to perform the Analyse Digital Evidence Phase. During this Phase, DFAs must thoroughly investigate and test data that was organised in the Examination Process against the hypothesis that was formulated in the Develop a Hypothesis Phase in the Analysis Process. DFIs must also question the legal validity of the possible digital evidence by considering issues such as relevance, admissibility and weight as discussed in (Montasari 2016a, 2017a). This will enable them to test the hypothesis by identifying the best possible evidence.

8.3.2.3 Attribute

Digital evidence should then be linked and attributed to a specific user or the event which is the root cause of the incident or crime. In order to link an individual to the incident or crime, DFAs must be able to correlate the results of the digital crime scene with physical evidence. For instance, in some investigations, DFAs are likely to need to correlate data center access logs to logins, linking online chat activities found on the computer with the activity with an undercover officer, and correlating activity on a compromised server with activity on the suspect's home system and network activity recorded by an ISP.

8.3.2.4 Evaluate Analysis Results

After the attribution has been made, during the Evaluate Analysis Results Phase, the DFAs must then evaluate their findings in order to ensure that the hypothesis they have developed holds true. Finally, in order for the Analysis Process to be most effective, DFAs might need to request other digital crime experts to assist them in correlating the event from numerous sources of digital evidence. At this stage of the Investigative Process, backtracking from the Analysis Process to the Examination Process is often to be expected as the investigators acquire a better understanding of the events which resulted in the investigation in the first place. Having completed all the Phases of the Analysis Process, this Process is now complete, and DFAs must start preparing for the interpretation of the analysis in the next process. The output of the Analysis Process will become the input to the Interpretation Process discussed in the next section.

8.3.3 Interpretation Process

The main purpose of the Interpretation Process is to use scientifically proven methods to explain facts discovered throughout the Analysis Process within the context of the investigation (Montasari 2016a, b; Palmer 2001). Therefore, after investigators have evaluated their findings in the Analysis Process and have determined that the hypothesis they formulated holds true, they will need to interpret the digital evidence in order to produce meaningful statements in the legal context for later reporting and presentation. During this Process, DFAs must be able to reconstruct the events associated with the digital investigation aspect. They should now be able to employ the results of the analysis techniques that they performed during the Analysis Process to put together the pieces of digital puzzle so that an accurate reconstruction of events can be made.

Figure 8.4 represents the UML activity diagram of the SDFIPM's interpretation process followed by the description of its lower-level components, i.e. phases and sub-phases.

8.3.3.1 Interpret Analysis Results

Interpretation of any evidence should depend on the available information regarding the circumstances surrounding the creation of that item of digital evidence (Valjarevic and Venter 2015; International Organisation for Standardization 2015). Investigators will need to obtain information from individuals involved in the day-to-day operation of the system under investigation. This will enable them to carry out a more effective interpretation of evidence. Moreover, investigators must

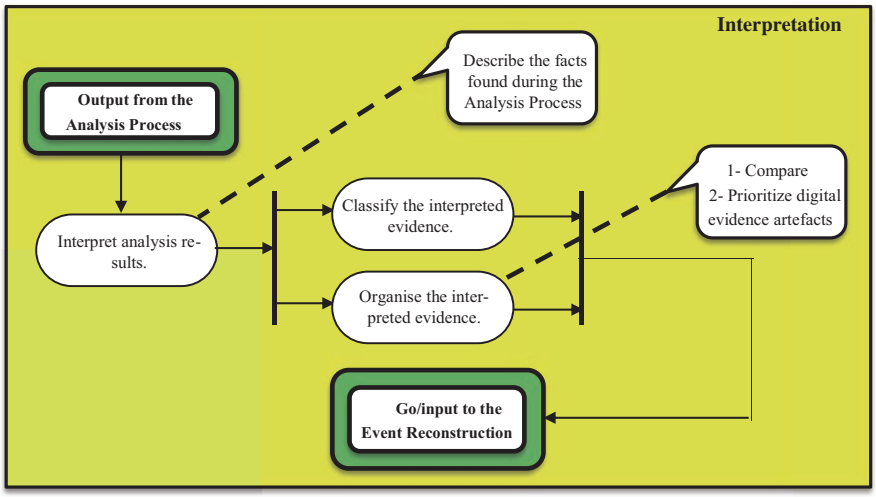

Fig. 8.4 The UML activity diagram of the interpretation process

consider information concerning the goal as well as the scope of the investigation. In cases where the contextual information changes, investigators might also need to change the interpretation so that the interpretation can reflect any such changes regarding the contextual information. Finally, during this process, DFAs must utilise link analysis and timeline tools to enable them in the digital reconstruction.

8.3.3.2 Classify and Organise the Interpreted Evidence

Having interpreted the analysis results, investigators will now need to classify and evaluate the interpreted evidence in order to ascertain the amount of trust that they can place in it. DFIs will also need to organise the interpreted digital evidence according to relevance in such a way that they can differentiate which digital evidence items are more important than the others. DFIs following the SDFIPM should perform the Classify the Interpreted Evidence Phase and Organise the Interpreted Evidence in the Interpretation Process in parallel. This is due the fact that although both phases have different activities, they have the same aim. Finally, during the Analysis Process, DFAs will need to employ scientific methods in order to prove or refute theories based on digital evidence. After performing this process, DFAs should be able to determine how digital evidence came into existence and what its presence denotes. After completing the Interpretation Process, DFIs will need to reconstruct the events in the next process of the SDFIPM. Therefore, the output of the Interpretation Process will become the input to the Event Reconstruction Process discussed in the next section.

8.3.4 Event Reconstruction Process

In the SDFIPM, the Event Reconstruction Process and Interpretation Process are closely related in that both Processes will require DFAs to reconstruct the events associated with the digital investigation. Similar to the Interpretation Process, the Event Reconstruction Process requires DFAs to employ scientific methods in order to prove or refute theories based on the results of the analysis, and digital evidence that they have discovered. The only difference between the two Processes is that in the Event Reconstruction Process, DFIs will need to consolidate, review and test their findings against the original hypothesis that they formulated in the Analysis Process.

Having completed the Interpretation Process in the previous stage, DFAs should now be able to reconstruct a possible event sequence under the Event Reconstruction Process which reflects the incident result as accurately as possible. In order to reconstruct the events, DFIs will need to utilise the series of events that they have deduced from digital evidence which is known to them. During this Process, DFAs must ensure that they are not dealing with reconstruction as a finding based on the original digital evidence (Kohn et al. 2013). Moreover, as Kent et al. (2006) state,

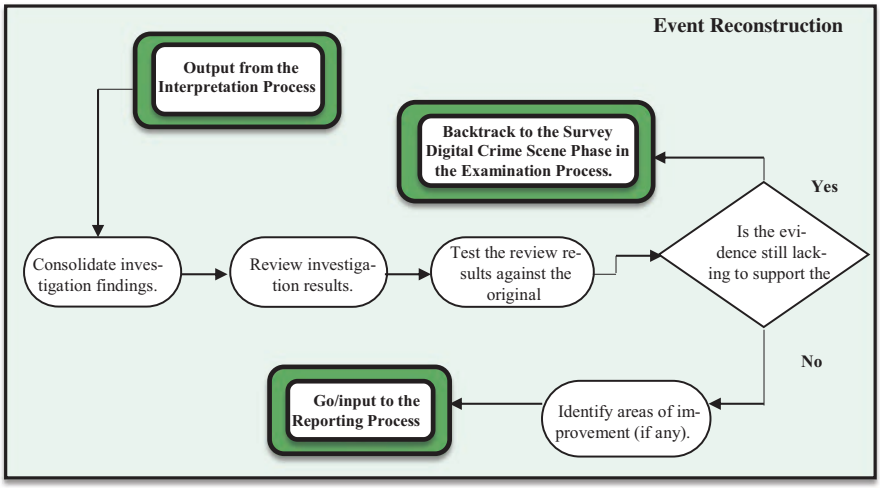

Fig. 8.5 The UML activity diagram of the event reconstruction process

Event Reconstruction should not be established as factual. Instead, DFAs who perform the Event Reconstruction Process should use this Process to explain how the incident might have taken place.

Figure 8.5 represents the UML Activity Diagram of the SDFIPM's Event Reconstruction Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

8.3.4.1 Event Reconstruction Components

During the Event Reconstruction Process, the investigation findings must be consolidated and refined prior to assessing the review results against the original hypothesis, which was formulated in the Analysis Process. This will be to determine whether DFAs have acquired all the evidence required to support the original hypothesis. If all the evidence has not been captured, DFAs will need to backtrack to the Survey Digital Crime Scene Phase in the Examination Process, in which this Phase and subsequent Phases form a cycle that needs to be repeated until DFAs can identify additional evidence and explain the incident.

As an example, in cases where a server intrusion has taken place, this iteration would involve DFIs linking the exploitation of a service that is open to attack with the installation of a rootkit and utilization of a network sniffer. The source IP address of network connections could result in the acquisition of additional digital evidence to examine. If there is no need to iterate to the Examination Process at this stage, DFAs must identify any areas of improvement and address those required improvements. In order to press charges against the perpetrator and explain the incident in a court, DFAs must have a valid hypothesis accompanied by relevant admissible digi-

tal evidence to support the findings that they have deduced. Finally, during the Event Reconstruction Process, DFAs might benefit from using link analysis and timeline tools to assist them in the digital reconstruction. The Event Re-construction Process of the SDFIPM is completed at this stage and DFAs should prepare for the next Process where they will need to compile a report to be presented in a court or the management in a company. The output of the Event Reconstruction Process will become the input to the Reporting Process, discussed in the next section.

8.3.5 Reporting Process

After conducting the Event Reconstruction Process, DFAs will need to compile, write and print out on paper a detailed and concise report in the Reporting Process. Regardless of digital evidence or physical evidence, a forensic report must contain conclusions that can be reproduced by independent third parties. Forensic reports that include opinions based on accurately documented digital sources are much more likely to withstand judicial scrutiny than opinions based on less reliable sources (Garrie 2014). DFAs following the SDFIPM must detail in their report all the findings and results of the entire digital investigative process including the Concurrent Processes (Overriding Principles) of the SDFIPM such as documentation, chain of custody, digital evidence preservation, authorisation and management, and ultimately the investigators' findings that are constructed in an opinion to be presented in a court. In addition, the forensic report should follow "the 'ABC's of writing' (accuracy, brevity, and clarity)" and be restricted only to what is known (Beebe and Clark 2005). DFAs will need to write their report in such a manner that it contains conclusions that can be reproduced by independent third parties regardless of digital or physical evidence. Also, since digital forensic investigation might produce many incriminating digital evidence items, DFAs must therefore ensure that they list all digital evidence items in the report so that no valuable item of evidence is left out. Furthermore, DFAs must ensure that they include in the report all other relevant documentation that was compiled during the investigation and that might be relevant in reaching a decision.

Figure 8.6 represents the UML Activity Diagram of the CDFIPM's Reporting Process.

DFAs should also ensure that they reference accepted and known protocols and methods applied during the Examination, Analysis, Interpretation and Event Reconstruction Processes in order to increase the credibility of the investigation and its results. Finally, DFAs employing the SDFIPM must ensure that their report is in a simple language and is well-defined, concise and unambiguous in order for the lay person to be able to understand it. After DFIs have compiled the report and are satisfied with its content, the report will then need to be presented in a court. The output of the Reporting Process becomes the input to the Presentation Process of the SDFIPM, discussed in the next section.

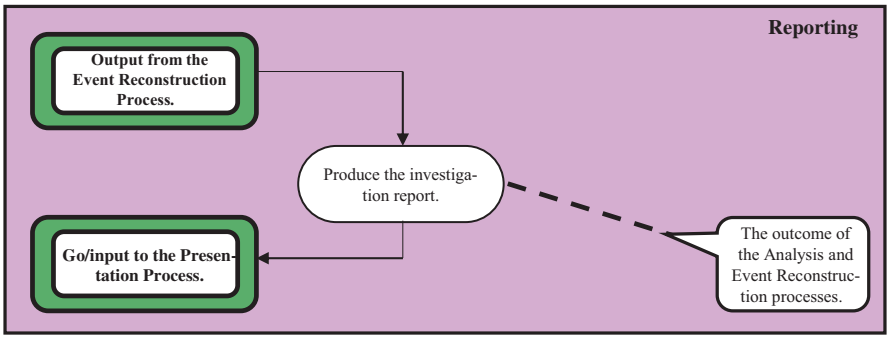

Fig. 8.6 The UML activity diagram of the reporting process

8.3.6 Presentation Process

The output of the Reporting Process in the form of a well-written report must be presented to a wide variety of audiences such as courts, legal personnel, law enforcement, technical personnel and management. Presenting the report can be carried out in the form of the expert report or can be accompanied by other formats such as multimedia presentation, deposition and expert witness (testimony). During the Presentation Process, DFAs will need to be able to prove the hypothesis that they formulated during the Analysis Process using supporting evidence. In order to prove that all of the SDFIPM's previous Processes were conducted accurately, evidence that DFAs present must hold up in a court.

Although Presentation Process is very important in that it meets the main requirement needed by the definition of the word 'forensic', authors of the existing models have paid little attention, if any, to this Process. Researchers have often taken a cursory approach when dealing with the Presentation Process and have often confused this Process with the Reporting Process. In the existing models, Presentation Process and Reporting Process are regarded the same, and as a result they are assigned one single process under the naming either "Report" or "Presentation". This approach is flawed on the basis that the Reporting Process and Presentation Process are carried out at different times and under different circumstances during the course of an investigative process and as a result have different aims. The purpose of the Reporting Process should be to document relevant information deduced from the findings and results of the investigative process, whereas the aim of the Presentation Process should be to communicate such information and findings to the said audience. Therefore, in the SDFIPM, the Presentation Process has been distinguished from the Reporting Process, and as a result each has been assigned a separate and discrete Process in the model. Moreover, the "Report/Presentation" in the existing models is often a high-level Process without providing adequate details to assist DFAs in effectively preparing for this important Process. Since careful planning is essential especially when the investigation findings are to be presented

in a court, the Presentation Process of the SDFIPM has incorporated lower-level and generic phases to guide the DFIs on how to prepare for this Process.

During the Presentation Process, DFAs must communicate their findings in such a way that facilitates future validation and that can be understood by both technical and non-technical audience. Mumba and Venter (2014) state that during the Presentation Process, it is vital that all of the processes are utilised to prove that the investigation was conducted in a forensically sound manner. Beebe and Clark (2005) highlight that a presentation should be based on "careful consideration about how to best communicate information to various audiences". Therefore, during the Presentation Process, DFAs following the SDFIPM must provide both concise and detailed confirmatory information obtained from the Interpretation and Event Reconstruction Processes of the model concerning the data examined and analysed in the Examination and Analysis Processes of the model. The presentation must also include relevant documentation and processes conducted during the investigative process, as well as any relevant physical evidence that can further consolidate the case against the perpetrator.

Figure 8.7 represents the UML Activity Diagram of the SDFIPM's Presentation Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

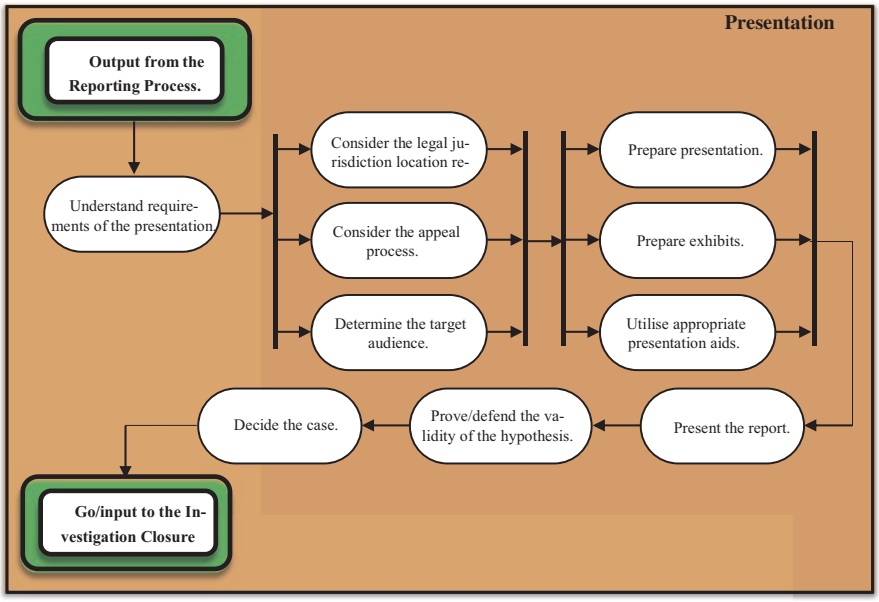

Fig. 8.7 The UML activity diagram of the presentation process

8.3.6.1 Components of the Presentation Process

Prior to delivering the presentation, DFAs must address the following four issues:

- choosing their main points carefully based on the results of the CDFIPM's Interpretation and Event Reconstruction Processes;
- selecting their supporting information;
- developing a conclusion; and
- reviewing their presentation prior to its delivery.

Since the judge and jury or other interested parties are very likely to be non-technical users, DFAs must ensure that in their presentation they avoid complex arguments, unless providing the audience with significant help so that they understand the technical points made. DFAs must deliver their conclusion in a logical and structured manner and build upon their previous points. In addition to preparing the presentation itself, DFAs will also need to prepare supporting information in order to assist the audience in better understanding the points they make. This should include the factual data itself that they have deduced from Interpretation and Event Reconstruction Processes and also the explanation of the process. DFAs might also need to use diagrams, pictures and video if it enables the audience to understand the explained concepts more clearly. Another important stage in the Presentation Process is the conclusion that DFAs have arrived at. They must ensure that they remind the audience of their main points and leave the audience with a clear understanding of them and their judgments on the case.

After preparing the presentation and prior to appearing before the relevant audience, DFAs will need to review their presentation to ensure that its content meets the objectives of the report, is logically structured and contains the material at the right level for the audience. In cases where DFAs will have to appear before judge and jury to give expert witness, they must ensure that they are fully aware of the jurisdiction legal requirements (the U.K. in the context of this research) concerning the digital evidence. Not being aware of the legal requirements might render the incriminating evidence being thrown out of the court. Moreover, DFAs must find out in advance what legal proceedings will concern the appeal process so that they can be better prepared in case they might need to reappear before the court. Often the person who presents the findings of the case is not often involved in various stages of the investigative process such as Acquisition, Examination, Analysis, Interpretation and Event Reconstruction Processes. Therefore, DFA who is required to appear before a court as an expert witness must determine who his target audience are prior to preparing the presentation if this is not already known.

Investigators also need to ensure that they identify the exhibits (i.e. digital evidence) by a label or other mark. The exhibit must also be properly described in the report as discussed in the Reporting Process section. When delivering the presentation, DFAs must take into account that the target audience are often non-technical and might have a variety of experiences and level of knowledge concerning the digital investigations. Therefore, in order to help the audience to understand the explained concepts better while giving the presentation, DFA might need to link

their investigation findings to the things that the audience already understand. DFAs need to ensure that they have targeted their findings at the right level for the needs of the audience. They must also avoid using technical jargon and should attempt to explain the abstract concepts with clear practical examples.

During the presentation, often the hypothesis is challenged by the defence lawyers. A contradicting hypothesis and supporting evidence are placed before judge and jury. DFAs will need to prove the credibility of their hypothesis and to be well-prepared to defend the hypothesis against criticism and challenge. In circumstances in which challenges are successful, investigators will need to backtrack to the earlier stages to obtain and examine more evidence and develop a better hypothesis. The case will be decided based on the presentation report. If the decision is made in a court, it will be decided whether to convict the accused or whether to refute the allegations. If the decision is made in the context of an organisation, it will be decided what disciplinary actions must be taken if the incident can be attributed to the individual under investigation. At this stage, the Presentation Process of the CDFIPM is concluded, and its output becomes the input to the Investigation Closure Process, discussed in the following section.

8.3.7 Investigation Closure Process

It is vital not only to close the investigation and apply the decisions associated with it but also to maintain the knowledge obtained to improve subsequent investigations (Beebe and Clark 2005). As the title suggests, the Investigation Closure Process of the SDFIPM involves concluding the investigation and also the decision-making on the credibility of the hypothesis presented in the Presentation Process. This denotes that after completing the Investigation Closure Process, investigators can backtrack to any of the preceding processes that follow the First Response Process.

Figure 8.8 represents the UML Activity Diagram of the SDFIPM's Investigation Closure Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

8.3.7.1 Review the Outcome of the Case

After the case has been presented to the appropriate audience and decided in the Presentation Process, the outcome of the investigation will need to be used to review the existing policies and procedures of the organisation. The aim of this Phase should be to make and act upon the outcome of the decisions reached from the CDFIPM's Presentation Process. During this Phase, the investigating organisation will also need to collect and maintain all the information associated with the case that has been investigated.

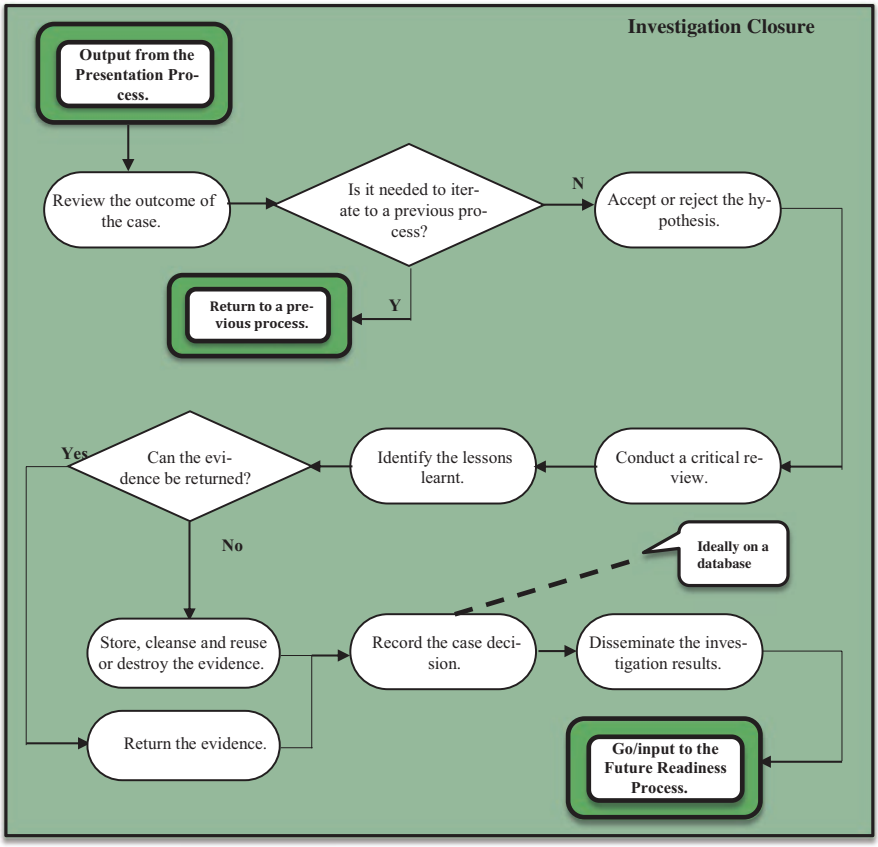

Fig. 8.8 The UML activity diagram of the investigation closure process

8.3.7.2 Accept or Reject the Hypothesis

Since the CDFIPM is an iterative process model, it will allow investigators to backtrack to any of the preceding Processes in the model. Having carried out the initial review, at this stage the investigators can return to any of the CDFIPM's previous Processes that follow the First Response Process if required.

8.3.7.3 Conduct a Critical Review

During the Conduct a Critical Review Phase, the entire investigative process detailed in the SDFIPM must be reviewed to identify any lessons learnt and potential areas of improvement. During this Phase, the investigating organisation will also need to address issues such as what went well, what did not go well and how things could have been carried out better, etc. Based on this information, the investigating

organisation will need to identify and learn the lessons from the incident or crime in order to be able to apply the findings and be better prepared for the future incidents or crimes. Also under this phase, the outcomes and their ensuing interpretation must be used for refining the Acquisition, Examination, Analysis, Interpretation and Event Reconstruction of digital evidence in future investigations. As already stated, often backtracking between Examination, Analysis, Interpretation and Event Re-construction Processes are to be expected in order to obtain the full picture of the incident or crime. Such information could also assist law enforcements' HTCUs and corporates in establishing more effective policies and procedures.

8.3.7.4 Evidence Management

A decision will also need to be made to determine whether digital and physical evidence should be returned to the proper owner or not and to determine what criminal evidence must be removed. This is a complicated issue and not an explicit step in a digital forensic investigation. However, any of the existing models that has emphasized the seizure of evidence has seldom addressed this aspect. Jurisdiction in which the investigation is taking place (in the context of this thesis, the U.K.) and the type of authorisation determine whether the evidence should be returned, cleansed and reused or destroyed or whether the evidence should be stored for a certain period of time before any of the three possibilities can be applied.

8.3.7.5 Record the Case Decision

Under the Record the Case Decision Phase, DFIs will need to record (ideally on a database) the investigation results, case decision as well as all the evidence that might be used for reference in the future and for training purposes. For instance, the results could be recorded by the category of evidence found as follows:

- Evidence of refutation or defence,
- Evidence vital to the case,
- Evidence important to the case,
- Evidence that supports other evidence,
- Evidence peripheral to the case,
- Evidence that is intelligence only, and
- No evidence found.

Such an approach could also benefit authorities in other jurisdictions in circumstances in which the case will be likely to have some kind of connection with their investigation.

8.3.7.6 Disseminate the Investigation Results

In the final part of the Investigation Closure Process, relevant information concerning the entire investigation will need to be disseminated and communicated to all stakeholders. This includes communicating the need to return to a previous Process, deciding on the acceptance or rejection of the hypothesis or providing any reports or documents from the Presentation Process. During this Phase, the investigating organisation might decide to make some information available only within the organisation, whereas they might decide to disseminate other information more widely. According to (Ciardhuáin 2004), the investigating organisation's policies and procedures should determine the details in this regard. The information will have an impact on future investigations and might have an effect on the policies and procedures.

Thus, the accumulation and preservation of this information is a key part of supporting the work of investigators and might be a productive aspect for the development of innovative applications that integrate techniques such as data mining and expert systems. Hauck et al. (2002) provide a detailed example of the dissemination activity where they define a system titled Coplink, that provides real-time support for law enforcement DFIs through an analysis application on the basis of a large accumulation of information from past investigations. An additional example is provided by Harrison et al. (2002), whose system is not real-time, but instead delivers an "archival function" database to support investigators. At this stage, the Investigation Closure Process of the SDFIPM is concluded, and its output becomes the input to the Future Readiness Process Class, discussed in the following section.

8.3.8 Overriding Principles

In order to ensure the admissibility of digital evidence in courts, a set of eight Overriding Principles or Concurrent Processes have also been developed and grouped into a unique class, entitled Concurrent Processes Class (see Fig. 8.1). These eight Principles are objectives that need to be achieved in a given digital investigation and should be performed concurrently throughout the whole or parts of the other Processes in the SDFIPM. The inclusion of the proposed Overriding Principles or Concurrent Processes is justified by their significance and applicability to other digital investigation processes. Thus, due to their extreme importance, investigators must maintain these Principles at all times throughout the whole or parts of the digital investigative process. Since the SDFIPM is aimed at the U.K. jurisdiction, the proposed Overriding Principles are based on the following standards and guidelines: (International Organisation for Standardization 2012, 2015; ACPO 2012), as well as other relevant scientific papers such as (Montasari 2016b; Montasari et al. 2015; Valjarevic and Venter 2015; Casey 2011; Carrier and Spafford 2003; Beebe and Clark 2005; Ciardhuáin 2004).

8.3.8.1 Preserve Digital and Physical Evidence

Preservation is the process to maintain and safeguard the integrity and original condition of both physical and digital evidence. In order for evidence to be able to withstand scrutiny in courts, investigating organisations will need to prove that both digital device and digital evidence that they have handled during an investigation have not been altered, or justify their actions if unavoidable changes were made. In the best-case scenario, there should be no contamination to data itself or any metadata associated with it (e.g. date and time-stamps).

In some cases, the confidentiality of digital evidence is a requirement, either a business requirement or a legal requirement. This denotes that digital evidence should be preserved in a manner that ensures the confidentiality of data. Thus, since the correct handling of evidence is essential in any digital investigation (Montasari 2016a, b, 2017b; Valjarevic and Venter 2015; International Organisation for Standardization 2012; ACPO 2012; Holder et al. 2009), this Overriding Principle or Action Principle has been incorporated into the CDFIPM to enable investigating organisations to preserve the integrity of both digital and physical evidence throughout the entire investigative process in a forensically sound manner. Preserving this Overriding Principle will enable investigating organisations to protect both physical and digital evidence from being tampered with, contaminated or altered and as a result to ensure the efficacy of evidence presented to a court.

Almost all the existing models have undertaken a flawed approach towards the issue of preservation and have provided a superficial discussion of this aspect of digital investigative process by simply stating that digital evidence needs to be preserved without elaborating on this important aspect. Moreover, preservation in some existing DFIPMs refer only to preservation of physical evidence or crime scene (Casey 2011; Carrier and Spafford 2003) while in some other models it refers to preservation of only digital evidence (Kohn et al. 2013; Carrier and Spafford 2003; Reith et al. 2002), or digital evidence during the transportation or storage (Valjarevic and Venter 2015; Reith et al. 2002; Ciardhuáin 2004).

Although some existing models (Casey 2011; Carrier and Spafford 2003) have discussed preservation in more depth, their approach of dealing with this principle is still flawed as the "preservation activity" in these models is restricted to a 'single Phase' at a particular stage of the investigative process. It is, however, argued that preservation has a much wider scope beyond being limited to a single point in time. Each stage of investigative process requires digital and physical evidence to be preserved in a different manner. In order to address the stated issues, in the SDFIPM, preservation has been introduced as an Overriding Principle or Actionable Principle that should be applied concurrently throughout the entire investigative processes of the model from the time the incident is detected in the Incident Detection Process up to and including the time when the investigation is formally completed in the Investigation Closure Process. Preservation does not need to be applied during the Readiness and Future Readiness Processes on the basis that evidence (both physical and digital) is not handled during these two Processes. The remainder of this section provides some practical examples of how the investigating organisations should

apply the preservation aspect of the investigative process throughout the entire stages of the SDFIPM.

During the SDFIPM's Secure and Evaluate the Crime Scene Process, the preservation might involve investigators preventing unauthorised people from entering or leaving the crime scene, isolating the system from the network, acquiring the volatile data that would be lost after the system is powered down, and detecting suspicious processes that are running on the system, etc. During the Acquisition and Collection Process, preservation involves DFIs securing log files in case that they are lost before the system is imaged. Preservation also requires DFIs to make a full forensic image backup of the system so that it can be examined and analysed at a later stage in a DFL. DFIs must note that a full forensic image of the system preserves the whole digital crime scene whereas copies that are system backups preserve only the allocated data within the digital crime scene. Moreover, in terms of preserving the state of the network, this can be achieved by network monitors when they save network traffic.

Finally, as part of preservation, investigating organisations will also need to establish and maintain certain strict procedures (Valjarevic and Venter 2015), effective quality systems such as Standard Operating Procedures (SOPs) (Bulbul et al. 2013) or procedural workflows (Mukasey et al. 2008).

8.3.8.2 Preserve Chain of Custody

The processes for documenting, collecting and protecting both physical and digital evidence are called the establishing of the chain of custody. Establishing a chain of custody during the course of an investigation is of extreme importance since digital evidence is very likely to be handled by various parties. Cases where Chain of Custody has not been properly preserved have been easily challenged in courts and rejected irrespective of evidence discovered from the suspect's computer system. Therefore, due to its extreme importance in relation to conducting a successful investigation, Chain of Custody has been incorporated into the SDFIPM as an Overriding Principle, namely Preserve Chain of Custody, that will need to be applied concurrently throughout other Processes of the SDFIPM. In order to preserve Chain of Custody, DFIs will need to adhere to all legal requirements and must document each given process of the SDFIPM thoroughly. Documentation (discussed later) is a vital aspect of a Chain of Custody as it will need to detail the activities associated with the chronology of the movement and handling of evidence such as those associated with the seizure, custody, control, transfer, examination, analysis and disposition of both physical and digital evidence.

The issue of establishing Chain of Custody has been ignored by almost all the existing models, a problem identified also by the authors in Kohn et al. (2013), Ciardhuáin (2004 and Carrier and Spafford (2003). Although Chain of Custody has been addressed to some extent by four guidelines and standards including: (International Organisation for Standardization 2011, 2012, 2015; ACPO 2012), these appear to be contradictory in terms of the point at which Chain of Custody will

need to be established during an investigative process. For example, according to (International Organisation for Standardization 2012; ACPO 2012), Chain of Custody should be initiated from the Acquisition Process onwards, whereas (International Organisation for Standardization 2011, 2015) state that Chain of Custody must be maintained throughout the entire investigative process.

The approach taken by (International Organisation for Standardization 2012; ACPO 2012) appears to be flawed on the basis that digital device containing potential digital evidence is identified in the incident detection stage prior to the Acquisition Process. It is in the Incident Detection stage that the investigating organisations will need to process both physical (where items of evidentiary value exist) and digital crime scenes and therefore initiate the chain of custody. Consequently, in line with (International Organisation for Standardization 2011, 2015), DFIs following the SDFIPM must observe this Overriding Principle from the Incident Detection Process, during which incident is detected, up to and including the Investigation Closure Process, where incident is formally closed. One of the benefits of such an approach taken by author's is that it will enable DFIs to trace back the history of any digital device containing evidence to the time that it was first identified until its present status and location. Another benefit of this approach is the enabling of the identification of access and movement of potential digital evidence at any given point in time.

In any type of investigation, investigators within the investigating organisations are often accountable for all the acquired evidence (both physical and digital) during the period in which evidence is within their custody. The SDFIPM's Preserve Chain of Custody Principle also requires DFIs to keep records of who was responsible for handling both physical and digital evidence. Investigators must keep a record of all information associated with different activities undertaken in relation to Chain of Custody. The Chain of Custody record itself may comprise more than one document and include a series of related documents. For instance, for potential digital evidence, there should be a contemporaneous document recording the acquisition of digital data to a particular device, the movement of that device and documentation recording subsequent extracts or copies of potential digital evidence for analysis or other purposes.

An example of preserving Chain of Custody is when evidence copies are required to be shared with other experts in other locations. This handling of evidence must be properly documented to preserve Chain of Custody. Another example of Chain of Custody is when the first responders (who are the first custodian to preserve Chain of Custody of potential digital evidence) arrive at the crime scene where they will need to describe the scene in the preliminary drafting of documentation. These include taking photographs, videos and sketches.

The SDFIPM's Preserve Chain of Custody Principle does not impose any particular format in which information related to Chain of Custody should be recorded. The documents detailing Chain of Custody can be in the form of digital data or other formats such as paper notes, depending on the organisation or the agency conducting the investigation. The SDFIPM's flexibility allows investigating organisations to design and incorporate into the model their own Chain of Custody forms according to their needs.

8.3.8.3 Manage Information Flow

One of the major issues with the existing models is the lack of identifying 'Information Flow' which could have a negative impact on the other processes such as Chain of Custody. In this regard, Ciardhuáin (2004) criticizes the past models stating, "The single largest gap in the existing models is that they do not explicitly identify the information flows in investigations." Ciardhuáin (2004) proceeds to propose what would become one of the most widely referenced research papers in relation to Information Flow within a digital investigation. In his research paper, Ciardhuáin (2004) is able to define, identify and describe Information Flows within his process model so that its stages can be protected and supported technologically. Moreover, he clearly shows Information Flow that must exist amongst various stakeholders.

Due to the fact that the subject of Information Flow within the field of digital forensics has been extensively covered by the aforementioned reference, this chapter does not aim to focus on Information Flow in any further details. However, due to its importance in a digital investigation, Information Flow has been incorporated into the SDFIPM as an Overriding Principle, namely Manage Information Flow, which needs to be managed concurrently throughout the entire processes of the SDFIPM. The rationale for including this principle in the SDFIPM is to enable investigating organisations to deal with the different laws, practices, languages, etc. correctly in digital investigations. An example of Information Flow could be the interaction between two investigators involved in the same investigation, or the exchange of digital evidence between various parties during digital investigation process. Information Flow can be protected, for instance, by utilising trusted public key infrastructure (PKI) and time stamping to identify the different investigators and authenticate evidence in addition to protecting the confidentiality of the evidence through PKI-based encryption.

8.3.8.4 Maintain a Detailed Case Management

As the title suggests, Case Management refers to managing the case under investigation and keeping track of evidence items, events and vital forensic discoveries. Case Management mainly pertains to the tasks that a case officer should undertake throughout the entire investigative process in an investigation, and also to some extent relates to the responsibilities of the case officer's investigative team members. Activities associated with the Case Management can have significant impact on the entire investigative process tying together all of the activities and their outcomes. Casey (2011) highlights the importance of the Case Management stating, "Effective case management is one of the most important components of scaffolding, helping digital investigators bind everything together into a strong case." Similarly, Khatir et al. (2008) proclaim that the effectiveness of a digital investigation is reliant upon Case Management.

The lack of effective Case Management methods will result in investigative opportunities being easily neglected, digital evidence being disregarded or lost, and incriminating information representing potential digital evidence remaining undiscovered or not being passed onto decision makers. Therefore, due to its importance in a digital investigation, Case Management has been incorporated into the SDFIPM as an Overriding Principle, namely Maintain a Detailed Case Management, that will need to be applied from the Readiness Process up to and including Investigation Closure Process. The rationale for including this principle into the SDFIPM is as follow:

> to outline the responsibilities and certain important tasks that both a case officer and his investigative team members will need to undertake in order to ensure a successful investigation (Khatir et al. 2008),
>
> to enable a smooth transition between different Processes of the model, and also to ensure that all applicable information that results from each Process is acquired, documented and intertwined together in order to reconstruct the events associated with the crime or incident in a vivid and compelling manner.

The remainder of this section provides some examples of the tasks and types of responsibilities that a case officer and his investigative team members are to undertake under this Overriding Principle, Maintain a Detailed Case Management.

The tasks of a case officer start after the incident has been reported in the Incident Detection Process (the discussion of which is outside the scope of this chapter), where he needs to decide whether to accept or reject the case and determine the time and budget required to carry out the investigation. The case officer will subsequently need to develop an accurate and detailed plan that investigators can follow; this plan must define clearly the milestones, goals and sub-goals within the investigative process (Khatir et al. 2008). The case officer must also allocate tasks to individual team members, oversee these tasks as well as drawing a complete picture of the entire investigative process and its outcomes so that the investigation does not deviate from its correct course. In circumstances where the investigation has deviated from its correct course, the manager will need to identify the root cause of the deviation and guide the team members into the correct path. Case officers will also be responsible for obtaining written authorisation so that the investigation can proceed as well as determining what level of attention to give to a particular case comparative to all of the other cases that they are dealing with (Khatir et al. 2008).

As already stated, in addition to the case officers, the Maintain a Detailed Case Management Principle also pertains to the investigative team members who will need to undertake various tasks under this Overriding Principle. These include communication and prioritization such as sharing information amongst DFIs, meeting the requirements of non-technical stakeholders, prioritizing and assigning administrative tasks amongst multiple DFIs in a digital investigation, etc. In certain investigations, communication becomes a key aspect of case management (Khatir et al. 2008). For example, in complex investigations that might last for long time, daily or weekly status meetings are required in order to discuss and analyse progress, combine up-to-date information and discuss and review the following steps in the inves-

tigation. Finally, logging digital evidence in archives is another important factor in managing an investigation effectively. This task can be carried out by both the case officer or the investigative team members (Khatir et al. 2008).

8.3.8.5 Prepare and Test Tools and Techniques

It is vital that DFIs prepare an appropriate set of tools and techniques during the course of an investigation so that each process of the investigative process can be carried out effectively. DFIs might require different sets of tools and techniques to be able to carry out each given process in the investigative process. Therefore, this aspect of the digital investigative process has been incorporated into the SDFIPM as an Overriding Principle, namely Prepare and Test Tools and Techniques, that will need to be followed throughout all the other Processes of the model. This Principle has been extensively covered in technical standard documents such as (International Organisation for Standardization 2005, 2013), guidelines such as National Institute of Standards and Technology (Kent et al. 2006) and (NIST 2015), as well as technical reports such as Information Assurance Advisory Council (IAAC) (Sommer 2008).

For instance, under a comprehensive project, entitled CFTT (Computer Forensics Tools Testing), carried out by the National Institute of Standards and Technology (NIST 2015), various methodologies have been established for testing computer forensic software tools through the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. This detailed guideline provides necessary information for digital forensic tools developers to improve their tools, and also enable DFIs to make informed choices about obtaining and testing digital forensic tools and understand the tools' capabilities.

Therefore, due to the fact that tools and techniques testing and preparation have already been covered in detail, this chapter does not aim to focus on this aspect of the investigative process in more details. However, some examples on certain steps that DFIs will need to undertake in relation to this Overriding Principle will still be provided only for illustrative purposes. Some activities that DFIs will need to perform in relation to Prepare and Test Tools and Techniques Principle include, but are not limited to:

> determining which tools must be used for each given Process of the CDFIPM,
> identifying which tools must be utilised for different data analysis tasks,
> investigating and establishing which tools have been scientifically tested, and
> identifying the degree of error in connection with tools.

Cases where untested tools have been used to carry out digital investigations are easily challenged in courts. Therefore, one key element that DFIs will need to consider at all times under this Principle is the need to select tools that are court-proven such as EnCase, AccessData FTK, ProDiscover, Sleuthkit and Autopsy. Another important aspect that investigators will need to adhere to under this Overriding Principle is the need to have up-to-date training on how to use the latest versions of different forensic tools in order to make effective use of them.

Finally, as already stated, each Process within an investigative process might require different sets of tools. For example, to conduct the Examination Process, the software tools such as FTK and EnCase, that are capable of revealing hidden, deleted, swapped and corrupted files or performing data carving, will need to be utilised. In terms of techniques, for example in cases where public and private IP addresses need to be acquired and mapped to the country and institutions, IP addresses can be readily acquired by performing the following commands: ping, nslookup, dig, tracert from a DNS server. Moreover, DFIs can easily locate a county by various online tools such as IP Location (2016) or WhatIsMyIPAddress (2016).

8.3.8.6 Obtain and Adhere to Authorisation

Any digital investigation that is commissioned to be carried out necessitates proper authorisation, whether it is an internal or an external authorisation. In fact, each single stage of digital investigation should be authorised, and therefore an authorisation is required for each given process. Due to its significance on the investigative process, authorisation has been incorporated into the SDFIPM as an Overriding Principle, namely Obtain and Adhere to Authorisation. This Overriding Principle requires investigating organisations to obtain proper authorisation from one of the following groups: government authorities, system owners, system custodians, principles or users etc., when undertaking a digital investigation. The significance of this Principle for activities carried out during the digital investigation processes is justified by the fact that the rights of the system owners, custodians, principles or users should not be infringed. Moreover, this principle ensures that no law is violated. The environment in which digital investigation is carried out determines the type of authorisation required. The authorisation might be needed both within a legal environment or an organisational environment. Authorisation for investigations involving law enforcement often requires a search warrant or other legal approval that requires sufficient evidence or suspicion. For corporate incidents, search warrants are not usually required so long as the proper privacy policies are in place. This Overriding Principle must be adhered to concurrently throughout the entire processes of the SDFIPM.

8.3.8.7 Maintain a Detailed Documentation

It is extremely important to document all the activities carried out throughout the entire investigative process in order to enable other investigators to authenticate the process and results. As well as being incorporated as a single Phase, documentation has also been incorporated into the SDFIPM as an Overriding Principle, namely Maintain a Detailed Documentation, that will need to be applied throughout the whole investigative process. The aim of this Overriding Principle is to record all information applicable or produced during the investigative process to support decision making and the legal, administrative processing of those decisions. This

Overriding Principle involves documenting both physical and digital crime scene. For instance, documentation of the physical crime scene involves creating sketches and making video of a physical crime scene, while documentation of digital crime scene involves investigators properly documenting each item of digital evidence when it is discovered.

8.3.8.8 Interact with Physical Investigation

A digital investigation and a physical investigation are often interrelated and dependent on one another (Carrier and Spafford 2003). In cases where a physical investigation requires an assistance from a digital investigation, an example can be to use a digital forensic investigation to reveal communications between terror suspects via computers, mobile phones, online social network activities, email communication, communication via chat rooms and forums, etc. (Montasari 2016a, b; Valjarevic and Venter 2015). An example of digital investigation being dependent on a physical investigation is when a suspect is interviewed to provide a password to a system under investigation (Valjarevic and Venter 2015). In the SDFIPM, Interact with Physical Investigation has been included as an Overriding Principle since defining the relationship between a digital investigation and a physical investigation is required to preserve chain of custody, preserve the integrity of the digital evidence, protect the digital evidence from damage and ensure an efficient investigation.

8.4 Conclusion

This chapter covered the Design and Development of our Advanced Investigative Process Model (SDFIPM) for conducting digital forensic examination of digital evidence after it has been identified and acquired. It is argued that the SDFIPM is the most comprehensive, detailed and structured DFIPM presented to date. Each Process of the model was discussed and justified. Due to its top-down approach, an overview of the model was firstly formulated specifying the first-level components, i.e. Processes. Each first-level component was further broken down to specify the second-level components, i.e. Phases. In turn, each second-level component was further refined in greater details to specify the third-level components, namely Sub-Phases. The SDFIPM is also both generic and formal, enabling DFIs to reach conclusions that are reliable, repeatable and well-documented. Due to its scientific approach, the SDFIPM will enable DFIs to follow a uniform approach, to overcome biased and predetermined theories, and authenticate their discoveries by attempting to prove themselves wrong. This, in turn, will result in well-established conclusions that support expert testimony in courts of law.

References

AccessData (2016) Forensic toolkit (FTK). Available at http://accessdata.com/products/computer-forensics/ftk. Accessed 14 May 2018

ACPO (2012) ACPO good practice guide for digital evidence. U.K. Association of Chief Police Officers. Available at: http://www.digital-de-tective.net/digital-forensics-docu-ments/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. Accessed 14 May 2018

Adams R (2012) The advanced data acquisition model (ADAM): a process model for digital forensic practice. PhD thesis. Murdoch University

Adams R, Hobbs V, Mann G (2014) The advanced data acquisition model (ADAM): a process model for digital forensic practice. J Digit Forensic Secur Law 8(4):25–48

Agarwal A, Gupta M, Gupta S, Gupta C (2011) Systematic digital forensic investigation model. Int J Comput Sci Secur 5(1):118–130

Armstrong C, Armstrong H (2010) Modeling forensic evidence systems using design science. IFIP WG 8.2/8.6 international working conference, pp 282–300

Ashcroft J (2001) Electronic crime scene investigation: a guide for first responders. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf. Accessed 10 June 2016

Baryamureeba V, Tushabe F (2004) The enhanced digital investigation process model. 4th digital forensic research workshop, 1–9

Beebe N, Clark J (2005) A hierarchical, objectives-based framework for the digital investigations process. Digit Investig 2(2):147–167

Bulbul H, Yavuzcan H, Ozel M (2013) Digital forensics: an analytical crime scene procedure model (ACSPM). Forensic Sci Int 233(1):244–256

Carlton H, Worthley R (2009) An evaluation of agreement and conflict among computer forensic experts. 42nd Hawaii international conference on system sciences, pp 1–10

Carrier B, Spafford E (2003) Getting physical with the digital in-vestigation process. Int J Digit Evid 2(2):1–20

Casey E (2011) Digital evidence and computer crime: forensic science, computers and the internet, 3rd edn. Elsevier Academic Press, New York

Ciardhuáin O (2004) An extended model of cybercrime investigations. Int J Digit Evid 3(1):1–22

Cohen F (2009) Digital forensic evidence examination, 2nd edn. Fred Cohen & Associates, Livermore

Cohen F (2010) Towards a science of digital forensic evidence examination. In 6th IFIP WG 11.9 international conference on digital forensics, pp 17–35

Cohen F (2011) Putting the science in digital forensics. J Digit Forensic Secur Law 6(1):7–14

Cohen F (2012) Update on the state of the science of digital evidence examination. In: Proceedings of the conference on digital forensics, security, and law, pp 7–18

Farrell M (1993) Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemilogy and legal process. Cardozo L Rev 15:2183

Freiling C, Schwittay B (2007) A common process model for incident response and computer forensics, 3rd international conference on IT-incident management & IT-forensics, pp 19–40

Garfinkel S, Farrell P, Roussev V, Dinolt G (2009) Bringing science to digital forensics with standardized forensic corpora. Digit Investig 6:2–11

Garrie D (2014) Digital forensic evidence in the courtroom: understanding content and quality. Northwest J Technol Intellect Prop 12(2). [i]–128

Grobler CP, Louwrens CP, Solms SH (2010) A multi-component view of digital forensics. In: ARES'10 international conference on availability, reliability and security, pp 647–652

Guidance Software (2016) EnCase forensics. Available at https://www.guidancesoftware.com/encase-forensic. Accessed 14 May 2018

Harrison W, Heuston G, Morrissey M, Aucsmith D, Mocas S, Russelle S (2002) A lessons learned repository for computer forensics. Int J Digit Evid 1(3):1–9

Hauck R, Atabakhsh H, Ongvasith P, Gupta H, Chen H (2002) Using coplink to analyze criminal-justice data. IEEE Comput 35(3):30–37
Holder E, Robinson L, Rose K (2009) Electronic crime scene investigation: an on-the-scene reference for first responders, U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/227050.pdf. Accessed 14 May 2018
Ieong R (2006) FORZA-digital forensics investigation framework that incorporate legal issues. Digit Investig 3:29–36
International Organisation for Standardization (2005) ISO/IEC 17799:2005. In: Information technology – security techniques – code of practice for information security management. International Organization for Standardization, Geneva
International Organisation for Standardization (2011) ISO/IEC 27035:2011. In: Information technology – security techniques – information security incident management. International Organization for Standardization, Geneva
International Organisation for Standardization (2012) ISO/IEC 27037:2012. In: Information technology – security techniques – guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, Geneva
International Organisation for Standardization (2013) ISO/IEC 27001:2013. In: Information technology – security techniques – information security management systems – requirements. International Organization for Standardization, Geneva
International Organisation for Standardization (2015) ISO/IEC 27043:2015. In: Information technology – security techniques – incident investigation principles and processes. International Organization for Standardization, Geneva
IP Location (2016) Where is geolocation of an IP address?. Available at: https://www.iplocation.net/. Accessed 14 May 2018
Karyda M, Mitrou L (2007) Internet forensics: legal and technical issues. 2nd international workshop on digital forensics and incident analysis, pp 3–12
Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response. U.S. Department of Commerce. Available at: http://cybersd.com/sec2/800-86Summary.pdf. Accessed 16 June 2016
Kessler C (2010) Judges' awareness, understanding, and application of digital evidence. PhD thesis, Nova Southeastern University
Khatir M, Hejazi M, Sneiders E (2008) Two-dimensional evidence reliability amplification process model for digital forensics. Third international annual workshop on digital forensics and incident analysis, pp 21–29
Kohn M, Eloff J, Olivier M (2006) Framework for a digital forensic investigation. In: Information security South Africa conference, pp 1–7
Kohn M, Eloff M, Eloff J (2013) Integrated digital forensic process model. Comput Secur 38:103–115
Leigland L, Krings A (2004) A formalization of digital forensics. Int J Digit Evid 3(2):1–32
Montasari R (2016a) The comprehensive digital forensic investigation process model (CDFIPM) for digital forensic practice. PhD thesis, University of Derby
Montasari R (2016b) A comprehensive digital forensic investigation process model. Int J Electron Secur Digit Forensics 8(4):285–302
Montasari R (2016c) An ad hoc detailed review of digital forensic investigation process models. Int J Electron Secur Digit Forensics 8(3):205–223
Montasari R (2016d) Formal two stage triage process model (FTSTPM) for digital forensic practice. Int J Comput Sci Electron Secur 10(2):69–87
Montasari R (2016e) Review and assessment of the existing digital forensic investigation process models. Int J Comput Appl 147(7):41–49
Montasari R (2017a) Digital evidence: disclosure and admissibility in the United Kingdom jurisdiction. In: Proceedings of the 11th international conference on global security, safety, and sustainability, London, UK, pp 42–52

Montasari R (2017b) A standardised data acquisition process model for digital forensic investigations. Int J Inf Comput Secur 9(3):229–249
Montasari R (2017c) An overview of cloud forensics strategy: capabilities, challenges, and opportunities. In: Hosseinian-Far A, Ramachandran M, Sarwar D (eds) Strategic engineering for cloud computing and big data analytics. Springer, Cham, pp 189–205
Montasari R (2018) Testing the comprehensive digital forensic investigation process model (the CDFIPM). In: Dastbaz M, Arabnia H, Akhgar B (eds) Technology for smart futures. Springer, Cham, pp 303–327
Montasari R, Peltola P (2015) Computer forensic analysis of private browsing modes. In: Proceedings of 10th international conference on global security, safety and sustainability: tomorrow's challenges of cyber security, pp 96–109
Montasari R, Peltola P, Evans D (2015) Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. International conference on global security, safety, and sustainability, London, UK, pp 83–95
Mukasey M, Sedgwick J, Hagy D (2008) Electronic crime scene investigation: a guide for first responders. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. Accessed: 14 May 2018
Mumba E, Venter H (2014) Testing and evaluating the harmonized digital forensic investigation process in post mortem digital investigations. ADFSL conference on digital forensics, security and law, pp 83–97
Nance K, Hay B, Bishop M (2009) Digital forensics: defining a research agenda. 42nd Hawaii international conference on system sciences, pp 1–6
NIST (2015) Computer forensics tool testing handbook. U.S. Department of Commerce. Available at: http://www.cftt.nist.gov/CFTT-Booklet-08112015.pdf. Accessed 14 May 2018
Palmer G (2001) A road map for digital forensic research. 1st digital forensic research workshop (DFRWS), pp 27–30
Pollitt M (2008) Applying traditional forensic taxonomy to digital forensics. In: Advances in digital forensics IV. Springer, New York, pp 17–26
Reith M, Carr C, Gunsch G (2002) An examination of digital forensic models. Int J Digit Evid 1(3):1–12
Rogers M (2004) DCSA: a practical approach to digital crime scene analysis, vol 3, 5th edn. Purdue University, West Lafayette
Rogers M, Goldman J, Mislan R, Wedge T, Debrota S (2006) Computer forensics field triage process model. Conference on digital forensics, security and law, pp 27–40
Selamat S, Yusof R, Sahib S (2008) Mapping process of digital forensic investigation framework. Int J Comput Sci Netw Secur 8(10):163–169
Sherman S (2006) A digital forensic practitioner's guide to giving evidence in a court of law. Proceedings of the 4th Australian Digital Forensics conference, 1–7
Sommer P (2008) Directors' and corporate advisors' guide to digital investigations and evidence. U.K. Information assurance advisory council. Available at: https://www.ucisa.ac.uk/~/media/Files/members/activities/ist/DigitalInvestigationsGuide.ashx. Accessed 14 May 2018
Stanfield A (2009) Computer forensics, electronic discovery and electronic evidence. LexisNexis Butterworths, Chatswood
Trcek D, Abie H, Skomedal A, Starc I (2010) Advanced frame-work for digital forensic technologies and procedures. J Forensic Sci 55(6):1471–1480
Turnbull B (2008) The adaptability of electronic evidence acquisition guides for new technologies. In: Proceedings of the 1st international conference on forensic applications and techniques in telecommunications, Information and Multimedia and Workshop
US-CERT (2012) Computer forensics. U.S. Department of Homeland Security. Available at: https://www.us-cert.gov/security-publica-tions/computer-forensics. Accessed 14 May 2018
Valjarevic A, Venter H (2012) Harmonised digital forensic investigation process model. In: Proceedings of information security for South Africa, pp 1–10

Valjarevic A, Venter H (2015) A comprehensive and harmonized digital forensic investigation process model. J Forensic Sci 60(6):1467–1483

Venter J (2006) Process flow for cyber forensics training and operations. Available at: http://researchspace.csir.co.za/dspace/handle/10204/1073. Accessed 17 June 2015

WhatIsMyIPAddress (2016) How you connect to the world. Available at:http:/whatismyipaddress.com/. Accessed: 14 May 2018

Yusoff Y, Ismail R, Hassan Z (2011) Common phases of computer forensics investigation models. Int J Comput Sci Inf Technol 3(3):17–31

Zainudin N, Merabti M, Llewellyn-Jones D (2011) Online social networks as supporting evidence: a digital forensic investigation model and its application design. International conference on research and innovation in information systems, pp 1–6

Chapter 9
Hybrid Cyber Security Framework for the Internet of Medical Things

Danisa Nkomo and Raymond Brown

Abstract Despite IoMTs benefits in healthcare, emphasise that attaining robust security and privacy is becoming a huge challenge. The increased flow of information from IoMTs endpoints and applications increases the risk landscape; therefore, their security needs to be addressed. The risk to IoMTs includes potential harm to patient safety, compromise to patient health information and unauthorised access to devices. In 2013, 44% of data breaches occurred in the healthcare and in 2017, the National Health Service (NHS) England reported a ransomware attack which affected an estimated 80 trusts and an additional 603 primary care organisations. It is argued that for a sector (healthcare) under constant attack, the introduction IoMTs may be too big of a security risk. However, when the right security measures are in place, IoMTs can deliver more benefits than risk. With regards to The General Data Protection Regulation (GDPR), IoMTs raises compliance issues in the domain of consent. Cyber security frameworks such as ISO 27000 x series, NIST CSF 2018 or COBIT can be used as a guideline to implement security controls in IoMTs. However, some of them are out of date or lack the required approach to protect IoMTs technology. There is a lack of specific standards tailored to IoMTs security, and the need to safeguard patient safety, maintain the security and privacy of patient information that could all help towards more secure IoMT use cases. What is presented in this Chapter is a method to create a hybrid cyber security framework for IoMT. The framework is an extension of the NIST cyber security framework Version 1.1. This could be very useful to the UK healthcare industry as it is moving towards full adoption of IoMTs for benefits explained earlier.

Keywords Internet of medical things · IoT · BIG data · Blockchain · Privacy · Patient safety · IoMT endpoints · IoMT applications · Hybrid cyber security framework (HCSF) · NIST · Design science

D. Nkomo
Barnsley Local Authority, University of Northumbria, Newcastle upon Tyne, UK

R. Brown (✉)
Northumbria University London with QA Higher Education, Newcastle upon Tyne, UK
e-mail: Ray.brown@northumbria.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_9

9.1 Introduction

The Internet of medical things (IoMTs) or medical IoT are medical endpoints and applications with the ability to gather patient medical information and transmit to the desired remote visual platforms. The devices and software applications can self-connect to a gateway to transmit collected patient information (Alsubaei et al. 2017). The new technical ability of medical devices has led to more improved and efficient health care delivery, improved doctor-patient collaboration, adequate diagnosis and medical decision making. Whilst this is great for technological advancement and associated benefits, increasingly this involves the risk of security vulnerabilities.

Marr (2018) reported that the IoMTs endpoints and applications market is expected to reach a staggering 136.8 billion by 2021 worldwide and mentions that the number of medical devices connected to collect data and monitor patients will increase in the future. Marriott (2017) accepts that connected medical devices have considerable benefits in healthcare and the obvious advantages are; remote monitoring, automation, adaptability, precision medicine and local activity recording.

9.1.1 IoMTs Threat Landscape

IoMTs in healthcare present challenges in the privacy and security of information. According to FortiGuard cited in Adefala (2018), the most common threats are triggered by botnets which may take advantage of compromised IoT devices. Zhou et al. (2018) state that a compromised IoMTs device or application is more likely to initiate multiple attack vectors which may be hard to mitigate. Alsubaei et al. (2017) assert that IoMTs devices and applications increase the attack vector due to the complexity of the enabling technology (IoT). Most IoMTs are not secure by design; their wireless capability exposes them to the dangers of wireless sensor network security violations (Jadhav and Vatsala 2017). Most IoMTs solutions are operated, monitored and controlled by software applications. Therefore, there is risk coming from authentication and authorisation violations. Due to the issues mentioned above, the threat landscape for IoMTs has widened. These issues compromise the Confidentiality, Integrity and Availability (CIA) of critical patient data.

9.2 Attack Taxonomy

The need for intelligent patient monitoring and big patient data for effective decision making means the adoption of IoMTs will continue grow. It is expected that the threat landscape will also continue to increase. According to Ali and Awad (2018)

different types of security threats can compromise the functionality of IoMTs networks. Some threats may be hard to predict, while other are obvious. The existing threats to IoMTs can be classified according to their attributes; network, information and host.

9.2.1 Information Based Attacks

Data in transit and data at rest can be intercepted by an adversary to remove information integrity (Chen et al. 2018). For an adversary to perform information-based attacks, the following methods are used:

- **Interception** – an attacker eavesdrops on medical information transmitted through the IoMTs network to compromise data privacy and confidentiality.
- **Modification** – an attacker gets unauthorised access to patient information, tampers with it to create confusion and deceive decision makers.
- **Fabrication** – false information is injected to threaten message authenticity as a result confuses decision makers such as doctors, surgeons, nurses or multidisciplinary teams.
- **Replay Attack** – can replay existing messages to threaten the message freshness.
- **Interruption** – an attacker instigates a distributed denial of service attack which breaks the IoMTs communication gateway. This type of attack threatens network functionality, device functionality, availability and is a risk to patient safety.

9.2.2 Host Based Attacks

These types of attacks are carried by taking advantage of host attributes;

- **User compromise:** an adversary compromises the users IoMTs device and network by obscurity or stealing. Such an attack is known to reveal sensitive information such as date of birth, social security, patient health data (Cafasso and Tarral 2018)
- **Hardware compromise**: an adversary tampers with the physical device where they can extract on device keys, data or programs. A tampered device can be reprogrammed or injected with malicious codes (Alharbi and Aspinall 2018).
- **Software compromise**: an attacker takes advantage of an out of date firmware, operating system of application to force to malfunction (Jadhav and Vatsala 2017).

9.2.3 Network Based Attacks

These types of attacks focus on the network layers and protocols protocol;

- **Standard protocol compromise**: an attacker compromises standard application and networking protocols and behave maliciously to threaten availability, integrity, privacy and authenticity.
- **Network Protocol Stack**: each layer of the protocol stack is vulnerable to attack. Therefore, an adversary may exploit this vulnerability by launching malicious activities (Gupta 2014).

9.3 IoMTs Privacy and Security Classification

The traditional architecture of IoMTs is composed of the perception layer, network layer and application layer, two more layers have been added; middleware and business layer (Ray 2016). The perception layer is composed of sensory devices. A sensory device detects and responds to some form of input from the physical environment. The most common inputs are heat, motion temperature, pressure or other things that can be sensed (Jadhav and Vatsala 2017). The output is a signal that is converted to human readable data. In most cases these will be transmitted over a network for further processing (Jadhav and Vatsala 2017). The Internet of Medical Things is classified into; wearable devices, implantable devices, ambient devices and stationary devices. Wearable devices enable continuous, real time and accurate monitoring of patients. The most common found in a modern healthcare set-up are pulse sensors, heart monitoring sensors, activity sensors, body temperature sensors, location sensors and glucose sensors. Other classifications are as follows:

Implantable devices – provide a visual of the body's internal systems such as a swallowable camera capsule or the embedded cardiac (Marriott 2017).

Ambient devices – these are used to monitor the patient's environment. Ambient devices are designed to monitor activity patterns such as the number of toilet visits, sleep quality or falls. Ambient sensors make the surrounding of the patient smarter. The most common ambient devices are motion, temperature, door, vibration, and pressure and daylight sensors (Marriott 2017).

Stationery devices – are devices isolated or not attached to the patient. These devices include imaging and surgical devices.

9.3.1 IoMTs Architecture and Attack Classification

The IoMTs defines a 3 layer architecture composed of the perception layer, network layer and the application layer.

The perception layer is the physical devices, which transfer the collected data to the network through a gateway. It is important to note that the perception layer is composed of physical devices which are wearable, implantable, ambient and stationery (Alsubaei et al. 2017). The perception layer as the lowest layer of the IoMTs architecture. Suo et al. (2012) also refers to the perception layer as the recognition layer. The role of the perception/recognition is to collect specified information from its surroundings; it collects parameters such as pulse rate, blood pressure, visual images, heartbeat and so on. The information collected is later digitised and transmitted to the healthcare network (HCSN) through a gateway.

The network layer is a data propagation platform; its main role is to facilitate content delivery to its specific destination. The network layer ensures the routing to the destination and network addressing is in check (Alsubaei et al. 2017). The network layer provides wired or wireless capabilities for IoMTs to be able to transmit the collected data. For example, magnetic resonance imaging requires high speed connection and reliable power source therefore require a wired medium (Alsubaei et al. 2017). Low powered IoMT devices may use wireless or radio technology to connect to each node or gateway. IoMT may also connect through to the IoT platform (Wireless Sensor Networks) which has Wi-Fi technology enabled (Anandarajan and Malik 2018).

The application layer is the highest level of IoMT architecture which consists of the middleware and business layer. This layer provide the information collected from the perception layers and displays them in various formats(Suo et al. 2012). The application layers provide the intelligence to make effective medical decisions.

9.4 Attack Classification and Mitigation

9.4.1 Perception Layer

Side Channel attacks: the attack method is based on the measurement of trends and frequencies of an IoMT device to ascertain a pattern. This can be used to extract private information from a system. In IoMT endpoints the transmission timing and power used probes can be used as an attack vector through the analysis of electromagnetic activity on the endpoints to extract patient sensitive data (Zhang et al. 2014; Yessad et al. 2017)

- **Tag cloning**: allows for the creation of a backdoor for data exfiltration from already established tags. The tag(cloned) may then be used to access patient data or a gain access to secure buildings (Ahson and Ilyas 2017).
- **Device tampering:** An IoMT endpoint's physical attributes can be compromised to alter its expected functionality therefore creating a potential risk to patient safety. For example, unsecure USB ports can be an entry point for malware injection (Yessad et al. 2017).

- **Sensor Tracking**: IoMTs endpoints have global positioning systems (GPS) to send patient location during an emergency; an attacker can spoof the GPS of an IoMTs and use this as an attack vector. Patient privacy is at risk from compromised sensors with fall detection capabilities (Yessad et al. 2017).

9.4.2 Network Layer

The network layer interfaces IoMT and the wider internet. Network technologies enables IoMT endpoints and applications communicate with other devices, applications and services in the internet (cloud) (Yessad et al. 2017). It is responsible for connecting IoMT endpoints and applications. Standard protocols define the rules and format that devices adopt to establish a connection. The IoT network is the underlying technology that enables IoMT and is composed of a 4 layer stack (Ahson and Ilyas 2017). The network layer in IoMT is susceptible to various attacks and the most common are;

- **Eavesdropping**: patient sensitive information can be captured during transmission and can be used as a path to launch a more evasive attack (Yessad et al. 2017). Encryption technology solves most of the eavesdropping attacks however it adds overheads which may affect the functionality of IoMT endpoints (Zhang et al. 2014).
- **Replay**: an attacker may recycle an authenticating message that has been exchanged before between authenticated users (Zhang et al. 2014). The authentication message would have been captured through eavesdropping. For example, replay attacks were highly effective in the One Touch Ping Insulin pump due to a vulnerable communication channel (Zhang et al. 2014).
- **Man-in-the-Middle**: a backdoor in IoMTs can allow an unauthorised user to replay legitimate authentication sequences to get access to the gateway (*Communication interface between IoMT and the healthcare network*) (Riahi Sfar et al. 2018).

9.5 The Importance of Cyber Security in IoMTs

From a cyber security perspective, the need for data security has become mandatory. Therefore, having the right security levels is essential to maintain the CIA of information. The application of good measure security controls builds confidence in the use of IoMTs and its use in healthcare improves patient quality of care and quality of experience. However, the exploitation of these devices through cyber hacking creates privacy and patient safety concerns. Marr (2018) states that cyber security in the healthcare industry helps to prevent patient information leakage and maintains patient safety. Therefore, any breach in this domain threatens patient privacy and

exposes them to health risk. For example, a breach in a life critical IoMTs endpoint may compromise patient safety. Therefore, the security of IoMTs is critical to maintaining the privacy and safety of a patient.

9.5.1 Privacy

The lack of security by design of IoMTs creates vulnerabilities that can easily be exploited by an adversary (Ali and Awad 2018). IoMTs are the weakest link in healthcare information security chain. Therefore, insufficient controls may impact on patient privacy. An attacker using different attack techniques can penetrate the network and attack other IoMTs devices then control their operability (Zafari et al. 2016). A compromised, IoMTs device or software application can breach regulatory compliance such as the Data Protection Act (2016) and the General Data protection regulation (GDPR) 2016 which all attracts different fines under its provisions. Despite the general awareness of cyber security in healthcare, there has been a slow response to the constant emerging threat. It is essential to have security measures in mitigating against the ever-changing threat and to maintain the privacy of patient information.

9.5.2 Patient Safety

Patient safety is an essential aspect of the healthcare sector. The adoption of IoMTs in healthcare creates a huge concern for patient safety. Access to patient information may not be attractive to the attacker compared to the deadly cyber-attack on insulin infusion pumps attached to a patient in critical care (Yessad et al. 2017). This type of cyber breach may have a negative impact on the patient's life.

Chen et al. (2018) point out that malware leaks which are designed to steal personal information may impact on the IoMTs which create a risk to patient safety. Antonucci (2017) also points out that the reasons of prolific attacks in the healthcare sector are IoMTs lack robust security. Therefore, this leaves them more vulnerable to malware threats that probe them for such weakness. Many IoMTs devices such as the Continuous Glucose Monitors and insulin pumps run on the same operating system as consumer devices. Therefore, an automated hack cannot differentiate life-critical systems connected to the internet (Kurtz 2017).

A malware attack on a sensitive IoMTs device, such as glycaemic control device, may mean a patient could have severe consequences from an evasive device delivering hazardous drug loads to the patient (Kurtz 2017). There is overwhelming evidence that the threat to patient safety emanating from insecure IoMTs is real. In 2011 a study by Paul et al. (2011) reviewed the security of CGM and the insulin delivery system. The outcome of the study showed that an adversary could eavesdrop on the wireless communication and could control and alter the intended usage

through impersonation. This potential harm to patient safety by vulnerabilities in IoMTs is a huge concern; it compromises the core principles of the healthcare sector. Any attack to IoMTs can have huge implications which are beyond malicious. For example, an attacker can wirelessly exploit vulnerabilities in pacemakers or make a deadly modification to insulin pumps of a large group of users, this may have a devastating impact on patient safety. Therefore, it is crucial to ensure adequate controls are put in place to maintain patient safety.

Following the privacy and security compromises to IoMTs, Zhou et al. (2017) stated that most cyber security risks can be prevented using existing frameworks, technology and standards. However, the dynamic nature of IoMTs creates new security challenges, and the key consideration is the accountability of risk which may not be aligned with today's threats landscape.

9.5.3 IoMTs Impact and Risk

Risk is the likelihood that a specified threat will take advantage of a weakness of an information asset (Jones and Ashenden 2005). Risk is measured as the likelihood of an event and the severity of an event (Katsikas 2013). Impact refers to the action of one object coming forcibly into contact with another (Jones and Ashenden 2005). In cybersecurity, the impact of a security breach is divided into economic cost, reputational damage and legal consequences (Ulsch 2014).

According to Biener et al. (2015), breaches often result in financial losses. Many people have entrusted the healthcare sector with their personal information, and any cyber breach compromises those trusting relationships (Biener et al. 2015). This could also damage the healthcare reputation and erode the trust held by patients. Data protection and privacy laws require organisations including healthcare to manage the security of personal data they hold. A security breach can comprise the personal data. Therefore, the organisation may face fines and regulatory sanctions under the new Data Protection Act of 2016 and GDPR (2016) provisions (Coventry and Branley 2018).

There is no doubt that IoMTs devices introduce risk, malicious actors may manipulate the flow of information from these devices or can tamper with the device. This may lead to a breach of valuable patient information resulting in loss of patient privacy and potential disruption to critical infrastructure. The implementation of security in IoMTs depends on its function within the healthcare organisation. What is more essential is to ensure the risk assessment is done following cyber security best practice, and that controls are in place to safeguard against the risk. The National Cyber Security Centre(NCSC) (2018a, b, c) points out that implementing security best practice is correlated to organisational risk. Therefore, this needs careful and robust attention.

9.6 Cyber Security Best Practice Frameworks

The best security practice should be strategic, operational and tactical. Following the past cyber security breach in healthcare. The best practice involves following the prescribed framework, standards and regulation that govern alignment with the healthcare sector. The best practices involve policies and procedures, frameworks and standards to identify any threats and vulnerabilities. These are then used to formulate incidence response methods along with recovery in case of disaster. In a healthcare environment the best practice assigned to cyber security are the following;

- ISO/IEC 27000: series is an international cyber security best standard and best practice (Van Haren 2014; International Standards Organisation 2018). It outlines how risk should be managed in information systems and provide controls for the security of information systems.
- ISO/IEC 27030: Internet of Things standards and best practice
- ISO/IEC 27799: offers guidance on security controls in healthcare and medical organisations (ISO 27001 Security 2018).
- NIST Cyber Security Framework Version 1.1: provides a framework for information security. It provides a policy framework of how an organisation can, identify, detect, protect, respond and recover from a cyber-attack (NIST 2018). CSF V1.1 now in incorporate the internet of things which is the enabling platform for IoMTs (NIST 2018).
- NIST Special Publication 800-53: a cyber security framework that incorporates the risk management framework to address cyber security controls for federal information (NIST 2018)
- Information Security forum: provide more thorough controls and direction on existing and evolving cyber security issues. it offers a comprehensive coverage of the provisions set out in the ISO/IEC 27002: 2013, COBIT 5 for information security, NIST CSF and the Payment Card Industry Data Security Standard (PCI DSS) version 3.1 (Information Security Forum 2016).
- HMG security policy framework (SPF) – a framework that provides principles to cover cyber security and these include; good governance, risk management, awareness, personal and physical security (NCSC 2018a, b, c).
- Health Information Trust Alliance (HISTRUST)- a framework that ensures information security in the healthcare sector. Through its common security framework, it ensures compliance with regulations and standards.

The above standards are focused on implementing the right security control, policies and procedures within an organisation. The best practice should be able to fit into the internal organisational processes. The complexity of the healthcare sector means the best practice adopts one framework combined with elements from other frameworks to ensure robust security.

9.6.1 Review of Cyber Security Best Practice Frameworks

The ISO/IEC 27000x series is a governance framework to manage cyber security in the organisation using policies and procedures at an operational level (International Standards Organisation 2018). The NIST SP 800-53 provides a practical way of implementing control through identification, protection, detecting, responding and recovering from an operational level. The Information Security Forum (ISF) is a process and business-driven, it provides a guideline for managing cyber security from a business perspective (NIST 2018). The ISF operates at a strategic and operational level within the organisation through the identification of gaps and setting goals to maturity levels (Information Security Forum 2016). Cyber essential is an entry-level assurance framework which provides guideline against the most common cyber threats on the internet and demonstrates that an organisation is committed to cyber security through implementation of the five technical controls (NCSC 2018a, b, c). HITRUST provide clear guidance to improve security using a risk-based approach to secure critical infrastructure and provide alternative controls.

9.6.2 IoMTs Best Practice and Principles

The cyber security best practice framework discussed above is not usable for IoMTs adoption. IoMTs adoption requires consideration of artefacts from various cyber security frameworks. It is important to note that there is no defined best practice in IoMTs. However, the best practice can be derived from the enabling technology (IoT) The best practice landscape within IoMTs are based on framework from other information systems. In IoT cybersecurity, consideration of frameworks tailored to other sectors is vital to secure IoT environment (Alsubaei et al. 2017). The Department of Homeland Security (2016) suggests that the best practice to manage risk and security of IoT enabled devices is adopting strategic principles. The best practice principles to security the IoT environment should;

- Ensure integration of cyber security in the design phase
- Advanced patch and vulnerability management
- Ensure cyber security measures are aligned with the potential impact of risk
- Promote transparency across IoT devices and infrastructure
- Perform proactive risk assessments and Identify whitelist applications
- Use of multi-factor authentication
- Create staff awareness and create incident response plans
- Regular data backup and limit administrative privileges

The IoT best practices support how cyber security is handled within an organisation. The adoption or introduction of new technologies such as IoMTs needs a new and different approach that is distinct from the generic cyber security framework and best practice. Alharbi and Aspinall (2018) state that the best practice can be

used as requirements to design a framework and these should be based on the threat and vulnerability analysis. The requirements of IoMTs are risk specific, therefore, the best practice approach may fail to address cyber security in their complex environment.

9.6.3 Blockchain for IoMT Security

The adoption of IoMT provides the potential for big data analysis and effective medical decision making. However, the adoption of IoMT exposes the patient safety and privacy at risk. Therefore, there is an urgent need to find the most effective way to secure patient sensitive data. Also, failure to ensure the safety and privacy of patient information amounts to a breach of legislation and compliance. The security attributes offered by the blockchain technology have been considered to offer robust security of patient privacy. In addition, the technology (Blockchain) promises to reduce the risk of IoMT endpoints to be compromised through a central authority (Rivas and Wac 2018). Blockchain allows the creating of consensus groups on anomalous network behaviours and has the potential to fail-safe infected IoMT endpoints (Rivas and Wac 2018). Blockchain technology can quarantine any IoMT endpoints whose behaviour is questionable. However, the risk on this capability need to be clearly defined as it has the potential to impact on patient safety.

Blockchain embeds strong cryptography to each IoMT endpoint and creates a secure communication channel (Jesus et al. 2018). It is also ensures anonymity in IoMT use and guarantees patent privacy. Adopting the Blockchain technology offers effective traceability, patched management and maintains data security of IoMT (Trend Micro 2018). Other potential benefits includes the removal of single point of failure and building trust zones between IoMT processed (Trend Micro 2018).

9.6.4 IoMT and Big Data: The Impact of IoMT on Clinical Trials

In a clinical trial space, electronic record storage, data capture and digital trial management is the norm in most clinical research. IoMT as the enabler of Big data captures that data from patients from clinical trials. Using IoMT in clinical trials means behavioural change can be monitored effectively (Mishra et al. 2018). The IoMT capability of metric tracking allows the collection of accurate biological data from patients, which can then be shared between clinical research organisations (Iqbal 2017). Using data captured from IoMT along with accumulated clinical results creates more valuable clinical trials with ground-breaking results (Iqbal 2017).

IoMT capability to collect large volumes of data from patient creates the potential to make effective healthcare decisions(Ahmed et al. 2017). In healthcare, Big Data is mainly focused on machine or clinical data, transactional data and social data The Chartered Society of Physiotherapy (2018) state that big data is the future of healthcare delivery and data can be shared and analysed to improve patient safety and care. Big Data plays a big role in healthcare because of its potential to predict any outbreaks, improve quality of life and cure diseases. In a clinical setting, big data is used in evidence based practice to ensure patient safety.

9.6.5 Hybrid Cyber Security Framework (HCSF)

According to NIST (2018) a robust framework should focus on technology, processes and people.

Therefore, developing a cyber security framework must be based on several approaches for it to be effective.

A cyber security framework 's primary objective is to safeguard the CIA of IoMTs devices and applications. The framework incorporates guidelines from standards, regulatory compliance, best practice such as the ISO 27032, NISA CSF, Data Protection Act 2018 and GDPR 2018.

These features provide robustness in the security of IoMTs endpoints and software applications.

An effective cyber security framework requires the management of information security and is based on people, processes and technology. The HCSF pillars consist of IoMTs, Stakeholders, Technical and operational controls and Governance as illustrated in Fig. 9.1.

Consideration of this asset pillar involves the protection and mitigating critical IoMTs endpoints and applications. The protection should be done through the processes defined in the NIST CSF Version 1.1. IoMTs endpoints and software application are classified into; life critical, non-critical monitoring systems and wellness devices.

- ***Life critical IoMTs devices and applications*:** These are safety critical medical endpoints and software applications. Any breach can have an adverse impact on patient safety. Therefore, their availability is critical. The security of life-critical systems and applications should be a top priority in an organisation. Assets in this category are; pacemakers, ventilators, defibrillator and insulin pumps.
- ***Non- critical monitoring devices and applications:*** Non- critical monitoring devices and applications record and transmit data in the same way as life critical systems, they do not monitor life-threatening conditions. Assets in this domain are glucose monitors. if a glucose monitor fails, the patient will require medical attention but not at the same level of urgency as a pacemaker or ventilator.
- ***Wellness devices*:** Wellness devices and application track sleeping patterns, personal health and wellness such as fitbits or activity trackers. Wellness devices do not gather data to be relayed back to the healthcare professional.

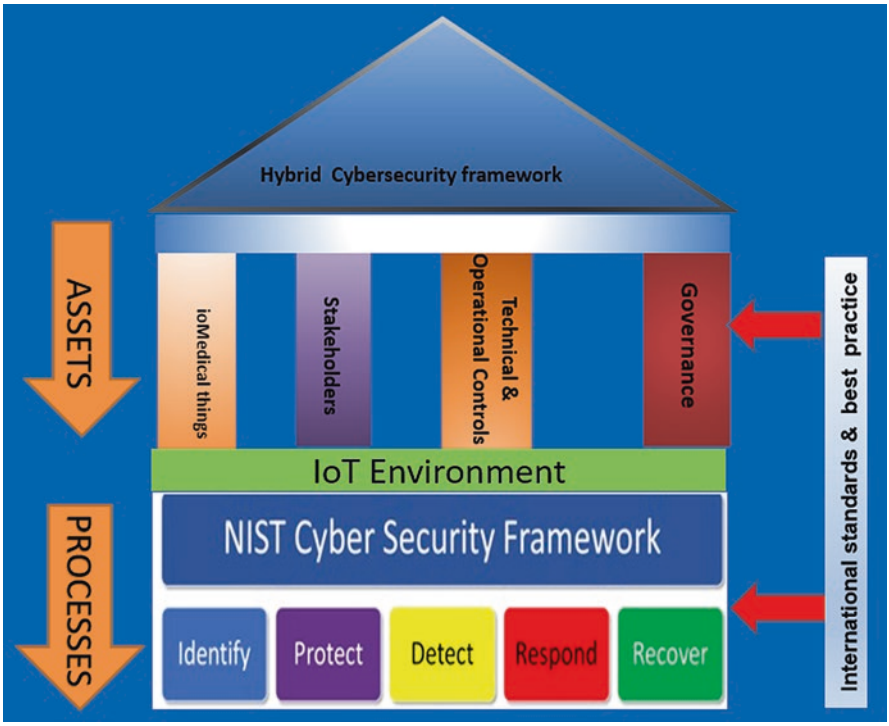

Fig. 9.1 Assets and processes in IoMTs

According to Harbers et al. (2018), the development of a cyber security framework is challenged by a fractured process which mostly leads to more legislation to keep up to date with emerging threats. It is important to consider current legislation in a framework as it ensures compliance. The HCSF incorporate the Data Protection Act (2018), GDPR (2018), The Network and Information Systems Regulations 2018, the Health Insurance Portability and Accountability Act, PCI DSS. Also, it also incorporates the provisions of ISO 27030, 27779, Risk management in connected healthcare ISO 80001. Governance also involves best practice in the implementation of security controls.

9.6.6 Operational and Technical Controls

The operational and technical considerations include the security control measures to safeguard the CIA of critical infrastructure and assets pillars.

9.6.6.1 Stakeholders

These are people with a vested interest in and are affected by IoMTs. Such stakeholders include vendors, patients, clinicians, supplier, CISO, infrastructure teams and healthcare facilities. The CISO should be the primary stakeholder and driver of the HSCF. The internet service providers and power supply organisations will be among the key stakeholders.

9.6.6.2 Processes

The HCSF is governed by processes to support its main pillars. These processes form the activities that occur within the pillars of the framework. The processes are taken from cyber security best practices such as NIST CSF Version 1.1 draft 2. The figure shows the processes from the NIST framework (Fig. 9.2).

- **Identify**

The identification of IoMTs assets and keeping an asset register is a practical approach towards maintaining the availability of services. The identification process in HCSF involve;

Asset Management IoMTs endpoints and application should be managed through an asset register. This should be done in line with their relative importance to the organisation risk strategy. The classification of endpoints and applications should be based on the value of maintaining patient safety, best practice and regulatory compliance.

Governance the policies, procedures and processes to manage and monitor regulatory, legal, risk, operational and environmental requirements are determined, and these should be part of the risk management.

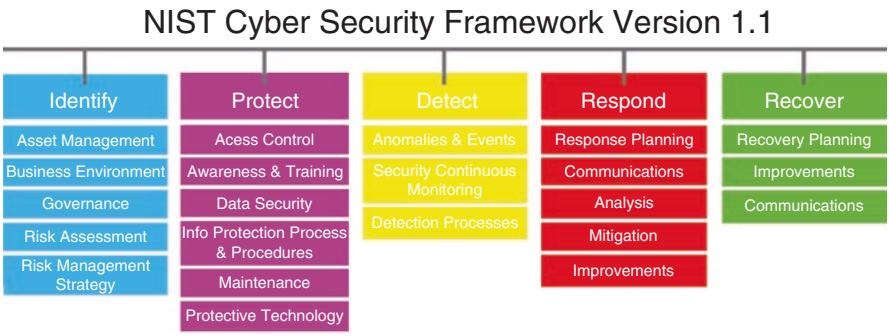

Fig. 9.2 NIST Cyber Security Framework Version 1.1

Risk Assessment IoMTs endpoints and application threats and vulnerabilities are identified and documented following industry best practice. The potential impact and likelihood of a compromise to the IoMTs environment, endpoints and applications are identified.

Risk Management stakeholders should agree on risk assessment processes and how they should be managed. Risk tolerance should be established and clearly expressed.

- **Protect**

Access Control access to IoMTs environment, endpoints and application must be limited to authorised users or endpoints and applications limited to authorised activity. Identity and credentials should be managed for authorised endpoint and applications, and access permission should be granted on the principle of least privilege. For life-critical endpoints and application network integrity should be enforced through network segregation.

Awareness and Training users should be trained and informed of their roles and responsibilities within IoMTs. This also includes 3rd party stakeholders.

Data Security IoMTs data at rest and data in transit should be protected, and Integrity checking mechanism should be used to verify IoMTs software applications, firmware and information integrity. To ensure data security in IoMTs endpoints and applications, the production environment should be isolated from testing and development.

Protection Processes and Procedures IoMTs security policy should be integrated into a more comprehensive information security policy. The policy should address the scope, roles, coordination and management commitment. Protection policies must comply with current legislation and be improved on a regular basis. Response and recovery plans must be managed and tested in line with policies.

Protective Technology technical security solutions should be auditable and reviewed according to policies and procedures.

- **Detect**

Monitoring Monitoring at discrete intervals should be enforced to identify security compromises and to determine the effectiveness of protective measures. Monitoring for unauthorised personnel, connections, devices, and software should be performed.

Detection Processes roles and responsibilities should be defined to ensure accountability. Event detections reported to appropriate parties and that they comply with best practice. Detection processes should be tested on a regular basis to ensure applicability.

- **Respond**

Communication response activities should be coordinated with internal and external stakeholders. Where appropriate this should include support from law enforcement. Communication should be established in line with service level agreements and regulatory compliance. Information sharing should also ensure broader situational awareness.

Analysis this should be carried out to ascertain sufficient response and support recovery actions. This involves investigating notifications from IoMTs devices and applications. The impact of an incident should be understood, and forensics performed following cyber security best practice.

Mitigation activities should be carried out to prevent the spread of an event and mitigate its effect and get rid of the incident.

Improvement improvement should be developed from lessons learned from current and previous detection response activities.

- **Recovery**

Recovery Planning the recovery plan should be implemented during or after an event, and the recovery plan should integrate lessons learnt. The recovery strategy should be updated according to organisational policies and procedures.

Communication restoration of activities should be coordinated with internal and external stakeholders (Internet Service Providers, vendors, patients).

9.6.7 IoT Environment

The IoT environment is an enabling infrastructure for IoMTs endpoints and software application functionality. The IoT environment is interfaced with either the cloud environment or desired remote location. The IoT environment is composed of the gateway which manages the communication between IoMTs endpoints and the back-end systems. The IoT primary function is to route messages to and from endpoints (IoMTs devices and applications). Through the gateway, the environment can perform critical tasks such as device discovery, network driver deployment, management functionality, authentication and security set up. The IoT environment is a critical asset in this framework.

9.6.8 International Standards and Best Practice

International standards ensure the right policies and procedures are in place to comply with regulation and best practice. HCSF is supported by international standards in such ISO 2700 x series, HIPAA, ISO 80001 and the NIST CSF V1.1 draft 2. Also, HCSF is supported by cyber security best practice which creates a security culture within the organisation. The best practice in this domain means the stakeholders responsible for security should have a layered approach to security. In the case of medical IoT, they should have the ability to fail safe. In addition, best practice means following a risk-based approach to determine risk exposure and potential impact.

9.7 Conclusions

The key assets of a hybrid Cyber Security framework are IoMTs endpoints, software applications, stakeholders, technical and operational controls and governance. The processes are used to support the efficiency of control assets with requirements based on regulatory compliance. The application of Design Science Research informs the development and attempts to stretch the boundaries of human and organisational ability by creating new and ground-breaking artefacts such as methods, constructs, models and instantiations (Hevner and Chatterjee 2010).

The proposed hybrid cyber security from IoMT is adopted from the NIST Version V1.1. The framework is supported by security best practice and international standards. A layer of the IoT environment sits between the framework processes and the asset pillars. This is a gateway to the corporate network. Although, the lack of relevant cyber security framework in the UK in this domain meant benchmarking is restricted, however, an attempt to benchmark was made to determine how the framework performs against well-established cyber security framework. The prototype hybrid security framework is specific to medical IoT and is based on the NIST framework making it more robust in the provision of cyber security control medical IoT.

References

Adefala L (2018) Healthcare experiences twice the number of cyber attacks as other industries. Retrieved from https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

Ahmed E, Yaqoob I, Hashem I, Khan I, Ahmed A, Imran M, Vasilakos A (2017) The role of big data analytics in internet of things. Comput Netw 129:459–471. https://doi.org/10.1016/j.comnet.2017.06.013

Ahson S, Ilyas M (2017) RFID handbook. CRC Press
Alharbi R, Aspinall D (2018) An IoT analysis framework: an investigation of IoT smart cameras' vulnerabilities. Living in the internet of things*:* cybersecurity of the Iot – 2018. https://doi.org/10.1049/cp.2018.0047
Ali B, Awad A (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 18(3):817. https://doi.org/10.3390/s18030817
Alsubaei F, Abuhussein A, Shiva S (2017) Security and privacy in the internet of medical things: taxonomy and risk assessment. 2017 IEEE 42Nd conference on local computer networks workshops (LCN Workshops). https://doi.org/10.1109/lcn.workshops.2017.72
Anandarajan M, Malik S (2018) Protecting the Internet of medical things: a situational crime-prevention approach. Cogent Med 5(1):1–23. https://doi.org/10.1080/2331205x.2018.1513349
Antonucci D (2017) The cyber risk handbook, 1st edn. Wiley
Biener C, Eling M, Wirfs J (2015) Insurability of cyber risk: an empirical analysis. SSRN Electron J. https://doi.org/10.2139/ssrn.2577286
Cafasso M, Tarral M (2018) Designing flexible sandboxing solutions to adapt to new malware trends. Comput Fraud Secur 2018(2):5–9. https://doi.org/10.1016/s1361-3723(18)30013-7
Chen K, Zhang S, Li Z, Zhang Y, Deng Q, Ray S, Jin Y (2018) Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. J Hardw Sys Secur 2(2):97–110. https://doi.org/10.1007/s41635-017-0029-7
Coventry L, Branley D (2018) Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 113:48–52. https://doi.org/10.1016/j.maturitas.2018.04.008
Department of Homeland Security (2016) Strategic principles for securing the internet of things (IoT). Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
Gupta M (2014) Handbook of research on emerging developments in data privacy advances in information security, privacy, and ethics (1st edn.). IGI Global
Harbers M, Bargh M, Pool R, Van Berkel J, Van den Braak S, Choenni S (2018) A conceptual framework for addressing IoT threats: challenges in meeting challenges. In: Proceedings of the 51St Hawaii international conference on system sciences. https://doi.org/10.24251/hicss.2018.278
Hevner A, Chatterjee S (2010) Design research in information systems. Springer, New York
Information Security Forum (2016) The standard of good practice for information security 2016. Retrieved from https://www.securityforum.org/uploads/2016/07/SoGP-2016-Exec-Summary-FINAL-260716.pdf
International Standards Organisation (2018) ISO/IEC 27030 — Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT) [DRAFT. Retrieved from http://www.iso27001security.com/html/27030.html
Iqbal S (2017) IoMT and big data: the impact of the Internet of medical things on clinical trials. Retrieved from https://knect365.com/clinical-trials-innovation/article/5024ec64-030e-4ba6-bc2b-c701a28b2b95/big-data-and-iomt-the-impact-of-the-internet-of-medical-things-on-clinical-trials
Jadhav R, Vatsala V (2017) Security issues and solutions in wireless sensor networks. Int J Comput Appl 162(2):14–19. https://doi.org/10.5120/ijca2017913256
Jesus, E., Chicarino, V., de Albuquerque, C., & Rocha, A. (2018). A survey of how to use blockchain to secure internet of things and the Stalker attack. Secur Commun Netw, 2018, 1–27. doi: https://doi.org/10.1155/2018/9675050
Jones A, Ashenden D (2005) Risk management for computer security. Elsevier Butterworth-Heinemann, Amsterdam
Katsikas S (2013) Risk management. Comput Inf Secur Handb:507–527. https://doi.org/10.1016/b978-0-12-803843-7.00034-x
Kurtz J (2017) Hacking wireless access points. Syngress, Amsterdam
Marr B (2018) Why the internet of medical things (IoMT) will start to transform healthcare in 2018. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#74b4d7504a3c

Marriott N (2017) Why the internet of medical things is the future of healthcare [Infographic, Video]. Retrieved from https://www.nexeonmed.com/media/why-the-internet-of-medical-things-is-the-future-of-healthcare

Mishra D, kumar S, Ashu A (2018) Internet of things: a survey on enabling technologies, application and standardization. SSRN Electron J. https://doi.org/10.2139/ssrn.3170749

National Cyber Security Centre (2018a) Homepage. Retrieved from https://www.cyberessentials.ncsc.gov.uk/

National Cyber Security Centre (2018b) Risk management and risk analysis in practice – NCSC Site. Retrieved from https://www.ncsc.gov.uk/guidance/risk-management-and-risk-analysis-practice

National Cyber Security Centre (2018c) 10 steps to cyber security – NCSC Site. Retrieved from https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

NIST (2018) NIST releases version 1.1 of its popular cybersecurity framework. Retrieved from https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Paul N, Kohno T, Klonoff D (2011) A review of the security of insulin pump infusion systems. J Diabetes Sci Technol 5(6):1557–1562. https://doi.org/10.1177/193229681100500632

Ray P (2016) A survey on internet of things architectures. J King Saud Univ Comput Inf Sci 30(3):291–319. https://doi.org/10.1016/j.jksuci.2016.10.003

Riahi Sfar A, Natalizio E, Challal Y, Chtourou Z (2018) A roadmap for security challenges in the internet of things. Digit Commun Netw 4(2):118–137. https://doi.org/10.1016/j.dcan.2017.04.003

Rivas H, Wac K (2018) Digital health: scaling healthcare to the world health informatics, 1st edn. Springer, Cham

Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. 2012 International conference on computer science and electronics engineering. https://doi.org/10.1109/iccsee.2012.373

The Chartered Society of Physiotherapy (2018) Big data is key to the future of the NHS, conference hears. Retrieved from https://www.csp.org.uk/news/2018-03-01-big-data-key-future-nhs-conference-hears

Trend Micro (2018) Blockchain: the missing link between security and the IoT? – Security news – Trend micro PH. Retrieved from https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/blockchain-the-missing-link-between-security-and-the-iot

Ulsch N (2014) Cyber threat!: how to manage the growing risk of cyber attacks, 1st edn. Wiley, Hoboken

Van Haren (2014) Global standards and publications. Van Haren Pub, [Place of publication not identified]

Yessad N, Bouchelaghem S, Ouada F, Omar M (2017) Secure and reliable patient body motion based authentication approach for medical body area networks. Pervasive Mob Comput 42:351–370. https://doi.org/10.1016/j.pmcj.2017.06.009

Zafari F, Papapanagiotou I, Christidis K (2016) Microlocation for internet-of-things-equipped smart buildings. IEEE Internet Things J 3(1):96–112. https://doi.org/10.1109/jiot.2015.2442956

Zhang M, Raghunathan A, Jha N (2014) Trustworthiness of medical devices and body area networks. Proc IEEE 102(8):1174–1188. https://doi.org/10.1109/jproc.2014.2322103

Zhou J, Cao Z, Dong X, Vasilakos A (2017) Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag 55(1):26–33. https://doi.org/10.1109/mcom.2017.1600363cm

Zhou W, Jia Y, Peng A, Zhang Y, Liu P (2018) The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J:1–1. https://doi.org/10.1109/jiot.2018.2847733

Chapter 10
BMAR – Blockchain for Medication Administration Records

I. Mitchell and S. Hara

Abstract Medication Administration Records are crucial documents in the care and quality offered to service users. Audits will inspect MAR sheets and these will form a significant impact on the outcome of Medication Management. This impact will be combined with inspections of registered hospitals, care and residential homes across the healthcare profession. The proposal is to build a prototype using blockchain technology to implement MAR sheets, essentially building a blockchain application that stores electronic health records (EHR). The use of permissioned blockchain technology provides confidentiality and trust with the auditors (e.g., CQC). The prototype is tested on two scenarios and results are encouraging. The results indicate that reminders can be sent to healthcare professionals and other consequences of the implementation of EHR and *permissioned* blockchain.

Keywords Medical Administration Records (MAR) · Electronic Health Records (EHR) · Care Quality Commission (CQC) · Blockchain

10.1 Introduction

The medication administration is an important procedure for ensuring the high quality of care delivered by healthcare professionals. Healthcare providers use a Medication Administration Records sheet to record the information about the administration of medicine by healthcare professionals to its service users.

Many systems have been developed and significant improvements to medication management can be achieved by using automated systems (Bates et al. 1998) and mild improvements to medication management can be achieved by sending reminders to healthcare professionals (Bennett et al. 2003). So, the design, development and implementation of an automated system for the completion of MAR sheets is

I. Mitchell (✉) · S. Hara
Middlesex University, London, UK
e-mail: I.Mitchell@mdx.ac.uk; s.hara@mdx.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_10

not new, what is new is the ability to implement MAR sheets using blockchain technology and the advantages it may bring.

It is difficult to write a paper on blockchain without mentioning BitCoin (Nakamoto 2008) since it is the predecessor of all blockchain applications. Bitcoin uses blockchain to record transactions between two or more Bitcoin wallets. So what is blockchain? In simple terms, it is an append-only encrypted ledger, that requires consensus to be updated. There are two important terms here that make blockchain ideal for auditability, which are: append-only – means that data added to the blockchain is immutable, without considerable effort it cannot be changed; and consensus – there is a decentralised component that requires all nodes in the network to have consensus before updating, this promotes trust between parties in the network.

Tokens, or coins, are often used when items of value are exchanged, in many applications tokens are not required since items of value are not exchange. Whilst information is exchanged in BMAR, it does not have monetary value and therefore no tokens are required – BMAR will be tokenless.

Finally, there are two important differences in the implementation of blockchain applications, these are *permissioned and* permissionless. Permissionless, allows the nodes, that are part of a consensus, to be added without permission of the system. This is compared with permissioned blockchain that only allows authorised nodes to be added to the network – this has the added benefit of keeping data confidential to only those authorised nodes and further restrictions can be added to individual users.

In summary, the application developed is a tokenless permissioned blockchain, this results in data being append-only and immutable, which is ideal for audits, and keeps data confidential due to the encryption used in the blockchain technology. The implementation will be carried out using Hyperledger Fabric and Composer (Hyperledger architecture 2017, 2018) and results and recommendations are reported in Sects. 10.3 and 10.5, respectively.

10.2 Design

There are some key transactions of information in Medical management, which are as follows:

Prescription
A qualified individual has to prescribed the medication and dosage, e.g. a Medical Doctor.

Administration
A qualified individual has to administer the medication, e.g. Nurse.

Management
A manager would oversee the schedules, delegate appropriate staff to the administration of medication, and register service users with the Healthcare Provider.

Observe
Administration of controlled substances requires observation of the administrator that provides a witness. This account is also recorded.

Audit
External and Internal Audits occurs

There are key individuals involved in the transactions of information in BMAR application. For the scope of this application this includes:

Doctor
Ability to *prescribe* medication to patients. There are many individuals that can prescribe medication, but for the scope of this paper, the individual will be referred to as a Doctor.

Nurse
Ability to administer medication to patients. There are many individuals that are qualified to complete this task and come under the umbrella term, healthcare professionals.

Patient
Receives medication and uses the services of the home, often referred to as a resident or service user.

Home
The location of the patient, could be a hospital or a care home. The home is inspected and 1 or more patients reside there. The home offers a service and is often referred to as a healthcare provider.

Auditor
Qualified individual that inspects the home and reports if it is fit for purpose. Typically from an external agency, e.g., in the UK the Care Quality Commission (CQC).

Manager
Manager of the home and responsible for the quality of care given to patients.

Witness
Controlled substances require observation of the individual administering the medication. Usually, a manager or a different healthcare professional.

With the above terms of reference, Fig. 10.1 illustrates the interaction between users and the system. Whilst it is appreciated that not all healthcare professionals who administer medication have Nurse qualifications, it is done for simplicity and understanding, likewise for other users in the system.

The five use cases coincide with the five stages identified in the list above. These are the transactions and is the data stored on the network. There is a worry about such data being immutable and therefore care has to be taken about the rights of individuals to remove data (Council of European Union 2018). Data on the blockchain cannot be removed, so transactions would have to store data that is at least pseudo-anonymised. The data stored in the system, registries referring to unique

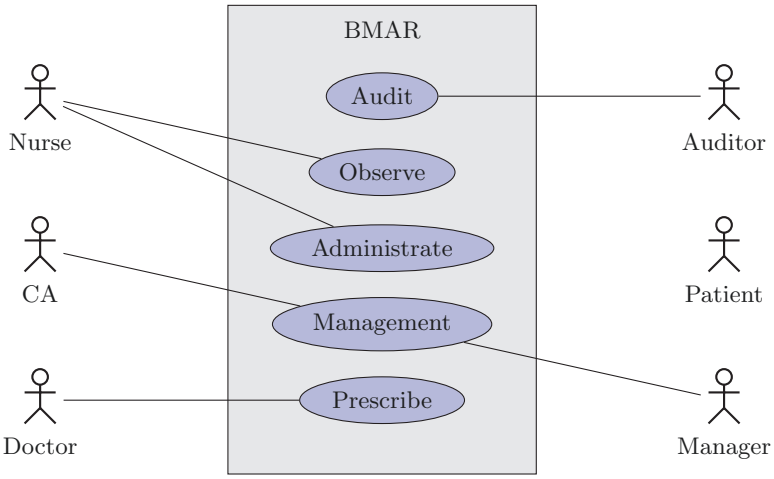

Fig. 10.1 Use: Case diagram for BMAR. Central Authority (CA) is a NHS trust, or private healthcare provider

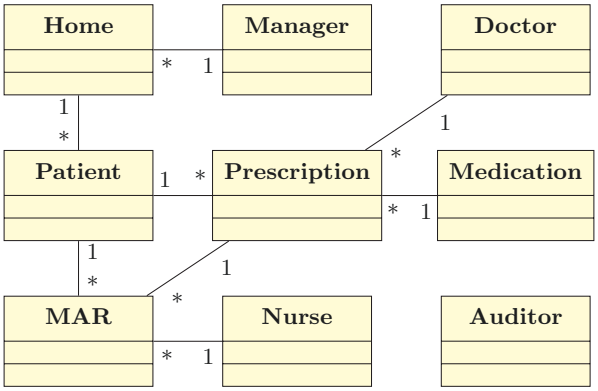

Fig. 10.2 Simplified class diagram for BMAR, omitting attributes

identifiers on the blockchain, can be removed and thus protect the rights of individuals. However, the security of data on permissioned blockchain applications is encrypted and secure, see (Gupta 2018, ch. 5) for further details (Fig. 10.2).

10.2.1 Data Protection

In the UK all e-Health applications need to comply with the seven Caldicott principles (Caldicott 2013). BMAR would be no exception and the following has been considered during the design of the system:

1. Justify the purpose: MAR sheets already exist and data is being collected on service-users and their medication administration. The justification is to design an automatic system to complete the task and store the data electronically for future audits.
2. Don't use personal confidential data unless it is absolutely necessary: The transactions are immutable and therefore considerable care has been taken to ensure that the minimum amount of data is included. The transactions are designed to include no personal information to identify participants, including healthcare professionals and service users. Permissioned blockchain technology is highly secure and encrypted, therefore protecting data.
3. Use the minimum necessary personal confidential data: De-duplication of data are kept to a minimum in the design. Data on both the participants and the assets, stored in the registries, have low volatility, and whilst changes occur it is not every second. However, data transferred in the transactions, stored in the blockchain, have high volatility.
4. Access to personal confidential data should be on a strict need-to-know basis: Access control language allows only certain users to access certain registries and therefore access is strictly on a need to know basis. Role-based attribute control (RBAC) (Richard Kuhn et al. 2010) is employed to ensure correct and appropriate access.
5. Everyone with access to personal confidential data should be aware of their responsibilities: Training at induction and regular supervision would ensure that all staff are aware of their responsibilities, something that is outside the scope of the system.
6. Comply with the law: BMAR would meet with current laws and regulations about sharing and using e-Health information.
7. The duty to share information can be as important as the duty to protect patient confidentiality: At all times patient confidentiality is kept. The ingenuity of blockchain not only allows and promotes sharing of data but also extends it. For example, a Healthcare Provider, X, intends to join the BMAR blockchain, which already hosts 20 other Healthcare Providers. The disintermediatory nature (Gaur et al. 2018) allows new organisations to join the blockchain without compromising existing data. So, our new Healthcare Provider, X, can join BMAR without viewing MAR sheets from other organisations, allowing its own staff to manage its own information, GPs to complete prescription information, and, more importantly, seamlessly allow auditors, such as the Care Quality Commission (CQC) to view their MAR sheets.

10.2.2 Prescription

The scope of BMAR is not to include prescriptions, however, it is appreciated that a qualified individual, e.g., a medical doctor, would have to prescribe medication. Figure 10.3 shows a simplified prescription process, the prescriber has to write one

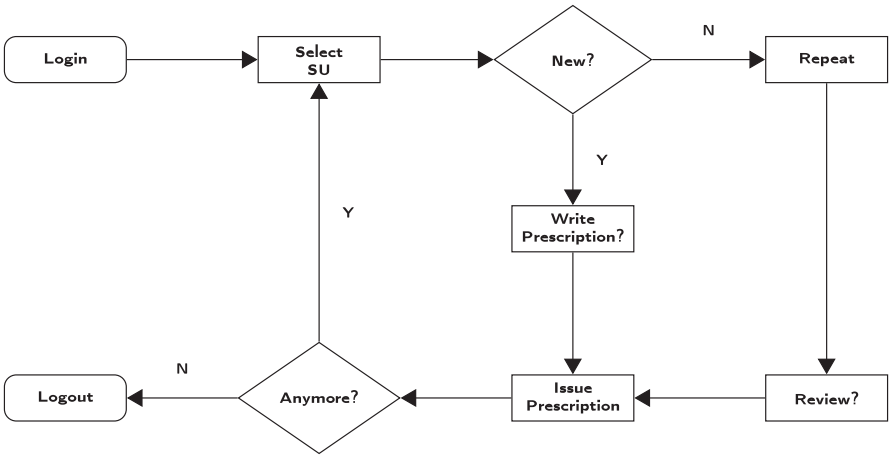

Fig. 10.3 Flowchart for completion of prescription. (Note, the scope of this application is not to implement the prescription processes and procedures and therefore simplified. Abbreviation: *SU* Service User)

medication per prescription. This means that an individual requiring multiple medications would receive multiple prescriptions.

The flowcharts in Fig. 10.3 is by no means to replace the expertise available to the GP, this goes for the other flowcharts. However, the flowcharts do cover the process of issuing a prescription, and in particular looks at a selection of a service user and issuing repeat or new prescriptions. Once complete the GP either selects another, or the same service-user to issue another prescription. Such processes do not simulate the process of issuing multiple prescriptions and would annoy the user. This is the process, the procedure for issuing multiple prescriptions could easily be completed concurrently.

10.2.3 Management

There are many managerial tasks that could be included here, two were chosen to demonstrate that permissioned blockchain has the capabilities to facilitate such tasks. Two tasks were chosen and discussed below.

10.2.3.1 Assign Key Worker

Whilst outside the scope of this prototype, it is recognised that key workers are assigned to service users and have important responsibilities. Assigning a key worker is a managerial duty and is demonstrated here to show how blockchain applications can accommodate such processes as a transaction.

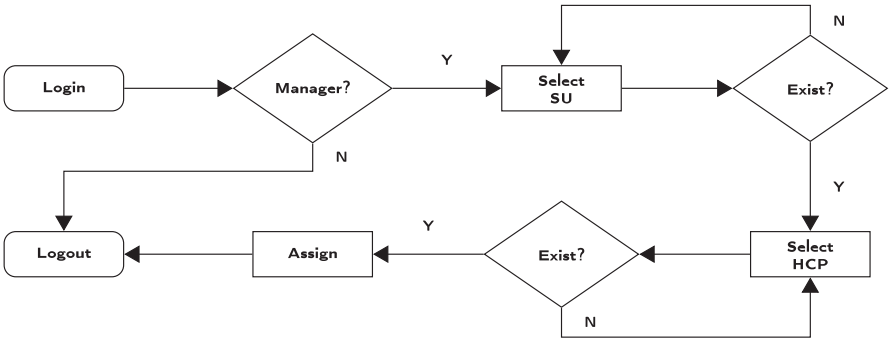

Fig. 10.4 Flowchart for completion of assigning keyworker to service-user (Patient). (Abbreviations: *SU* Service User, *HCP* Healthcare Professional)

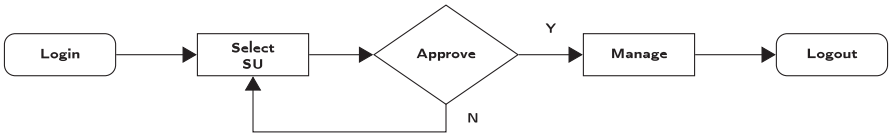

Fig. 10.5 Flowchart for registering a service-user with a healthcare provider. (Abbreviations: *SU* Service User)

The procedure is simple and shown in Fig. 10.4, only a manager can have access to the transaction to assign a healthcare professional as a key worker to a service user (patient). Whilst comparisons can be made to databases, blockchain applications are different and checks should be completed to ensure that both the service user and healthcare professional exist. Once the necessary checks are completed the assignment of the key worker is complete and the manager can log out, or assign another key worker.

Each of these assignments is included on the blockchain, this includes the date, time, manager, service-user and healthcare professional.

10.2.3.2 Register Service-User with Home

The flowchart in Fig. 10.5 illustrates the process of registering a service user with a healthcare provider. The issue here is one of access control and cannot be shown on a simplified flowchart, as soon as the service-user is registered, the access control to their records changes. The healthcare provider they were moving from relinquishes access control to the individual's records, whilst the healthcare provider they are moving to gains access control to the individual's records.

A central authority issues the approval, in the case where the service user is moving between different healthcare providers this could be an NHS Trust or GP. In the

case where the service user is moving to a different residence owned by the same healthcare provider, this authority would come from the area manager for that organisation.

The smart contract would be enacted when the move of the service user has been approved. Using ABAC (Vincent et al. 2014), which is support by Hyperledger Fabric, the access control is changed on the attributes of the participants and assets, so the implementation is seamless and requires no further work. For example, the healthcare professional administrating medication requires access to the service user's records, for this the healthcare professional needs the required attributes to have 'READ' access to these records. Put simply, the residence would have to be equal for both the service user and the healthcare professional, further attributes can be added, such as the healthcare professional has to be registered, qualified and if there is a system to clock-in then confirmed that he or she is on-site. Hyperledger's Access Control Language (ACL) can easily implement such conditions and ensure that confidentiality is not breached.

Two additional systems have been introduced here, a central authority to approve the move of the service user, and a system to monitor employees when they are present at the residence (all visitors and employees have to register when they are enter and leave the premises). Permissioned blockchain can easily allow additional authenticated users with limited access control, even of a non-person entity (NPE) variety, as in the case of a clock-in system.

10.2.4 Medical Administration

Completion of the Medical Administration Records Sheet is an important task for the welfare of the service-user. BMAR does not make any claims that it improves this procedure, merely that it can be implemented and all actions recorded without modification. In fact, caution should be taken if this was implemented since there are effects of introducing automated systems, e.g., post-completion error, whereby the appropriately qualified Healthcare Professional completes the form, but forgets to complete the task and administer the medication, see (Yau Wai et al. 2005) for further information.

Whilst caution and further research should be taken, there is evidence that the (Bates et al. 1998; Bennett et al. 2003), that medication administration could benefit from the introduction of such technologies (Fig. 10.6).

10.2.5 Medical Observation

As expected the process for observation of medication is similar to the administration of medication and is shown in Fig. 10.7. This process is mandatory for all controlled drugs. After logging-in the observer selects the correct service user and

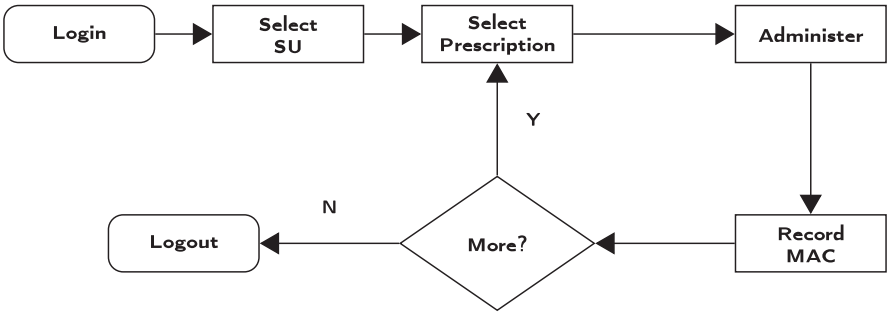

Fig. 10.6 Flowchart for completion of MAR sheet. (Abbreviations: *SU* Service User, *MAC* Medication Administer Code, can be values such as taken, refused, vomit, sleeping or absent)

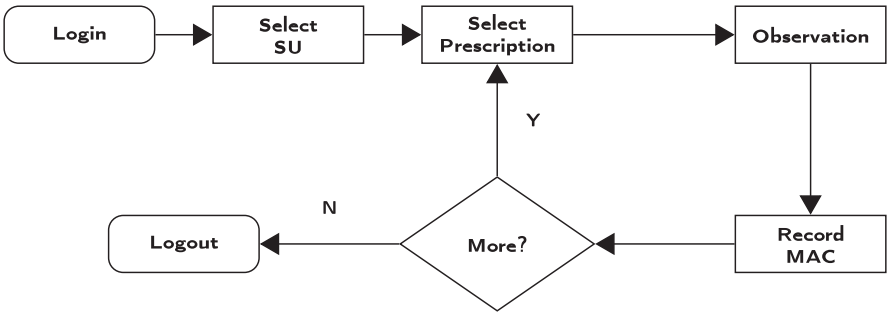

Fig. 10.7 Flowchart for completion of observation for MAR sheet. (Abbreviations: *SU* Service User, *MAC* Medication Administer Code, can be values such as taken, refused, vomit, sleeping or absent)

associated prescription, and this would be completed in parallel with the person administrating the medication. Once the medication has been administered the observer enters the correct MAC. If there are multiple prescriptions then the process is repeated.

There are some anomalies that the audit can reveal, for example when an observation is recorded as a transaction on the blockchain before the administration. This, and other queries are discussed in Sect. 10.2.6 audits.

10.2.6 Audit and Security

An audit agency, such as the Care Quality Commission, would have 'READ' access to all records and transactions on the system. Predefined queries can be completed for each healthcare provider, grouped by residence and service user. Often the accumulation of these reports makes it difficult to find anomalies, however, search algorithms can be deployed and queries can be designed to find any issues that may

arise. For example, a MAR sheet error can be self-audited and left to the expertise of the auditor to question the manager of the care home. This is nothing new, however, the innovative part is the use of blockchain technologies to ensure a disintermediatory append-only ledger of MAR sheets, which makes it impossible to retrospectively delete or correct. There are arguments about a 51% attacks (Bastiaan 2015), which are theoretical and often discussed with permissionless blockchain technology. Firstly, with permissioned blockchain, the likelihood of such an attack is diminished further since all nodes in the network are authenticated by an access control layer. Secondly, such an attack would require changing more than $\frac{2}{3}$ of nodes since the consensus algorithm, PBFT (Castro et al. 1999), used requires a higher percentage of agreement. This vulnerability of permissioned blockchain has an extremely low probability of success, nevertheless, it is mathematically possible and discussed in (Zyskind et al. 2015). The transaction process is fully encrypted and Hyperledger Fabric requires participants to be certified and therefore providing a security infrastructure for authorisation and authentication, see (Cachin 2016) for more details.

10.3 Results

The access latency for transactions is instantaneous, for BMAR there are relatively small amounts of data, <1Kbyte, uploaded to the permissioned blockchain and the delay is negligent. Hyperledger has demonstrated elsewhere with documents (>10Kbyte) the access latency is less than 2 s (Androulaki et al. 2018). The latency has not been fully tested, however, other implementations (Thakkar et al. 2018) indicate that access latency is dependent on transactions per second and block size.

The tests were mainly completed to see how the blockchain could be accessed and processed by key personnel involved in the care and support of a service-user. The development and implementation gave a valuable and insightful understanding of the nuances of administration of medication process. The decision to separate data was based on some rationale regarding access to data, e.g. should auditors be able to identify a service-user or healthcare professional by name? Is there a need for an auditor, when the system can audit itself? These questions are visited in the conclusions. The data stored in asset and participant registries has restricted access.

10.3.1 Prescription

The prescription process has been simplified, but it is possible that the details provided below can be provided from other systems used by the healthcare profession. The prescription process is outside the scope of this project, and essentially the list

```
========== REGSITRY ============
{
  "$class": "org.bmar.net.Prescription",
  "ID": "5579",
  "Patient": "resource:org.bmar.net.SU#S111",
  "PrescribedMedication": "resource:org.bmar.net.Medication#111",
  "initialisation": "2018-10-25T17:26:56.674Z",
  "Form": "Pill",
  "Route": "Oral",
  "Controlled": false,
  "Duration": "4",
  "Dose": "25",
  "Quantity": 1,
  "Instructions": "One (1) tablet two (2) times a day"
}
========== TRANSACTION =============
{
 "$class": "org.bmar.net.Prescribe",
 "actualPrescription": "resource:org.bmar.net.Prescription#5579",
 "transactionId": "91a39021-d1b7-4c8e-9eb2-540b82e641fe",
 "timestamp": "2018-10-25T17:30:29.706Z"
}
```

Fig. 10.8 Transaction for prescription, output shows entry for a prescription in the asset registry, 'Prescription'

of information provided in Fig. 10.8 is minimal requirement. The information can only be provided by a qualified GP or equivalent, and 'READ' access is given to other participants in the system. The transaction records the date and the participant who issued the prescription (not shown). A quick breakdown of the code in Fig. 10.8 shows on line 4 a unique identifier for the prescription, line 5 the unique identifier for the service user, line 6 the unique identifier of the medication and lines 7–14 the details of the prescription.

10.3.2 Medical Administration

Records in the registry can be altered, every update of the records in the registry is written to the blockchain. So, all changes to assets and participants are recorded on the blockchain in perpetuity. Medical Administration is no exception and is conducive to blockchain technology due to its auditable nature.

Lines 1–32 in Fig. 10.9 shows the result of a change in the records for an administration of a prescription, '5579', to a service-user, 'S111', at a Healthcare Provider, 'H1'. Line 29 indicates that actual medication administration code (MAC) recorded by the Healthcare professional was 'taken'. Line 30 indicates that this was not confirmed by the observer, which is completed by a different transaction and updated accordingly.

There are some important omissions of information that are required. This vital information is stored in the associated transaction display between lines 34–42. Here the relationship to the service user is stored, 'S111' (line 36), the prescription, '5579', the timestamp and finally, the transaction ID. The healthcare professional completing the medication administration is recorded as access on the blockchain, not shown here.

```
========== REGSITRY =============
{
  "$class": "org.bmar.net.MAR",
  "time": "1540490058276",
  "actualPrescribedMed": {
    "$class": "org.bmar.net.Prescription",
    "ID": "5579",
    "Patient": "resource:org.bmar.net.SU#S111",
    "PrescribedMedication": "resource:org.bmar.net.Medication#111",
    "initialisation": "2018-10-25T17:26:56.674Z",
    "Form": "Pill",
    "Route": "Oral",
    "Controlled": false,
    "Duration": "4",
    "Dose": "25",
    "Quantity": 1,
    "Interval": 0,
    "Instructions": "One (1) tablet two (2) times a day"
  },
  "actualPatient": {
    "$class": "org.bmar.net.SU",
    "ID": "S111",
    "firstName": "S",
    "lastName": "U",
    "Allergies": "none",
    "DoB": "1991-08-10T00:00:00.000Z",
    "KeyWorker": "resource:org.bmar.net.HCP#HP111",
    "Home": "resource:org.bmar.net.HealthCareProvider#H1"
  },
  "actualMAC": "taken",
  "ObservedMAC": "unconfirmed"
}
========== TRANSACTION =============
{
 "$class": "org.bmar.net.Administer",
 "Patient": "resource:org.bmar.net.SU#S111",
 "actualPrescribedMed": "resource:org.bmar.net.Prescription#5579",
 "time": "2018-10-25T20:02:29.832Z",
 "recordedMAC": "taken",
 "transactionId": "7d919a4c-2c71-4ea6-a073-deffb3e19fc3",
 "timestamp": "2018-10-25T20:03:15.236Z"
}
```

Fig. 10.9 Ouput for transaction for administration. Top half is stored on registry, the bottom half is stored on blockchain

10.3.3 Observation

Lines 2–13 in Fig. 10.10 shows the changes to the asset as a result of the observation transaction. Lines 6 and 9 are the same information as the information stored in the administration transaction in Fig. 10.9 and for brevity not repeated here. On line 11 the recorded MAC is entered as 'taken' as entered in a previous transaction. The important change is to compare lines 31 and 12 in Figs. 10.9 and 10.10, respectively. The value assigned to the attribute, 'ObservedMAC' has changed from 'unconfirmed' to 'confirmed', which matches the value in the transaction (line 18 in Fig. 10.10. In the transaction, the timestamp is recorded at, '2018-10-25T20:25:02.478Z', some 22 min are the administration of the medication.

The ID of the individual MAR was completed as converting a timestamp to a string, in fact on line 4 in Fig. 10.10 the asset attribute name is 'time'. In a system where there are potentially millions of MAR entries, this could be a little simplistic, although it works for our prototype. In such situations, Hyperledger suggests to merge and split attributes to maintain their unique identity, so an obvious candidate is the prescription ID.

Finally, not shown in the transaction is the identity of the healthcare professional conducting the observation, this is included on the blockchain and not shown here.

```
========== REGSITRY =============
{
  "$class": "org.bmar.net.MAR",
  "time": "1540490058276",
  "actualPrescribedMed": {
          ............
    },
  "actualPatient": {
          ............
  },
  "actualMAC": "taken",
  "ObservedMAC": "taken"
}
========== TRANSACTION =============
{
 "$class": "org.bmar.net.Observe",
 "unconfirmedMAR": "1540490058276",
 "ObservedMAC": "taken",
 "transactionId": "22b1d98c-70e2-46c6-83a2-9637ad36698e",
 "timestamp": "2018-10-25T20:25:02.478Z"
}
```

Fig. 10.10 Ouput for transaction for observation. For brevity, the information in the 'actualPrescribedMed' and 'actualPatient' are not displayed here and are the same as in Fig. 10.8

10.4 Management

Access to management functions would be restricted to Managers and entirely role-based. However, there are the attributes of the asset or participant being managed to take into consideration. These two options demonstrate the participant management.

Lines 2–11 in Fig. 10.11 shows the data stored in the blockchain as a result of the transaction. The service user, identified as 'S444' (line 4), has been assigned a key worker 'HP333' (line 9) and registered at a healthcare provider, identified as 'H1' (line 10).

The transaction of the service user to the healthcare provider is shown in lines 13–18 in Fig. 10.10. An existing service user and home have been selected. The transaction timestamp is on line 17 and should pre-date the following transaction.

The transaction of assigning a key worker to the service user is shown in lines 20–26 in Fig. 10.10. The pre-conditions for this is that the service user selected has to be registered to a healthcare provider managed by the manager completing the transaction, and the key worker is a healthcare professional working at the same healthcare provider. The transaction timestamp is on line 25 and post-dates registering a service user with a healthcare provider.

10.4.1 Audit

Various queries can be set up to produce reports for auditors. Figure 10.12 illustrates one of many views an auditor may have, here is a sample of the transactions made for management. The key problem in the above examples is seeing who completed the transactions, here by simply matching the timestamps reveals who submitted the transaction:

```
1  ==========REGISTRY=============
2  {
3    "$class": "org.bmar.net.SU",
4    "ID": "S444",
5    "firstName": "B",
6    "lastName": "C",
7    "Allergies": "",
8    "DoB": "1994-07-25T00:00:00.000Z",
9    "KeyWorker": "resource:org.bmar.net.HCP#HP333",
10   "Home": "resource:org.bmar.net.HealthCareProvider#H1"
11 }
12 ==========REGISTER SU TRANSACTION=============
13 {
14  "$class": "org.bmar.net.RegisterSU",
15  "Patient": "resource:org.bmar.net.SU#S444",
16  "Home": "resource:org.bmar.net.HealthCareProvider#H1",
17  "transactionId": "4b25df90-5dec-47e0-b58d-511908225343",
18  "timestamp": "2018-11-01T13:29:07.629Z"
19 }
20 ==========ASSIGN KEYWORKER TRANSACTION============
21 {
22  "$class": "org.bmar.net.assignKeyWorker",
23  "newKeyWorker": "resource:org.bmar.net.HCP#HP333",
24  "Patient": "resource:org.bmar.net.SU#S444",
25  "transactionId": "e2d55441-813e-4785-8e6c-04b44bca5818",
26  "timestamp": "2018-11-01T13:31:16.812Z"
27 }
```

Fig. 10.11 Output for management transactions. Registry shows data held on particpant after two transactions completed below

Data, Time	Entry Type	Participant
2018-11-01, 13:31:16	assignKeyWorker	M111 (Manager)
2018-11-01, 13:29:53	assignKeyWorker	M111 (Manager)
2018-11-01, 13:29:07	RegisterSU	M111 (Manager)

Fig. 10.12 Audit view for transactions

2018-11-01T13:29:07.629Z:

Matching this transaction from Fig. 10.11 (line 18) to Fig. 10.12 shows that the transaction was to 'RegisterSU' and conducted by 'M111(Manager)'.

2018-11-01T13:31:16.812Z:

Matching this transaction from Fig. 10.11 (line 26) to Fig. 10.12 shows that the transaction was to 'assignKeyWorker' and conducted by 'M111(Manager)'.

10.5 Conclusions

There are many proposed blockchain healthcare systems, e.g., see (Azaria et al. 2016; Griggs et al. 2018; Vithanwattana et al. 2017; Zhang et al. 2017). However, whilst these proposed systems are all meaningful, the prototype for BMAR is for a

different application and designed for the recording and auditing of medication administration records.

All Caldicott principles have been considered in the design of this application and meaningful-use would be the reduction of MAR sheet errors with the overall intention of improving health services and safeguarding vulnerable adults. The permissioned blockchain application provides the security and privacy required for health informatics. The data is permanent and immutable, which makes it an ideal technical solution to the MAR sheet problem.

During the design and implementation stages, it was considered that much of the data will already be available as EHR. It is highly likely that such an implementation would require the use of EHR in an existing database and therefore it is recommended to keep registries relatively static since it is the transactions that change. Such designs lead to keeping databases relatively static and a reliance on blockchain for transactions and change. As a recommendation, when designing a blockchain application it is useful to identify transactions. As yet, there is no standard modelling technique for blockchain and therefore remains a challenge in designing applications. It is recommended that robust modelling techniques are required for building blockchain applications, especially for the modelling and differentiation between transactional, asset and participant data.

From the prototype of BMAR the benefits of using blockchain to manage EHR are as follows:

- Disintermediation is often referred to as the 'removal of the middleman' (Gaur et al. 2018, ch. 1). One of the many promises of permissionless blockchain is the to complete financial transactions without the need of a central banking authority. Permissioned blockchain is no exception and aims to reduce the number of intermediaries between producer and consumer. Whilst BMAR may not have many intermediaries, the process of integration of existing services does not pose a problem.
- Prevention and reduction of medication administration errors. Further research would be required for evidence that BMAR would reduce medication administration errors, however, similar studies (Bates et al. 1998; Bennett et al. 2003) give supporting evidence that medication administration errors can be reduced by the introduction of automated systems. The prevention would come in the form of sending reminders to appropriate healthcare professionals that an administration of medication is due.
- Integrity of EHR. BMAR requires generates a report of MAR sheets, inspected by quality assurance agencies (e.g. CQC) and produced by a healthcare agency. Normally, the inspection would be completed by paper and there would be an issue of trust. Unlikely as it is, physical MAR sheets are designed as append-only, which is why permissioned blockchain are so apt as a technological solution. However, there is only one MAR sheet that normally covers a week for each service-user, and it is not inconceivable for this paperwork to be exposed to the temptation to adjust or rewrite them given the correct circumstances. There has to be an element of trust between the auditor and the healthcare provider to assess

the integrity of the information provided. With permissioned blockchain, even given the correct circumstances the ability to make any amendments to the form retrospectively is virtually impossible. The integrity of the EHR generated by BMAR is to be trusted by all parties.

- Cost in Health Information Technology (HIT) has mixed reviews, with many claiming the high costs and investment (Adler-Milstein et al. 2011) in healthcare systems simply do not deliver. This is often referred to as the productivity paradox (Bui et al. 2018). Nevertheless, there are examples of closed studies that report immediate benefits of HIT (Bates et al. 1998; Bennett et al. 2003). BMAR is to implement a prototype for a blockchain application for MAR sheets and report on self-auditing and reminders sent to assigned staff.
- Interdependency between agencies in the healthcare sector is high. At its best, this can affect cost, with duplicate tests for patients issued by different physicians due to 'information blocking', whereby physicians do not have sufficient privileges to access data from other organisations (Azaria et al. 2016). At its worse provide opportunities for rogue physicians to exploit the system. Even for the production of MAR sheets, there is some interdependency between healthcare provider, primary carer and auditors, see principle 7 of Caldicott. Blockchain not only provides a technical solution but in addition provides a system whereby the other interdependent agencies can trust each other's information.
- Security and Integrity of personal data. In BMAR there is pseudo-anonymous data stored in transactions, and personal and confidential data about service users stored in the registries. With de-anonymity algorithms, e.g., (De Montjoye et al. 2013), and enough reference points pseudo-anonymised data can easily be used to identify individuals. All data needs protection and permissioned blockchain provides the security and ensures the integrity of the data, see (Gupta 2018, ch. 5) for further details.
- Auditability of MAR sheets. Blockchain provides transparent governance and/or auditing. Viewing information in reports generated by a system can be difficult to search. BMAR can assist this since it has the information when medication is to be administered and to who. Therefore, it can self-regulate and highlight errors, essentially highlight errors after reminders have been sent. The auditing agency can review the generated reports at any time and then look into further details as to why there are MAR errors. BMAR is not going to replace the expertise of the individuals but simply give individuals the information required to complete an inspection.

The prototype for BMAR requires further research and development, however, for the reasons above the introduction of such a system would benefit healthcare professionals, healthcare providers and service users.

Acknowledgements The authors would like to thank the invaluable information gain from interviewing healthcare professionals in the design and implementation of BMAR.

Competing Interests None identified.

References

Adler-Milstein J, Bates DW, Jha AK (2011) A survey of health information exchange organizations in the united states: implications for meaningful use. Ann Intern Med 154(10):666–671

Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth eurosys conference. ACM, New York, p 30

Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: using blockchain for medical data access and permission management. In: Open and Big Data (OBD), International conference on. IEEE, Los Alamitos, pp 25–30

Bastiaan M (2015) Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. In: Available at http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf

Bates DW, Leape LL, Cullen DJ, Laird N, Petersen LA, Teich JM, Burdick E, Hickey M, Kleefield S, Shea B et al (1998) Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. JAMA 280(15):1311–1316

Bennett JW, Glasziou PP et al (2003) Computerised reminders and feedback in medication management: a systematic review of randomised controlled trials. Med J Aust 178(5):217–222

Bui Q, Hansen S, Liu M, Tu Q (2018) The productivity paradox in health information technology. Commun ACM 61(10):78–85

Cachin C (2016) Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, vol 310

Caldicott F (2013) Information: to share or not to share? The information governance review. Department of Health, UK

Castro M, Liskov B et al (1999) Practical byzantine fault tolerance. In: OSDI, vol 99, pp 173–186

Council of European Union (2018) Council regulation (EU) no 2016/679. http://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX\%3A32016R0679. Accessed July 2018

De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD (2013) Unique in the crowd: the privacy bounds of human mobility. Sci Rep 3:1376

Gaur N, Desrosiers L, Novotny P, Ramakrishna V, O'Dowd A, Baset SA (2018) Hands-on Blockchain with hyperledger: building decentralised applications with hyperledger fabric and composer. Packt

Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42(7):130

Gupta R (2018) Hands-on cybersecurity with blockchain. Packt

Hyperledger architecture (2017) Volume 1. https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf. Accessed July 2018

Hyperledger architecture (2018) Volume 2. https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf. Accessed July 2018

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system

Richard Kuhn D, Coyne EJ, Weil TR (2010) Adding attributes to role-based access control. Computer 43(6):79–81

Thakkar P, Nathan S, Vishwanathan B (2018) Performance benchmarking and optimizing hyperledger fabric blockchain platform. arXiv preprint arXiv 1805:11390

Vincent C, Hu DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K (2014) Guide to attribute based access control (ABAC) definition and considerations. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf. Accessed July 2018

Vithanwattana N, Mapp G, George C (2017) Developing a comprehensive information security framework for mhealth: a detailed analysis. J Reliab Intell Environ 3(1):21–39

Yau Wai LI, Blandford A, Cairns P, Young RM, et al (2005) Post-completion errors in problem solving

Zhang P, White J, Schmidt DC, Lenz G (2017) Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv preprint arXiv 1706:03700

Zyskind G, Oz N, et al (2015) Decentralizing privacy: using blockchain to protect personal data. In: Security and privacy workshops (SPW). IEEE, 180–184

Chapter 11
Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions

Jake Beavers and Sina Pournouri

Abstract Cyber-attacks are targeting different businesses including medical sectors. From medical devices such as pace makers to medical institutions like hospitals and clinics are all vulnerable targets for cyber criminals. Cyber breaches in medical area not only can risk patients' life but also can lead to leakage of sensitive and confidential data. Due to the nature of medical targets and their importance and sensitivity, there is a significant need to review and investigate the current and past vulnerabilities and weaknesses within the devices and medical institutions. This research aims to investigate recent and current vulnerabilities of medical devices and institutions and highlight the importance of cyber security issues in this area.

Keywords Medical IoT · Medical institutions · Cyber attack · cyber security · medical devices · confidential data · vulnerabilities

11.1 Introduction

Whilst computing technology has made life easier, they have also become a vulnerable and attractive target for cyber criminals. Cyber-attacks have become a common threat to all different aspects of daily life and they can cause a varied level of disruption with respect to their target, type of threat, impact caused, etc. Cyber-attacks have a huge negative implication of their targets and the damages caused by them are not always technological. This of course depends on the victims as the effects can be varied from monetary loss to reputation damage. For instance, the impact of cyber-attacks to a bank, not only can have a negative financial effect but also can damage the reputation of the bank and that may lead to decreasing the number customers and partners in their ecosystem. A cyber-attack to a country's critical national infrastructure can also lead to major damage such as losing confidential and secret information to adversaries.

J. Beavers · S. Pournouri (✉)
Sheffield Hallam University, Sheffield, UK
e-mail: j.beavers@shu.ac.uk; s.pournouri@shu.ac.uk

© Springer Nature Switzerland AG 2019

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_11

Existing and new cyber threats to businesses and critical infrastructure have made cyber security experts to plan and implement efficient strategies for prevention and protection to mitigate the risk of cyber-attacks. Managers and authorities are always attempting to find an efficient way to be prepared and secured against current and future cyber-attacks. One of the common methods is applying security standards and policies including cyber security awareness programs. "How to improve cyber security awareness" is a significant challenge for security experts therefore they always try to understand the current and past trends of cyber security world (Pournouri and Craven 2014). Understanding trends of cyber security can be divided into 2 different levels as follows:

1. **Detection of weakness and bugs in the system**: This step can be taken by security specialists by examining systems using penetration tests in order to find security bugs and weaknesses. By detection of weaknesses in the system, security managers can implement and design effective and solid security standards and procedures. In addition, in order to fill technical bugs and gaps, security patches and equipment will be installed.
2. **Identifying cyber hackers and their methods:** This level completes the previous stage and it aids security managers to be aware of cyber-attacks recent methods. The concept of cyber-attack analysis will be highlighted in this stage, in other words by analysing past historical cyber-attacks to cyber firms and finding the relationship between different involved factors, a better landscape will be obtained and allow managers to make effective decisions based on recent cyber threats (Pournouri and Craven 2014).

In this chapter the aim to review possible vulnerabilities to medical devices and healthcare organizations as they are becoming a permanent target for cyber attackers. According to Fu and Blum (2013) cyber experts are witnessing security vulnerabilities in medical devices and healthcare institutions which they can lead to patients suffering from harm in a number of ways. Cyber-attack to medical devices can pose a potential threat to patients and on the other hand cyber-attacks to healthcare organizations holding sensitive information about patients can lead to a disaster. For instance in 2015, a cybercriminal group claimed they stole 1.5 million records of the database of Planned Parenthood and they threatened to release the information of employees of this abortion clinic along with their patients' identities (Oh 2015).

11.2 Medical Implants: Data Transmission

IoMT is an important concept within IoT, to fully understand and appreciate its complexity one must know both the background information of medical technology as well as security principles. To date, RF (Radio Frequency) modules are commonly used within medical implants as the method of data transmission; therefore it is important to review some of the background knowledge to understand the

security issues these devices face. The following section explains the background information required to understand RF on a technical level, as well as the issues it faces.

11.2.1 Radio Frequency (RF) Technology

Radio frequencies are electromagnetic wave frequencies operating in a range between 20 kHz up to 300 GHz, this can also be defined as 10^4–10^{12} Hz. Pacemakers and ICD units utilize the Medical Implant Communication System (MICS), which is a minimal power, short-range frequency operating on 402–405 MHz (Yuce and Islam 2016). This frequency band is internationally reserved for the communication of medical implant devices, so it is universal for all medical implants. The publicised fact that all medical implants operate on the same band frequency may be detrimental, it may have been more prudent to keep this knowledge reserved on a need-to-know basis.

RF technology has many issues and vulnerabilities, these are mostly unavoidable and are a failing of the technology. In the UK radio frequency technology and broadcasting comes under the jurisdiction of OfCom, the Office of Communication. Broadcasting on RF is a criminal offence without a license. This may deter some, however, "radio pirates" are not put off by this. Pirate radio stations are a popular pastime for some, and those performing illegal broadcasts have to become experts to avoid getting caught. It is therefore not inconceivable to deduce that some of these experts may have come across the MICS band range, possibly going so far as to perform their own home research.

11.2.2 Electromagnetic Interference (EMI)

In airports, hospitals and in general areas with electronic devices sending signals there are usually notices concerning interference with medical implants. The American Heart Association warns users fitted with an ICD against exposure to close proximity with electrical devices (Cheney: Heart implant hack credible 2013). Some devices such as airport scanners, mobile phones, and even a heart rate watch have the possibility of interfering with an implanted medical device.

There is conflicting information to this, as for at least the last 20 years pacemakers, ICDs and other implants have been protected against EMI. The design of pacemakers for example were altered to incorporate a shielded airtight sealed case, typically made from either titanium or steel, lined with an insulated coating. The use of bipolar leads also decreased the susceptibility of pacing systems to EMI (Erdogan 2002).

There are filtering methods such as a Bandpass filter (BPF) which, when specifically incorporated into a pacemaker, can filter out non-cardiac signals reducing external interference. The RF modules in medical implants typically employs BPF

filtering, though it is unknown if this is enforced or just commonly used as best practice.

11.2.3 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is an aspect of RF technology, RFID differs from RF in that it can carry more data, though they have a shorter range because of this. This is the reason why RFID technology utilizes tags, a small readable device containing data to be read by a receiver.

There are two types of RFID, passive and active. Passive RIFD tags send and receive less data and at a shorter range than active, whereas active tags are more complex and require a battery source which makes them larger and more expensive.

There are three frequency bands for RFID:

- Low frequency (LF): 30–300 KHz, read range of up to 10 cm
- High frequency (HF): 3–30 MHz, read range of up to 1 m
- Ultra-high frequency (UHF): 300 MHz to 3 GHz, read range of up to 12 m

There are three main defining advantages to choosing which band to use; first, higher frequencies can carry more data however cost more financially to produce, second, the interference experienced is intensified as the frequency increases, and third, where security is concerned it is safer to have a shorter range to reduce the surface area of attack. However, this does not mean that lower RFID frequencies are secure. Banking cards for example, contain an RFID chip within them and have in recent years been hacked.

The RFID chips within contactless debit and credit cards are short range, to use them a point of sales (POS) terminal must be touching the card to charge money to it. Intelligent scammers took to using a POS terminal on public transport systems, as someone bumping into you on a crowded train would be dismissed as an accident, in actuality the scammer stole money by charging the victims card (Horton 2016). Given that a POS device is just a pre-programmed RFID reader it is not inconceivable to conclude that it may be possible for a pacemaker, or ICD, to be attacked from close range by swiping a reader against the victim's chest.

Further proof to support this claim comes from a study published in a medical journal in 2010, which showed that passive RFID tags can interfere with pacemakers (O'Connor 2010). The FDA performed tests on fifteen ICDs and fifteen pacemakers, thirty units in total. In the tests thirteen different RFID readers were used, operating on either low-frequency, high-frequency or ultra-high frequency. The results showed that 67%, around 20 out of the thirsty units tested, were affected by LF RFID interference. As stated in the study they pose no urgent risk, however due to the rate at which technology advances it does pose the question of if it could become an issue.

11.3 Pacemakers and ICDs Background Knowledge

11.3.1 Operational Functions of a Pacemaker

In a normal heart, the sinus node sends an electrical impulse to trigger a heartbeat, hence why it is called the "natural" pacemaker (pacemakers n.d.). In an abnormal heart, the sinus node does not function as it should, in these cases the patient requires an artificial pacemaker to be fitted.

The number of pacemakers being fitted has risen to at least 25,000 per year, which is around 500 per week. This number will continue to rise and not just with pacemakers, according to the UK national audit of cardiac rhythm management devices 2015–2016 there was a clear rise in implant rates for all types of medical devices (Cunningham et al. 2017).

The type of pacemaker used depends on the type of heart condition and can function in one of two ways:

- **On-demand:** the pacemaker triggers an impulse as and when required.
- **Fixed rate:** the pacemakers triggers all of the impulses all of the time.

The interior of a pacemaker is comprised of a pulse generator, a circuit powered by a battery source, and up to three bipolar electrode leads. These leads carry the electrical impulses and are embedded directly in the heart through a vein. There are different types of pacemaker and the name defines how many leads the device has (Gillard 2017).

11.3.2 Implantable Cardioverter Defibrillator (ICD)

An Implantable Cardioverter Defibrillator, or ICD for short, is a small implantable unit designed to induce fibrillation via an electrical impulse in the event of an abnormal heart rhythm (Implantable cardioverter defibrillator n.d.). These devices differ from the pacemaker as they have the added functionality of delivering an electrical shock to the heart. If an abnormal heart rhythm or cardiac arrest is detected this triggers the ICD to initiate one or more of the therapies listed below:

- **Pacing:** a series of paced electrical impulses, these are low voltage and attempt to correct an abnormal rhythm.
- **Cardioversion:** a series of electrical shocks, these are more intense than pacing and attempt to restore the normal rhythm.
- **Defibrillation:** a series of intense electrical shocks, this is performed to attempt to restore the heart to the normal rhythm.

An ICD is used by patients with life-threatening abnormal heart rhythms. In some cases, they can be fitted pre-emptively to patients who are at risk of one in the future. Regular check-ups are required, the frequency of these depends on the type

of condition the patient has and the type of ICD the patient had implanted. As with living with any condition, the patient must change their lifestyle. Part of the advice given is to be aware that there is the potential for interference from electronic devices.

11.3.3 Home Monitoring Units

The home monitoring unit is a device which connects to the user's internet line at home, it transmits data from the pacemaker to a specified source (What is remote monitoring n.d.). In the case of NHS patients, this data is sent directly to a dedicated server and is remotely monitored by NHS staff. This concept moves into the realms of pre-emptive medicine, as patients can be notified by their doctors if it appears as though they are about to have a cardiac attack, thus giving them time to correct the problem before it occurs. It also reduces the number of hospital visits, as otherwise a medical implant can only be checked by the specialized equipment in a hospital.

Since the unit is connected to a users home network there is cause for concern. If these units are not adequately secure, or the users home network is not, then it is possible that these units could be a point of attack for malicious third parties. Data must be encrypted and only accessible by those who are authorised to view it, if the medical data being transmitted could be taken with, or altered, then it would be possible to send a fake report that appears that the user is healthier or worse than they actually are. In legal terms all private and confidential data must be protected, therefore data protection laws clearly must be enforceable for the home monitoring unit.

A version of St Judes monitoring units, known as Merlin@Home, was previously found to be vulnerable to a man-in-the-middle exploit (Seals 2018). This vulnerability exploits the data during transmission, when the data is sent between the home monitors and the implants it was possible to intercept it. As previously mentioned this data could contain statistics from the implants, commands to the implants and even a patient's private medical information.

11.3.4 RF Implants

Implants such as Pacemakers were originally accessed by medical practitioners using a magnetic switch, which worked by introducing a small magnetic field over the device to turn on the wireless functions. After this device manufacturers changed from a magnetic switch to an RF broadcasting module, this was to modernize the units and paved the way for advanced setups such as home monitoring capabilities.

RF technology can be considered outdated now, as more efficient and effective forms of wireless communications exist.

11.3.5 Bluetooth Implants

The next generation of implants will replace the RF modules with wireless Bluetooth transceivers. The idea behind this change is to increase the data bandwidth to allow more data to transmit and to increase compatibility with devices that can receive the transmissions. The home monitoring unit was fundamentally a life-changing idea, however the major flaw is that it is not portable, with the new generation of Bluetooth devices it would be possible to use a mobile device instead and remove this flaw.

Bluetooth devices are slowly coming into circulation, within time they may replace the RF modules entirely. Bluetooth has its own issues, it can be argued that it is easier to hack than RF. Since Bluetooth can carry more data than standard RF it is now commonly used in phones and other portable devices. Any commonplace technology gets a higher focus on it from the hacking community, as to attempt to hack something you first need to have easy access to it. A recent vulnerability called Blueborne allows unauthorised third parties to install malware, intercept data and even take over a device entirely (Spring 2017). If a pacemaker or ICD was connected to a vulnerable device it is entirely possible that classified medical data could be tampered with, and in a worst case scenario some degree of control could be gained over the connected medical implant.

11.4 Industrial Practices

This section focuses on laws and legislations within the field of medical technology and implants. At the time of this recent research, no definitive evidence concerning laws and legislation regarding the security of such devices had been found. The closest most notable case is the FDA in the US whereby its suggested that, upon discovering a vulnerability, manufacturers notify their customers within 30 days and correct the issue within a further 60 days (Hatmaker 2016).

In 2017 the National Health Service (NHS) was hit with a ransomware attack called "WannaCry" (Lam 2017). This malicious code began to wreak havoc and spread across the NHS network, infecting and locking down systems as it was spread. In the aftermath of the attack the government pleaded to set up a 20 million pound cybersecurity centre to prevent this from happening again (BBC 2017). Best practices for security are always a pre-emptive approach, to keep the system safe and prepare for any attack; this approach is usually adopted by companies on the forefront of defence. The backend systems of the NHS and any medical organisation should be just as secure as the devices, equipment and implants embedded within users.

In 2018 the UK government issued a report on the state of cybersecurity legislations within IoT and how it can be improved (*Secure by Design: Improving the cyber security of consumer Internet of Things Report* 2018). The report discussed how a Coordinated Vulnerability Disclosure (CVD) has been standardised by the

International Organisation for Standardisation (ISO), however, it is currently not standard practice across the industry. A CVD means that when a vulnerability is discovered the finder can disclose it to the manufacturer, without fear of legal reprisal. Currently there is a fear amongst the online community that they may face legal action upon finding a bug, as some companies have prosecuted individuals for doing so. There are companies however who have welcomed this and adopted something similar to the concept of CVD, an incentivised bug bounty program. The programs have set rules but mean that anyone can perform bug testing on their product, so long as they responsibly disclose their findings directly to them.

The 2018 report also refers to the shortage of cybersecurity skills and links it with the rapid growth of the IT industry as a whole, specifically how a lack of security knowledge means that technology is advancing but remains vulnerable to exploitation. This can be applied to the medical field as well; medical technology is advancing but the security is not. There are various security companies and expositions claiming to be aimed at medical security, though at first glance these appear to only be focused on the internal network of the companies and manufacturers. Simply put they do not appear to have anything to do with the internal security of the medical devices produced. It may however, be the case that there are experts out there but that this is not openly publicised.

11.4.1 Legal Cases

Legal action against medical manufacturers, specifically cases involving cybersecurity, is very rare. One of the most recent legal cases was in 2017, where legal action was taken against the medical conglomerate Abbot. They were hit with a $10 million class-action lawsuit over St Jude devices (Wendling 2017). In 2014 St Jude failed to inform the relevant authorities of serious issues within their own devices, even going as far as to conceal a known fatal battery related defect for 5 years before recalling the device. The FDA assisted in the recall and also found that other serious security-related issues were present within the devices, security flaws which were deemed to be potentially fatal. One of these flaws related to exploiting a simple indicator alert within the device which coupled with the faulty battery caused the power to run out in less than 24 h. During this time nearly half a million implanted devices were affected worldwide and vulnerable.

11.4.2 Encryption and Software

The primary fault with the St Jude/Abbot devices was found to be with the encryption protocols used, the devices had been encrypted with 24-bit RSA authentication and a three-byte hardcoded override code (Nohe 2018). To put this into context, the

National Institute of Standards and Technology (NIST) recommends that the current average length of an RSA key should be 2048 bits (Giry 2017). Furthermore, NIST state that the RSA key length, based on current estimates, should only be safe to use until the year 2030. By this point it may have already reached the end of its lifecycle as quantum computing appears to be the next big thing in the industry and could threaten all current methods of encryption when it comes into circulation (Kobie 2017).

A secondary issue was also discovered within the same devices, some models had been found to be still running an embedded version of the Windows XP operating system. This operating system was released in 2001 and reached the end of its official lifespan in 2009 (Callaham 2014). During an operating systems lifespan it is updated by the development team who designed it, this includes security updates if vulnerabilities or major flaws are discovered with it. These updates only apply if the operating system can connect to the internet, and the system is set to update automatically. Medical implants connect to the internet through a monitoring unit, however, this does not imply that they have been set to update. The most likely conclusion is that the implants were running an old, vulnerable, unpatched version of XP. This is further supported by the fact that the software would have to restart to apply these update, and in most cases a medical implant should not be switched off for any length of time.

Almost 1 year after the initial recall the FDA finally approved a firmware update, this came with a recommendation that those affected should get the update. A further recommendation for the affected users was to consult a local doctor to see if they wanted the update, as a health warning had been issued for it. The update had potential side effects to the implant's functions and the user's health. In a few cases, it was possible that some of the functions would be disabled, in other cases the device would be reset and no longer programmed for those user's needs, thus making an uncomfortable feeling in the user's chest until this was corrected.

11.4.3 Vulnerabilities in Pacemakers

In recent years it has been documented and openly reported that implanted medical devices ranging from pacemakers, insulin pumps and heart rate monitors have been compromised. Newspapers and journalists are reporting on such attacks with increasing frequency. This may be due to the increase in the number of individuals that are being fitted with a pacemaker, which would in turn create more opportunities for a malicious hacker to attempt to bypass the device.

The FDA have assisted in security vulnerabilities within various medical devices and implants, in a public statement they openly declared that they have found severe vulnerabilities in multiple brands of pacemakers, the most notable example being an exploit whereby a pacemaker could be entirely reprogrammed by a malicious attacker (New York Post 2016).

The most renowned expert in medical device security was Barnaby Jack (2017), now deceased. Barnaby Jack was reported to have developed software that allowed him to remotely trigger defibrillation within a 50-foot radius, thus potentially killing anyone in the area with an implanted ICD. Barnaby Jack also exploited other medical equipment including an insulin pump, he was able to wirelessly deliver a lethal dose from a distance of 90 meters away. The issue of security in medical devices may be more widespread than first envisaged, and potentially a problem throughout the industry.

A recent ethical hacking attempt from 2016 (Fatal flaws in ten pacemakers make for Denial of Life attacks 2016) involved a team of experts conducting black box testing on a pacemaker, this involves no prior knowledge of the defences, and were able to gain access wirelessly from up to 5 m away as well as delivering fatal shocks to the device. Black box testing is the closest to a real-world scenario as testing can get, so it raises concerns about the effort required to perform this action.

A paper in 2008 investigated the possibility of hacking pacemakers with a magnetic switch (Halperin et al. 2008), magnetic induction pacemakers are still being used however the technology was replaced in favour of RF. With their setup, these researchers were able to both disclose and modify the data within a pacemaker, as well as induce fibrillation. As previously stated these devices are still embedded within some users, it is common policy to not perform surgery to replace an implant if it can be repaired or upgraded from the outside.

In a BBC article entitled "Dick Cheney: Heart implant attack was credible" (BBC 2013) it was stated that former vice-president Dick Cheney had fears over his own pacemaker being hacked, even going so far as to disable the wireless functionality. Mr. Cheney admitted that his doctor disabled the wireless functions in his ICD, over his fears of possible assassination through targeted hacking of the defibrillator function of the device. Political assassinations via medical hacking may be an interesting idea for a film, but it does not mean that this has actually happened before. Though if it had, this kind of information would most likely not be made public knowledge.

11.4.4 Vulnerabilities in Medical Equipment

Examples of known hacked medical equiptment (Zetter 2015)

Equipment	Description	Vulnerability
Medtronic Paradigm insulin pumps; Models 512, 522, 712, and 722	The Medtronic Paradigm is a range of insulin pumps, a device that delivers insulin to patients with diabetes. These units are designed to deliver a specific dose of insulin when the device detects changes in blood sugar levels.	The vulnerability in these units is that the systems don't encrypt the commands that patients send their pumps, nor do they authenticate the source of the commands. Unauthorised parties in the vicinity of a pump could intercept the legitimate commands and replace them with malicious commands that could potentially deliver a fatal insulin dose to a patient

(continued)

Equipment	Description	Vulnerability
J&J Insulin pumps	The J&J (Johnson and Johnson) brand of insulin pumps function in the same way as any other model. J&J learnt of a potential vulnerability and shocked the industry by issuing a recall themselves, demonstrating a clear commitment to industrial practices.	The insulin pumps had the potential to be hacked to deliver a fatal dosage of insulin (Finkle 2016). Though it is unknown if this could have been exploited, as the pumps were promptly recalled.
Hospira LifeCare Drug Infusion Pump	The Hospira intravenous drug infusion pumps are designed to give accurate dosages of medication at specified intervals.	Authorisation vulnerabilities were discovered in five separate models of the pump. Unauthorised parties in the vicinity of a pump could remotely change the number of drugs administered to patients to deliver a fatal dosage.
	There are an estimated 400,000 of these units installed in hospitals around the world.	
X-Ray Systems	Patient X-rays can be accessed via the computer network in hospitals since these images are private patient data they require authentication to view the images. In accordance with best practices for cyber-security, they also maintain a log of everyone who accesses the network. This includes what they have accessed, to protect patient privacy and guard against misuse.	The X-Ray images are backed up to a centralized storage unit, in some hospitals this unit previously did not require any authentication to access which resulted in all X-ray images being accessible by anyone.
Blood Refrigeration Units	Blood refrigeration units are specialised in cold storage with accurate temperature controls and failsafes to perfectly preserve the contents. The units can even notify hospital staff if the units are out of the predefined temperature boundaries.	Some of the units have a web interface to allow hospital staff to alter the temperature range remotely. It was discovered in some units that the systems were protected by an embedded hardcoded password, which can be deciphered.
		Unauthorised parties, once in the system, could alter the temperature and turn off the alert feature thus preventing the system from alerting hospital staff.
CT Scans	A computerised tomography scan, or CAT scan, uses X-rays and advanced computer systems to create a cross-sectional image of a patient's body.	Unauthorised third parties could alter the configuration files in a hospital's CT scanning unit, this included the files that control the radiation exposure limiter. By removing this limiter it is possible that this vulnerability could have led to a fatal dose of radiation while a patient was being scanned.

(continued)

Equipment	Description	Vulnerability
iStan	The iStan is a specialised robotic medical dummy, designed to mimic the human cardiovascular, respiratory, and neurological systems. Although this unit is a training simulator for medical students, it has been designed and programmed by people responsible for programming various other medical equipment.	In 2015 researchers at the University of South Alabama bypassed the security in the operating system that controls the iStan, gaining full control over the unit they were able to shut down some of the embedded implants including the Pacemaker (Glisson et al. 2015).
NHS Trust Systems	A network is the backbone of all modern organisations. The NHS uses their internal network for the same reasons as other companies; the fast speed exchange of data and communication to authorised members of departments.	The "WannaCry" ransomware infected 47 NHS trusts in England and 13 NHS organisations in Scotland. This malicious code locked whole segments of the organisations systems, issuing a ransom demand to unlock them.

11.4.5 Cyber-Attack Trends to Healthcare Section

This section aims to investigate the trend of cyber-attacks to healthcare section. There are 93 cyber-attacks taken place in healthcare organizations from 2013 to 2016 recorded to a dataset which has been obtained from Open Source Intelligence (OSINT). In this study OSINT includes websites, blogs and news which is accessible for public.

Types of cyber-attacks happened from 2013 to 2016 are as follows:

1. Account Hijacking (AH): Any online account such as email, social media, etc., associated with a person or a company hijacked by a hacker(s).
2. Defacement (DF): Unauthorized changing a web page by hackers through penetration to web server.
3. DDOS (DS): Disturbing availability of victims' server by hackers through sending high volume of requests.
4. Malware (MWV): A piece of malicious code including virus, worm, Trojan horse and etc. designed by hackers for compromising victims' system.
5. Phishing (PH): A malicious method tries to steal sensitive information by deceiving victims through an email conversation,
6. SQL injection (SQL): Attackers' codes try to compromise the database
7. Targeted Attacks (TA): Anonymous and un trackable attackers actively are trying to penetrate to victims' system
8. Unauthorized access (UA): Any unauthorized access to computer devices and software by hackers
9. Unknown Attacks (UNK): Those attacks when type of threat has not been reported in OSINT resource.
10. Zero day attacks (ZD): Unresolved Security bugs get exploited by hackers.

Motivation of cyber-attacks in the dataset also have been categorised as follows:

1. Cyber Espionage (CE): It refers to attempts to gain access to confidential and secret information held by organizations or governments without their knowledge and cyber attackers use sophisticated techniques such as malware to spy on victims. For instance in 2011 Mitsubishi was targeted by cyber espionage attack claimed that their data on missiles and submarines were spying for unknown amount of time through a malware detected in their computer systems. (Nitta 2013)
2. Hacktivism (HA): These types of cyber-attacks are motivated by social or political goals and hackers (Hacktivists) use attacking techniques to penetrate into victims' system and send their political or social message either to public or victims themselves. One of the notable examples of hacktivism was the cyber-attack carried out by Anonymous against child pornography hidden websites in October 2014. Anonymous group managed to take down 40 child pornography websites which were hidden from search engines. (Goode 2015)
3. Cyber Crime (CC): it refers to those type of crimes when a computer device is being used as a tool or as a target. Cybercrime is more general term using for description of cyber-attacks in smaller scale. (Saini et al. 2012)

As Fig. 11.1 shows there is an increasing trend in the number of cyber-attacks during recent years. In 2013, 11 attacks were reported to healthcare section and then towards 2015 this number increased to 33 cyber-attacks. These changes can indicate that healthcare organizations are becoming more vulnerable and favourable targets for cyber criminals, however, in 2016 there is downward trend which can demonstrate past cyber-attacks had been highlighted for cyber experts and they might adopt some sort of cyber defence strategy against these attacks. The number of

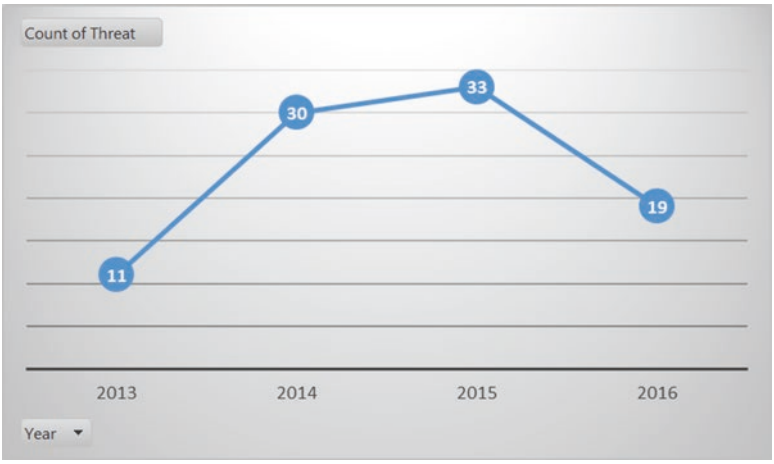

Fig. 11.1 Cyber Attack trend from 2013 to 2016

cyber-attacks can be more than what have been reported in the news as in some cases healthcare organizations might not reveal that they were targeted due to reputation loss which can lead to customer dissatisfaction. Another reason for increasing trend of cyber-attacks can be because of usage of computer resources in healthcare organizations which makes them targets for cyber-attacks.

Another statistic which can be highly important shows that healthcare organizations are more vulnerable against Account Hijacking attacks. 27% of cyber-attacks to healthcare organizations were categorized as Account Hijacking then the second most common attack was Malware attack has 24%. SQL injection attacks were in the third place in terms of occurrence which indicates that database of healthcare organizations is one of those assets that needs to be protected by cyber experts. Figure 11.2 demonstrates a pie chart which shows the occurrence percentage of each type of cyber-attack in healthcare organizations. This statistic shows that cyber experts need to prioritize their defence strategy based on most common attacks. Account Hijacking and Malware attacks are main threats to healthcare organizations which can be tackled by adopting different countermeasures such as raise the security awareness for staff within healthcare institutions and updating anti-virus and install security patches in the computer systems.

Figure 11.3 shows the trend of each type of cyber-attack since 2013. As it is shown, unknown attacks have increasing trend which shows either they were not

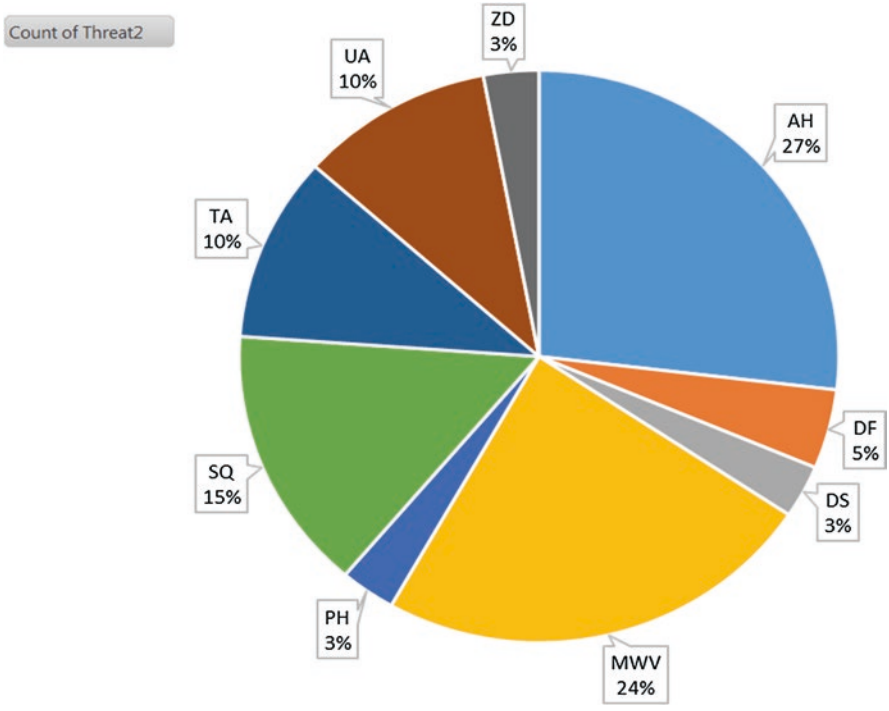

Fig. 11.2 Type of attack to healthcare institutions

Fig. 11.3 Type of Attack trends from 2013 to 2016

reported accurately in the news or cyber experts were not able to identify the type of attack. Account hijacking has had an uprising trend over past couple of years whereas Malware attacks have been consistent since 2014. In 2015 SQL injection attacks reached its maximum then during in 2016 it dropped again. There are still many unknown attacks happened in recent years that their type of threat was either unknown or not reported in OSINT.

In terms of location of targeted healthcare organizations almost 73% of them located in the US, 5.6% in the UK. The reason can be because generally these countries can be more favourable for cyber criminals or these 2 countries get more cover in the news compared to others. Figure 11.4 shows the distribution of cyber-attacks to healthcare organizations in terms of location.

In terms of motivation of cyber-attacks to healthcare organization, 86% were categorized as cyber-crime, however, 6.7% were carried out because of hacktivism purposes, therefore attackers tried to send a political or social message to public (Fig. 11.5).

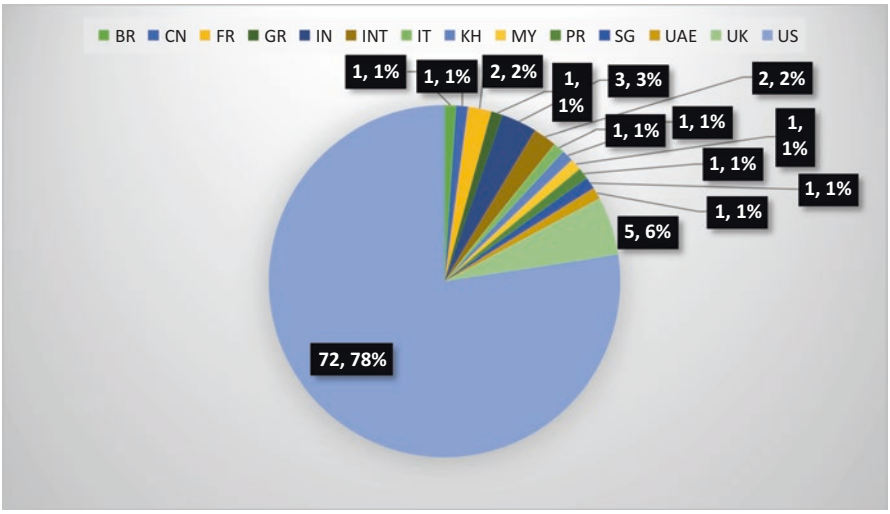

Fig. 11.4 Location of Targeted Healthcare organizations

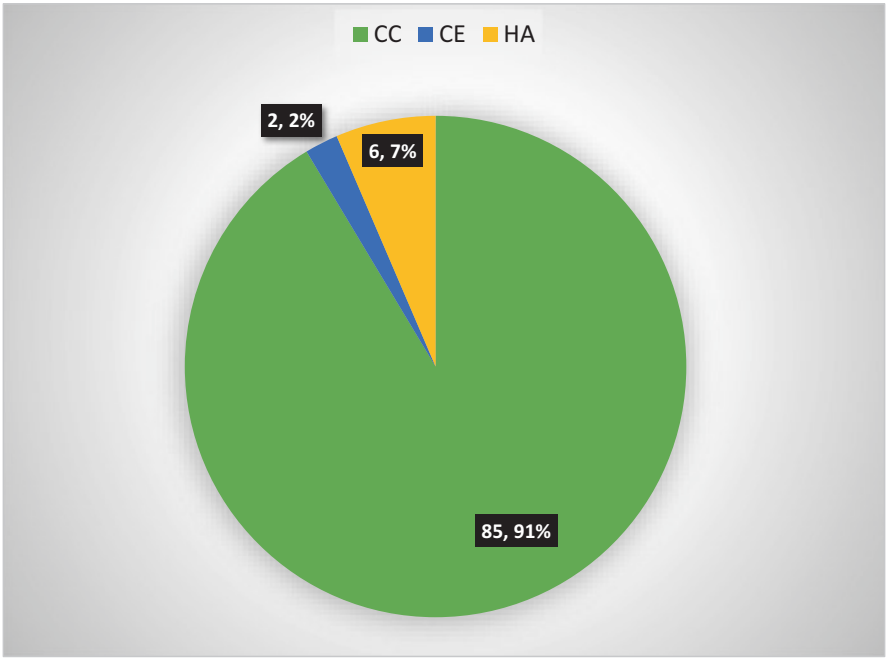

Fig. 11.5 Motivation of cyber-attacks to Healthcare organizations

11.5 IoMT and Its Future Security

At first glance, it does not appear that much has been much done to pioneer the field of medical IoT (IoMT). Primarily this appears to be due to a disconnect between the field of security and the medical industry. This is understandable as a specialist on medical devices would not know about security principles and vice versa, however, this should not be the case. Forensic investigation within the police has branched into cybercrime due to its rapid increase in recent years, this is not likely to decrease anytime soon.

It is easy to find papers and news articles on pacemakers and other medical equipment being vulnerable and exploited, however, there are little to no papers to be found on securing them. This is due to the nature of cybersecurity and data protection, it would not be secure to explain how a device is being protected as this can give hackers leverage. If its known what security measures are in place within a device then it is possible to reverse engineer them, to work out the vulnerabilities of the security measures used and how to exploit them.

Concerns around the abuse of medical devices stretches across a broad range and should not just be isolated to researching pacemakers, however pacemakers should be the starting point as they are the most vital piece of equipment and lives of individuals depend on these devices being secure. As discussed previously, there is an outline issue with security vulnerabilities across a whole range of medical equipment. There is also a clear argument for the necessity of security in these devices, given that in the majority of cases the exploitation of these vulnerabilities was proved to be potentially fatal.

Healthcare institutions also need to adopt comprehensive cyber security strategies as this Chapter has explained that the attacks are increasing due to the nature of computer devices that are being used in healthcare industry. Patients' sensitive information can be a potential target for cyber attackers as well as medical equipment. The cyber security strategy should be a dynamic approach in healthcare institutions that can be flexible against different cyber threats which over time change frequently.

References

BBC (2013) Dick Cheney: heart implant attack was credible. Retrieved from http://www.bbc.co.uk/news/technology-24608435

BBC (2017) Ethical hackers to boost NHS cyber-defences. Retrieved from http://www.bbc.co.uk/news/technology-42137409

Callaham J (2014) A (very) brief history of Windows XP. Retrieved from https://www.neowin.net/news/a-very-brief-history-of-windows-xp

Cunningham D, Cunningham M, Donkor A, Linker N, Murgatroyd F (2017) National audit of cardiac rhythm management devices. Retrieved from http://www.ucl.ac.uk/nicor/audits/cardiacrhythm/documents/annual-reports/crm-devices-national-audit-report-2015-16_v2

DMCA Exemption Granted for Med Device Research, Patient Access to Data (2015.) Retrieved from https://clinic.cyber.harvard.edu/2015/10/27/dmca-exception-granted-for-medical-device-research-patient-access-to-data/

Erdogan O (2002) Electromagnetic interference on pacemakers. Indian Pacing Electrophysiol J 2(3):74–78. PMCID: PMC1564060

EU Directive 95/46/EC – The Data Protection Directive (n.d..) Retrieved from https://www.data-protection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.htm

Fatal flaws in ten pacemakers make for Denial of Life attacks (2016.) Retrieved from https://www.theregister.co.uk/2016/12/01/denial_of_life_attacks_on_pacemakers/

Finkle J (2016) J&J warns diabetic patients: Insulin pump vulnerable to hacking. Reuters. Retrieved from https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L

Fu K, Blum J (2013) Controlling for cybersecurity risks of medical device software. Commun ACM 56(10):35–37

Gillard D (2017) Living with a Pacemaker. British Heart Foundation, pp 4–20

Giry D (2017) Keylength. Retrieved May 19, 2018, from https://www.keylength.com/en/4/

Glisson WB, Andel T, McDonald T, Jacobs M, Campbell M, Mayr J (2015) Compromising a medical Mannequin. Comput Res Repository arXiv:1509.00065

Goode L (2015) Anonymous and the political ethos of hacktivism. Pop Commun 13(1):74–86

Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH (2008) Pacemakers and implantable Cardiac Defibrillators: software radio attacks and zero-power defenses. IEEE Symp Secur Priv

Hatmaker T (2016) FDA issues new security guidelines so that your pacemaker won't get hacked. Retrieved from https://techcrunch.com/2016/12/28/fda-issues-new-security-guidelines-so-that-your-pacemaker-wont-get-hacked/?guccounter=1#

Horton H (2016) Contactless card owners warned against public transport scanner hack. The Telegraph. Retrieved from https://www.telegraph.co.uk/technology/2016/02/17/if-you-have-a-contactless-card-watch-out-for-this-scam/

Implantable cardioverter defibrillator (n.d.). Retrieved from https://www.bhf.org.uk/heart-health/treatments/implantable-cardioverter-defibrillator

Barnaby Jack (2017.) Retrieved from https://en.wikipedia.org/wiki/Barnaby_Jack

Jamming & Radio Interference: Understanding the impact. (n.d.) The Institute of Engineering and Technology. https://doi.org/10.1049/etr.2012.9002

Kobie N (2017) The quantum clock is ticking on encryption – and your data is under threat. Retrieved from http://www.wired.co.uk/article/quantum-computers-quantum-security-encryption

Lam B (2017) NHS cyber attack: views from the front line. Pharm J. Retrieved from https://www.pharmcaceutical-journal.com/opinion/qa/nhs-cyber-attack-views-from-the-front-line/20202794.article

New York Post (2016) Yes, pacemakers can get hacked. Retrieved from http://nypost.com/2016/12/29/yes-pacemakers-can-get-hacked

Nitta Y (2013) Japan's approach towards international strategy on cyber security cooperation. Retrieved September, 13, p 2014

Nohe P (2018) FDA: 465,000 Pacemakers need a firmware update. Retrieved https://www.thesslstore.com/blog/fda-465000-pacemakers-need-a-firmware-update/

O'Connor MC (2010) Study finds RFID readers may affect pacemakers, but pose no urgent risk. Retrieved from http://www.rfidjournal.com/articles/view?7307

Oh I (2015) Anti-Abortion hackers claim to have stolen data that could take down planned parenthood. Mother Jones

Pacemakers (n.d..) Retrieved from https://www.bhf.org.uk/heart-health/treatments/pacemakers

Pournouri S, Craven M (2014) E-business, recent threats and security countermeasures. Int J Electron Secur Digit Forensics 6(3):169–184

Saini H, Rao YS, Panda TC (2012) Cyber-crimes and their impacts: a review. Int J Eng Res Appl 2(2):202–209

Seals T (2018) Abbott addresses life-threatening flaw in a half-million pacemakers. Retrieved May 19, 2018, from https://threatpost.com/abbott-addresses-life-threatening-flaw-in-a-half-million-pacemakers/131709/

Secure by Design: Improving the cyber security of consumer Internet of Things Report (pp. 4–27, Rep.) (2018). Department for Digital, Culture, Media & Sport. Retrieved from https://www.gov.uk/government/publications/secure-by-design

Spring T (2017) Wireless 'BlueBorne' attacks target billions of bluetooth devices. Retrieved May 15, 2018, from https://threatpost.com/wireless-blueborne-attacks-target-billions-of-bluetooth-devices/127921/

Wendling P (2017) Abbott hit with $9.9 million class-Action over St Jude devices. Medscape. Retrieved from https://www.medscape.com/viewarticle/886026

What is remote monitoring (n.d..) Retrieved from http://www.medtronic.com/us-en/patients/treatments-therapies/remote-monitoring.html

Yuce MR, Islam MN (2016) Review of medical implant communication system (MICS) band and network. ICT Express 2(4):188–194. https://doi.org/10.1016/j.icte.2016.08.010

Zetter K (2015) Medical devices that are vulnerable to life-threatening hacks. Retrieved from https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/