EAI/Springer Innovations in Communication and Computing

Giuseppe Andreoni
Paolo Perego
Enrico Frumento *Editors*

m_Health Current and Future Applications

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series editor

Imrich Chlamtac, CreateNet, Trento, Italy

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

Giuseppe Andreoni · Paolo Perego ·
Enrico Frumento
Editors

m_Health Current and Future Applications

EAI
RESEARCH MEETS INNOVATION

Springer

Editors
Giuseppe Andreoni
Politecnico di Milano
Milan, Italy

Paolo Perego
Politecnico di Milano
Milan, Italy

Enrico Frumento
Cefriel Scarl, Politecnico di Milano
Milan, Italy

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-02181-8 ISBN 978-3-030-02182-5 (eBook)
https://doi.org/10.1007/978-3-030-02182-5

Library of Congress Control Number: 2018966114

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

Preface

Introduction to Mobile Health Systems

Mobile technologies have revolutionized our lives in many ways, not only for the ubiquitous communication they support but above all because of the infinite services and possibilities they are able to offer.

Together with the increase in electronics miniaturization and energy optimization today, small connected devices and systems have pervaded our world and even our body.

A mobile health system is hierarchically characterized by four main elements:

1. sensing component capable to measure and process at least one signal from the human that is related to his/her health status: from the simple temperature, to electrocardiogram or even more complex signals or their combination;
2. a processing unit, to directly elaborate the main features of the signals to support an immediate and on-site feedback to the user thanks to dedicated software;
3. the software, nowadays the so-called apps running on mobile devices, smartphones or tablets or similar platforms, that can support the device functions or even be itself the sensing and dialoguing elements with the remote service usually resident on a web-based platform;
4. a cloud/web-based repository with analytical and interpretation capabilities to deliver instant feedback to the user or making available data and information to healthcare supervisors or caregivers.

The Sensing Component

Smart electronic and sensorized textiles, technological fashion accessories like necklaces, bracelets, earrings or pins, belts up to smart tattoos (the last discovery which can upgrade significantly the so-called smart patches) have now been

enriched with sensing capabilities to monitor several body signals describing our activity, our lifestyle, and our health.

We can also identify three main categories of sensing systems:

1. wearable systems that are smart integrated systems close to or in contact with the human body and able to measure, process, and transmit biomedical, physical and chemical data or parameters, and/or even execute mechanical actions if necessary;
2. environmental sensors that are exploiting our physical interaction with objects of our everyday activities: some examples could be the steering wheel while driving or the armrests of our chairs when seated can embed sensors for the two hands thus making possible the collection of heart rate or the bed sensors to detect sleep quality;
3. dedicated devices: they are medical products like portable arterial blood pressure measuring systems or glucose meters that can work both in a standalone mode (in this case, the user has to enter the measurements into a software on the mobile device) or in the more recent systems wireless connectivity can directly implement the data transmission to the mobile host.

The Processing Component

The processing and communication unit is undergoing a very quick and sudden revolution. We have seen the evolution from the cellphone to Personal Digital Assistant to smartphone to tablet to phablet to smartwatches. We are assisting at the development of Web-of-Things paradigm, even if the Internet-of-Things society is still at the beginning and the web-based society is again in the growing phase. Small connected items support data collection and real-time user feedback. This means to have the possibility to have short-term or long-term data-supported intervention in different domains: physical functions and activity, nutrition, and physiological monitoring are the most common ones.

Today, data processing is no more a single device issue: thanks to cloud computing and to sensors networks, this has become a distributed process with redundancy that has increased personal data and information amount, quality, reliability, and specificity.

The Web Component

Together with the basic data processing, the web resources can now offer a new set of capabilities and services: smart storage, analysis services (at personal level or for selected cluster of people), impact and/or forecast analysis for pathologies and for

welfare costs, coaching and/or alerting for chronic diseases management, are the most innovative and common state-of-the-art experiences.

This is crucial to identify new exploitation strategies to improve peoples health and quality of life, to reduce healthcare cost, and to set up a new integrated community of stakeholders including new actors like familiar and not familiar caregivers, technologists, and doctors according to the services purposes and needs.

The Book Structure

From all the above, it is clear that mHealth product-service systems are integrating a great complexity evolving day by day. This book aims at presenting some of the most recent solutions and experiences in mHealth and the related factors: technology, regulatory, innovation, services. Some of these aspects are already on the market, other are still under research and development.

The book opens with a vision provided by the editors about the future of health care in a 20 year horizon: we envisage future devices and services and even pathologies that will characterize our next society. If technology evolves in decades (like in the recent past), health is more resilient to innovation but maybe the coming decades can disrupt this mechanism and mHealth could be an extraordinary tool in this process.

Chapter 2 provides a better contextualization of the mHealth framework, highlighting the implemented and possible solutions for patients and healthcare systems. The benefits and challenges are presented and discussed and provide a vision for the future directions.

Services also mean mHealth exploitation. An analysis and the related methodology to understand risks and opportunities for researchers and stakeholders is therefore important. Chapter 3 is dedicated to this aspect, including in particular the analysis of the relevant Intellectual Property Rights elements and market data. Mobile Health manages sensible data about users at a higher level. For this reason, also in light of the recent adoption of the new legal framework for data management (General Data Protection Regulation, GDPR entered into force on 25 May 2018 in all EU countries), Chap. 4 starts presenting the Hospital 2.0 and the new patient ecosystem scenarios; a specific section of the chapter also explores the threats (together with solutions) for data and service delivery due to possible cyber-attacks. This issue is relevant due to always connected healthcare vision that mHealth is developing.

Chapter 5 describes the data protection issues in detail, offering a synthetic but complete description of the rules, principles, security measures, and policies with a specific application to healthcare professionals training.

This distributed health system paradigm is made possible, thanks to a variety of devices that support the monitoring of most of the basic vital signs and other functions. These systems are presented and analyzed in Chap. 6 for a general overview of state-of-the-art solutions and designing some perspectives.

These devices are more and more miniaturized and embedded in our lives: in our body-worn accessories, in our clothes, and in our environments. Nowadays we can be always measured, 24 hours a day, seven days a week. A huge amount of data and with quasi standard clinical quality due to the wearable measurement paradigm is made available by mHealth devices. This factor represents a crucial issue in mHealth and a recent and growing field of research. Chapter 7 focuses on Big Data and signal processing in mHealth, presenting the most recent algorithms and solutions to extract health parameters and subjects profiles for treatment follow-up, critical events detection, and short/long-term prevention.

The availability of devices and data is the core factor to design new services to improve our health or the management of pathologies. In particular, it is interesting to foresee new services to improve patients care and quality of life together with the reduction of the social cost related to the healthcare processes. This is the central topic of Chap. 8, in which the authors describe these new opportunities through examples and experiences in small-scale experimentations. It is important to understand how to evolve towards a full implementation of the mHealth paradigm to exploit all these positive features and outcomes.

But this exploitation means sometimes and somehow to redesign our Healthcare systems, our structures, and even the current processes. Chapter 9 provides a perspective on the design of the new healthcare systems for the next generations, and the actual and future mHealth directions to contribute in facing new challenges for a better, equal, and advanced world.

Final Remark

This book does not aim to be the ultimate compendium of mobile Health, but proposes the design of a pathway for the development of it: from understanding the basics and the analysis of technologies and available innovation, to the design of new systems and services in its complete chain up to the final stakeholders: users, caregivers, and institutional or private institutes managing or delivering health services to care people and not simply to cure them.

Milan, Italy
July 2018

Giuseppe Andreoni

Contents

Contributors

Giuseppe Andreoni Dip. di Design, Politecnico di Milano, Milan, Italy;
Consiglio Nazionale delle Ricerche (CNR), Istituto di Bioimmagini e Fisiologia Molecolare (IBFM), Segrate, Milan, Italy

Massimo Barbieri Technology Transfer Office, Politecnico di Milano, Milan, Italy

Gabriella Borghi Cefriel Scarl, Politecnico di Milano, Milan, Italy

Enrico Frumento Cefriel Scarl, Politecnico di Milano, Milan, Italy

Maria Renata Guarneri Dip. di Design, Politecnico di Milano, Milan, Italy

Erik Kamenjasevic The KU Leuven Centre for IT & IP Law (CiTiP), Leuven, Belgium

Karim Keshavjee Institute for Health Policy, Management and Evaluation (IHPME), University of Toronto, Toronto, ON, Canada
InfoClin Inc, Toronto, ON, Canada

Loredana Luzzi University of Milano Bicocca, Milan, Italy

Cristina Masella DIG Department, Politecnico di Milano, Milan, Italy

Alfonso Mastropietro Consiglio Nazionale delle Ricerche (CNR), Istituto di Bioimmagini e Fisiologia Molecolare (IBFM), Segrate, Milan, Italy

Dora Mugambi InfoClin Inc, Toronto, ON, Canada

Alessia Paglialonga Consiglio Nazionale delle Ricerche (CNR), Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni (IEIIT), Milan, Italy

Anisha A. Patel Institute for Health Policy, Management and Evaluation (IHPME), University of Toronto, Toronto, ON, Canada

Paolo Perego Dip. di Design, Politecnico di Milano, Milan, Italy

Erica Pinto Institute for Health Policy, Management and Evaluation (IHPME), University of Toronto, Toronto, ON, Canada

Danaja Fabcic Povse The KU Leuven Centre for IT & IP Law (CiTiP), Leuven, Belgium

Massimo W. Rivolta Department of Computer Science, University of Milan, Milan, Italy

Giovanna Rizzo Consiglio Nazionale delle Ricerche (CNR), Istituto di Bioimmagini e Fisiologia Molecolare (IBFM), Segrate, Milan, Italy

Roberto Sassi Department of Computer Science, University of Milan, Milan, Italy

Elisa Scalco Consiglio Nazionale delle Ricerche (CNR), Istituto di Bioimmagini e Fisiologia Molecolare (IBFM), Segrate, Milan, Italy

Roberto Sironi Dip. di Design, Politecnico di Milano, Milan, Italy

Acronyms

ANN	Artificial Neural Networks
ARIPO	African Regional Intellectual Property Organization
CDAC	Cyberterrorism Defense Analysis Center
CPC	Cooperative Patent Classification
DDoS	Distributed Denial-of-Service
DFA	Detrended Fluctuation Analysis
DI	Digital Integration
EAPO	Eurasian Patent Organization
ECG	Electrocardiography
EHR	Electronic Health Record
EKG	Electrocardiography
EMA	Ecological Momentary Assessment
EMR	Electronic Medical Record
EPO	European Patent Organization
FERMA	Federation of European Risk Management Associations
FHIR	Fast Healthcare Interoperability Resources
HIE	Health Information Exchange
HRV	Heart Rate Variability
IPC	International Patent Classification
IPR	Intellectual Property Rights
LDA	Linear Discriminant Analysis
NACOR	Normalized Auto-correlation Function
OAPI	Organization Africaine de la Propriété Intellectuelle
PAM	Patient Activation Measure
PPG	Photo-plethysmography
PSD	Power Spectral Density
RMS	Root Mean Square
RMSSD	Root Mean Square of Successive Differences
SDNN	Standard Deviation of Normal-to-Normal Beat Intervals
SDVA	Social Driven Vulnerability Assessments

SE	Social Engineering
SVM	Support Vector Machine
TAs	Targeted Attacks
TAT	Time Above Threshold
USCYBERCOM	US Department of Defense Cyber Command
VM	Vector Magnitude
WIPO	World Intellectual Property Organization
ZC	Zero-crossing

Chapter 1
Introduction

Maria Renata Guarneri, Roberto Sironi and Paolo Perego

Abstract Health care is undergoing a true revolution towards new paradigms for all actors involved, first of all the scientific and clinical side, where traditional reactive approach based on symptoms and disease management is progressively giving way to a systemic approach oriented to proactive, preventive and personalised medicine. In this revolutionary scenario, technological innovation and, in particular, ICT and mobile health play the role of key enablers.

1.1 Introduction

Health care is undergoing a true revolution towards new paradigms for all actors involved, first of all the scientific and clinical side, where traditional reactive approach based on symptoms and disease management is progressively giving way to a systemic approach oriented to proactive, preventive and personalised medicine. In this revolutionary scenario, technological innovation and, in particular, ICT and mobile health play the role of key enablers.

Indeed, the digital transformation which is encompassing all economic sectors is mainly characterised by the so-called big data. A huge amount of digitalised information and data have to be managed, stored, analysed and used by means of advanced semantic annotation and algorithm which allow to understand and interpret the information in relation to specific application field. These software elements, with machine learning algorithm, allows to understand and interpret the information in relation to the specific context, making sense to seemingly incoherent amount of data.

M. R. Guarneri (✉) · R. Sironi · P. Perego
Dip. di Design, Politecnico di Milano, via G. Durando 38/A, 20158 Milan, Italy
e-mail: mariarenata.guarneri@polimi.it

R. Sironi
e-mail: roberto.sironi@polimi.it

P. Perego
e-mail: paolo.perego@polimi.it

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_1

This allows the development of new models and new approaches to consolidated field of applications like the health care.

The healthcare sector is in fact the most blazoned example, where consolidated models of care are undergoing a deep transformation which is strictly related to the digital revolution; indeed, as evidenced also by Flores et al. [1], three converging megatrends are behind such transformation:

1. The progress of the biomolecular disciplines, the so-called omics, and the increased ability to understand the biological complexity of disease.
2. The digital revolution, with the explosion of the Internet of Things (IoT) and consequently Internet of Medical Things (IoMT), the 'big data' phenomenon, the digitalisation of medical/clinical data together with the enhanced capacity to store and analyse and make sense of such amount of information.
3. A population always connected, with the large use of social networks where people (with the role of citizens, consumers or patients) communicate with others, provide information and, most importantly, have access to information.

1.2 P4 Medicine

The concept of P4 medicine was introduced and illustrated by Leroy Hood in 'A personal view on Systems medicine and the emergence of proactive **P4 Medicine**…' [2]. The four P's are:

- predictive,
- preventive,
- personalised and
- participatory.

As mentioned above, P4 medicine focuses on prediction and prevention; thanks to the results coming from the Human Genome Project,[1] P4 postulates that, ideally, the risk of disease can be predicted at cellular level well before symptoms develop, and therefore, the actual occurrence of disease can be prevented through the participation of the 'patient' in preventive action.

P4 leverages large-scale social participation; patient must be activated and engaged to become protagonists of their well-being. They must be willing to collect and share personal health data, to participate in the development of medical devices, co-design their own monitoring and healthcare treatment system together with physicians, engineers and other welfare actors. As Hood and colleagues indicated in [1], '… the driver of an emerging P4 healthcare system will be information consumer can use to better manage their health'. In the same paper, the authors claim that the P4 approach, combining the integrated/multidisciplinary approach of system medicine with active participation of networked users, will reduce the incidence of disease while providing a more personalised cost-effective healthcare system (Fig. 1.1).

[1] https://www.genome.gov/12011238/an-overview-of-the-human-genome-project.

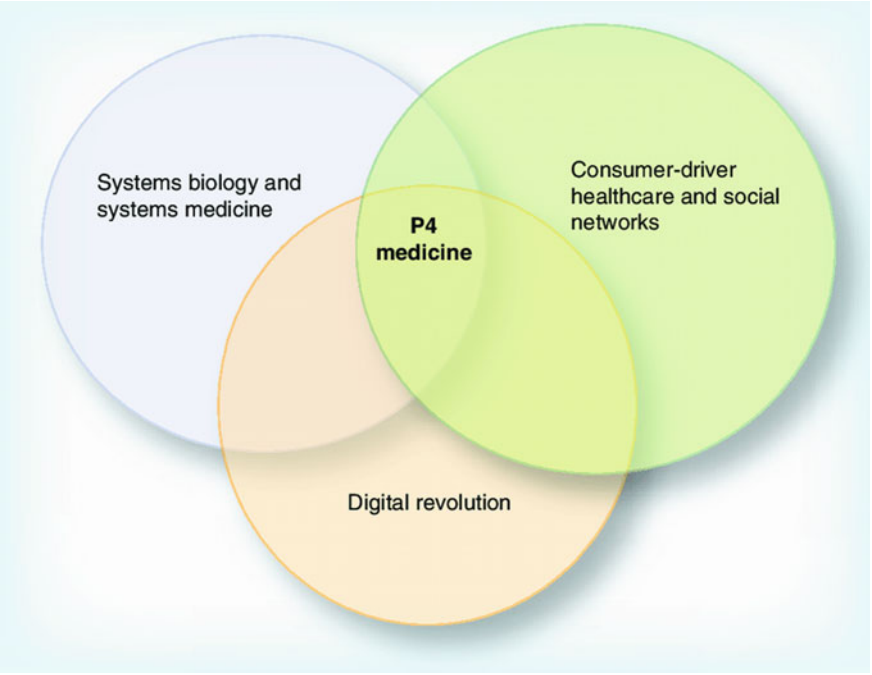

Fig. 1.1 Three converging megatrends driving the transformation of health care. P4 health care is emerging at the intersection of these megatrends [1]

The role of individuals—who more and more take interest in managing their own health, also in unconventional ways thinking of the booming of the well-being sector—is a core aspect for the healthcare revolution. Thanks to the growing number of empowerment tools like apps or portable medical devices, health care is no longer an aspect linked mostly to hospitals, but monitoring also takes place at home, modifying the relation between physicians and patients. Consumers—citizens and patients—and their new attitudes and awareness with regard to health are actually driving the transformation in health care. The advent of eHealth with the digital management of patient information and the wide adoption of Electronic Health Records (EHR) has changed the way health care is managed; in particular from an administrative point of view, concept such as patient empowerment, personalised medicine will have an impact on the development of new healthcare models, that will become patient-centric (personalised according to the P4 Medicine) models.

1.3 Future and Perspective for Healthcare System

A more cost-effective health care is a key priority of the European political agenda; *Better Health and care, economic growth and sustainable health system* together with *Digital transformation in Healthcare* are two of the key objectives of the EU research in the H2020 programme [3], and many projects have been proposed and funded to further the research in these areas. Active involvement of users and patients and the development of sustainable care models that respond to the new needs and exploit the advancements enabled by biomolecular research and by the digital revolution are key elements (and often pain points) of such projects.

Currently, there are about 7 billion smartphones on earth; it is possible to predict that between 10 and 20 years every planet's inhabitant will have a smartphone powerful enough to receive, store and process personal health data. This fact also leads to another consideration: the smartphone will be the vault of sensitive personal data such as those related to health status or biometric; a discussion on security and privacy is, for this reason, mandatory. Moreover, figuring out what motivates both caregivers and consumers to adopt and continue to use digital technologies is critical for sustainability.

The access to this healthcare evolved technological system is going to increasingly influence the way we live and perceive our biological environment; it will be fundamental for designers, engineers and developer in general, to consider the future human nature in relation to the two most promising technologies for health: wearable and implantable.

References

1. Flores, M., Glusman, G., Brogaard, K., Price, N.D., Hood, L.: P4 medicine: how systems medicine will transform the healthcare sector and society. Per. Med. **10**(6), 565–576 (2013)
2. Hood, L., Flores, M.: A personal view on systems medicine and the emergence of proactive P4 medicine: predictive, preventive, personalized and participatory. New Biotechnol. **29**(6) (2012)
3. H2020.: Work Programme 2018–2020. 2017. http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-introen.pdf

Chapter 2
The mHealth

Alessia Paglialonga, Alfonso Mastropietro, Elisa Scalco and Giovanna Rizzo

Abstract The rapid growth and popularity of mobile technology have opened an entirely new area in healthcare. Mobile health (mHealth) encompasses any use of mobile applications and devices for health and is a lively area of development and research. mHealth apps and devices hold great promise in terms of potential benefits for the several actors involved (patients, citizens, and professionals). For example, the promotion of preventive behaviors and health monitoring, enhanced patient-doctor engagement, improved service delivery in resource-limited settings, patient empowerment, and patient-centered care. At the same time, this mobile revolution in healthcare can bring along peculiar challenges and risks that are entirely new and that need to be carefully addressed. For example, the digital divide and related health inequalities, the risk of increased dropout in clinical studies compared, and the issue of guaranteeing evidence base, validation, and in general, quality and effectiveness of mHealth. These challenges push for more and more focused research in the field and for increasing collaboration among researchers, physicians and healthcare professionals, developers, industries, as well as representatives of the target user groups.

A. Paglialonga (✉)
Consiglio Nazionale delle Ricerche (CNR), Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni (IEIIT), Milan, Italy
e-mail: alessia.paglialonga@ieiit.cnr.it

A. Mastropietro · E. Scalco · G. Rizzo
Consiglio Nazionale delle Ricerche (CNR), Istituto di Bioimmagini e Fisiologia Molecolare (IBFM), Segrate, Milan, Italy
e-mail: alfonso.mastropietro@ibfm.cnr.it

E. Scalco
e-mail: elisa.scalco@ibfm.cnr.it

G. Rizzo
e-mail: giovanna.rizzo@ibfm.cnr.it

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_2

2.1 Introduction

Mobile health (mHealth) is the use of health-related mobile applications (apps), mobile, and wearable devices to deliver medical information, to access or capture data, to provide clinical and personal services, or to support healthcare delivery in clinical and nonclinical settings. Noticeably, the World Bank has defined mHealth as the use of mobile technology to improve the well-being of people around the world [50]. It becomes thus clear that mHealth can be an entirely novel facilitator to address key healthcare challenges such as, for example, access to care, quality of services, affordability of technology, or matching of resources [47]. Mobile apps and devices can be of value to help people manage their own health, to promote healthy living, and to gain access to useful information when and where they need it [20].

In the past few years, we have witnessed a rapid development of mobile apps and devices for healthcare, with increasing penetration into clinical practice and into the daily life of patients and citizens[53]. The characteristics and context of mHealth are largely new compared to conventional eHealth approaches and, thanks to its peculiar characteristics, mHealth can have a significant impact on public health, healthcare services settings, as well as in nonclinical settings, including home use and patient monitoring. The core characteristics, as well as the general context of mHealth, are discussed in Sect. 2.2.

Documented opportunities and benefits of mHealth include, but are not limited to increased patient motivation toward behavior change [65], promotion of preventive behaviors and health monitoring in the general population [32, 28], enhanced patient–doctor engagement [56], recording of patient-reported measures and Ecological Momentary Assessment [14], improved service delivery in resource-limited settings (e.g., [2]), patient empowerment, and patient-centered care [52, 56].

Moreover, the mobile revolution in healthcare brings along entirely novel risks and challenges that are a matter of debate and that need to be carefully addressed. Examples are the so-called "digital divide," which could exacerbate health inequalities among different populations [30]; attrition and increased dropout in clinical studies compared to conventional protocols [51]; and the prominent issue of guaranteeing evidence base, validation, and in general, quality and effectiveness of mobile technology and applications [37, 41, 58]. Some of the most relevant benefits and challenges of mHealth are discussed in Sect. 2.3.

2.2 Core Characteristics and Context

Four core characteristics of mHealth have been conceptualized recently. These characteristics are specific to the field, unforeseen in earlier applications of information and communication technology (ICT) in Health, and essential to the design, implementation, and adoption of mHealth-based solutions [17]:

- penetration into populations, due to communication access to population and subgroups (although with substantial inequalities);
- availability of apps, due to increasing smartphone capabilities, functionality, and sensors integration and due;
- wireless broadband access to the internet thanks to increasing communication speed and device connectivity; and
- technology tethered to individuals due to increasing capability of locating, measuring data, monitoring function, and communicating with others.

With respect to the general objectives and context of mHealth, the US Federal Communications Commission [19] emphasized that mHealth can use mobile networks and devices in supporting e-care, leveraging health-focused applications on general-purpose tools such as mobile phones to drive active health participation by consumers and clinicians. Nowadays, mHealth apps and devices are used with proven success in several medical specialties, as well as in general health management and disease prevention. The fast increasing availability of mobile applications dedicated to health prevention and care supports management of chronic conditions and risk factors, medicines uptake, as well as the achievement of lifestyle/health objectives as obtained using ICT for personalization and real-time feedback. Unprecedented opportunities arise thanks to personal devices connected to mobile phones such as, for example, smartwatches, wristbands, and wearable sensors. Unique, innovative capabilities provided by the combined use of apps and wearable devices include, e.g., blood pressure monitors, pulse oximeters, blood glucose meters, environmental exposure measures (e.g., for asthma), single lead electrocardiogram (ECG), and sleep monitors [17].

The range of uses of mobile applications and devices is large and supported by growing evidence. In terms of categories, mHealth solutions can be classified into: general solutions for medical providers (physicians, nurses, and assistants), for example drug-referencing tools, clinical decision-support tools, electronic health-record system access and medical education materials; apps for medical education, teaching, and learning; tools for telemedicine and tele-healthcare; apps/wearables for patients and the general public over a wide array of functions; and specialty- or disease-specific apps [12]. Several examples can be found in the literature, related to a variety of specialties and disease groups such as, e.g., asthma risk management [27], cardiology [34], diabetes care [24], emergency medicine [61], nutrition [6], mental health [23]; sensory systems healthcare [54, 48], or infectious diseases monitoring [46].

2.3 Benefits and Challenges

Of the several documented benefits of mHealth, this Section discusses the opportunities offered by mHealth in terms of Ecological Momentary Assessment (EMA), patient empowerment and engagement, and service delivery in undeserved settings.

On the other hand, among the potential risks and challenges related to mHealth use, this section outlines the problem of health inequalities related to the digital divide, the issue of potentially increased dropout in clinical/research studies, the need for robust validation and evidence base in mHealth and the open debate on how to assess quality in mHealth.

2.3.1 Ecological Momentary Assessment (EMA)

The huge potential of mHealth approaches can have an enormous impact on surveillance, epidemiological, and intervention studies in both social and health sciences. Most of these studies were typically based on static retrospective self-report methods [22] that can be vulnerable to reporting errors and recall biases [4]. EMA has been widely proposed as a valuable alternative to overcome bias and errors coming from the traditional approaches.

EMA is referred to a group of techniques and methodologies allowing the subjects to self-report on detailed information about their status, activity, and experience (e.g., symptoms, feelings, behaviors, and cognitions) in real-time. This information is usually acquired many times through the course of their normal daily life in a natural environment [57]. Since the 80s, just after its introduction, EMA was usually carried out in the form of a daily diary. Nowadays, thanks to the progress of mobile, electronic, and wearable sensors technology, new approaches to EMA have become possible. The feasibility of frequent self-assessment sessions and real-time monitoring, based on non-obtrusive monitoring of mHealth apps and devices, makes it easier to monitor the individual's health status and self-reported measures.

A recent paper [14] has addressed the necessary steps and the related challenges to plan and prepare a longitudinal study using mobile technology to administer EMA. The paper was based on the EMPOWER project aimed to examine the triggers of lapses and relapse following intentional weight loss in adults. The adherence to completing EMA surveys was high, ranging from 88.3 to 90%. The EMPOWER infrastructure can be used as an example showing the technological solutions adopted (smartphones, apps, web server, database server, IoT approach, and Wi-Fi communication) and their interactions.

A slightly different approach, based on real-time sensor-informed context-sensitive EMA (CS-EMA) was developed to analyze physical activity [18]. CS-EMA is an innovative strategy that automatically triggers survey prompts at opportune times based on detected information from internal or external sensors using a mobile phone app. The average CS-EMA prompt compliance and survey completion rates were 80.5%.

The feasibility and acceptability of using smartphone-based EMA to capture daily functioning and other behaviors were also assessed in HIV + adults [39]. The authors report a high EMA adherence (86.4%) and assert that participants rated their experience with EMA methods positively.

The use of mobile technologies is a promising way to enable and boost EMA applications in research and in clinical practice, as it was already effectively tested in different fields of social and health science. Currently, EMA is mostly based on mobile phones and mobile apps and the use of integrated monitoring sensors can improve the EMA approach including more quantitative data. However, it is important to implement strategies that maximize patient feedback and participation as one relevant risk in EMA and, more generally, in using mobile tools for recording data/measures from patients, is potentially increased dropout compared to face-to-face or PC-based procedures, as discussed in Sect. 2.3.5.

2.3.2 Patient Empowerment and Engagement

mHealth has the potential to empower patients to self-manage their chronic diseases through instant tailored feedbacks [52]. With respect to clinic-based care, mHealth data can be collected much more intensively through a self-management support, allowing more detailed patterns to emerge in the outcomes of interest [56]. Patient empowerment is also reached by a support for decision-making about self-management directly to patients rather than through health care providers [28].

Moreover, mHealth has a potential impact on the patient engagement with treatment, which includes behavioral, affective, and cognitive components that contribute to maximize treatment outcome. In particular, the influence of mHealth intervention on health behavior change is an interesting field of research, showing encouraging results [65]. The use of mobile applications can monitor how engagement changes during treatment and factors associated with changes in the level of engagement [56].

Enhanced patient empowerment and engagement with treatments through the use of smart device-based interventions have demonstrated a clinical and health impact on different chronic conditions. Among these conditions, cardiovascular pathologies and diabetes have been widely studied. For example, it was reported in numerous studies a health improvement in HbAlc control among patients with diabetes [28].

Regarding cardiovascular risk factor control, mHealth has an impact on different situations, from the use of text message reminders to take medications to the application of biosensors that record and transmit blood pressure readings to databases for analysis and feedback [52]. In this field, the management of hypertension through mHealth interventions was extensively evaluated, reporting a high use of text messaging as the preferred instrument to monitor and control blood pressure. For example, a Russian study reported a significantly higher proportion of patients reaching target blood pressure in the intervention group in which regular text message reminders were sent to them to monitor home blood pressure, compared with the control group receiving usual care [29]. In more recent years, mHealth interventions were much more focused on the use of biosensors and mobile phone applications, such as the use of a smartphone-based home service delivery which has improved the uptake, adherence, and completion of cardiac rehabilitation in post-myocardial infarction patients as demonstrated by a randomized control trial [60]. Smartphone apps and

wearable technology have demonstrated their potential also in the achievement of lifestyle/health objectives such as smoking cessation [64] and exercise promotion in middle-agers [32].

However, several studies have identified hurdles that challenge wide usage, including poor user interface designs, differing user literacy levels, implementation issues, and organizational structures. To take full advantage of the potential of mHealth as a trigger for behavior change, it is important to consider elements of patient engagement since the design as well as to introduce strategies that are specific to the target users group [16].

2.3.3 Service Delivery in Underserved Areas

The social, economic, and educational level, as well as age, gender, and ethnicity of an individual can strongly affect his health status. In particular, limited income and education affect individuals' health negatively by reducing their capability to access health services and to acquire and understand health information needed to prevent or adequately care pathologies [44].

mHealth technology is potentially a valuable approach to limit the disparities among people as it can effectively strengthen health systems in low-income countries through better access to knowledge and information, improved service delivery and reduced intervention time and cost, thus extending the number of persons who can take advantage of health services [2].

Mobile technologies could assist vulnerable patients who live in rural regions, far away from hospitals, by allowing clinicians to monitor them remotely. This may improve access to quality care, and prevent frequent and costly trips to the urban health care facilities [43]. In addition, the use of mHealth approaches can improve the screening of pathologies in populations that have no access to health services and screening protocols. As an example, a smartphone-based hearing screening system was validated in South Africa to improve healthcare in underserved communities at a primary care level [63] allowing for quality control and remote monitoring for surveillance and follow-up. Using a similar technological approach, individuals who are vulnerable to health disparities were successfully able to use mHealth programs designed to promote colorectal cancer screening [36].

Finally, in low-income areas, where the health literacy of the population can be modest, mobile-assisted health care systems can increase the quality and efficacy of both diagnosis and care by helping health workers, caregivers, and patients to access a higher level medical knowledge (guidelines and manuals) using mobile devices [38]. However, specific efforts are needed to tailor mHealth to the peculiar needs of underserved contexts and disadvantaged populations to try to limit possible drawbacks due to poor access to technology, low digital skills, and low literacy levels, i.e., the so-called digital divide.

2.3.4 The Digital Divide and Health Inequalities

While the use of mHealth may bring along several important benefits, indeed mHealth can be effective to the extent that individuals are in a position to use it well. Yet, the "digital divide" along with demographic and socioeconomic inequalities can create a gap between users and nonusers in terms of the improvement of health services, leading to (or exacerbating) health inequalities [30]. Health inequalities can become a prominent issue because they can translate into differences in the prevalence of illness and of illness repercussions, mortality rate, and burden of illness and other health conditions among different population groups [42].

Demographic and socioeconomic inequalities among different population groups (e.g., ethnicity, socioeconomic status, age and gender, literacy, health literacy, and access/affordability of technology) can lead to differences among individuals in terms of skills and ability to use mHealth effectively and this, in turn, can amplify health inequalities [30, 35].

Unequal access to technologies such as computers, smartphones or the Internet is referred to as "primary" digital divide, and is known to influence the utilization of services [33]. This is frequently related to geographical, demographical, and economic disparities. Widespread use of smartphones and other mobile devices and the reduced cost of technology and the Internet can, at least in part, diminish the "primary" digital divide. Yet, gaps still remain, for example, in smartphone adoption for individuals over 65, with less than high school education, with a disability, and living in poverty [31].

However, even though access to technology is a crucial element in the utilization of a technology, this is not sufficient so the primary digital divide accounts only for a part of the potential health inequalities [35]. For example, digital literacy and knowledge related to the utilization of modern technology also have an impact. This gap in digital knowledge between users is called the "secondary" digital divide [7] and pushes for research toward mHealth tools that need to be easy and simple to use for individuals with limited digital skills.

Moreover, a "tertiary" digital divide exists [9]. Much more widespread, the tertiary digital divide refers to the concept of significant (or universal) access encompassing technology, Internet connection, skills development, technical assistance, and appropriate content, i.e., content understandable and useful for disadvantaged populations. This tertiary digital divide is much more difficult to overcome and calls for a common effort of developers, healthcare providers, policymakers, researchers, and industry.

So, although mHealth can, in principle, be a means to bring healthcare closer to people in disadvantaged settings, nevertheless efforts need to be done to ensure that mHealth holds its promise to reduce inequalities among individuals. It is important to bring technology closer to those with reduced digital capabilities and health literacy so to enable any individual along the socioeconomic scale to adopt mHealth technology effectively.

2.3.5 Attrition and Increased Dropout

A common issue in mHealth is the difficulty in recruiting and retaining people for testing the feasibility and the efficacy of new mobile applications and services. A very recent study aimed to evaluate a mHealth application to increase tobacco cessation medication adherence. In this work, the final users had been involved during the development of the mHealth service, thus allowing its optimization from the usability and acceptability point of view. However, high attrition was found due to technical (lost/upgraded phones) issue, insufficient human contact between staff and participants, medication side effects, and enrollment procedures [21], resulting in an eligibility of 42% and a dropout of 43%.

Analogously, another study [26] reported the patient recruitment and engagement, as vulnerable phases in an text message-based trial of mHealth intervention of people with serious mental health problems. In this study, the main factors related to attrition were patients gender, age, vocational education, and employment status, while the need of staff extra support seems necessary to reduce attrition.

Interestingly, a recent study compared the efficacy and the appreciation of a PC-based eHealth physical activity intervention with its mHealth version [51], reporting that the eHealth version resulted in a more effective intervention and better usability and appreciation. This finding suggests that mHealth is not preferable to eHealth in any circumstances and that mobile phone could be per se a distracting factor; a very careful co-design to optimize subject's engagement and appreciation could help in minimizing this aspect.

Noncompliance and nonadherence of the participants to the study are certainly a detrimental factor to the benefits provided by mobile EMA self-assessment. A systematic review and meta-analysis collecting 42 studies involving young people (<18 years old) showed that the weighted average compliance rate was 78.3% [62]. Study design and protocols may affect compliance, whereas including additional wearable devices did not significantly change the participant's adherence.

It is worth to notice, however, that there is a need for new, more robust, experimental studies to investigate the real impact of mobile technologies on participant adherence and engagement.

2.3.6 Need for Methods to Ensure Quality in mHealth

The high number of mHealth apps and devices available on the market is not always demonstrated to be based on documented evidence and/or developed involving all the relevant stakeholders. The number of apps that are validated or tested for evidence base is still very low in several application areas [13, 59]. More scientific-based, controlled, clinical trials are mandatory to increase the quality of mHealth solutions and to fully understand the feasibility and benefits of introducing these solutions into clinical practice before promoting their routine use in healthcare.

The need for methods to characterize and assess mHealth apps and devices is particularly urgent as a means to support physicians and healthcare professionals in the identification of the most appropriate solutions for themselves and for their patients and families. This need has inspired a significant amount of research to try to devise assessment methods to inform potential users of apps and wearable devices that can be accurate and at the same time simple and easy to use. Basically, the main source of information for the end users still remains the web, including not only online markets (app and wearable markets) but also the manufacturer's websites, health-related web portals, expert communities, and voluntary review and evaluation systems [11]. Attempts to develop certification frameworks such as, for example, the Happtique Health App Certification Program (HACP) have failed so far due to security shortcomings [12]. In general, certification and standardization are difficult to achieve due to key market factors such as the number of features, diversity of information, and the very rapid pace of development [15].

The characterization and assessment of mHealth tools is an important area of research in and of itself. The concept of quality of health apps is complex, subjective in nature, and a matter of debate. It includes, for example, elements of safety, trustworthiness, user-oriented quality (e.g., operability, usability, depth of understanding, and quality of experience), effectiveness, and evidence base.

Many examples of methods for the characterization and assessment of mHealth tools have been introduced so far [8, 25]. For example, some classification frameworks have been proposed, based on features such as the type of health management strategies, user engagement approaches, or the potential to influence behavior change and the drivers used [55]. Some other studies in the literature proposed to code mHealth tools not only for the enabling drivers and functions but, also, for their content and features. For example, data analysis capabilities [24], fulfillment of clinical guidelines [1], completeness of information [40], or the degree of medical professional involvement and the availability of evidence-based content [45]. Some studies have tried to develop characterization frameworks in the area of mHealth safety and trustworthiness, but these aspects are difficult to measure [3]. Some other studies introduced methods to address user-oriented attributes that are directly or indirectly related to elements of quality such as, e.g., operability, usability, depth of understanding, and quality of experience. Expert-based evaluations have been suggested [5] as well as to user-oriented, easy-to-use tools to collect meaningful information about a core set of relevant features [10, 49, 58].

Overall, although the literature in this area is ample, the question of how to characterize and assess mHealth is still an open and challenging one.

2.4 Conclusions

The popularity and usage of mobile technology are growing along with the number and variety of mHealth solutions and applications. Increasingly, patients and citizens are inclined to seek health-related guidance from mobile devices due to practical-

ity in communicating, information resourcefulness, portability, affordable costs, and widespread availability. Along with the many opportunities and benefits that mHealth can bring in public health, healthcare service settings, and personal health management, there are also some important potential risks that need to be considered and as far as possible, minimized by design.

The field of mHealth is a lively area of research where scientists, physicians and healthcare professionals, developers, industries and the target user groups should work together toward the common goal of delivering mHealth applications and devices that guarantee evidence base, reliability, effectiveness, and quality and that can be affordable and accessible for everyone.

References

1. Abroms, L.C., Padmanabhan, N., Thaweethai, L., Phillips, T.: iPhone apps for smoking cessation: a content analysis. Am. J. Prev. Med. **40**(3), 279–285 (2011)
2. AHO.: Leveraging eHealth to improve national health systems in the African Region. In: African Health Monitor, issue 14 (2012) http://www.aho.afro.who.int/en/ahm/issue/14/reports/leveraging-ehealth-improve-national-health-systems-african-region. Accessed 29 June 2017
3. Albrecht, U.V.: Transparency of health-apps for trust and decision making. J. Med. Internet Res. **15**(12), e277 (2013)
4. Ainsworth, B.E., Caspersen, C.J., Matthews, C.E., Msse, L.C., Baranowski, T., Zhu, W.: Recommendations to improve the accuracy of estimates of physical activity derived from self report. J. Phys. Act. Health **9**(Suppl 1), S76–S84 (2012)
5. Arnhold, M., Quade, M., Kirch, W.: Mobile applications for diabetics: a systematic review and expert-based usability evaluation considering the special requirements of diabetes patients age 50 years or older. J. Med. Internet Res. **16**(4), e104 (2014)
6. Bardus, M., van Beurden, S.B., Smith, J.R., Abraham, C.: A review and content analysis of engagement, functionality, aesthetics, information quality, and change techniques in the most popular commercial apps for weight management. Int. J. Behav. Nutr. Phys. Act. **13**, 35 (2016)
7. Beacom, A.M., Newman, S.J.: Communicating health information to disadvantaged populations. Fam. Community Health **33**(2), 152–162 (2010)
8. BinDhim, N.F., Hawkey, A., Trevena, L.: A systematic review of quality assessment methods for smartphone health apps. Telemed J. E Health **21**(2), 97–104 (2015)
9. Bodie, G.D., Dutta, M.J.: Understanding health literacy for strategic health marketing: eHealth literacy, health disparities, and the digital divide. Health Mark. Q. **25**(12), 175–203 (2008)
10. Bonacina, S., Marceglia, S., Pinciroli, F.: A pictorial schema for a comprehensive user-oriented identification of medical apps. Methods Inf. Med. **53**(3), 208–224 (2014)
11. Boudreaux, E.D., Waring, M.E., Hayes, R.B., Sadasivam, R.S., Mullen, S., Pagoto, S.: Evaluating and selecting mobile health apps: strategies for healthcare providers and healthcare organizations. Transl. Behav. Med. **4**(4), 363–371 (2014)
12. Boulos, M.N., Brewer, A.C., Karimkhani, C., Buller, D.B., Dellavalle, R.P.: Mobile medical and health apps: State of the art, concerns, regulatory control and certification. Online J. Public Health Inform. **5**(3), 229 (2014)
13. Bright, T., Pallawela, D.: Validated smartphone-based apps for ear and hearing assessments: a review. JMIR Rehabil. Assist. Technol. **3**(2), e13 (2016)
14. Burke, L.E., Shiffman, S., Music, E., Styn, M.A., Kriska, A., Smailagic, A., Siewiorek, D., Ewing, L.J., Chasens, E., French, B., Mancino, J., Mendez, D., Strollo, P., Rathbun, S.L.: Ecological momentary assessment in behavioral research: addressing technological and human participant challenges. J. Med. Internet Res. **19**(3):e77 (2017)

15. Chan, S.R., Misra, S.: Certification of mobile apps for health care. JAMA **312**(11), 1155–1156 (2014)
16. Chindalo, P., Karim, A., Brahmbhatt, R., Saha, N., Keshavjee, K.: Health apps by design: a reference architecture for mobile engagement. Int. J. Handheld Comput. Res. (IJHCR) **7**(2), 34–43 (2016)
17. Davis, T.L., DiClemente, R., Prietula, M.: Taking mHealth forward: examining the core characteristics. JMIR Mhealth Uhealth **4**(3), e97 (2016)
18. Dunton, G.F., Dzubur, E., Intille, S.: Feasibility and performance test of a real-time sensor-informed context-sensitive ecological momentary assessment to capture physical activity. J. Med. Internet Res. **18**(6), e106 (2016)
19. FCC, US Federal Communications Commission.: Washington, DC: Federal Communications Commission Connecting America: The National Broadband Plan (2010) https://www.fcc.gov/general/national-broadband-plan. Accessed 29 June 2017
20. FDA, U.S. Food and Drug Administration.: Digital Health. (2015) https://www.fda.gov/medicaldevices/digitalhealth/ Accessed 29 June 2017
21. Gordon, J.S., Armin, J.S., Cunningham, J.K., Muramoto, M.L., Christiansen, S.M., Jacobs, T.A.: Lessons learned in the development and evaluation of RxCoach, an mHealth app to increase tobacco cessation medication adherence. Patient Educ. Couns. **1100**, 720–727 (2017)
22. Haskell, W.L.: Physical activity by self-report: a brief history and future issues. J. Phys. Act Health **9**(Suppl 1), S5–10 (2012)
23. Helf, C., Hlavacs, H.: Apps for life change: critical review and solution directions. Entertainment Comput. **14**, 17–22 (2016)
24. Huckvale, K., Adomaviciute, S., Prieto, J.T., Leow, M.K., Car, J.: Smartphone apps for calculating insulin dose: a systematic assessment. BMC Med. **13**, 106 (2015)
25. Hussain, M., Al-Haiqi, A., Zaidan, A.A., Zaidan, B.B., Kiah, M.L., Anuar, N.B., Abdulnabi, M.: The landscape of research on smartphone medical apps: coherent taxonomy, motivations, open challenges and recommendations. Comput. Methods Programs Biomed. **122**(3), 393–408 (2015)
26. Kannisto, K.A., Korhonen, J., Adams, C.E., Koivunen, M.H., Vahlberg, T., Valimaki, M.A.: Factors associated with dropout during recruitment and Follow-up periods of a mHealth-based randomized controlled trial for mibile.net to encourage treatment adherence for people with serious mental health problems. J. Med. Internet Res. **19**(2):e46 (2017)
27. Kenner, A.: Asthma on the move: how mobile apps remediate risk for disease management. Health Risk Soc **17**(7–8), 510–529 (2016)
28. Kim, B.Y., Lee, J.: Smart devices for older adults managing chronic disease: a scoping review. JMIR mHealth uHealth **5**(5), e69 (2017)
29. Kiselev, A.R., Gridnev, V.I., Shvartz, V.A., Posnenkova, O.M., Dovgalevsky, P.Y.: Active ambulatory care management supported by short message services and mobile phone technology in patients with arterial hypertension. J Am Soc Hypertens **6**(5), 346355 (2012)
30. Latulippe, K., Hamel, C., Giroux, D.: Social health inequalities and eHealth: A literature review with qualitative synthesis of theoretical and empirical studies. J. Med. Internet Res. **19**(4), e136 (2017)
31. Lewis, J.: Handheld device ownership: reducing the digital divide? In: U.S. Bureau of the Census, March 2017 Report, Working Paper number SEHSD-2017-04 (2017). https://www.census.gov/library/working-papers/2017/demo/SEHSD-WP2017-04.html. Accessed 29 June 2017
32. Liao, G.Y., Chien, Y.T., Chen, Y.J., Hsiung, H.F., Chen, H.J., Hsieh, M.H., Wu, W.J.: What to build for middle-agers to come? Attractive and necessary functions of exercise-promotion mobile phone apps: a cross-sectional study. JMIR mHealth uHealth **5**(5), e65 (2017)
33. Lindsay, S., Bellaby, P., Smith, S., Baker, R.: Enabling healthy choices: is ICT the highway to health improvement? Health (London) **12**(3), 313331 (2008)
34. Martnez-Prez, B., de la Torre-Dez, I., Lpez-Coronado, M., Herreros-Gonzlez, J.: Mobile apps in cardiology: review. JMIR Mhealth Uhealth **1**(2), e15 (2013)

35. McAuley, A.: Digital health interventions: widening access or widening inequalities? Publ. Health **128**(12), 11181120 (2014)
36. Miller Jr., D.P., Weaver, K.E., Case, L.D., Babcock, D., Lawler, D., Denizard-Thompson, N., Pignone, M.P., Spangler, J.G.: Usability of a novel mobile health iPad app by vulnerable populations. JMIR Mhealth Uhealth **5**(4), e43 (2017)
37. Misra, S., Lewis, T.L., Aungst, T.D.: Medical application use and the need for further research and assessment for clinical practice: creation and integration of standards for best practice to alleviate poor application design. JAMA Dermatol. **149**(6), 661–662 (2013)
38. Mondal, S., Mukherjee, N.: Mobile-assisted remote healthcare delivery. In: Proceedings of the 4th IEEE International Conference on Parallel, Distributed and Grid Computing (IEEE PDGC 2016), IEEE Press, pp. 630–635 (2016)
39. Moore, R.C., Kaufmann, C.N., Rooney, A.S., Moore, D.J., Eyler, L.T., Granholm, E., Woods, S.P., Swendsen, J., Heaton, R.K., Scott, J.C., Depp, C.A.: Feasibility and acceptability of ecological momentary assessment of daily functioning among older adults with HIV. Am. J. Geriatr. Psychiatry **S1064-7481**(16), 30323-2 (2016)
40. Muessig, K.E., Pike, E.C., LeGrand, S., Hightow-Weidman, L.B.: Mobile phone applications for the care and prevention of HIV and other sexually transmitted diseases: a review. J. Med. Internet Res. **15**, e1 (2013)
41. Murfin, M.: Know your apps: an evidence-based approach to evaluation of mobile clinical applications. J. Physician Assist. Educ. **24**(3), 38–40 (2013)
42. National Institutes of Health. NIMHD.: Strategic Research Plan and Budget to Reduce and Ultimately Eliminate Health Disparities Volume I Fiscal Years 2002–2006 (2002). http://www.nimhd.nih.gov/docs/. Accessed 29 June 2017
43. Ni, Z., Wu, B., Samples, C., Shaw, R.J.: Mobile technology for health care in rural China. Int. J. Nurs. Sci. **3**, 323–324 (2014)
44. Nutbeam, D.: The evolving concept of health literacy. Soc. Sci. Med. **67**(12), 2072–2078 (2008)
45. ONeill, S., Brady, R.R.W.: Colorectal smartphone apps: opportunities and risks. Colorectal Dis. **14**:e530534 (2012)
46. Oehler, R.L., Smith, K., Toney, J.F.: Infectious diseases resources for the iPhone. Clin. Infect. Dis. **50**(9), 1268–1274 (2010)
47. Ozdalga, E., Ozdalga, A., Ahuja, N.: The smartphone in medicine: a review of current and potential use among physicians and students. J. Med. Internet Res. **14**(5), e128 (2012)
48. Paglialonga, A., Pinciroli, F., Tognola, G.: Apps for hearing health care: trends, challenges and potential opportunities. In: Saunders, E. (ed) Tele-Audiology and the Optimization of Hearing Health Care Delivery, IGI Global, Hershey, 161–195 (2019)
49. Paglialonga, A., Pinciroli, F., Tognola, G.: The ALFA4Hearing model (At-a-glance labelling for features of apps for hearing healthcare) to characterize mobile apps for hearing healthcare. Am. J. Audiol. 26(3S), 408–425 (2017)
50. Qiang, C.Z., Yamamichi, M., Hausman, V., Miller, R., Altman, D.: Mobile applications for the health sector. World Bank, Washington, DC (2012). http://documents.worldbank.org/curated/en/2012/04/16742613/mobile-applications-healthsector. Accessed 29 June 2017
51. Quinonez, S.G., Walthouwer, M.J.L., Schulz, D.N., de Vries, H.: mHealth or eHealth? Efficacy, use and appreciation of a web-based computer-tailored physical activity intervention for Dutch adults: a randomized controlled trial. J. Med. Internet Res. **18**(11), e278 (2016)
52. Rehman, H., Kamal, A.K., Morris, P.B., Sayani, S., Merchant, A.T., Virani, S.S.: Mobile health (mHealth) technology for the management of hypertension and hyperlipidemia: slow start but loads of potential. Curr Atheroscler Rep **19**(3), 12 (2017)
53. Research2guidance.: mHealth App Developer Economics 2016—The State of the Art of mHealth App Publishing (2016). https://research2guidance.com/product/mhealth-app-developereconomics-2016/. Accessed 29 June 2017
54. Rodin, A., Shachak, A., Miller, A., Akopyan, V., Semenova, N.: Mobile apps for eye care in Canada: an analysis of the iTunes store. JMIR Mhealth Uhealth **5**(6), e84 (2017)
55. Sama, P.R., Eapen, Z.J., Weinfurt, K.P., Shah, B.R., Schulman, K.A.: An evaluation of mobile health application tools. JMIR Mhealth Uhealth **2**(2), e19 (2014)

56. Scherer, E.A., Ben-Zeev, D., Li, Z., Kne, J.M.: Analyzing mHealth engagement: joint models for intensively collected user engagement data. JMIR mHealth uHealth **5**(1), e1 (2017)
57. Shiffman, S., Stone, A.A., Hufford, M.R.: Ecological momentary assessment. Annu. Rev. Clin. Psychol. **4**, 1–32 (2008)
58. Stoyanov, S.R., Hides, L., Kavanagh, D.J., Zelenko, O., Tjondronegoro, D., Mani, M.: Mobile app rating scale: a new tool for assessing the quality of health mobile apps. JMIR Mhealth Uhealth **3**, e27 (2015)
59. Torous, J., Levin, M.E., Ahern, D.K., Oser, M.L.: Cognitive behavioural mobile applications: clinical studies, marketplace overview and research agenda. Cogn. Behav. Pract. **24**, 215–225 (2017)
60. Varnfield, M., Karunanithi, M., Lee, C.K., Honeyman, E., Arnold, D., Ding, H., Smith, C., Walters, D.L.: Smartphone-based home care model improved use of cardiac rehabilitation in postmyocardial infarction patients: results from a randomised controlled trial. Heart **100**(22), 17701779 (2014)
61. Wallis, L.A., Fleming, J., Hasselberg, M., Laflamme, L., Lundin, J.: A smartphone app and cloud-based consultation system for burn injury emergency care. PLoS ONE **11**(2), e0147253 (2016)
62. Wen, C.K.F., Schneider, S., Stone, A.A., Spruijt-Metz, D.: Compliance with mobile ecological momentary assessment protocols in children and adolescents: a systematic review and meta-analysis. J. Med. Internet Res. **19**(4), e132 (2017)
63. Hussein, S.Y., Swanepoel, D.W., de Jager, L.B., Myburgh, H.C., Eikelboom, R.H., Hugo, J.: Smartphone hearing screening in mHealth assisted community-based primary care. J Telemed Telecare **22**(7), 405–412 (2016)
64. Zeng, E.Y., Heffner, J.L., Copeland, W.K., Mull, K.E., Bricker, J.B.: Get with the program: Adherence to a smartphone app for smoking cessation. Addict. Behav. **63**, 120124 (2016)
65. Zhao, J., Freeman, B., Li, M.: Can mobile phone apps influence peoples health behavior change? An evidence review. J. Med. Internet Res. **18**(11), e287 (2016)

Chapter 3
mHealth Market Exploitation Through the Analysis of the Related Intellectual Property Rights

Massimo Barbieri and Giuseppe Andreoni

Abstract mHealth is one of the emerging markets offering numerous opportunities both for the involved stakeholders and for doctors to improve the quality of life of patients. For this reason, a smart analysis of patents and innovations in mHealth together with the identification of the next future challenges is necessary for companies to enter the market and exploit their know-how to match consumer demand. This paper focuses on the analysis of the Intellectual Property Rights in the field of mHealth systems to draw a reference knowledge framework of the mHealth scenario. An up-to-date detailed categorization, the geographical distribution and the identification of top players in mHealth are presented.

3.1 Introduction

A common definition of mobile health is the practice of some medical services/interventions using mobile devices [1]. It combines two fundamental human needs: communication and health care. That is why this intergenerational technology is so relevant and rapidly spreading. For this reason, the WHO identified in mHealth a key technology and application: the use of mobile and wireless technologies to support the achievement of health objectives with the potential to transform the face of health service delivery across the globe [1]. The same concept and forecast are

M. Barbieri (✉)
Technology Transfer Office, Politecnico di Milano, P.zza L. Da Vinci 32, 20133 Milan, Italy
e-mail: massimo.barbieri@polimi.it

G. Andreoni
Dip. di Design, Politecnico di Milano, via G. Durando 38/A, 20158 Milan, Italy
e-mail: giuseppe.andreoni@polimi.it

G. Andreoni
Consiglio Nazionale delle Ricerche (CNR), Istituto di Bioimmagini e Fisiologia Molecolare (IBFM), via F.lli Cervi 93, 20090 Segrate, Milan, Italy

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_3

present among the European countries and in its Green Paper on mHealth, the European Union recognises that mHealth is an emerging and rapidly developing field that has the potential to play a part in the transformation of health care and increase its quality and efficiency [2].

This great potential has an enormous industrial and economic value so that a dedicated analysis about prior art in technology, systems and services and related Intellectual Property Rights is crucial to better understand the state of the art and future trends. This is one of the focuses of this chapter. In fact, innovations in the field of mHealth devices are rapidly multiplying and patents could offer an indicator of these innovative activities and their economic impact. The purpose of this analysis is to evaluate the progress of the technology of mHealth devices and to analyse the patent data in a more detailed way. For this reason, this paper focuses on the analysis of the Intellectual Property Rights (IPR) in the field of mHealth systems to draw a reference knowledge framework of the mHealth market scenario.

The mHealth market volume is rapidly growing. According to a recent study by Grand View Research, Inc., researchers predict the global mHealth market will reach USD 49 billion by 2020, growing at a rate of more than 47 percent between 2013 and 2020 [3]. The same trend was recorded by other sources as shown in Fig. 3.1 [4]. Again, according to another market analysis agency, the global mHealth market is projected to reach USD 62.84 billion by 2021, growing at a CAGR of 39.35% over the forecast period of 2016 to 2021 [5]. The global mHealth solutions market is expected to witness exponential growth in the coming years. This market is poised to reach USD 59.15 billion by 2020, growing at a CAGR of 33.4% during the forecast period. [6] Although slightly different, all these data are coherent in the estimate of market growth.

Growth in this market is mainly attributed to the increasing penetration of smartphones, tablets and other mobile platforms, increasing utilisation of connected medical devices and mHealth apps in the management of chronic diseases to reduce the rising health care cost; the growth of 3G and 4G networks to provide uninterrupted healthcare services, and rising focus on patient-centric healthcare delivery [3]. Regarding this last point, aging population and growing incidences of diseases linked to changing lifestyles have intensified the need for affordable and accessible health care. In fact, the rising incidences of chronic diseases such as cancer, heart ailments and diabetes are anticipated to drive market demand. With the introduction of new generation connected medical devices, healthcare providers are able to offer medical services at a reduced cost. This is crucial for the majority of the world nations that are facing major challenges when it comes to providing adequate healthcare services. Worldwide, each country is facing its own set of challenges in providing effective health care to its population. Various issues such as increased healthcare expenditure, rising incidences of chronic diseases and the expenses associated with treatment are still a major cause of concern to global populations. Because of increasing healthcare costs, the affordability and availability of healthcare services pose a challenge to the industry, governments and organisations are desperate to adopt measures which reduce healthcare expenditure.

In fact, according to different market reports, the global mobile health (mHealth) market can be segmented into:

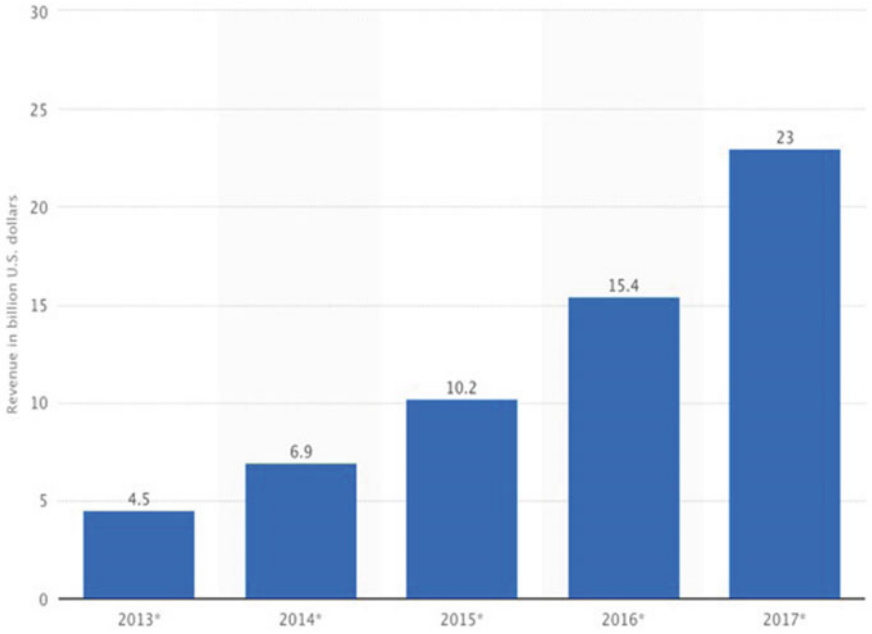

Fig. 3.1 Worldwide mobile health revenue from 2013 to 2017

(a) Monitoring device type,
(b) Apps and related services,
(c) Technology (3G/4G/5G, Wi-Fi, Zigbee, Ethernet, Z-Wave and others),
(d) end users (healthcare providers such as hospitals and clinics, but also home health care, content players, device vendors, mobile operators and others) and
(e) Geography (North America, Europe, Asia-Pacific, Middle East and Africa and Latin America).

Another but similar segmentation is presented in Table 3.1.

We are taking into account the first classification for a short survey and to drive the IPR analysis proposed here.

mHealth products are usually portable devices (connected or integrated into mobile systems such as smartphones or tablets), which use software applications (or apps) for health monitoring purposes, prevention and detection of diseases as well as basic diagnosis [5]. Considering the equipment only, mHealth devices cover various technological solutions that, amongst others, measure the basic vital signs. The connected medical devices segment comprises blood glucose meters, ECG monitors, blood pressure monitors, pulse oximeters, peak flow meters, neurological monitoring devices, sleep apnoea monitors, multiparameter trackers and others. Blood pressure monitors accounted for the largest share of the global connected medical devices market in 2014. New generation mobile/smartphones are equipped with embedded and advanced sensors such as accelerometers, gyroscopes, GPS, microphones (that

Table 3.1 mHealth market segmentation according to [7]

Category Rank	Equipement	Service	Stakeholder	Therapy	Geography
1	Blood Glucose Meters	Wellnes	Mobile Operators	Cardiovascular	North America
2	Blood Pressure Monitor	Prevention	Device Vendors	Diabetes	Europe
3	Pilse-Oximeter	Treatment	Healthcare providers	Respiratory	Asia Pacific
4	Neurological Monitoring	Diagnosis	Application Players	Neurology	Rest of the world
5	Cardiac Monitors	Monitoring		Others	
6	Apnea & Sleep Monitor	Healthcare System Strengthening Solution			
7	Wearable fitness sensor device and Heartrate meters				
8	Others				

can be used as stethoscopes to detect heart rate) and cameras. Today, mobile phones are also useful in advanced biosensing applications. Techniques like ultrasound, fluorescence imaging and even a combination of imaging cytometry and fluorescent microscopy were developed using a smart phone. For example, mobile smart phones may be coupled to a portable Enzyme-Linked Immunosorbent Assay (ELISA) for the detection of different proteins or can be used for detecting glucose or food allergens or for measuring pH. Mobile phone cameras can detect harmful elements in a sample (for example, the bacterium Escherichia coli on spoiled meat). Mobile phones can also be coupled to paper-based biosensors, which can perform luminescence assays. Another interesting biosensing application of smart phones is microscopy applied for microbial detection, DNA imaging and blood cell characterisation. It is possible to perform spirometry with a phone microphone, to detect chemical gases or to monitor skin wounds [8–10].

mHealth applications, or simply apps, are software programs. The most common categories of related services are applications aimed at disease management (chronic care management apps) and those for general health and fitness (designed to increase monitoring of user lifestyles, e.g. promoting physical activity and/or facilitating behavioural change) [8–12]. Both of them implement remote monitoring of different biomedical parameters (mainly in relation to prior mentioned devices or

with the sensors embedded in the smart phone, e.g. for activity tracking). Diagnostic services, in particular, enable healthcare professionals to connect with patients and offer diagnosis of ailments or health-related issues. Other services are dedicated to consultation, prevention (and we can identify a specific category dedicated to women's health) and motivation tools such as medication reminders or tools offering clinical and wellness recommendations. Finally, we have the availability of some administrative services (appointments, personal health record consultation, etc.). The main market segment is covered by apps relating to general health care or fitness monitoring functions with a share of about 35% in 2014. In this category, we can include fitness and nutrition apps, health tracking tools and weight loss apps. Another important market segment including different mHealth apps is the one regarding solutions for the management of chronic pathologies. In this framework, data-gathering management apps include those for mental health and behavioural disorders, diabetes, blood pressure and ECG, and cancer. As a result of the rise of the silver economy, the market for monitoring-type apps is expected to become the fastest growing in the coming years. An important role is also played by the remote monitoring services segment, which in 2014 was leading the mHealth market with a share of 63.7%. As a final point, it is worth considering the recent push for prevention via a healthy lifestyle, i.e. having an active life and eating a balanced diet have been identified as healthy lifestyle by WHO and all healthcare stakeholders as key strategies for future wellness. This general wellness campaign has been reflected in the increasing availability of fitness, diet, nutrition and health services. In recent months, this increased awareness of the benefits of maintaining a healthy lifestyle which has meant that this has now become the fastest growing mHealth market segment.

There is a huge market potential to be exploited through this widespread category of software applications that are now to be considered as medical devices according to the specific and corresponding regulations [14, 15]. This heralds a new era in the development and management of medical apps, for example, the growing need for a secure infrastructure for data safety and security, and interoperability and standardisation have to be assured and certified. The regulatory process could be a significant restraint on mobile health market growth [3], but fulfils a need for reliability, quality and user safety. The IMS institute for healthcare informatics recently reported that nowadays the number of available mHealth apps has increased to more than 165,000 [11]. Since 2010 users and patients have downloaded more than 200 million apps [12].

Concerning the technology, the enabling factors for the mHealth revolution are computational power and connectivity. The computing capacity of smart phones/tablet PCs is becoming more and more advanced in parallel with the quality of their components. mHealth solutions are also rapidly growing and evolving thanks to cloud computing and network protocol systems (3G, 4G and 5G), and are now available in every area of health care such as physical activity, anti-obesity, diabetes and asthma self-management [6]. Improving the software platforms (iOS or Android), the battery life of smart phones and the Graphical User Interfaces (GUI) are the current critical challenges for the industry.

Concerning the stakeholders, it is worth noting that according to all reports mobile operators make up nearly 50 percent of the overall market in 2012, with most revenue coming from monitoring services like independent aging solutions. Mobile operators offer solutions that include health call centres, content-based wellness information and mobile telemedicine with tools for transmitting captured information over mobile networks.

In relation to geography, North America represented the largest regional market in 2014, followed by Europe, Asia-Pacific, Latin America, the Middle East and Africa. Asian countries (particularly, China and India) and Latin American countries (particularly, Brazil) are expected to offer significant growth opportunities for market players in the forecast period.

Researchers and professionals identify enormous opportunities in mHealth and recent literature focuses on technological innovation and medical outcomes in using this approach in clinical practice. Existing review articles generally utilise engineering or medical literature and categories, but none investigates mHealth by the related IPR. For this reason, we carried out this analysis. For the IPR analysis, we were mainly interested in devices, apps and integrated systems. Patent prior art searches are extremely important because a large percentage of the information contained in patents are not published in scientific journals or in conference proceedings. So, patent state-of-the-art (or informative) searches can help to pinpoint technological trends.

3.2 Materials and Methods

Different methods can be used to retrieve patent information from specific databases; the two basic solutions are a search by keywords or a search by classification symbols.

Searching by keywords attempts to identify the basic functions of a novel system, or the inventor/s or the applicant or the specific claims. The keywords used in a search are not always obvious or known, thus a good search strategy is not necessarily so straightforward. Furthermore, searching by keywords is not always effective because it is also affected and limited by the language used [17, 18]. Not all patent titles and abstracts are translated into English. Sometimes Chinese, Japanese and Korean patents are automatically translated but the quality of the translation is poor. The choice of keywords, which is subjective, and the use of neologisms in the patent descriptions also do not help when trying to carry out a thorough search. Patent applications are written in a very complicated legal and technical jargon in order to be defended in a court and not to be easily found in patent databases. Therefore, the drafting of an application may also affect a search. The objective of patent searches is to find documents that claim similar technical features and not a mere match of words. These drawbacks can be overcome using classification systems. The patent classification systems are language-independent tools that help to retrieve patent information. The most popular systems used worldwide are International Patent Classification (IPC) and Cooperative Patent Classification (CPC). The IPC is used

Table 3.2 List of results of the quick search

CPC Codes	Definition	No of inventions
G06F-019/3+	Medical Informatics	140
A61B-005/00 rec	Detecting, measuring or reording for diagnostic purposes	172
G06Q-050/22	Health care	142

by more than 100 national and regional patent offices (World Intellectual Property Organization (WIPO), European Patent Organization (EPO), Eurasian Patent Organization (EAPO), African Regional Intellectual Property Organization (ARIPO) and Organization Africaine de la Proprit Intellectuelle (OAPI)). It is a hierarchical classification system revised annually and consisting of eight sections which are divided into around 70,000 subdivisions called classes, subclasses and groups. CPC is based on IPC and ECLA (the former European classification system). It is more frequently updated than IPC and has more detailed subdivisions (around 250,000), useful for faster moving technology field classification [19].

From all the above, the optimal solution for patent search is to use a combination of both methods.

Semantic search and citation analysis are further options but not useful for the scope of this work. Moreover, semantic search is a technology still under development and the results obtained so far are not so precise.

Another important issue is the choice of the patent database. Usually, free of charge databases (such as Espacenet, Patentscope or Depatisnet) are limited both in coverage and in full text search capability. Moreover, they rarely offer a tool for the statistical analysis of the results. Professional patent tools can overcome these drawbacks, even if they do not contain a complete history of documentation.

All patent searches included in the following section were performed using keywords and classification symbols across several databases, but especially using Orbit [20], which is a fee-based patent database with good data coverage, provided by Questel.

3.3 Results

A search with the keywords (mHealth or mobile health) in the "title/abstract/claims/concepts/object of invention" search fields showed 936 results (Orbit database accessed May, 31st 2017). We performed a statistical analysis to retrieve the main IPC/CPC codes, as reported in Table 3.2. Patent applications relating to medical information are generally classified within the generic subgroup G06F 19/00 of IPC [21], but other subgroups are also relevant, such as A61B5 and G06Q50.

Table 3.3 List of queries used to search for mHealth inventions

No	No of results	Query
1	7564	(M_HEALTH OR (MOBILE 1W HEALTH) OR SMARTPHONE? OR, PERSONAL_DIGITAL_ASSISTANT OR PHABLET? OR (TABLET 1W PC) OR, PDA)/TI/AB/IW/CLMS/OBJ/ADB/ICLM/KEYW AND (G06F-019/3+ OR G06Q-050/22 OR, A61B-005+)/IPC/CPC
2	7651	(M_HEALTH OR (MOBILE 1W HEALTH) OR SMARTPHONE? OR PERSONAL_DIGITAL_ASSISTANT OR PHABLET? OR (TABLET 1W PC) OR PDA)/TI/AB/IW/CLMS/OBJ/ADB/ICLM/KEYW AND (G06F-019/3+ OR G06Q-050/22 OR A61B-005+ OR G06Q-050/24)/IPC/CPC
3	7655	(M_HEALTH OR (MOBILE 1W HEALTH) OR SMARTPHONE? OR PERSONAL_DIGITAL_ASSISTANT OR PHABLET? OR (TABLET 1W PC) OR PDA OR (MOBILE 1W HEALTHCARE))/TI/AB/IW/CLMS/OBJ/ADB/ICLM/KEYW AND (G06F-019/3+ OR G06Q-050/22 OR A61B-005+ OR G06Q-050/24)/IPC/CPC
4	12,377	(M_HEALTH OR (MOBILE 1W HEALTH) OR SMARTPHONE? OR PERSONAL_DIGITAL_ASSISTANT OR PHABLET? OR (TABLET 1W PC) OR PDA OR (MOBILE 1W HEALTHCARE) OR WRISTBAND?)/TI/AB/IW/CLMS/OBJ/ADB/ICLM/KEYW AND (G06F-019/3+ OR G06Q-050/22 OR A61B-005+ OR G06Q-050/24)/IPC/CPC
5	12,498	(M_HEALTH OR (MOBILE 1W HEALTH) OR SMARTPHONE? OR, PERSONAL_DIGITAL_ASSISTANT OR PHABLET? OR (TABLET 1W PC) OR PDA OR (MOBILE 1W,HEALTHCARE) OR WRISTBAND? OR SMARTWATCH?)/TI/AB/IW/CLMS/OBJ/ADB/ICLM/KEYW, AND (G06F-019/3+ OR G06Q-050/22 OR A61B-005+ OR G06Q-050/24)/IPC/CPC
6	9121	SS 5 AND STATE/ACT = ALIVE
7	1333	SS 6 AND EAPD >= 2016

We expanded the terms used in the first explorative search to ensure a better coverage of relevant patent documents in mHealth applications. These results (see Table 3.3) showed that keyword choice was critical for a complete information retrieval. Another CPC code (G06Q50/24, referred to "Patient record management") was added and this returned 87 extra patent documents.

The addition of terms such as "wristband" and "smartwatch" dramatically increased the number of results.

All keywords were searched for in the following text fields: title, abstract, claims, independent claims, description, object of invention, concepts and advantages over prior art drawbacks.

The statistical analysis was carried out on the results of query n°5.

The distribution of search results by publication years is shown in Fig. 3.2.

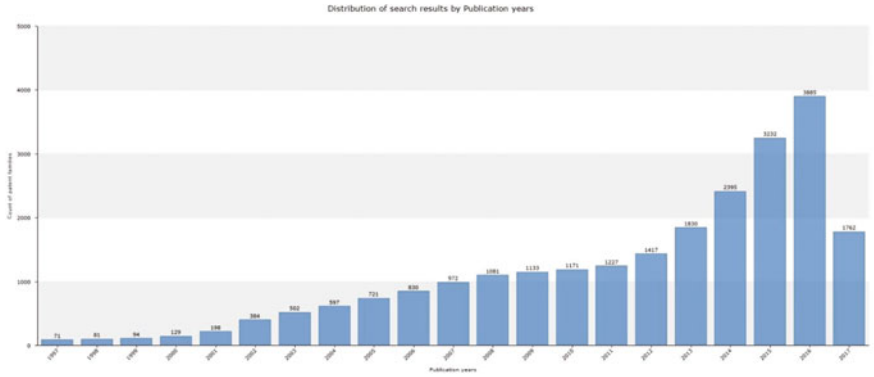

Fig. 3.2 The evolution of patent numbers in the last 20 years by Publication year

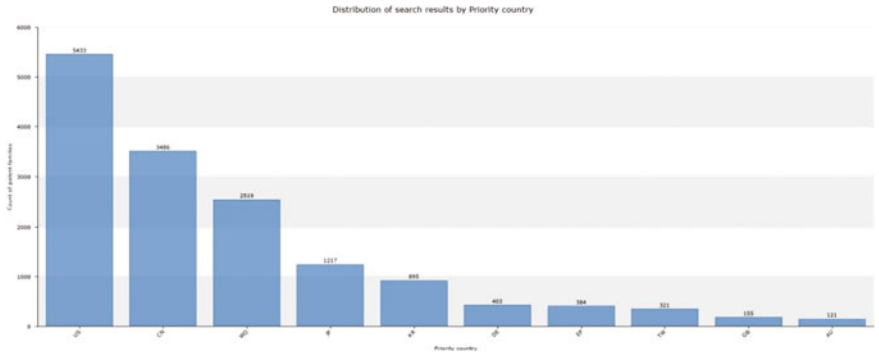

Fig. 3.3 The distribution of search results by Priority Country

Since patent applications are published 18 months after the filing date, it could be said that the number of patent applications grew rapidly from 2011, reaching its peak in 2015. The distribution of search results by Priority country reveals that most inventions are generated in the United States of America (Fig. 3.3). The main patent applicants are reported in Fig. 3.4.

Some recent market reports [3, 5, 7] have identified the following major players in the mHealth solutions market: Medtronic, Inc. (U.S.), Apple, Inc. (U.S.), Sanofi (France), Mobisante, Inc. (U.S.), AirStrip Technologies, Inc. (U.S.), AliveCor, Inc. (U.S.), LifeWatch AG (Switzerland), Nike Inc. (U.S.), Koninklijke Philips N.V. (Netherlands), Johnson & Johnson (U.S.), Jawbone (U.S.), Omron Corporation (Japan), Withings (France), BioTelemetry Inc. (U.S.), Athenahealth, Inc. (U.S.), Aga-Matrix, Inc. (U.S.), iHealth Lab, Inc. (U.S.), AT&T (U.S.), Qualcomm (U.S.), Cerner Corporation (U.S.), Diversinet (Canada), Cisco, Inc. (U.S.), Samsung Elec- tronics Co. Ltd. (KR), Vodafone (U.K.), Cardionet, Inc. (U.S.), Qualcomm Life (U.S.), Allscripts Healthcare Solutions (U.S.) and mQure (IN). In contrast, the results of the IPR patent applicant search showed a different ranking with three main outstanding

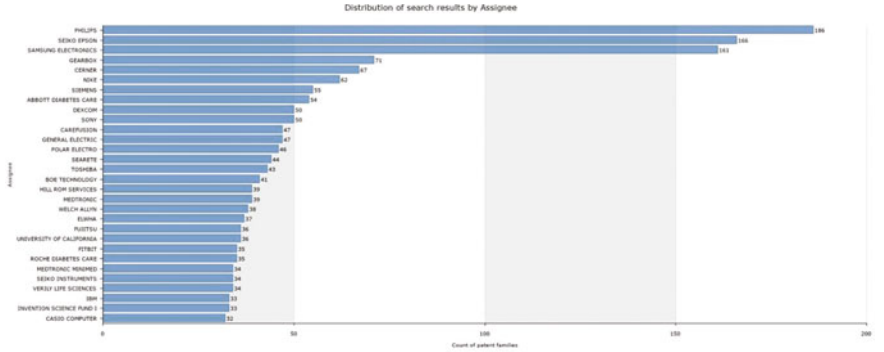

Fig. 3.4 The distribution of search results by Assignee

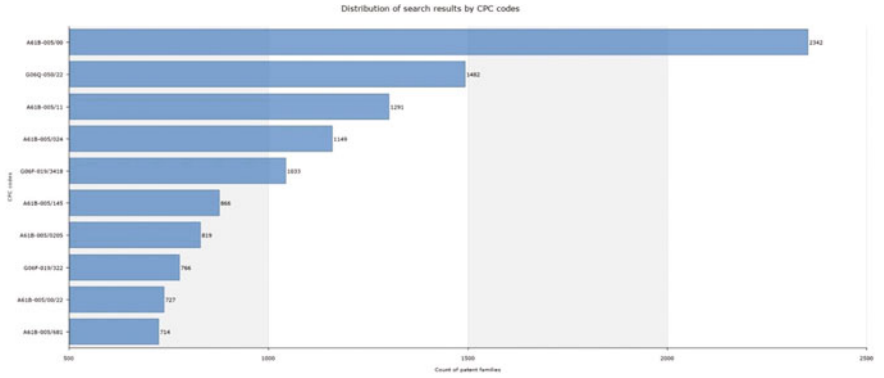

Fig. 3.5 The distribution of search results by CPC codes

players, Philips, Seiko Epson and Samsung, having a similar number of applications, more than the double that of the next ranking companies (Fig. 3.4).

The distribution of search results by main CPC codes is reported in Fig. 3.5. The definition of each CPC classification code is reported in Table 3.4.

The legal status is reported in Fig. 3.6: the percentages of granted and pending patent applications are almost the same.

In order to establish a technological trend, the results of query n°5 were filtered based on the legal status of the application (pending or granted patent—query no. 6) and the date of the first application year (after 2015 query no. 7): this returned 1333 results.

Table 3.4 Definition of the main CPC codes of mHealth inventions

CPC Codes	Definition
A61B5/00	Detecting, measuring or recording for diagnostic purposes
G06Q50/22	Systems or methods specially adapted for a specific business sector Health care
A61B5/11	Measuring movement of the entire body or parts thereof
A61B5/024	Detecting, measuring or recording pulse rate or heart rate
G06F19/3418	Telemedicine
A61B5/145	Measuring characteristics of blood in vivo
A61B5/0205	Simultaneously evaluating both cardiovascular conditions and different types of body conditions
G06F19/322	Management of patient personal data
A61B5/0022	Monitoring, a patient using a global network
A61B5/681	Wristwatch-type devices

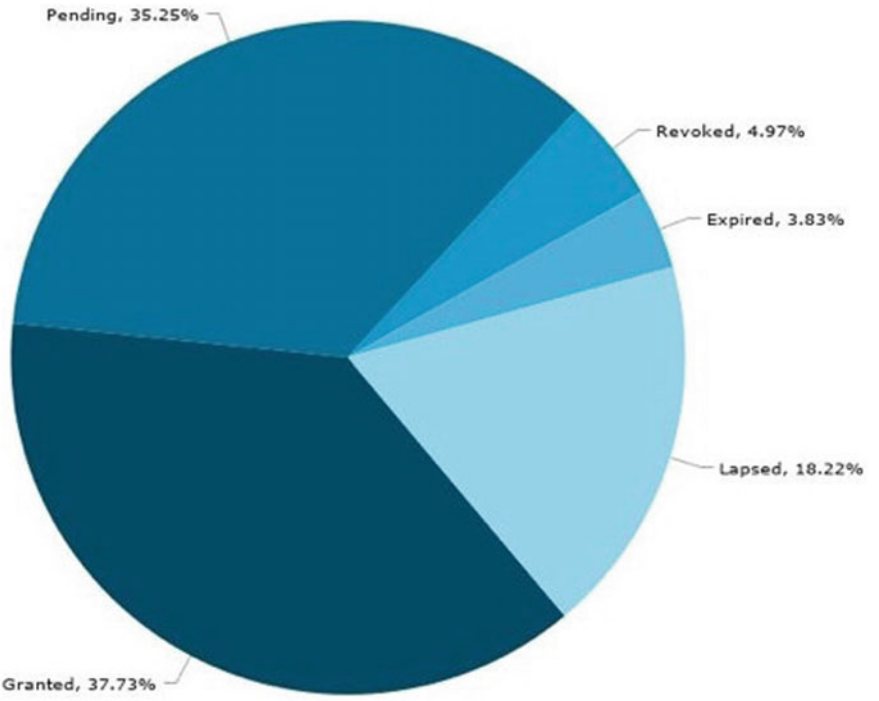

Fig. 3.6 The distribution of search results by Legal Status

Table 3.5 No of inventions versus physiological parameter monitored

No of inventions	Physiological parameter
203	Glucose level
481	Heart rate
320	Blood pressure
124	Oxygen saturation

3.4 Selected and Recent mHealth Patent Applications

Starting from the results of query no. 7, a keyword search was carried out in order to estimate what kind of physiological parameter is monitored by the wearable device described in the patent application claims.

The results are listed in Table 3.5.

Many wearable devices calculate a certain number of physiological parameters by means of biometric sensors, such as energy expenditure (e.g. calories burned, floors climbed and/or descended), heart rate, heartbeat waveform, heart rate variability, blood pressure, skin and/or body temperature. They may also provide motion sensors (an accelerometer, a gyroscope, an altimeter) and environmental sensors to measure parameters such as barometric pressure, weather conditions (temperature, humidity, air quality, wind speed), light, noise and radiation exposure.

Some devices evaluate the users stress or relaxation levels using a combination of heart rate variability, skin conduction, noise pollution and sleep quality. To detect heart rate variability, an optical sensor [such as a photoplethysmography (PPG) sensor] can be used (see US patent application nº 2016/0166197 A1 "Method and apparatus for providing biofeedback during meditation device", filed by Fitbit).

PPG signals are used to measure biological information on cardiac functions, including blood oxygen saturation levels (SpO2). In a recent patent application (US 2017/0020420 A1), filed by Huinno (http://www.huinno.com), one of the claims is for a new technique which accurately measures PPG signals external light sources create varying levels of brightness.

The North Carolina State University has patented a hydration monitoring device (see US 2016/338639 A1), which includes at least one flexible electrode comprising a plurality of silver nanowires embedded within a polydimethylsiloxane (PDMS) substrate.

Another interesting invention relates to the monitoring of a persons food consumption (US 2016/317060 A1, filed by Medibotics). The device is a finger ring with an electromagnetic energy sensor that measures changes in the electromagnetic impedance, resistance, conductivity or permittivity of finger tissue.

LifeQ Global (http://www.lifeq.com) has patented a system and a method for performing SpO2 measurements using reflective PPG technology (see WO 2016/178986 A1).

Last but not least, Stanford patent application no. WO 2017/058806 A1 relates to a wearable sensing platform which analyses bodily fluids such as sweat and/or urine, and a users temperature.

These are just some examples of selected new inventions used within mHealth products found in the patent literature. Every day, new patent applications are filed in this fast moving technical field that must be constantly monitored in order to have a complete overview.

3.5 Discussion

Data looking at the publication year indicates the presence of different mHealth epochs, until 2001 there were few experiences and innovations probably due to the immaturity of technologies related to this field; later, with the diffusion of communication technologies, from 2002 to 2008 specifically, an increasing number of applications/inventions appeared. Another stable period continued until 2011. Since 2012 with the introduction and rapid global rise of the smart phone and related apps, a new intensive development era has been entered.

In the top patent applicant data, seen in Fig. 3.3, multinational biomedical companies rank first, but it is interesting to note the presence of big software developers and also one university in the first 15 ranks.

Concerning the methodology, a big difference is noticeable in the results coming from other research engines or sources and using the search phrase mhealth or mobile health, the Scopus database provided 1117 patent results, while Espacenet (accessed 5 June 2017) only returned 824 if analysing the full text (74 if only the title or 138 including title and summary). This suggests that general data can be obtained by these sources, but the detail level provided by a specific database, such as Orbit, is more useful for analytical purposes.

The technical fields where innovation is more prevalent include the following:

1. Telemedicine,
2. Management of patient personal data (e.g. patient records),
3. Local monitoring of medical devices (e.g. graphical user interfaces),
4. Computer-assisted prescriptions (e.g. prescription filling or compliance checking),
5. Medical expert systems (e.g. medical decision support systems).

3.6 Conclusion

This IPR analysis demonstrates that mHealth is currently experiencing an enthusiastic period of expansion. Mobile health is expected to manage health care at various levels using minimal resources and avoiding unnecessary healthcare expenditures.

The global mobile health market is definitely on the rise and many organisations are on the verge of exploiting the immense potential of this market. The technology is mature and related inventions are starting to cover all the market opportunities. A saturation and more discerning process of IPR are expected in the near future. Today, the market is driven by major factors such as those given below:

- Need to reduce healthcare expenditure,
- Rising incidence of chronic diseases,
- Increase in aging population,
- Widespread mobile smart phone penetration globally,
- Prospect of personal healthcare management,
- Technological advances in the form of 5G networks,
- Need for cost-efficient healthcare delivery,
- Increased awareness levels among the population about the need for proper healthcare management.

These several factors are catalysing the development of the different mHealth app segments exponentially.

Despite this, we cannot forget the restraints acting in this field. First of all, there is a lack of a specific stringent regulatory framework. Many of these apps deal with the measurement and management of vital signs and, therefore, should follow the rules for medical devices, which are certified as medical devices or software. Another crucial issue concerns data privacy and safety. According to the responses of European Commission public consultation, privacy and security, patient safety, a clear legal framework and better evidence of cost-effectiveness will all be required to help mobile health care (mHealth) flourish in Europe [2]. This also means the mHealth operators and service providers should have the capability to create a proper ICT infrastructure (e.g. cloud services with proper privacy and security levels). Furthermore, it should be understood that these apps are generally adopted and used not by skilled personnel but by lay users; therefore, improved intuitiveness, usability and error compensation should be included in their code.

These factors represent challenges for the near future in order to fully exploit the immense potential of the mobile health market for health care.

References

1. World Health Organisation.: mHealth New horizons for Health Through Mobile Technologies, Global Observatory for eHealth Series, vol. 3 (2011)
2. EU Commission.: GREEN PAPER on mobile Health (“mHealth”) (2014)
3. http://www.marketsandmarkets.com/PressReleases/mhealth-apps-and-solutions.asp
4. https://www.statista.com/statistics/218843/forecast-of-the-worldwide-mobile-health-revenue-since-2013/
5. https://www.mordorintelligence.com/industry-reports/global-mobile-health-market-segmented-by-monitoring-and-diagnostic-medical-device-and-services-cardiac-monitors-diabetes-management-devices-multi-parameter-trackers-diagnostic-devices-mobile-h-industry

6. http://www.marketsandmarkets.com/Market-Reports/mhealth-apps-and-solutions-market-1232.html
7. https://www.alliedmarketresearch.com/mobile-health-market
8. Gagneja, A.P.S., Gagneja, K.K.: Mobile Health (mHealth) technologies. In: IEEE 17th International Conference on e health networking, Applications and Services (Healthcom), pp. 37 43 (2015)
9. Quesada-Gonzlez D., Merkoi A.: Mobile phone-based biosensing: an emerging diagnostic and communication technology. Biosens. Bioelectron. **92**, 549 562 (2017)
10. Baig, M.M., GholamHosseini, H., Connolly, M.J.: Mobile healthcare applications: system design review, critical issues and challenges. Australas. Phys. Eng. Sci. Med. **38**, 23–38 (2015)
11. http://www.imshealth.com/en/about-us/news/ims-health-study:-patient-options-expand-as-mobile-healthcare-apps-address-wellness-and-chronic-disease-treatment-needs
12. Silva, B.M.C., Rodrigues, J.J.P.C., de la Torre Dez, I., Lpez-Coronado, M., Saleem, K.: Mobile-health: a review of current state in 2015. J. Biomed. Inform. **56**, 265–272 (2015)
13. Helbostad, J.L., et al.: Mobile health applications to promote active and healthy ageing. Sensors **17**, 622 (2017)
14. IEC 60601-1 Ed.3.1 (2013)
15. EU Commission, DG Health and Consumer.: MEDICAL DEVICES: Guidance document—-Classification of medical devices, Guidelines relating to the application of the Council Directive 93/42/EEC on Medical Devices, MEDDEV 2. 4/1 Rev. 9 (2010)
16. Miah, S.J., Gammack, J., Hasan, H.: Extending the framework for mobile health information systems research: a content analysis. Inform. Syst. https://doi.org/10.1016/j.is.2017.04.001 (2017)
17. White, M.: Patent Searching: Back to the Future How to Use Patent Classification Search Tools to Create Better Searches. In: First Annual Conference of the Canadian Engineering Education Association, Kingston, Ontario (2010)
18. White, M.: Patent Classification Reform: Implications for Teaching, Learning and Using the Patent Literature. In: American Society for Engineering Education Annual Conference, San Antonio, Texas (2012)
19. List, J.: Editorial: On Patent Classification World Patent Information, vol. 41, pp 1–3 (2015)
20. Questel Orbit Patent Search Database, http://www.orbit.com. Last accessed 26 June 2016
21. Closa, D., Gardiner, A., Giemsa, F. Machek, J.: Patent Law Computer Scientists. http://www.springer.com/us/book/9783642050770. (Springer 2010)

Chapter 4
Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution

Enrico Frumento

Abstract Healthcare is among the fields that adopted ICT very early to improve physicians' work. The digital transformation in healthcare started already some years ago, with the computerization of hospitals. Todays' healthcare is at the forefront again, as one of the most attacked and profitable areas of exploitation for cybercriminals and cyberterrorists. The overabundance of valuable information, its nature of critical infrastructure and its mobile services, are at the centre of cybercriminals attentions. Besides, patients and physicians, both went through a massive digital transformation; nowadays, healthcare operators and users are highly digitalized and mobile. This evolution influences how, respectively, healthcare operators and patients offer and consume services. The present chapter starts from a presentation of how the modern workforces changed their working paradigms and then introduces the concepts of Hospital 2.0 and patient ecosystem. The chapter also explores the cyberterrorism and cybercrime, present and future threats landscapes, including the mobile health example.

4.1 Introduction

Today the flexibility to work at any time from different locations led to a blending between private and professional lives. A blending facilitated by the diffusion of ubiquitous technologies that allows to merge seamlessly physical and virtual encounters. The recent global recession directly increased the dynamicity of the labour market fostering the adoption of more flexibility and more mobility. A user could complete a task in any possible place, thanks to mobile and highly mobile terminals. Home, public spaces or company offices are all equivalent. From a technological point of view, this trend promotes the evolution of the so-called digital ecosystems. People interact from heterogeneous places at any time, on different terminals, to exchange information and evolve in terms of knowledge, skills and contacts and, ultimately to improve

E. Frumento (✉)
Cefriel Scarl, Politecnico di Milano, Viale Sarca, 226, 20126 Milan, Italy
e-mail: enrico.frumento@cefriel.com

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_4

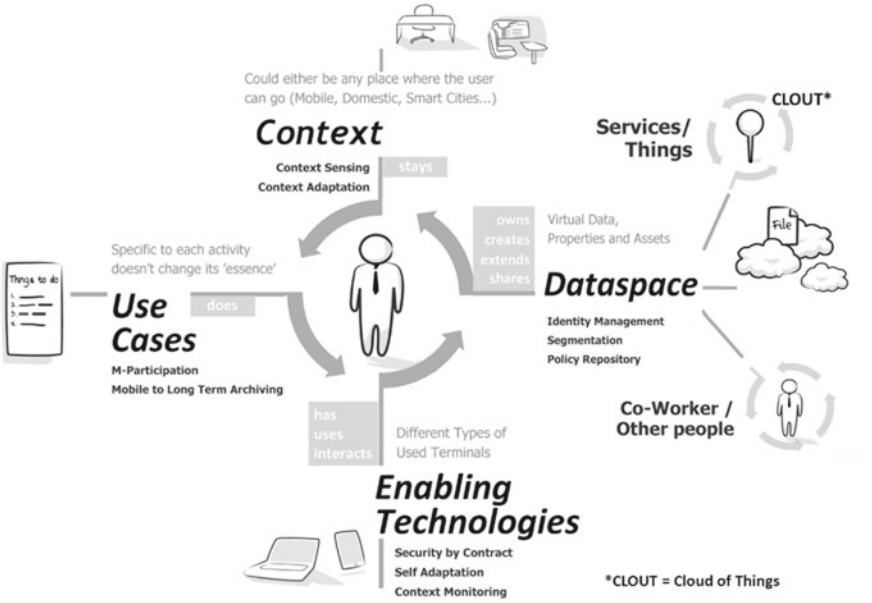

Fig. 4.1 Schematization of modern mobile workforces (*source* Cefriel)

their lives and meet their needs. The evolution of workforces (i.e. the evolution of how people are accustomed to work) arises mainly from the wide adoption of mobile technologies. In general terms, the digital devices and the digital transformation of many services have strongly influenced the way people work and collaborate.

Figure 4.1 reports a conceptual representation of the most important trends in modern workforces. It represents a user-centric schema of the modern way of working. The figure reports a central handler (i.e. a worker) surrounded by four base directions, which are affecting his/her working habits: Dataspace, Enabling Technologies and Use-Cases and Context. The following list reports a brief explanation of each element.

DataSpace. In general, it is important to define the role of the 'handler'. A handler is a person or a system, that operates and/or owns (i.e. has rights to access and edit the information) a **Personal Information Space**[1] (PIS) that stores some or all of her data. The handlers' typical activities are to extend, elaborate and create new elements in the PIS, eventually with the collaboration of other co-handlers (e.g. people in the case of collaborative working or entities in the case of connected smart objects). The PIS could be either private or shared, in the second case it is usually 'segmented in different slices', according to the editing rights of the co-handlers. A possible definition of a personal information space, in this model, is, therefore: *a virtual space where a handler and the possible co-handlers stores, elaborate and accesses, shared or strictly personal data*. Therefore, in line with this terminology, at a high

[1] A. VV [1].

level of abstraction, everyday working activity is a process that continuously update PIS.

During the recent years, PISs increasingly migrated on cloud services eroding the prevalence of disjoint data islands. This migration led to two different trends: an increasing number of co-handlers and the constant growth and 'contamination' of the PIS with data belonging to the working domain.[2] Today's typical composition of a PIS is a usually inextricable mix of data, belonging to both work and private lives.

Enabling Technologies. A handler can use several Enabling Technologies to access PIS. The choice is based on the usability characteristics, mediated by the context of access (e.g. on an airplane or from a bench at the park). The choice of the right enabling technology is a matter of convenience and easiness in that moment and place. Where *easiness* means how 'easy' it is to perform a task, or a use-case, with an enabling technology, in a specific context (place) and moment, by the cognitive and physical points of view.[3] Nowadays, the offerings of new 'methods' to access a user's own dataspace is growing: smartwatches are just the newest one, but others are behind the corner, like for example the new wave of wearable or implantable electronic.[4,5,6]

Summing up so far the model includes a handler that accesses a PIM he controls with an enabling technology, selected among several, using criteria of easiness and personal preferences.

Use-Cases. With reference to Fig. 4.1, a Use-Case is the 'invariant' portion of the workflow that the technologies do not affect. A typical example are the knowledge-driven workflows, for example the writing of a commercial letter. Over the years, a user could have written a commercial letter in different ways: using a typewriting machine, a video terminal with a word processor and, more recently, a tablet. Market forecast anticipates the appearance of wearable smart glasses that understands the speech or even the brain waves.[7] What remains always the same is the knowledge and expertise required to write a commercial letter.

Context. The context refers to the physical environment where a handler executes a use-case, modifying PIS through an enabling technology. Thanks to evolution of mobile and ubiquitous terminals, a user could complete a task in any possible place, company offices, home or public spaces. Where he executes the work does not matter, only ergonomics do (as an example of different ergonomics, imagine completing a task using a laptop, in an office or a public transportation, such as a train). Therefore, sensing the context of a handler is of paramount importance to define the usability criteria and therefore the most appropriate enabling technologies.[8] An application of the context sensing is the definition of the logical security perimeter: it helps

[2]Gartner [2].

[3]For a definition of usability, see Nielsen [3].

[4]Canina and Bellavitis [4].

[5]Talk to my shirt blog [5].

[6]Crunchwear [6].

[7]Control Your Mobile Phone or Tablet Directly from Your Brain [7].

[8]Context-Aware Computing: Context-Awareness [8].

to understand which portion of the PIM a handler has the right to access, without incurring security problems in a specific place. As an example, consider a situation where a user (in general a handler, a term that includes also a smart object) wants to access a reserved document, from a crowded place, over a public data network. In this case, a security system decides to deny the request because, from a crowded place, someone else may spy over the user's shoulders while he types the password or reads the document.[9]

The model described so far eases the understanding of which are the potential impacts of cybercrime. From a high-level point of view, the essence of cybercrime is to abuse the so-called trust chains, to steal assets. Hacking always implies finding and abusing the trust or confidence chains among entities of the system. A trust chain is a trust relationship existing among two or more peers (either humans or ICT devices) that exchange assets, trusting that they will be handled correctly and that nothing intercepts and alter the transaction.

More precisely, according to Mayer, Davis,[10] a definition of trust is '*the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party*'. This definition applies to a relationship with another identifiable party (either human or IT system) who is perceived to act and react with volition towards the trustor. Being vulnerable implies that there is something of importance to be lost because of this relationship. The concepts of risk, trust and vulnerability are therefore tightly connected to one another. However, trust is not taking risk per se, but rather a willingness to take a risk. There is no risk taken in the willingness to trust. The risk is inherent in the behavioural manifestation of a willingness.

As an example consider the situation where a user is at risk of opening a potential phishing email: if the victim does not consider alternatives (every morning he/she opens the email without worrying too much) she is in a situation of confidence. Confidence, hence, is connected to the concept of risk-taking. The confidence of people in the systems is one of the most abused elements in attacks to the human layer because it relates to the risk-taking behaviour. In the example given, the user chooses to follow the instructions in the email or not, despite the possibility to be hacked, based on his level of trust or confidence. With the IT system, we can use a similar approach: two communicating peers have, by construction, a mutual or mono directional trust relationship.[11] The concept is further discussed in the Sect. 4.5 of this chapter.

The schema of Fig. 4.1 embeds several trust relationships, among the handler and co-handlers, handlers and the enabling technologies, handlers and context sensing

[9] For additional information, see the concept of data context-aware security [9].

[10] Mayer et al. [10].

[11] In this context, we do not differentiate trust and confidence. Trust differs from confidence because it requires a previous engagement on a person's part, recognizing and accepting that risk exists. This is exactly the type of distinction that exists in the cyberattacks because every user knows that the risk of being hacked exists, but often does not recognize it correctly because of his confidence.

system, handlers and cloud technologies, etc. The identification and the consequent abuse of the underlying trust relationships of Fig. 4.1, defines the cybercrime tactics.[12]

4.2 The Healthcare Scenario

As explained in the previous section, one of the most important activities by the security point of view is to define the asset data space and the handlers that can access it. This leads to a better understanding of the scenarios, the use-cases and the trust chains.

'It is currently a trend in Europe that the population is aging'.[13] In other words, the proportion of the elderly people in our countries is increasing, due to both, fewer children being born as well as a longer life expectancy. According to the report Redesigning Health in Europe for 2020,[14] the healthcare costs in Europe are nowadays increasing. These costs are in most European countries a growing component of GDP, in some cases still a growing part of public finances, representing between 4 and 12% of GDP in EU Member States. Besides this aspect, approximately about 40% of the population above the age of 15, i.e. over 100 million citizens, are reported to have a chronic disease. This proportion climbs to 66% of the population who has reached retirement age, having at least two chronic conditions. The EU Member States are facing a situation where more than 70% of healthcare costs are spent on chronic diseases and this figure is expected to rise in the coming years. For this reason, as Mckinsey reports, '*as the price of healthcare rises and safety lapses persist, developed countries are seeking ways to lower costs and improve quality. Many are finding the solution in digital innovation*'.

Today's healthcare infrastructure is considered inadequate to meet the needs of a population that is increasingly getting older. One of the main problems is the increasing costs of hospitality and care, on the one hand, and the expected quality of care on the other. One possible solution is to develop ageing in place in which elders live safely and independently in their homes, for as long as possible (i.e. avoiding the transition to a care facility). This approach promotes a happier style of life of elderlies and the social connections while reducing the strain on healthcare infrastructure. This is the reason behind the interest in tele-homecare, telemedicine and home monitoring devices. They are useful to address the health needs of the senior population, even in rural and frontier communities. The recent evolution of mobile technologies and wearable devices is a funding force that drives the evolution of mobile healthcare and answers to the request for flexible and mobile health services.

Healthcare service in the last few years benefitted from a long-term radical change of perspective. This change goes under the name of '***Patient Ecosystem***' and consists of the evolution of the hospital from a place of care to a network of services for

[12] D2.1 The role of Social Engineering in the evolution of attacks [11].

[13] World Health Organization [12].

[14] eHealth Task Force [13].

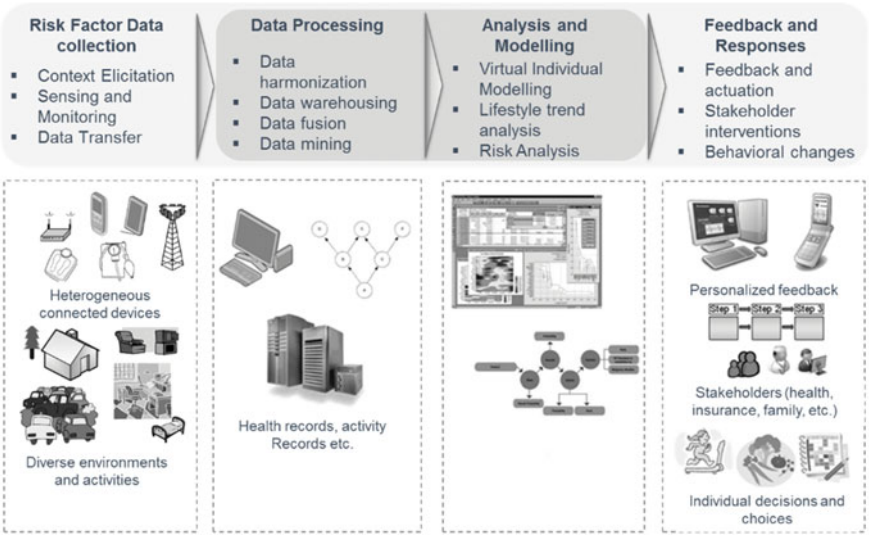

Fig. 4.2 Reference system for lifestyle management and diseases prevention (*source* PRECIOUS project)

patients, provided in home environments, smart cities, smart-things, through different technologies and channels.

Figure 4.2 reports the structure of a typical patient ecosystem (source PRECIOUS project[15]) and its four main elements:

1. Risk factor data collection refers to heterogeneous (e.g. using a range of methods that span from commercial wearable sensors, such as the smartwatches, to professional medical equipment, such as the insulin pumps) and ubiquitous sampling of biometric data (e.g. in the houses of the patients or outdoor, or in hospitals).
2. Data processing of the information collected.
3. Analysis and modelling of the data for the evaluation of lifestyle trends and the consequent evaluation of the risk posture of patients.
4. Feedback and responses, for example a possible application is the induction of behavioural changes in the patients (e.g. positive reinforcement or behavioural migration) either to promote wellness or health.

The motto '*Moving to the Humans is the new wave*' sums the discussed evolutive lines of health. This motto refers both to, (i) the many technological developments, that put the user at the centre of personal information space (e.g. through different enabling technologies such as wearable systems, natural interfaces, and emotional design for user-centred innovation), and, (ii) the novel access methods to the services.

These trends are increasing each year. As an example, the 'retaliation' of healthcare—based on the IoT—will fundamentally alter how life sciences and healthcare

[15] http://www.thepreciousproject.eu/.

organizations conduct business. As reported by Help net security[16]: '*Connected technology will take a more prominent role within the supply chain, as sensor-based track-and-trace technology will allow companies to verify product shipping information, monitor temperature issues and adjust routes based on environmental factors affecting drug viability, as well as utilizing cross-platform analytics based on tracking data to help improve route efficiencies and deliver critical medications to people who need them, when they need them*'.

In this scenario, the role of IT and IT security is predominant. The following definition, coming from ENISA's white paper on smart hospitals helps[17]: '*A smart hospital is a hospital that relies on optimized and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities*.' One consequence of this definition is that the mobile health becomes one aspect of a broader vision.

4.2.1 Hospital 2.0, Evolution of the Patient Ecosystem

Healthcare is migrating to an *Ecosystem* logic. The evolution of key technologies, such as the Body Sensor Networks, and their ubiquitous availability support the integration of several services[18] (see Fig. 4.3).

Until a few years ago, healthcare ecosystems were limited within the hospital walls or at least within the hospital subsidiaries. The latest evolutions instead, bypass the localization limits, in favour of a full network of outsourced services. However, the hospital will still preserve for a long time its traditional role of primary actor of this network, being the reference place where the clinical competence grows and the professionalism refers. Hospitals have evolved from a localized place of care to a *delocalised and extended network of care services*. This change of perspective has in effect created a '**Patient Ecosystem**', in which services are delivered to patients across a wide variety of locations, from hospitals to homes as well as 'on-the-go'. As importantly, services involve a *diversity* of HC professionals, channels and technologies. It has modified the relationship between patients and HC professionals, moving from a limited number of '*visits to the doctor*' to a *continuous* mode and a more permanent collaboration that has the potential to increase the quality, impact and effectiveness of HC on patients. While this evolution was introduced over the last decades, its adoption is growing thanks to the evolutions of mobile services,

[16]Connected technologies will accelerate security threats to healthcare industry [14].

[17]Cybersecurity and resilience for Smart Hospitals [15].

[18]It is important to distinguish between the *Services* and the *Ecosystems*. 'Ecosystem' means a network of integrated services that can interact with each other to offer the user a unique and seamless vision. Centering the vision of health services around the patient naturally leads to seamless servicing (the data are elaborated and accessed through different channels—e.g. mobile—without disruption or differences) and to a stronger control of personal data (which may be accessed through a unified ID).

the increased penetration rate of information technology to the complete HC supply chain actors. Similarly, it has increased the number and coverage of healthcare operators, extending from operating hospitals to remote care services facilities, nursing homes and tele-assistance.

Across these different profiles, very different perspectives govern the role and uptake of information technology.

For *healthcare operators*, information technology is deployed as a means to increase efficiency, required by the economic complexity of ensuring sustainable HC services towards a growing and increasingly ageing population.

For *healthcare professionals (doctors, nurses* etc.*)*, information technology is often *imposed to* them by the operators and/or public authorities, ranging from information exchange (electronic patient record, etc.) to monitoring (connected devices, etc.) and operational support (robotized interventions, etc.). HC professionals are not the drivers of change but are the main users and adopters of the technology that is provided to them—often without receiving a sufficient level of information to be fully aware of how best to use the technology.

Moving to the *patients*, this open up yet another group, or rather a variety of groups connected to the HC supply chains. Some of the patients are familiar with information

Fig. 4.3 Patient-centred healthcare is nowadays a service-based ecosystem (*source* Cefriel)

technology, and display a familiarity with, for instance, smart devices used in mobile wellness solutions.[19] Contrary to other domains in which a certain level of mistrust is pervasive, patients using health-oriented mobile devices tend to develop a high *inherent level* of trust—and consequently, they are often not aware of—or they simply overlook the *potential risks* of their use. For other patients, information technology is incomprehensible—and they will be unaware of the potential risks linked to health devices out of lack of understanding.

Healthcare is, therefore, a very rich and complex environment—it is a critical infrastructure through its central societal role, and it is populated by huge numbers of *human profiles*, varying widely as to their role, level of interest and awareness of the vulnerabilities introduced by the use of information technology. They will also vary widely in terms of feeling (un)concerned about their own role in relation to these vulnerabilities.

4.2.2 Personal Information Space

According to the model of Fig. 4.2 the prediction risk models of a clinical event use heterogeneous data. This includes medium-term (e.g. patient clinical history, exposure to environmental risk factors, occupational exposure and biological, therapeutic, environmental factors) and short-term information (e.g. biomedical signals, physical training and performance, lifestyle and diet, environmental data, social data, behavioural).

As a result, an increasing over time amount of information feeds the data processing algorithms. This trend is generic and goes beyond the healthcare sector. However, the sum of our personal data forms the **personal information space (PIS)** (also called personal big-data space). The different applications and services read and write the PIS (see Fig. 4.4 and Introduction) often with overlapping rights.

The regulation of this dataspace (e.g. the regulation of the following aspects: which data are stored, which are more sensible than others, who can access them, how to protect the PIS, when the data must be deleted and who control them) is one of the most problematic areas for the information security in Europe in general, and not only within the healthcare sector.[20]

4.3 Driving Forces

As reported by Frumento et al.[21] '*the main purpose of building scenarios is to explore different potential evolutions of a given field (including non-technological issues)*

[19] Healthcare Sector Report [16].

[20] Bowman [17].

[21] Frumento et al. [18].

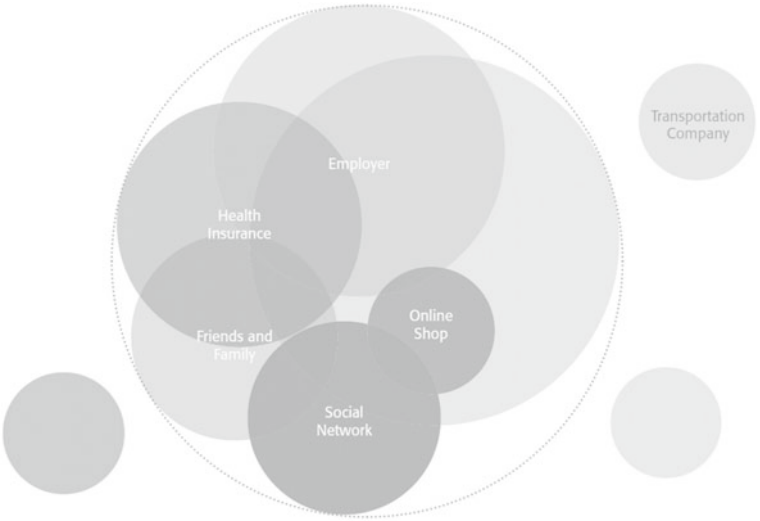

Fig. 4.4 An example of a personal information space or personal big-data space (*source* Talk-in-the-tower Taskforce#1 on the role of machines in our changing concepts of identity)

under the influence of some driving forces, to support proactive development and planning, and to cope with future challenges'. The term *scenario* indicates the whole set of technological, social, economic and political conditions that define the future context of an application area. Given the co-evolutive nature of cybercrime (CC) and cyberterrorism (CT), the definition of a scenario helps to identify and define the future threats and defences. A *driving force* is the critical leading factor that is expected to influence the future developments of an application area.

Table 4.1 reports a summary of the main evolutive driving forces of healthcare. These are also the driving forces of CC and CT in healthcare, as further described in the following sections because they set the context where the CC/CT's business plans try to exploit the system.

From Table 4.1 the connection of these forces emerges quite naturally, Fig. 4.5 reports a possible correlation between these concepts in a cause-effect diagram.

Overall, there is one crucial aspect that may sound obvious, when discussing the IT Security: healthcare is a particular type of mission-critical industry, where the patients' safety and health is at the centre. Consequently, a proper approach to healthcare security should reconsider the threat landscape and the corresponding risks. For example, consider two common types of attacks: data breach and Distributed Denial-of-Service (DDoS) attack, on hospital servers. What distinguishes a data breach from a DDoS is that it does not damage any life (except in individual cases), while instead, a DDoS is a life-threatening threat.[22] A correct approach to

[22]The type of Deny-of-Service that are life-threatening is not only those that touch the diagnostic systems but also in general, those that slow down operators: for example, not having access to

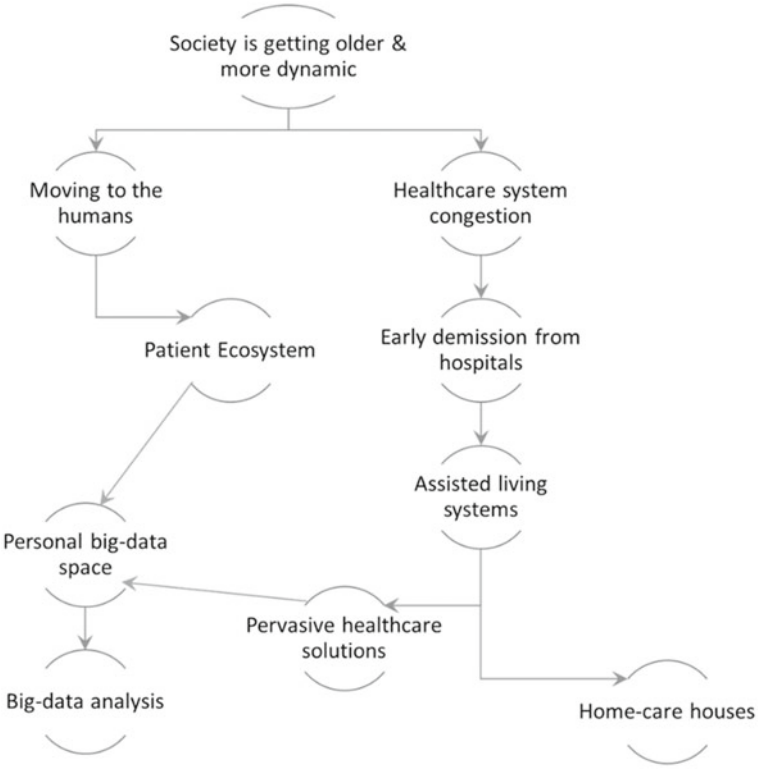

Fig. 4.5 A possible correlation of the driving forces in healthcare as a cause-effect tree

cybersecurity in healthcare cannot do without an analysis of threats from this specific angle.

4.4 Cybercrime and Cyberterrorism Scenario in Healthcare

The main motivation for cybercriminal activities, in healthcare as in many other sector, is the financial profit from stolen data also due to ransoms.[23] Protected Health Information (PHI) has incredible value on the black market. Reported costs of generic data breaches per lost or stolen record are approx. $154. That number skyrockets to

electronic health records obliges physicians to momentarily change their way of working, slowing down their service.

[23] FBI Malware warning issued over CryptoWall Ransomware [19].

Table 4.1 A summary of the main evolutive driving forces of healthcare

Driving force	Details
Society is getting older and more dynamic	An evident trend in Europe is the increasingly ageing of the population. The growing number of senior citizens urge the healthcare services to adapt their services and care tracks
Congestion of the Healthcare system	The increasing number of people that need to be served provokes congestion of the healthcare infrastructures; however, in parallel, technologies such as wearable and home-automation are foreseen to mitigate this trend
Moving to the humans	*Moving to the humans is the new wave*, a citation that represents the new trend in healthcare, of moving data and not people
Early demission from hospitals	Forecasts show an increasing number of people using healthcare services, pushing the hospitals to increase the turnover of patients encouraging access to remote healthcare services
Home care houses	The growth of the home-automation/domotics markets drives the increase of "hospitalized" houses
Assisted Living System	The evolution of Hospitals from a place of care to a network of delocalized services is driving the growth of the assisted living systems
Patient Ecosystems	The healthcare infrastructures are rapidly becoming a network of services. The increasing mix of health, assistance and wellness, is one of the aspects foreseen to shape the future healthcare services
Pervasive healthcare solutions	The ultra-mobile habits of people, who move more frequently and the increasing wish of patients to continue their lives as much as possible when cured drive the evolution of the pervasiveness of healthcare solutions
Personal big-data space	The increasing growth of our personal big-data spaces is one of the leading trends in several sectors; the healthcare is foreseen to contribute with a significant amount of sensible data
Big-data analysis	Beside the increasing production of health-related data, the advanced data analysis is a critical element that differentiates health services from each other. Healthcare just started to mine value from the "mass" of accumulated personal healthcare data

$363 on average for healthcare organizations.[24,25] The cost per leaked record for healthcare firms topped $402 in 2016.[26]

There are many different ways to compromise the IT security of modern healthcare ecosystems. The Hospitals became incrementally digitalized often with complex and still mostly unsolved security problems, tied to the used standards and the lack of harmonization of services.[27] Meantime, the modern cyberattacks are becoming liquid and extremely flexible, able to rapidly exploit all the possible paths of income. As reported by Chesla,[28] since several years '*the advanced attack campaigns are multi-vector, prolonged and adaptive to the defences they meet—unlike the defending side, which is inherently more rigid and structured around products and security solution silos. This siloed security approach presents an opportunity for advanced attack campaigns. While SOC (Security Operation Center) teams are occupied sifting through endless alerts and logs, with no real-time visibility and understanding of the "big-picture", attackers can exploit dead spots and misconfigurations to sneak between security policies*'.

Among the possible causes L. Vaas[29] reports: '*lack of executive support, improper implementations of technology, out-dated understanding of adversaries, lack of leadership, and a misguided reliance upon compliance are some of the factors that concur in making healthcare a very vulnerable sector to cyberattacks*'. The concrete result of these trend is that in 2015, one in three Americans were victims of healthcare data breaches, attributed to a '*series of large-scale attacks that affected more than 10 million individuals*'.[30] However, the year 2015 saw a considerable increase in the number of successful breaches. In 2016, many organizations took steps to limit the impact of data breaches. While the total number of breaches has risen, fewer patients and clients were affected as organizations have fortified their defences. Nonetheless, 16.6 million Americans' records leaked in 2016. Data summarized in Fig. 4.6 better clarifies the dimension of this phenomenon. Although the situation seems to improve almost only for the US, because the number of countries reporting breaches in healthcare data is 150 and the recent case of WannaCry proof the weakness even of the most evolved healthcare systems.[31] Despite 2015 is clearly the worst, the 2016 and 2017 trends must be seen as the stabilization of a trend towards its *plateau*. As a matter of facts, healthcare protection is one of the top priorities for EU security, still in the H2020 work programme.[32]

Healthcare is becoming a service-oriented ecosystem. This trend relies on stable market trends in the smart-object industry (e.g. wearable, internet-of-things industry),

[24] Why cybercriminals target healthcare data [20].

[25] The Need for Increased Investment in Medical Device Security [21].

[26] Healthcare Breach Report 2017 [22].

[27] HL7 Data Interfaces in Medical Environments [23].

[28] Chesla [24].

[29] Vaas [25].

[30] Security [26].

[31] Hospitals in UK National Health Service knocked offline by massive ransomware attack [27].

[32] H2020 [28].

Type of breach	Attacks reported **2014**	Attacks reported **2015**	Attacks reported **2016**	Attacks reported **2017**
Hacking/IT Incident	30	57	113	132
Loss/Theft	148	104	78	55
Unauthorized Disclosure	75	101	130	99
Other	36	6	7	8
Total	298	268	328	294
Individuals affected	12,564,137	113,200,387	16,600,000	4,721,844

Fig. 4.6 In 2016, one in three Americans were victims of healthcare data breaches, attributed to a series of large-scale attacks (*source* of data: BitGlass Healthcare Breach Report 2018)

the social needs of an ageing society and considerations on its economic sustainability. The number of remotely operated health services will increase in the coming years also thanks to the broader adoption of data processing algorithms based on the availability of big personal information spaces.

4.5 Cybercrime

4.5.1 Current Status of Cybercrime

Cybercrime is innovative and rapidly evolving,[33] with a variety of perpetrators ranging from highly skilled and collaborative teams to isolated individuals. Past attacks were mainly the work of technically skilled individuals, seeking personal revenue and/or notoriety amongst their peers; current trends point to the existence of a much more diversified and decentralized system, in which multiple actors contribute to an underground economy.[34] Each actor brings value either in the form of experience and skills, or resources, which can be shared and exchanged for services. In this heterogeneous context, the traditional figure of the lone hacker has been replaced by

[33] AA. VV [29].

[34] Cybercrime as a business: The digital underground economy [30].

an industry that offers illegal activities as a service.[35] This business model is guided by economic drivers: 'customers' requests and needs radically changed and shaped the services offered.[36] Motivations for cybercrime are often financially but also politically and industrially driven. The phenomenon has today resources to surpass the research efforts of IT security. Latest data (Apr 2018)[37] reports that the Global cybercrime economy generates over $1.5 trillion (1 trillion = 1000 billion). These numbers show that the cybercrime completed its transition from geek-driven to business-driven and that with that level of resources the distinction between state-sponsored vs private-sponsored attacks is not any longer significant. The complex attack scenarios are today common amongst topmost Organized Crime Groups (OCGs): recent FBI investigation report of the SONY hack[38] show how social engineering, ad hoc malware, classic hacking and complex business plans harmoniously interoperate in well-done cyberattacks.

Today we also witness the arising collaboration of crime and cybercrime 'industries'. The Global criminal networks began to expand dramatically almost two decades before cybercrime became a serious issue, and traditional and digital criminal cultures developed in parallel, so that people involved in drug cartels, or the people traffickers had never been associated with mass credit card fraud, systematic identity theft or ransomware. Nowadays, if the classic mafia is not getting on the cybercrime business, organized crime groups offer their services to cybercrime operations, such as 'offline' money laundering. At the same time, cybercriminals offer their services to organized crime as part of their operations.[39]

As proven by the EU DOGANA project (www.dogana-project.eu), Social Engineering (SE) (especially its evolution into SE 2.0[40]) plays an exceptional role as it became integral to attack strategies[41] and all 'types' of asset handlers (either human or system) are a target, with humans often providing a primary access point. Attackers always follow the path of least resistance and most profit: **employees are increasingly part of the attack strategies**.

Social engineering is the human side of hacking. Attacks can be divided into two categories: human-based social engineering, where sensitive information is gathered by person-to-person interaction exploiting human characteristics such as trust, fear or helpfulness (e.g. pretexting, eavesdropping, shoulder surfing, tailgating, dumpster diving), and computer-based social engineering, which is carried out with the help of computers (e.g. phishing, baiting).[42] From a general point of view, as long as there is a conscious interface between humans on the one side and systems and devices on

[35] Samani and Paget [31].

[36] Kurt et al. [32].

[37] See https://www.bromium.com/free-report-complex-cybercrime-economy/.

[38] Refer to FBI Criminal Complaint AO 91 (Rev. 11/11), https://www.justice.gov/opa/press-release/file/1092091/download.

[39] Higgins [33].

[40] Ariu et al. [34].

[41] Ibid. See Footnote 12.

[42] Ibid. See Footnote 17.

the other side, social engineering will persist. This is today a ubiquitous threat that is true for any IT system and place: in or outside of the hospitals, while using the PC in a hospital or the personal mobile phones, for physicians or patients.

Working and private lives become more and more mixed into a blended lifestyle: private and professional lives are blended due to the flexibility to work at any time from different locations. Nomadic workforces are the norm today. The seamless experience offered by digital ecosystems opens the door to seamless deception techniques as well. Recent statistic reports that approximately almost any modern attack involves some degree of Social Engineering.[43,44,45] **It has become the age of Human Hacking**.[46] Therefore, it is widely accepted amongst experts that an organization's capability to prevent, investigate and mitigate cybercriminal attacks is dependent on its ability to mitigate the human related threats. This means that organizations are increasingly under pressure to find new and effective ways to improve their defence mechanisms and that most of those in place, built on a different attack paradigm, are not anymore enough to protect the organizations.

As a general approach, we can divide the cyberattacks into two broad categories: *opportunistic attacks* and *Targeted Attacks* (TAs). Despite, there is not a clear differentiation line between the two categories of attacks, what drives the choice of the correct strategy is the (devilish) business plan. Attackers with varying degrees of skills are responsible for the different types of attacks.

- *Opportunistic attacks* rely on downloading offensive tools and use them to hit a broad spectrum of domains and users. In general, these players are low in technical skill and usually target less protected organizations, but are successful because of the large volume of the targets. The data obtained through opportunistic attacks are often resold multiple times to others, who then derive more opportunistic attacks or TAs.[47]
- *Targeted attacks*, at the other end of the spectrum, involve *skilled individuals* who leverage both high levels of technical skills, and 'human engineering' to target specific objectives. Attack planning can be very sophisticated and long in duration.[48]

[43] How modern email phishing attacks have Organizations on the hook [35].

[44] The Human Factor [36].

[45] 2017 Data Breach Investigations Report 10th Edition [37].

[46] As an example, see: Frumento [38].

[47] One recent opportunistic attack that hardly hit the healthcare world was WannaCry. Its incidence was higher than other sectors due to the high number of unpatched machines in hospitals. See for example Mullen [39].

[48] Defray—New Ransomware Targeting Education and Healthcare Verticals [40].

4.5.2 Current Threats in Healthcare

The health sector security nowadays suffers from a broader trend, which is the increasing number of attacks on secondary markets, not primarily targeted by cybercrime until now. Health is gaining much attention because it is a more straightforward target than banks, the hospitals' security landscape is jeopardized, and their employees are less trained.[49] This problem is getting even harder with the rise of Mobile Health. From the security point of view, Healthcare is a particular case, because it does involve not only the owner of the data (the user) and the official handler (the health services) but also external actors (e.g. consumers of health data or services suppliers).

Summing up, the most common threats in the healthcare are the following:

(1) Physical theft/damage/loss is maybe one of the most usual cases in areas where there is the presence of sensitive data, such as health- and government-related. In particular, in the area of healthcare, the physical theft ranks first among the breach methods.[50]

(2) Information theft is another critical element of incidents in the medical/healthcare industry. Identity theft in this sector has received particular attention from attackers.[51,52] The increase of data breaches if seen in combination with developments of the internet of things/wearables makes evident that there is potential misuse in the area of healthcare.[53]

(3) Targeted Attacks are those more actively using the Social Engineering techniques, for example, to facilitate data breaches. However, looking at the bare numbers, TAs are not the most used against Hospitals. Nonetheless, TAs have the highest impact and rate of success. The structural and security problems of several Patient Ecosystems are particularly vulnerable to TAs.[54] Mitigation for such attacks passes through the identification of which are the critical figures in the HC organizations and the estimation of their exposure based on their role and digital footprint/shadow.[55] Social engineering is a unique problem in organizations where workforce members do not necessarily know each other. In healthcare, this happens despite the existence of security policies (e.g. HIPAA

[49] The unlocked backdoor to healthcare data [41].

[50] Damage Control: The Cost of Security Breaches [42].

[51] Hiltzik and Times [43].

[52] Anatomy of a healthcare data breach [44].

[53] Koroneos [45].

[54] Barney [46].

[55] A possible definition of Digital Shadow is: '*A digital shadow, a subset of a digital footprint, consists of exposed personal, technical or organizational information that is often highly confidential, sensitive or proprietary. As well as damaging the brand, a digital shadow can leave your organization vulnerable to corporate espionage and competitive intelligence. Worse still, criminals and hostile groups can exploit a digital shadow to find your organization's vulnerabilities and launch targeted cyberattacks against them*', see 'Cyber Situational awareness', Digital Shadows, 2015. [Online]. Available: http://bit.ly/2wyLMhk.

in the US or HITEC Act which enforces the encryption of healthcare data) and employee training programs. As recently reported by C. Cook[56]: "*Social engineering attacks of any kind tend to be highly successful, but against an organization with uneducated and untrained employees, these attacks are lethal, an example are the multifaceted social engineering attacks"* which combine phishing and vishing attacks and works well in healthcare.

(4) Threatening of the hospital's users and infiltration through the external nodes (i.e. actors of the supply chain). In the case of Hospitals 2.0, which rely on a distributed system, the security of the overall ecosystem is equal to the security of the weakest node in the supply chain. In a distributed system, like that of Fig. 4.3, the vulnerable nodes are several: patients, wearable devices, peripheral ambulatories, inadequate security expertise of physicians and attendants, suppliers of software services. As stated by the Federation of European Risk Management Associations (FERMA) in its 2016 Position Paper[57] '*The resilience of the whole supply chain is also a pressing cybersecurity challenge for businesses. Weaknesses of only one sub-contractor can impact the rest of the supply chain leading to economic losses and even jeopardizing the existence of some partners.*' Complex and multivendor supply chains have become the norm in healthcare, and therefore the cyber resilience of hospitals requires strong commitments:

- by suppliers, to consider local and global security matters, and support and adopt appropriate standards, and to issue clear guidance to users;
- by users, who must implement and operate taking into account suppliers' recommendations;
- by users, suppliers and consultants, to understand and manage complex security;
- by organizations to adopt human factor best practices.

This must apply across all the dimensions of society, i.e. as healthcare operators, as patients, as servants and as citizens.

(5) Abuses of the patients and medical dataspaces. A threat comes from the abuse of patients' dataspace and medical information, for example through specific ransomware,[58] which uses Social Engineering techniques against exposed targets (e.g. aged patients).[59] Ransoms are a good sample of how rapidly the cybercrime interest for hospitals is growing,[60] as also reported by Cefriel[61]: '*ransomware is not actually the problem, but rather a consequence. The real problem is something*

[56] Cook [47].

[57] Federation of European Risk Management Associations (FERMA), 'Response to the European Commission consultation on the public–private partnership on cybersecurity and possible accompanying measures', FERMA, 2016 [48].

[58] Ossola [49].

[59] Peachey [50].

[60] Sjouwerman [51].

[61] See Frumento [52].

that happened before. The training of health operators was far from being effective and employees were not taught to correctly recognize the threat'.

Besides these problems, the hospitals suffer from another class of issues addressed for decades: the security standards in use in the eHealth world, mostly lack on-field testing against real-world attacks (e.g. penetration testing of protocols and their implementations).[62,63] The standards specified by SDOs (Standard Developing Organizations) are sometimes not using a coherent approach to security. However, the European Union started actions to increase the convergence of ISO/CEN, WHO, HL7, IHE standards. However, the work is still incomplete, and most of all the robustness of these evolutions still has to be proven against real attacks and penetration testing campaigns.[64]

4.5.3 The Problem of Social Engineering

No matter how complex the health services are, the centre of healthcare services is always on humans; this means that healthcare security has to take into account the impact of the new wave of '**moving to the humans**'. Unfortunately, **cybercrime is also** '**moving to the humans**' at the same, or even faster, pace: the so-called *human layer of security* has become, in recent years, the **number one** tactic to launch successful attacks, across industries worldwide. Today, only about 3% of malware exploit a technical flaw. The other **97% trick users through Social Engineering**.

To explain the human side of security it is important to explain some of the not-so-well-discussed characteristics of the recent waves of Ransomware attacks against healthcare organizations.[65] All of them have in common one single characteristics: the ransomware attack is not, except in rare cases such as WannaCry, spreading on its own with automatic infections, it instead requires the intervention of a human victim, who inadvertently clicks on a phishing link (for example), starting the infection process.[66] Without these consequential clicks, the infection would not spread.[67]

A recent example of this trend was disclosed in April 2018[68]: '*Hackers behind Healthcare Espionage Infect X-Ray and MRI Machines. Security researchers have uncovered a new hacking group that is aggressively targeting healthcare organizations and related sectors across the globe to conduct corporate espionage. Dubbed Orangeworm the hacking group has been found installing a* ***wormable trojan*** *on machines hosting software used for controlling high-tech imaging devices, such as*

[62] Alton [53].

[63] Newman [54].

[64] E.g. Mearian [55].

[65] As an example, U.K. Hospitals Hit in Widespread Ransomware Attack [56] and Bisson [57].

[66] As an example, Carpenter [58].

[67] Technically speaking, the humans are the so-called *kill switch* of an attack, meaning that without 'breaking' of the human layer of security the attack would not spread into the organization.

[68] See: https://thehackernews.com/2018/04/healthcare-cyber-attacks.html.

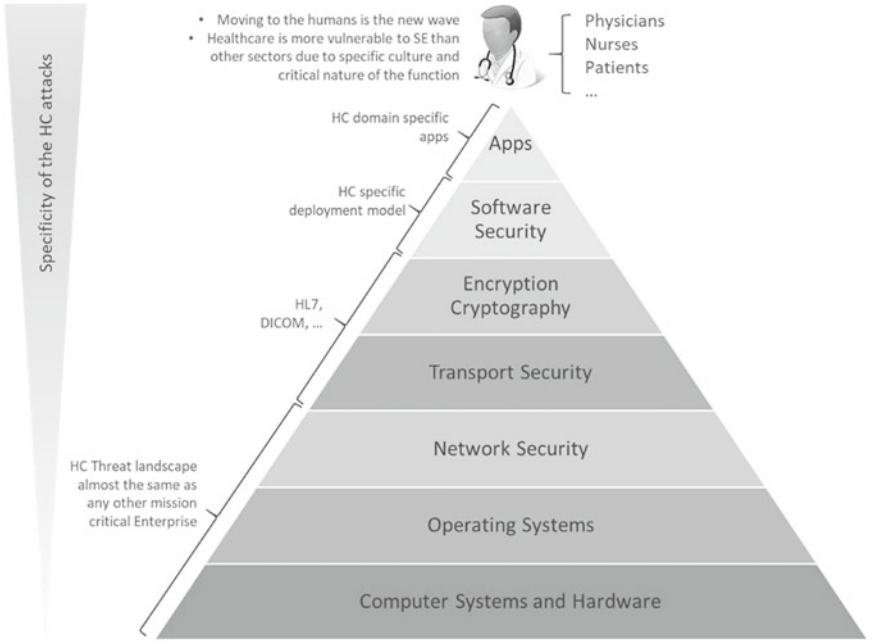

Fig. 4.7 The seven layers of security plus the human layer

X-Ray and MRI machines'. Beside any discussion on the technical dimension of the attack, it is worth to underline that the infection system is a Trojan, this implies phishing and definitely, it involves the human element as the first step of the attack.

Healthcare services are no different[69]**: the biggest portion of the HC threat landscape involves attacks whose 'kill switch' resides outside the ICT domain and whose mitigation requires actions on the humans or, in other words, hardening the human layer of security** (see Fig. 4.7). As shown by the DOGANA Project, the complexity level of attacks that actively exploit the human element is incredibly high and often the exploitation of the human element is the enabler element for the following technological part of an attack. However, Social Engineering is also evolving and today we are talking about SE 2.0 versus old school SE.[70] Social Engineering (SE) is the human side of hacking and we are currently in the 'era' of human hacking. A recent study[71] reports that **among the five biggest healthcare threats, three out of five are social engineering based and for them training remediation would have worked**.

[69] Ibid. See Footnote 12.

[70] Social Engineering 2.0 is the evolution of Social Engineering and its transformation from a limited threat to a crucial threat for the computer security.

[71] Nadeau [59].

Combining Social Engineering and healthcare, we, therefore, have the worst of both worlds—we have to decrease the impact of SE by *hardening the human layer of security*, and this has to be achieved across the *complete healthcare supply chain*. Any approach that limits itself to part of this complete supply chain will, by definition, fail to increase the resilience of healthcare to cyberattacks, as it will leave untouched one or more channels through which cyberattacks can reach the heart of the healthcare system.

However, how can we harden a human layer when it integrates such a wide variety of humans? This one is probably the biggest challenges in today's ICT security. While some automated solutions for the improvement of the human layer exist,[72] they are still new and have to prove their real effectiveness and scalability in many application areas.

4.5.4 Current Defences in Healthcare

Politico[73] in 2015 reported, '*After spending billions of dollars migrating to electronic health records, the healthcare industry is now looking to beef up its spending on data security*'. According to Politico's estimations of 2015, healthcare organizations should spend at least 10% of their IT budget to reach a correct cybersecurity level. Yet, the industry average is just 3%. However, Politico's estimation was somehow optimistic, because recent statistics reports,[74] '*healthcare cybersecurity spending will exceed $65B over the next 5 years*'. As an example, the ransomware attacks are foreseen to quadruple by 2020.

The essential elements required to prevent this growing wave of attacks are the following[75]:

(1) Innovative user awareness programs: the predominant element of the current threat landscape is the sophistication and extension of the attacks using social engineering (i.e. direct involvement of the victims in the attack tactics). Consequently, the users from being the most attacked entity become the weakest part of the defence systems. Building training programs, really able to drive a behavioural shift towards more secure habits, is one of the open issues of today's IT security (see the dedicated section of this chapter).
(2) Innovative mobile terminal management systems: the evolution of the perimetral defence solution is one of the problems arose from the proliferation of

[72] Korolov [60].

[73] Allen [61].

[74] Healthcare security $65 billion market [62].

[75] For a complete and recent overview look the '*Report on improving cybersecurity in the healthcare industry*' published by the Healthcare Industry Cybersecurity Task Force, Available: https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.

BYOD. New solutions are required, also mixing perimetral defence and pervasive awareness solutions (see, for example, the EU project MUSES).[76]

(3) Mitigate the jeopardizing problem of security: in hospitals is essential not only to promote the adoption of best practices, which often have been developed in other application areas, like banks, but also to study specific defence strategies, and also to try to foster a shared culture of security.

(4) Consider the specific aspects of healthcare: healthcare is a mission-critical industry whose primary goal is to save lives; this implies a modification in priorities (see the discussion in Sect. 4.1 of this chapter).

4.5.5 Future Threats in Healthcare

As previously reported in this chapter, the personal information space is growing in size and complexity. This evolution happens thanks to the diffusion of heterogeneous personalized healthcare services, which generate a growing amount of data. These trends are fundamental for CC. The attack surface of a health information system develops when interconnected objects, such as mobile and medical devices and applications, are authorized to connect to EHRs.[77] The personal information space is, hence, growing also in exposure. However, its handlers (e.g. patients or physicians) do not fully understand the implications.[78] Among healthcare operators, the comprehension of the consequences of the data sharing is not increasing. At the same time, the new developments of the personal information spaces are increasingly exposing new patients and healthcare operators to IT security issues.[79]

Another category of healthcare problems still comes from a lack of widely adopted secure standards and policies for the IT security. The adoption of the correct procedures to protect the privacy and security of the sensitive patient health information should be adopted uniformly by all the healthcare entities, including the supply chain.[80] The healthcare information security and privacy practitioners already benefit of some certifications,[81] but the final goal should be Europe-wide standards, to assess both IT security and privacy expertise within the healthcare industry.

Besides, as with the telemedicine services, one of the most challenging features of a mobile health service is the so-called '**immersion effect**'.[82] The term refers to the

[76] For example see MUSES 7th FWP EU Project (Multiplatform Usable Endpoint Security)–, www.muses-project.de.

[77] NIST published guidance around risks and best practices associated with accessing EHRs via mobile devices in NIST Special Publication 1800-1e DRAFT.

[78] Catalano [63].

[79] More than 75 percent of U.S. Adults express concern about security of healthcare data, reveals University of Phoenix survey [64].

[80] Small healthcare facilities unprepared for a data breach [65].

[81] See for example the HCISPP (Healthcare Information Security and Privacy Practitioner) [65].

[82] Immersion effect: '*a generic telemedicine application should create the user's immersion effect that means the physician should only think of his diagnosis without worrying about particular*

ability of both physicians and patients, to forget the means used and concentrate on the service. It's a fundamental feature for a physician operating through IT systems, needed to focus on the clinical problem without worrying of distracting security issues; the patient at the same time must be confident that his/her data are not 'abused' in any way. Nowadays, the way to obtain this immersion effect is to hide the security issues deeply into products, but often without real security. This problem is important for the IT security in healthcare and is the most robust trust chain (between users and devices) that attackers can exploit.[83,84]

These considerations translate into some problems tied to the poor usability of the security solutions in healthcare. As a matter of facts, the ubiquitous availability of mobile technologies and the easiness of sharing the media, even with high definitions, foster a more direct relationship between physicians and patients. These relationships result in the exchange of data through 'unofficial' channels (e.g. direct WhatsApp messages or discussion groups, unsecured email, etc.), skipping the healthcare infrastructure, whose IT security measures are 'cumbersome', due to the added layers of complexity. This scenario happens on the base of the personal 1:1 relationship, between patients and physicians and can be overlooked as 'spontaneous' mobile health in general. However, this scenario is open to misuses and data breaches.

4.6 Cyberterrorism

4.6.1 Current Status of Cyberterrorism

The cyberterrorism is also known as electronic terrorism or information wars. In an effort of summarizing, we can define it as an act of Internet terrorism, which includes deliberate and large-scale attacks and disruptions of computer networks against individuals, governments and organizations, using the same arsenal of cybercrime (made of malware, social engineering, hacking techniques, etc.). What drives the cyberterrorists is an ideology; on the contrary, motivations behind cybercrime are often economic gain and hacking or internet vandalism. The term 'cyber terror' is to some extent controversial since many cyberattacks fall into a grey area where hacking can be considered as an act of 'internet anarchy'. We can differentiate the two terms by looking at the definition of terrorism: the goal of terrorism is to create a feeling of terror in the minds of the victims.[85]

---

informatics operations that could divert his attention'. Source: Committee on Evaluating Clinical Applications in Medicine. Telemedicine: A guide to assessing Telecommunications in Health Care. Marilyn J Field Editor, Division of Health Care Services.

[83] The unlocked backdoor to healthcare data [41].

[84] Security risks of networked medical devices [66].

[85] Dawson and Omar [67].

Probably one of the clearer definitions comes from K. Harrison and G. White.[86] It defines the following two concepts:

- the event vector, which describes the threat agent and different abstract levels of objectives and methods by which the event occurs.
- the effect vector, which describes what critical infrastructure is affected, the reason it is affected, and what the effects are on the community.

The authors point out that '*when considering a large-scale attack on a community, the overall attack may be comprised of several event vectors. Additionally, an attack with one or more event vectors may have multiple associated effect vectors*'. Cyberterrorism fits this definition. Literature of cyberterrorism, especially after the radicalization of some attacks in the recent years, is quite extensive. For the sake of the discussion on healthcare, it is useful to report the Fig. 4.8, where healthcare is among the affected services. It is worthwhile to underline that healthcare can be a primary as well as a secondary target: it can be the directly affected service (primary target) but also it can be part of a wider attack strategy (secondary target). It is also important to differentiate between a cyber-event being an actual cyberterrorist attack and a cyber-event that provides technology support to terrorism in general.[87] The following sections tell more about.[88]

4.6.2 Current Threats in Cyberterrorism

A review of the recent researches in the healthcare security shows an almost exclusive focus on the protection of patient health records and scarce attention to several other threats, as the cyber-physical type of risk, such as the threatening of patients' life with cyberthreats.

The likelihood of physical and psychological harms, for ideological or religious beliefs, conducted by individuals or organizations through the Internet, is increasing. These activities fall under the definition of 'cyberterrorism'. In the healthcare, this can appear in different ways, for example, bringing down a hospital computer system or publicly disclosing private medical records. Whatever shape it takes, the general effects are the same: compromising of the patient care and loss of trust in the health system. As a matter of facts, resilience is a fundamental pillar for the trust and confidence of patients in eHealth services. These attacks mine the hospital resilience, as the perception of the hospital as a 'safe place'. Although not many past attacks are classified as cyberterrorism, it is a common perception that cyberterrorism threats

[86] Harrison and White [68].

[87] Veerasamy et al. [69].

[88] Several countries created specific departments exclusively dedicated to combat cyberterrorism (e.g. the Cyberterrorism Defense Analysis Center-CDAC—within the US Department of Defense Cyber Command-USCYBERCOM). For a discussion on the state of cyberterrorism refer to the project www.cyberroad-project.eu especially the deliverables from D6.1 to D6.6.

Effect Vector

Cause	Service Affected	Disruption Impact	Evaluation Metrics
Cyber Event within Service Cascade Disruption from <Service>	Energy	Economic Impact	% Revenue Lost, %GDP Lost
		Population Impact	% Population Denied Access
		Government Impact	% Government Effectiveness Reduced
	Telecommunications	Population Impact	% Population denied access to service
	Finance	Economic Impact	% Revenue Lost, %GDP Lost
		Population Impact	% Population Denied Access
	Water Supply	Population Impact	% Population Denied Access
	Healthcare	Population Impact	% Population Denied Access
	Transportation	Population Impact	% Population Denied Access
	Law Enforcement	Population Impact	% Population Denied Access
		Government Impact	% Government Effectiveness Reduced
	Emergency and Fire Response	Population Impact	% Population Denied Access
		Government Impact	% Government Effectiveness Reduced
	Govt. Administration	Government Impact	% Government Effectiveness Reduced
	Shipping	Economic Impact	% Revenue Lost, %GDP Lost
		Population Impact	% Population Denied Access
	Agriculture	Economic Impact	% Revenue Lost, %GDP Lost
	Commercial Facilities	Economic Impact	% Revenue Lost, %GDP Lost
		Population Impact	% Population Denied Access
	Critical Manufacturing	Economic Impact	% Revenue Lost, %GDP Lost

Fig. 4.8 The effect vector describes the community sector affected, the cause of the effect, and the impact of the affected sector, and metrics that can be used to further evaluate the impact (*source* K. Harrison and G. White)

are about to happen.[89] Literature reports some not-so hypothetical examples. All of these are hybrid war scenarios that, according to the current cybercrime landscape, are doable also with a relatively small technic and logistic preparation.

(1) Enemy agents who gain access to the immunization records of the fighting forces, allowing them to know which biological agents are most likely to decimate the troops.
(2) Cyberthreats happening in specific moments in time to magnify their effects. Such as, for example, malware casually knocking-off a control system or an integrated smart city transport information system (such as E015 use-case in Milano) during a strike. In healthcare, this happened already, during a flu peak a ransomware taken down the IT of a big hospital.[90]
(3) Malware explicitly developed and meant to exploit a system during a natural event, to magnify the effects of, for example, a natural disaster combined with the takedown of the healthcare infrastructure. This includes malware that infects a hospital system and stays dormant for a while, waiting for the 'perfect storm', for example, a deny-of-service during a storm or an earthquake or a movement of masses (e.g. big events) to increase the panic or support a terrorist attack.

Moreover, other types of attacks are possible: '*a disgruntled employee with a list of active passwords and access to a hospital's systems has the potential to inflict far more damage than someone who must first conquer perimeter security appliances*

[89] Knudson [70].
[90] https://www.theregister.co.uk/2018/01/16/us_hospital_ransomware_bitcoin/.

and hack into a system. Authorized individuals can download sensitive data, drop nasty viruses into the organization's network, and even open back doors for others to use'.[91]

The trust relationships are one fundamental element of healthcare, and an attack can target the trust of people in the system. The loss of integrity and trust into a highly digitized and distributed system may seem as a secondary concern, but it is really of primary importance in healthcare. Different level of trustworthiness is an essential element to rate the quality of different healthcare systems.

4.6.3 Current Defences in Cyberterrorism

Healthcare organizations adopt several 'best practices' to protect themselves against CC or CT cyberattacks. At the time of writing, the defences against cyberterrorism are the same of cybercrime, but in this case, the awareness is crucial: awareness must include terrorist logics and methods to be aware of the role of a healthcare organization (and its persons) in a terrorist attack.

Moreover, Rick Kam, president and cofounder of ID Experts: '*with the growth of mobile devices in the healthcare realm, many IT groups no longer have the tight grip on access and storage protocols that they used to. Those other data sources need to be included in IT's overall strategy because it is, unfortunately, a weak link in the chain*'.

4.6.4 Future Threats in Cyberterrorism

Large health systems generally have the expertise to ensure the adoption of the correct cybersecurity countermeasures. The same thing is not valid for smaller ones, which still forms the backbone of most European National Healthcare Services. In these cases, the organizations are sometimes stymied by leadership inertia, costs or lack of knowledge. This knowledge gap is a consequence of the frantic pace of technology innovation in the healthcare sector. The European policing agency reports '*Governments are ill-prepared to fight the looming threat of "online murder" as cybercriminals exploit internet technology to target victims*'. EUROPOL[92] warns about a rise in '*injury and possible deaths*' caused by computer attacks on critical safety equipment. Even the European Union H2020 framework program recognizes the connection of physical and cyberthreats.[93]

---

[91] G. V. P. Company [71].

[92] Peachey [72].

[93] For example, look the text of the call SU-TDS-02-2018 for project proposals, available at https://goo.gl/xPVKLV.

4.7 Future Defences

The cyber-risk space is a complex and continuously evolving ecosystem, and neither attack category should be neglected. Therefore, the defence strategy of an organization needs, by definition, to be flexible and adaptable and always adopt different tactics.

Bearing in mind that phishing is becoming more and more common among cybercriminals and has devastating outcomes; hospitals organizations are keen to fight this ever-increasing threat by any means.

Threat actors know where the weakest link resides and they are aggressively exploiting it: spear phishing attacks have proven to be incredibly effective for cybercriminals. Data suggests that one in five employees will click on a malicious link and the time to detect a breach is a staggering 15 months. The average time from an email phishing breach to detection is 146 days globally, and a colossal 469 days for the EMEA region.[94]

Organizations need a better way to fight back against targeted attacks and prevent data breaches.

In today's threat landscape, in order to prevent substantial financial and reputational damages caused by phishing, companies must implement an automatic response that can reduce the timeframe from discovery to remediation from weeks to minutes.

To effectively mitigate the risks of phishing attacks, companies must combine employee training (since over 90% of breaches are attributed to phishing emails targeting employees) with efforts on machine learning. The aim is to reduce the time of response to attacks and share attack intelligence.[95]

An article of 2013 in Telemedicine and e-Health[96] was already reporting '*healthcare organizations are at risk for attacks because they increasingly rely on computerized information; share sensitive data across multiple networks; use mobile devices; and are under-protected compared with other, less fragmented industries*'. According to the paper, most of the healthcare facilities reports cover hacking into their clinical data systems, including insertion of malware, denial-of-service attacks, and computer code attacks to steal or manipulate data. A more recent report, already cited before (see footnote 26) updates reporting that '*after two years of simulating attacks on monitors, health records, surgeries and more, researchers concluded that patients are pretty much sitting ducks*'.

ISE researchers[97] implemented a so-called **Patient Health Attack Model**, which focuses on the primary attack surfaces that directly affect a patient's health. Such a

[94] See https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf.

[95] See https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/30-employees-are-the-weakest-link-part-i.

[96] Harries and Yellowlees [73].

[97] ISE [74].

model includes some of the described threats, for example, hacks of medical devices to deliver a lethal dose.

The co-operation against cyberterrorism and other large-scale cyberattacks[98] is one interesting area of development because '*mutual legal assistance of law-enforcement authorities has to be improved and adapted with regard to technological developments. Security measures for the protection of critical services and infrastructure should be developed. States are internationally responsible for taking all reasonable measures to prevent large-scale cyberattacks from being launched by persons under their jurisdiction or emanating from their national territory*'.

4.7.1 The role of training to mitigate the threats related to the human layer of security

Previous sections already underlined the importance of the humans in ICT security. According to a research recently published by the Identity Theft Resource Center (ITRC),[99] 52% of the surveyed healthcare Operators agreed that *a lack of employee awareness and training affects their ability to achieve effective security*.

Training is almost all about modifying the trust in the ICT system changing the confidence of people, through cultural shifts or increasing the cyber-scepticism (also called in ICT security the *mind firewalls*). Confidence may be defined as '*the extent to which one is willing to ascribe good intentions to and have confidence in the words and actions of other people or systems*'.[100] If the victim does not consider alternatives (every morning he/she opens the email without worrying too much) she is in a situation of confidence. Confidence is hence connected to the concept of risk-taking. Therefore, the confidence of people in the systems is one of the most abused elements in human layer attacks, because it relates to the risk-taking behaviour. As an example, users choose to follow the instructions in the email or not, despite the possibility to be hacked, based on their level of trust or confidence.[101] The role of training is to influence this level of confidence.

However, several factors influence confidence. Mainly biases and habits but others are discovered every day by cognitive sciences, such as the mirror neurons,[102] co-

[98] Franken [75].

[99] Healthcare industry: Attacks outpacing investments in personnel, education and resources [76].

[100] Cook and Wall [77].

[101] For the same discussion, we do not differentiate trust and confidence. Trust differs from confidence because it requires a previous engagement on a person's part, recognizing and accepting that risk exists. This is exactly the type of distinction that exists in the cyberattacks because every user knows that the risk of being hacked exists, but often does not recognize it correctly because of his confidence.

[102] Hadnagy [78].

dependent relationship,[103] fear of missing out,[104] reverse psychology,[105] etc. This is not a simple problem: ICT security experts have been debating it in the last years as one of the most challenging problems. The point is to **measure the performances of the training programs and their correlation with the real reduction of the cyber risk for the organizations**.

The social-driven Vulnerability Assessments (SDVA) performed during the DOGANA project clearly show that not all training programs perform well, leaving the final risk for enterprises unchanged on the long run. As an example, ProofPoint (a leading cybersecurity company) reports that *people clicked on test phishing campaigns because they did not match the characteristics they had been trained to look for in the previous year*.[106] Another research reports the results of a phishing test run on a big sample of enterprise employees[107] before and 3 months after an awareness program. It clearly shows that the risk level was reduced immediately after, but increased again after three months.

One other important aspect to consider is the propensity of people to trust or to have confidence. This propensity requires some sort of psychological profiling to tailor the awareness programs to an individual's social and behavioural dispositions. The propensity to have confidence is influenced among others by personal culture, habits, environment and age. For example, a recent study[108] presents a co-dependent relationship: users perform better on cognitive tests when their smartphones are nearby (even if they are not using them) compared to when they are out of sight. Other studies[109] report an important change in everyday habits that affect risk-taking behaviour (e.g. extroversion and introversion).

The question of how to train users or 'patch the human side of security' remains an open issue despite having being on the list of open problems in the last years.[110] The lack of fully proven reliable and long-lasting awareness methods is still pressing in the cyber security community. Existing literature[111] highlights that, to effectively solve these problems through training, the best option is to have fully customized training programs and highly innovative methods, possibly mixing defence and training. The problem of personalization means to understand which methods are most effective in which context, taking into account the psychological assessment of users and in some cases considering how the brain works and learns. The problems of training described above, represent today one of the biggest issues of ICT security for healthcare, as well as across all other critical sectors.[112] However, healthcare is a 'low hanging fruit',

[103] Gilbert-Lurie [79].

[104] Chang [80].

[105] Dachis [81].

[106] The Human Factor 2018 [82].

[107] Frumento et al. [83].

[108] Clayton et al. [84].

[109] Harley et al. [85].

[110] See Is cybersecurity awareness a waste of time? [86] and Qin and Burgoon [87].

[111] Kirlappos and Sasse [88].

[112] Sjouwerman [89].

because the human layer in HC is usually weaker, meaning it has a higher likelihood of being compromised, for example, because of the chronic lack of cyberculture of the HC operators.

4.7.2 The role of intangibles in the nowadays attacks

Most of the current approaches to IT security and risk management tend to underestimate, or even ignore, the following key aspects:

- The **human factor** (covering subjective, organizational, societal and economic aspects) and how it contributes to vulnerabilities to cyberattacks: the management of SE enabled attacks is often incorrect, even though they generate the highest costs regarding consequences and protection.[113] Training is one of the possible mitigation measures, and the IT Security research is actively investigating this area. As discussed the healthcare world is very vulnerable to these attacks.
- The **strategy of the attacker** in the identification of vulnerabilities and assets at risk: OCG completed their migration to a business-driven approach for few years, and business logic now drives them as any other enterprise. From the defence point of view the same interdisciplinary approach, combining engineering, risk assessment, economic, cognitive, behavioural, societal and legal knowledge is needed to contrast the novel strategies of professional IT attackers properly.

However, as defined by the EU project HERMENEUT,[114] the **role of intangible assets** is a third often-neglected element, with a great importance in the quantification of the consequences of cyberattacks. As reported by Kerber R.[115] '*More than half the value of companies worldwide is in intangible assets, such as intellectual property, much of which is stored on computers and could therefore be vulnerable to hackers. That figure could be as high as $37.5 trillion of the $71 trillion in enterprise value of 58,000 companies, according to Brand Finance, a consultancy specializing in valuation of intangible assets*'. The consequences of data breaches in terms of impact on tangible and intangible assets is a problem studied since several years in healthcare.[116] In general, Cyberattacks can damage physical—tangible—assets of the victimized institutions. One real-world example are turbines destroyed because of the manipulation of its control systems.[117] More frequently, though, the damage will not be physical. **Intangible assets** (i.e. reputation, trust in the organization, patents, trademarks, knowledge, expertise, human-capital, wellness, etc.) are now recognized as critical to the performance of companies and nations. Increasingly the attacks are

[113] Ibid. Reference in Footnote 106.

[114] www.hemeneut.eu.

[115] Kerber and Jessop [90].

[116] Riddle et al. [91].

[117] Langner [92].

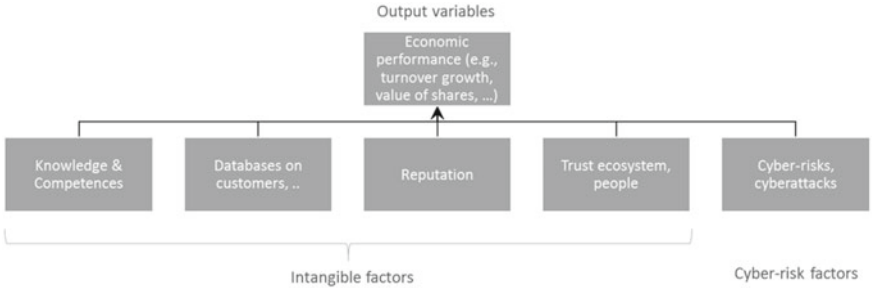

Fig. 4.9 Basic description of the economic cost model

hitting the intangible assets as a primary target (e.g. automated cyber *crowdturfing*[118] attacks) or, because of an attack (e.g. Uber data breach in 2017). Modelling of these attacks is difficult for the relative 'obscurity' of the cybercriminal attack plan.

At the macroeconomic level, a number of studies stress the dominant nature of intangible investment as well as its important contribution to economic growth and productivity.[119] At the microeconomic level, besides research, which focuses on specific intangibles such as R&D, patents or brands, studies also, stress the importance of intangibles assets for corporate performance, using a comprehensive approach.[120] Intangibles often contribute to **80% of the value of organizations**. The role that the intangible assets play is relevant for the healthcare, being organizations, as previously discussed, strongly based on trusts relationships (see Fig. 4.9).

Acknowledgements The research leading to these results was partially funded by the European Union's Horizon 2020 Research and Innovation programme as the **DOGANA project (aDvanced sOcial enGineering And vulNerabilityAssessment)**, under grant agreement No. 653618 and the **HERMENEUT project (Enterprises intangible Risk Management via Economic models based on simulation of modern cyberattacks)**, under grant agreement No. 740322.

References

1. A. VV: The Future of Identity Personal Information space. The Future of Identities in a Networked World, 1st ed. http://mcaf.ee/l209yu: Giesecke & Devrient (2013)
2. Gartner: 10 critical IT trends for the next five years, http://www.networkworld.com/news/2012/102212-gartner-trends-263594.html

[118]Crowdturfing is a combination of 'crowdsourcing', meaning recruiting large numbers of people to contribute a small effort each towards a big task (like labelling photos), and 'astroturfing,' meaning false grassroots support (in the form of bogus reviews or comments, for example. Automated crowdturfing attacks involves many AI-operated profiles, whose intention is to damage the reputation of a brand or person.

[119]Nakamura [93].

[120]Bounfour [94].

3. Nielsen, J.: Usability 101: Introduction to Usability. Available online https://www.nngroup.com/articles/usability-101-introduction-to-usability/
4. Canina, M., Bellavitis, A.D.: IndossaMe: il design e le tecnologie indossabili. FrancoAngeli, Milano (2010). (in Italian)
5. Talk to my shirt blog, http://www.talk2myshirt.com/blog/
6. Crunchwear, http://www.crunchwear.com/
7. "Control Your Mobile Phone or Tablet Directly from Your Brain", NextNature.net, http://www.nextnature.net/2013/05/control-your-tablet-directly-from-your-brain/
8. "Context-Aware Computing: Context-Awareness, Context-Aware User Interfaces, and Implicit Interaction", http://www.interaction-design.org/encyclopedia/context-aware_computing.html
9. https://www.gartner.com/it-glossary/context-aware-security
10. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative model of organizational trust. Acad Manag Rev **20**(3), 709–734 (1995)
11. D2.1 The role of Social Engineering in the evolution of attacks. DOGANA Project (GA. 653618) (2016). Available https://www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf [Online]
12. World Health Organization.: Active Ageing: A Policy Framework. Geneva (2002)
13. eHealth Health Task Force. Redesigning Health in Europe for 2020. European Union 2012
14. Connected technologies will accelerate security threats to health care industry. Help Net Security (2017). Available https://www.helpnetsecurity.com/2017/11/09/security-threats-healthcare-industry/ [Online]
15. Cyber security and resilience for Smart Hospitals (2016). Available https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals [Online]
16. "Health Care Sector Report. Cyber security for the health care sector", ECSO, WG3 I Sectoral Demand, March 2018
17. Bowman, C.M.: A primer on the GDPR: what you need to know. Privacy Law Blog (2015). Available http://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/ [Online]
18. Frumento, E., Freschi F., et al.: Yet Another Cybersecurity Roadmapping Methodology, FCCT 2015, The First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism, http://ieeexplore.ieee.org/document/7299984/
19. FBI Malware warning issued over CryptoWall Ransomware, in *Health care Data Security*, HIPAA J. (2015). Available http://www.hipaajournal.com/fbi-malware-warning-issued-over-cryptowall-ransomware-7095/ [Online]
20. Why cybercriminals target health care data, in Help Net Security (2016). Available: https://www.helpnetsecurity.com/2016/01/28/why-cybercriminals-target-healthcare-data/ [Online]
21. The need for increased investment in medical device security, in State of Security (2017). Available: https://www.tripwire.com/state-of-security/featured/need-increased-investment-medical-device-security/ [Online]
22. "Health care Breach Report 2017", Bitglass
23. HL7 Data Interfaces in Medical Environments: The State of Security (2017). Available: https://www.tripwire.com/state-of-security/security-data-protection/hl7-data-interfaces-in-medical-environments/ [Online]
24. Chesla, A.: Why advanced attack campaigns like security silos (2016). Available http://www.securityweek.com/why-advanced-attack-campaigns-security-silos [Online]
25. Vaas, L.: Hospitals vulnerable to cyber-attacks on just about everything. In: Naked Security (2016). Available: https://nakedsecurity.sophos.com/2016/02/26/hospitals-vulnerable-to-cyber-attacks-on-just-about-everything/ [Online]
26. Security, H.N.: Why cybercriminals target health care data. In: Don't miss, Help Net Security (2016). Available: https://www.helpnetsecurity.com/2016/01/28/why-cybercriminals-target-healthcare-data/ [Online]
27. Hospitals in UK National Health Service knocked offline by massive ransomware attack (2017). Available: http://www.healthcareitnews.com/news/updated-hospitals-uk-national-health-service-knocked-offline-massive-ransomware-attack [Online]

28. H2020, Work Programme 2018–2020: (2017). Available http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-intro_en.pdf [Online]
29. AA. VV.: Combatting cybercrime and cyberterrorism challenges, trends and priorities. In: Akhgar, B., Brewster, B. (eds.) Advanced Sciences and Technologies for Security Applications, 1st edn. Springer (2016). Available: http://link.springer.com/book/10.1007/978-3-319-38930-1 [Online]
30. "Cybercrime as a business: The digital underground economy", Europol, https://www.europol.europa.eu/newsroom/news/cybercrime-business-digital-underground-economy
31. Samani, R., Paget, F.: Cybercrime Exposed—Cybercrime as a Service. McAfee (2014)
32. Kurt, T., et al.: Framing dependencies introduced by underground commoditization. In: Workshop on the Economics of Information Security. Available: https://cseweb.ucsd.edu/~savage/papers/WEIS15.pdf [Online]
33. Higgins, K.J.: No, The Mafia Doesn't Own Cybercrime: Study (2018)
34. Ariu, D., Frumento, E., Fumera, G.: Social engineering 2.0: a foundational work: Invited Paper. In: Proceedings of the computing frontiers conference—CF'17, pp. 319–325 (2017)
35. How Modern Email Phishing Attacks Have Organisations on the Hook. IronScales (2017). Available http://bit.ly/2wyv1TJ [Online]
36. The Human Factor. ProofPoint (2016). Available http://bit.ly/2wypeO3 [Online]
37. 2017 Data Breach Investigations Report 10th Edition, Verizon (2017). Available http://vz.to/2wyod8C [Online]
38. Frumento, E.: CopyPhish: a recent case of a successful contextualized phishing attack which resulted in stealing the entire IP of a SME and damaged also their reputation. DOGANA Project (2017). Available http://bit.ly/2wyjF2b [Online]
39. Mullen, M.: Ransomware: Attack hits 150 countries, Europol says world is in 'disaster recovery mode'. CNNMoney (2017). Available http://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/index.html?iid=EL [Online]
40. Defray—New Ransomware Targeting Education and Health care Verticals. Proofpoint.com (2017). Available https://www.proofpoint.com/us/threat-insight/post/defray-new-ransomware-targeting-education-and-healthcare-verticals [Online]
41. The Unlocked Backdoor to Health Care Data, Help Net Security (2016). Available: http://www.net-security.org/secworld.php?id=17062 [Online]
42. Damage Control: The Cost of Security Breaches. Kaspersky Labs (IT Security Risks Special Report Series) (2015). Available http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf [Online]
43. Hiltzik, M., Times, L.A.: Anthem is warning consumers about its huge data breach. Here's a translation. Los Angeles Times, LA Times (2015). Available http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html [Online]
44. Anatomy of a health care data breach. Prevention and remediation strategies. ClearDATA (2015). Available http://net-security.tradepub.com/free/w_clec01/prgm.cgi?a=1 [Online]
45. Koroneos, G.L.: Enterprise Tech Spotlight: Wearable Security, Phishing Targets, Health Care Data Breaches. Verizon (2015). Available http://news.verizonenterprise.com/2015/06/wearable-security-phishing-healthcare-networkfleet/ [Online]
46. Barney, B.: Health Care: Recognize Social Engineering Techniques. Security Metrics Blog (2015). Available http://blog.securitymetrics.com/2015/08/healthcare-social-engineering.html [Online]
47. Cook, C.: The rise of multifaceted social engineering attacks. Social-Engineer.Com (2015). Available https://www.social-engineer.com/rise-multifaceted-social-engineering-attacks/ [Online]
48. Federation of European Risk Management Associations (FERMA), "Response to the European Commission consultation on the public-private partnership on cybersecurity and possible accompanying measures", FERMA, 2016
49. Ossola, A.: Hacked medical devices may be the biggest cyber security threat in 2016. Popular Science (2015). Available: http://www.popsci.com/hackers-could-soon-hold-your-life-ransom-by-hijacking-your-medical-devices [Online]

50. Peachey, P.: Cybercrime: first online murder will happen by end of year, warns US firm. The Independent - News (2014). Available http://www.independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774955.html [Online]
51. Sjouwerman, S.: Health care Industry Needs Prescription For Next Wave of Ransomware Threats. Blog.knowbe4.com (2017). Available https://blog.knowbe4.com/healthcare-industry-needs-prescription-for-next-wave-of-ransomware-threats [Online]
52. Frumento, E.: Which could be the consequences of a social engineering attack? http://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/9-which-could-be-the-consequences-of-a-social-engineering-attack
53. Alton, L.: Medical technology is advancing, but how secure is it? (2017) IT Pro Portal. Available at https://www.itproportal.com/features/medical-technology-is-advancing-but-how-secure-is-it/ [Online]
54. Newman, L.: Medical Devices Are the Next Security Nightmare. WIRED (2017). Available at https://www.wired.com/2017/03/medical-devices-next-security-nightmare/ [Online]
55. Mearian, L.: Many hospitals transmit your health records unencrypted. Computerworld (2017). Available: https://www.computerworld.com/article/3110506/healthcare-it/many-hospitals-transmit-your-health-records-unencrypted.html [Online]
56. U.K. Hospitals Hit in Widespread Ransomware Attack. Krebs on Security (2018)
57. Bisson, D.: WannaCryptor Ransomware Strikes NHS Hospitals, Telefonica, and Others. The State of Security (2018)
58. Carpenter, P.: Chief Strategy Officer at Knowbe4 reported: "Until we harden our people and our systems sufficiently, ransomware will continue to prove successful and gain more momentum. The vector they will continue to use is the human that will click on something or download something"
59. Nadeau, M.: 5 biggest health care security threats for 2018 (2018). CSO Online [Online]
60. Korolov, M.: 10 companies that can help you fight phishing. CSO Online (2018)
61. Allen, A.: Billions to install, now billions to protect. Politico (2015). Available http://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432 [Online]
62. "Healthcare security $65 billion market", https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/
63. Catalano, A.: Maintaining security during your health care merger or acquisition. Help Net Security (2016). Available http://www.net-security.org/article.php?id=2356 [Online]
64. More than 75 percent of U.S. Adults express concern about security of health care data, reveals university of phoenix survey. University of Phoenix (2015). Available http://www.phoenix.edu/news/releases/2015/10/us-adults-concerned-about-security-of-health-care-data.html [Online]
65. Small health care facilities unprepared for a data breach. Help Net Security (2016). Available http://www.net-security.org/secworld.php?id=17516 [Online]
66. Security risks of networked medical devices. Help Net Security (2016). Available http://www.net-security.org/secworld.php?id=18105 [Online]
67. Dawson, M., Omar, M.: New threats and countermeasures in digital crime and cyber terrorism, 1st edn. IGI Global (2015)
68. Harrison, K., White, G.: A Taxonomy of Cyber Events Affecting Communities (2011). Available https://www.computer.org/csdl/proceedings/hicss/2011/4282/00/04-06-01.pdf [Online]
69. Veerasamy, N., Grobler, M., Von Solms, B.: Building an Ontology for Cyberterrorism (2012). Available http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.456.4088&rep=rep1&type=pdf [Online]
70. Knudson, J.: Health care information: the new terrorist target. For The Record **25**(6), p. 10 (2013). Available http://www.fortherecordmag.com/archives/0413p10.shtml [Online]
71. G.V.P. Company: Health care information: The new terrorist target. Available: http://www.fortherecordmag.com/archives/0413p10.shtml [Online]
72. Peachey, P.: Cybercrime: first online murder will happen by end of year, warns US firm. The Independent - News, Independent (2014). Available http://www.independent.co.uk/life-

style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-us-firm-9774955.html [Online]
73. Harries, D., Yellowlees, P.M.: Cyberterrorism: is the U.S. Health care system safe? Telemedicine e-Health **19**(1), 61–66 (2013)
74. ISE, "Hacking Hospitals", https://www.securityevaluators.com/hospitalhack/
75. Franken, H.: Increasing co-operation against cyberterrorism and other large- scale attacks on the Internet. Committee Culture Sci Educ Media 2015. Available http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21806&lang=en [Online]
76. Health care industry: Attacks outpacing investments in personnel, education and resources. Help Net Security (2018) [Online]
77. Cook, J., Wall, T.: New work attitude measures of trust, organizational commitment and personal need non-fulfilment. J. Occup. Psychol. **53**(1), 39–52 (1980)
78. Hadnagy, C.: Unmasking the social engineer: the human element of security, P. K. F, Ed. Wiley, United States (2014)
79. Gilbert-Lurie, M.: Are you in a codependent relationship with your phone? Science says the struggle is definitely real. Bustle [Online]
80. Chang, L.: FOMO is a real thing, and it's adversely affecting teens on social media. Social Media, Digital Trends (2015)
81. Dachis, A.: How to plant ideas in someone's mind. LifeHacker (2014)
82. The Human Factor 2018. Proofpoint (2018)
83. Frumento, E., Lucchiari, C., Valori, A., Pravettoni, G.: Cognitive approach for social engineering. DeepSec (2010)
84. Clayton, R.B., Leshner, G., Almond, A.: The extended iSelf: the impact of iPhone separation on Cognition, emotion, and physiology. J Comput Mediated Commun **20**(2), 119–135 (2015)
85. Harley, D., Willems, E., Harley, J.: Teach your children well. ICT Security and the Young Generation. In: Proceedings of virus bulletin conference (2005)
86. Is cybersecurity awareness a waste of time? New Zealand Reseller News (2018)
87. Qin T., Burgoon, J.K.: An investigation of Heuristics of human judgment in detecting deception and potential implications in countering social engineering. IEEE Intelligence and Security Informatics (2007)
88. Kirlappos, I., Sasse, M.A.: Security education against phishing: a modest proposal for a major rethink. IEEE Sec Priv Mag **10**(2), 24–32 (2012)
89. Sjouwerman, S.: KnowBe4 reveals industries most at risk of phishing attacks. Blog Knowbe4 (2018)
90. Kerber, R., Jessop, S.: Asset managers urged to make cyber risk top priority. Available at http://www.insurancejournal.com/news/national/2015/09/01/380095.htm (2015)
91. Riddle, B., Nyman, S., Rees, J.: Estimating the costs of a data breach: an exercise at the new Hampshire state cancer registry (2011)
92. Langner, R.: To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve the Langner group. Langner (2013)
93. Nakamura, L.: A trillion dollars a year in intangible investment and the new economy. In: J.R.M. Hand, B. Lev (eds) Intangible Assets. Oxford University Pres, Oxford (2003)
94. Bounfour, A.: The Management of Intangibles: The Organisation's Most Valuable Assets. Routledge, United Kingdom (2003)

Chapter 5
A Data Protection Perspective on Training in the mHealth Sector

Erik Kamenjasevic and Danaja Fabcic Povse

Abstract The mHealth services have brought to the healthcare operators, professionals and patients numerous advantages and, at the same time, opened a door to new cyber-threats that might have a significant influence on patient's health and life. Often, cyber-attacks are successful due to a human error and a poor knowledge about the cyber-security. Therefore, deploying innovative trainings of healthcare professionals could lead to a higher level of the cyber-resilience. This chapter explores how the healthcare operators may do so in a legally compliant manner by examining the implications of the new General Data Protection Regulation.

5.1 Introduction

Adoption of mobile health services (mHealth) is exponentially growing in the last years due to broad acceptance and usage of smartphones, tablets, and computers. Thus, the healthcare operators (i.e., hospitals) use information technology to increase the efficiency of providing healthcare services. They usually impose the usage of such technology to healthcare professionals (i.e., physicians, nurses) in order to deploy information exchange more efficiently (for instance, via electronic health records) as well as to conduct monitoring and to provide the operational support.

Healthcare professionals are the main users and adopters of the technology who often do not have an appropriate knowledge of how to best use such technology. This consequently makes them vulnerable to falling victims of cyber-attacks. Such statement is further supported by the fact that the healthcare sector is the one that is the most frequently targeted by hackers.[1] These cyber-attacks influence patients,

[1] Arndt [2].

E. Kamenjasevic (✉) · D. F. Povse
The KU Leuven Centre for IT & IP Law (CiTiP), Leuven, Belgium
e-mail: erik.kamenjasevic@kuleuven.be

D. F. Povse
e-mail: danaja.fabcic@kuleuven.be

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_5

the healthcare operators and the healthcare professionals. On the one hand, patient's fundamental right and reasonable interest are to have her health data protected from the unauthorized or unwanted purposes since their disclosure might have a negative impact on her personal and professional life. On the other hand, healthcare operators and professionals collect very sensitive personal data, which is among the most intimate information about their patients and whose disclosure or loss might be critical for patient's life. According to the General Data Protection Regulation (the GDPR),[2] data concerning health belong to special categories of personal data.[3] It is defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".[4] It is crucial that the sensitive data are kept safe and secure during storage, transmission, and processing. Article 32 of the GDPR requires that technical and organizational measures are put in place in order to ensure an appropriate level of security of personal data in the course of a data security policy.[5] Training, as part of organization-wide measures, can raise the level of cybersecurity within an organization[6] and make an important contribution towards complying with the security requirements. European Cyber Security Agency stated in its recent Healthcare Sector Report [7] that one of the main needs within the eHealth "entails improving the skills both technical and behavioral of the personnel via **innovative training techniques** that are well received by the (non-IT-expert) workforce. The awareness level in cyber security aspects for all levels of healthcare personnel, e.g., nurses, technicians, administrative personnel and doctors, is an important aspect. The user is most often the weakest link when attacking the target".[8] Development of the innovative trainings is necessary for several reasons. First, their goal is to protect the patients' data concerning health which consequently means also protecting their reputation and trust in the system, preserving the reputation of the healthcare operator as well as avoiding direct and indirect costs [9] that cyber-data breaches may cause. Second, due to new threats stemming from the so-called social engineering 2.0 [10] where the main cyber-targets are humans instead of ICT domain, a successful training has to be designed in a way that decreases the impact of the above mentioned phenomenon by empowering the cyber-knowledge of targets. In other words, the training should be designed to focus on the human element of security, across the complete healthcare

[2]Reference [38].

[3]Ibid, Articles 4(15) and 9.

[4]Ibid, Article 4(15).

[5]Reference [3], WP250 p. 6.

[6]Ref [6].

[7]ECSO [17].

[8]Ibid, p. 8.

[9]Meisner [36]. In her article, Meisner draws a hypothetical situation regarding financial cost of cyber data breach in Polish hospital. These costs include forensic investigation, breach notification, post-breach patient protection, attorney fees and litigation expenses, regulatory compliance, cybersecurity improvements, loss of reputation and patients churn, other potential costs that would in total amount up to around 2.5 million euros.

[10]See, for example: Ariu D et al. [1].

supply chain, while taking into account the fact that humans are the main means of healthcare operator's exposure to cyber-risks as well as the main barrier to the spread of these risks. Third, the training should be tailored according to the trainee's personality and behavioral traits, hierarchical position, context of training and cybersecurity level. Finally, training's tailoring should take into account a reduction of the prioritized human-related cyber-risks and associated risks. The main question we ask in this chapter is what are the implications of the new GDPR in training healthcare professionals within the context of cybersecurity in adapting to a new mHealth environment. In order to answer it, we will examine the applicable legal framework on the European Union level. More specifically, we will focus on the novelties introduced by the GDPR which became applicable as of May 25, 2018. We will draw upon the research carried out in the DOGANA and COMPACT projects. We contribute this chapter in order to raise awareness of the legal challenges the healthcare operators and professionals will be facing when deploying the awareness trainings as well as to inform the legal practitioners and policy makers in the field about new challenges imposed by the Regulation.

5.2 Legal Framework

5.2.1 When Do Data Protection Rules Apply?

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller[11] or a processor[12] in the European Union, regardless of whether the processing takes place in the EU or not.[13] Processing means any operation or set of operations performed on personal data (such as collection, storage, use, erasure, etc.).[14] Personal data is considered to be any information relating to an identified or identifiable natural person (a data subject).[15] GDPR makes a distinction between "normal" personal data and special categories of personal data. Data concerning health belong to the latter group. The level of sensitivity with regards to the two categories of personal data is different, hence, different levels of protection apply to each of them. Such distinction becomes relevant especially in the context of mHealth due to development of a number of well-being and lifestyle

[11] Article 4(7) of the GDPR: "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

[12] Article 4(8) of the GDPR: "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

[13] Articles 2 and 3 of the GDPR.

[14] Article 4(2) of the GDPR.

[15] Article 4(1) of the GDPR.

apps.[16] Therefore, the definition of the data concerning health foreseen in the GDPR should be interpreted broadly. First, that is the data which concern physical or mental health status of a data subject that is generated in a professional/medical context. This also includes the data that is generated by devices or apps used in a professional medical context irrespective of their qualification as a medical device. Further on, data concerning health is also considered to be the data relating to the health status of a person but is not considered to fall within the former category (i.e., information about smoking and drinking habits or one's membership in a patient support group). This should also include data that is being used in the health-related administrative contexts and information about the purchasing of medical products, devices and services.[17] Third, certain data may at first seem as not revealing information about person's health but it may become health-related data when "(a) collected to in aggregated form make assumptions on a person's health, (b) are combined with other health related data or (c) are transferred to certain third parties.[18] In other words: when personal data (health-related or not) are used with the purpose of identifying the health status of an individual, these data will be qualified as health data".[19] Hence, it is important to highlight that "data which outside of the medical context would maybe not even qualify as personal data will depending on the purposes of the data processing after all be qualified as sensitive data".[20] Finally, such broad definition of data concerning health goes in line with the Recital 35 of the GDPR.

5.2.2 To Whom Do Data Protection Rules Apply

In the context of this chapter, a healthcare operator will have a role of a data controller when it determines the purpose and means of the processing of personal data. For instance, this will be the case every time the operator collects and uses information about its patient in order to decide which medication to prescribe. This will also be the case when it processes information about its employees who are participating in the cyber-training. The healthcare operator may as well decide to outsource performing of a training to an external organization who will be, in such case, acting as a processor. Further on, healthcare professionals whether employed by the hospital, or acting as external consultants, are considered employees (and data subjects) in the eyes of the data protection legislation.[21] This means that the GDPR applies to them in its entirety; nevertheless, under its Article 88, Member States may regulate certain aspects of data protection in an employment context. Such rules must safeguard the data subject's human dignity, legitimate interests, and fundamental rights, especially

[16] See, for example, Martnez-Prez et al. [37].

[17] Verhenneman et al. [45].

[18] Ibid, p 29.

[19] Veale and Binns [44].

[20] Verhenneman et al. [45].

[21] See Ref. [9].

regarding transparency, transfers of personal data, and monitoring systems put in place.[22] For example, under the new German data protection act,[23] employees' personal data may be processed for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council.[24]

5.2.3 Data Protection Principles

Data protection principles constitute the guidance for striking the right balance between the data protection of the employees participating in the training and the protection of the company's (cyber) security. The principles have not changed significantly with respect to prior rules in the Data Protection Directive (the DPD).[25] Namely, lawfulness, fairness and transparency principle, purpose limitation principle, data minimization principle, accuracy, storage limitation, and integrity and confidentiality principle are embodied in Article 5(1) of the GDPR and they should apply to any information concerning identified or identifiable person.[26] In the training context, special attention is given to the principles of purpose limitation principle and data minimization (both known under the umbrella name of the data quality principle). Purpose limitation principle requires from data controllers to collect the data for specific, explicit and legitimate purposes and not to process the data in a manner that is incompatible with those purposes (unless one of the exception applies). Data minimization principle states that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The main innovative step of the GDPR concerns the principle of accountability established by Article 5(2) and further detailed in Article 24 of the GDPR. It requires controllers to put in place "appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing meets the requirements"[27] of the law. In fact, this principle requires from a data controller to adopt a proactive role in ensuring the protection of personal data through appropriate technical and organizational measures and to be able to demonstrate compliance with the data protection requirements. In order to implement this principle successfully, controllers are rec-

[22] The implementation of specific rules is slow. An overview (from December 2017) is available here: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=9350, and here (from May 2018): https://iapp.org/resources/article/eu-member-state-gdprimplementation-laws-and-drafts/. Reference [22].

[23] Reference [10].

[24] Section 26(1) of the Federal Data Protection Act.

[25] Reference [15].

[26] Recital 26 of the GDPR.

[27] Article 24 of the GDPR.

ommended to adopt internal data protection policies and to promote cybersecurity awareness initiatives among their employees, for example through programs, trainings, and procedures that will help integrating employees' cyber security awareness into the process of corporate culture.

5.2.4 Security Measures and Security Policies

Similar to Article 17 of the DPD, GDPR requires controllers and processors to implement technical and organizational measures to ensure a level of security of personal data appropriate to the risk such as loss or unauthorized access, destruction, use, modification, or disclosure of the data. Article 32 of the GDPR suggests the security measures that might be considered 'appropriate to the risk', such as the pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to ensure the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Such list of measures is not exhaustive and a controller still has a duty to identify the adequate measures to put in place since the controller itself is in the best position to judge what would be an appropriate level of security while at the same time taking into account the state of the art and costs of their implementation. Finally, under the principle of security of processing, controllers have a duty to notify any breach of personal data to the supervisory authority and in certain cases to the data subject as well.[28] Company security policies consist of a combination to manage processes, people, and technologies in order to implement robust security values and to protect confidentiality, integrity, and availability of information and other valuable assets.[29] Policies, procedures, and training information need to be developed and documented in order to be easily accessible to all employees. Such documentation should explain the goals and the requirements (concerning but not limited to cyber-security), specifications of the technology and services that will be used and instructions on how to use devices/services, such as mHealth apps. The company should take a proactive role and focus on the development of information policies concerning (cyber)security as well as policies based on the solutions and techniques that will be implemented once the training has been deployed.[30] Following security policies should be carefully considered and implemented when deploying the training within the healthcare operators[31]:

[28] Articles 33 and 34 of the GDPR.
[29] Wu [42].
[30] Vogiatzoglou et al. [47].
[31] Custodio [12].

- Trainees must be fully informed through the corporate security policies about the possibility of conducting the training.
- All data must be traceable at any moment and it must be possible to identify in a human-readable report all personal data about an individual and the identity of the owner of data stored within the system.
- The system must allow deleting personal data of an individual. Data that is collected but not used for the training purposes must be deleted immediately.
- Data stored in a system may be kept according to the retention times matching national legal requirements where the training is taking place.
- Only publicly available, non-sensitive, professional data about trainees should be collected. All other data that cannot be categorized as professional must be discarded.
- All operations must be logged with the information about the date, time, location, system, user and action performed on data. Logs must be kept in order to conduct an independent verification of all actions performed on personal data through all the processing stages.
- System used within the training scheme for personal data storage and processing must be in line with ISO 27001 standard or another third-party verification scheme.
- Data controller has to be appointed within the organization deploying the training who has to provide answers to queries of individuals about their information.
- Access to personal data within the training must be subject to user authentication. Access level should be allowed only to authorized individuals.
- Personal data and the training results must be anonymized as soon as the state of the art technique allows it.

5.3 Playing by the Rules

Training deployment involves personal data processing in several phases. First, participants are chosen from among the employees and a specific type of (cyber-awareness) training is ascribed to them, which can lead to questions about profiling and automated decision-making. Second, employees' consent is rarely free, hence, this raises questions about appropriate legal grounds. Third, under the GPDR, the participants should be able to exercise the rights they have as data subjects, in a training context.

Not necessarily all the healthcare professionals within one healthcare operator will be trained. In the recruitment process, certain employees will be chosen and we will refer to them as "participants", "trainees", "employees", and 'healthcare professionals' interchangeably.

5.3.1 Choice of Participants and Appropriate Training

Employees' cyber-habits may vary due to their different personalities, human characteristics, and traits.[32] For example, students majoring in engineering tend to have more secure passwords than humanities majors, and extroverts are more likely to lock their devices than introverts. Due to those different factors, not everyone responds as effectively to a certain type of training.[33] Therefore, participants are categorized and trained accordingly. This is referred to as profiling.[34] The GDPR defines profiling in Article 4(4) as: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements". Three elements are important for this definition: (1) there must be automated processing, (2) that is carried out on personal data, and (3) such processing is carried out in order to evaluate personal aspects about a natural person.[35] It is important to point out that automated processing does not mean that the processing is done exclusively by a computer on the contrary, even if a human is involved in the categorization activities, they still fall under the definition. Categorization as such falls under this provision, even if there is no further inference or correlation involved.[36] As stated in Recital 72 of the GDPR, profiling is subject to the rules governing the processing of personal data, such as the legal grounds for processing or data protection principles. Therefore, when profiling physicians for training, the healthcare operator must ensure that its actions are compliant with the GDPR. For example, when using the already available data on employees' personal characteristics, compliance with the purpose limitation principle must be assessed. This means that the new purpose, i.e., profiling for training objectives, must be compatible with the original purpose, for which the data had been provided, for example, a personality test during the recruitment process.[37] Several criteria need to be taken into account to assess whether the secondary purpose is compatible with the original one; inter alia, whether there is an appropriate relationship between two purposes and whether the employee could have expected such further processing.[38]

Furthermore, the categorization of employees should not be done according to discriminatory criteria. Definitions of discriminatory criteria vary: for example, disparate treatment based on an individual's race, color, religion, sex, or national origin, according to the US Civil Rights Act[39]; the European Convention on Human Rights

[32] Gratian et al. [26]; Cain et al. [11].

[33] Gratian et al. [26].

[34] Reference [3].

[35] Ibid, p. 6.

[36] Unlike the prohibition of automated decision-making, which applies solely to purely automated processes, without human intervention.

[37] Reference [4].

[38] Ibid.

[39] Reference [43]. See also Gold [25].

prohibits discrimination, based on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status[40]; the proposed Equal Treatment Directive of 2008 mandates equal treatment outside the labor market, irrespective of age, disability, sexual orientation or religious belief. Discrimination is often mentioned together with unequal or disparate treatment, based on the above criteria.[41,42]

Categorisation can be carried out manually, by a human, or by a machine using an algorithm, or a combination of both, for example when the human relies on the decision made by the machine. While humans are fallible and biased, being treated solely by a machine in a'computational manner' in other words, as nothing but a number, is considered dehumanizing in Europe.[43] Moreover, while profiling and categorization promote accuracy in decisions, improved risk management and fraud prevention,[44,45] they also perpetuate discrimination and stereotypes. Even if there is no original intent to discriminate, the effects can still materialize when the algorithm learns to discriminate based on the data it has been fed with.[46] Hence, as the selection process is based on categorisation, certain safeguards should be put in place. For example, the employees should be aware of when and how the categorisation works in order to reduce the knowledge asymmetry between them and the decision-maker,[47] transparency should be ensured and meaningful information given[48] in order to comply with the information requirements set out in Articles 13 and 14 of the GDPR.

5.3.2 Ensuring Transparency

Participants involved in training must be notified about the processing of their personal data, their rights as data subjects, as well as other information, provided for in the Articles 13, 14, and 15 of the GDPR. These three articles provide for the

[40] See European Convention on human rights and its Protocol No. 2: https://www.echr.coe.int/Documents/ConventionENG.pdf. Reference [20].

[41] For example, in Ref. [19].

[42] One of the most debated criteria in Europe is gender. The European Court of Human Rights has recently confirmed that "the advancement of gender equality is today a major goal in the member States of the Council of Europe" and that justification for disparate treatment based on gender must pursue a legitimate aim and be justified with "very weighty reasons". A new Directive, addressing inequality and mandating equal treatment even between individuals, i.e., in the workplace, has been proposed by the European Commission. However, it has been debated for the last ten years and is currently being blocked by the Council. In that regard see, for example, Refs. [18] [34].

[43] Jones [32].

[44] Le-Khac et al. [35].

[45] Kamp et al. [33].

[46] Schermer [40].

[47] Gutwirth and Hildebrandt [27].

[48] See among others: Van der Hof and Prins [46]. Selbst and Powles [41].

provision of information to data subjects in three different situations. In the training context, personal data can come directly from the participants, for example when their improving skills are being monitored; or from a different source, for example from the HR department, which provides the trainers with the information on what kind of personality traits the participants have, or from their publically available social media profiles. Alternatively, the trainees can require access to their own personal data from the healthcare operator about the training they are undergoing, according to the Article 15 of the GDPR. In either scenario, the information must be provided in a clear and concise manner, in an easily understandable language. Infographics are often used since they are easier to read than a wall of text. Namely, the list of information the controller must provide is long and covers information, such as categories of data processed, the contact details of the data protection officer, time limitation for deletion of data, the existence of automated decision-making, etc.[49]

Whether or not the information duties include the data subject's right to an explanation[50] through ensuring transparency, the healthcare operator should also make sure the trainees know why they were chosen to participate and why they were assigned to a specific type of training. This information must be given either at the time of collection of personal data directly from the trainee. If the data come from a different source, then it must be done within a month of obtaining them. The notification is easily done before the training starts, and kept up throughout the training. Moreover, the transparent procedure should enable the trainees to exercise their rights as data subjects.[51] Since healthcare operators process sensitive personal data in the course of their business, they are required to, according to Article 37 of the GDPR, appoint a data protection officer who acts as a contact point for employees and other data subjects (especially the patients) and facilitates the exercise of their rights. Therefore, it is crucial that the DPO's name and contact details are communicated to the participants in due course of the training[52].

5.3.3 Legal Grounds

(a) Consent

Under the GDPR, consent must be freely given, specific, informed and unambiguous in order to be valid.[53] This means giving the trainee a genuine choice in giving or denying consent to participation in training as well as control over the processing.

[49] See Art. 13, 14 and 15 of the GDPR, and the Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, WP260rev.01, adopted on 29 November 2017 and as last revised and adopted on 11 April 2018. Reference [8].

[50] Due to inconsistencies and unclear wording, it is contentious whether the right to an expla- nation exists in the GDPR. See: Selbst and Powles [41]; see also Wachter et al. [48].

[51] Reference [5].

[52] Reference [6].

[53] See Article 4(11), Article 6(1)(a) and Article 7 of the GDPR.

However, due to power dynamics and lack of power balance between the employer and the employee, and the likelihood of the employees facing prejudice when they refuse to give consent, consent cannot be given freely and cannot be relied upon as legal grounds in the employment context[54]. Moreover, training can also be provided in the form of fake phishing attacks against healthcare professionals. Since this type of training must be as close to a real phishing attack, it would be unrealistic to deploy a phish against an aware (and consenting) target. Participants may be told they are taking part in some kind of a study, but are instead attacked with a phishing email. In research, this technique is called deception[55]. Deception can cause participants to feel distressed, humiliated and lose their trust in the employer, who seems to be sending them risky emails. Therefore, it is very important that the participants are fully debriefed about the reasons behind the phishing attack after it has been carried out; as well as given an opportunity to optout, thus giving effect to the right to object to processing, enshrined in Article 21 of the GDPR.[56]

(b) Alternatives: legitimate interest and compliance with the legal obligation

Alternative legal grounds can be found in paragraphs (c) and (f) of Article 6 of the GDPR. Namely, processing is lawful if it is necessary for compliance with a legal obligation to which the healthcare operator is subject, or if processing is necessary for the purposes of the legitimate interests pursued by the healthcare operator. In both instances, processing must be necessary—the goal (ensuring cybersecurity) cannot be reached with a less invasive measure, without processing personal data (or, in different words, without training the employees). However, due to human element's role, it would not be feasible to implement cybersecurity measures without training the employees. Nonetheless, where two or more alternative trainings are available, the less intrusive one should be chosen, so long as it contributes to the objective. Legitimate interests as such are not defined in the GDPR. Nevertheless, the GDPR provides few examples of situations that count as legitimate interests. This is the case when the data subject is a client or in the service of the controller and when the former can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.[57] More specifically, running and maintaining a website,[58] preventing fraud, direct marketing purposes, processing employees' data within a group of undertakings for internal administrative purposes, as well as for ensuring network and information security,[59] fall under the notion of legitimate interests. However, when ensuring network and information security, the processing must only be done to the extent strictly necessary and proportionate (for example, monitoring access to an email address but not its correspondence[60]).

[54] Reference [7].

[55] Finn and Jakobsson [24].

[56] Resnik and Finn [39].

[57] Recital 47 of the GDPR.

[58] Reference [14].

[59] Recitals 47 and 48 of the GDPR.

[60] IAPP [30].

Reliance on legitimate interests of the controller comes with one more caveat; if the data subject's fundamental rights and interests outweigh those of the controller, then the latter cannot rely on this legal basis. Since training healthcare professionals to adapt to a new mHealth environment can drive down the costs and provide better service to the patient, such interests can be considered legitimate in the sense of the GDPR. After all, prominent international and regional treaties and documents, such as the constitution of the World Health Organisation and the European Social Charter [21],[61] contain reference to the health-related rights and the need to provide the highest possible standard of health (care) attainable. It is not very likely that a single healthcare professional's fundamental rights and freedoms would outweigh a common human concern; nonetheless, this balance should be continually assessed.[62]

Alternatively, the healthcare operator can rely on processing being necessary for compliance with a legal obligation to which it is subject. Such a legal obligation and the purpose of processing can be found on European Union level or in national law.[63] In European Union law, the Network and Information Systems Directive (the NIS Directive)[64] provides that operators of essential services, to whom healthcare operators can belong under certain conditions,[65] must take appropriate and proportionate technical and organizational measures in order to counter the risks against the networks. Training healthcare professionals and raising awareness of cybersecurity can help in complying with this requirement, as the Recital 38 of the Directive suggests. However, the processing of personal data must not go beyond what is necessary to attain the goal pursued, otherwise this cannot be considered as valid legal grounds.

5.4 Conclusion

Healthcare operators play a highly important role in our society. Central to them are the patients whose data is collected, used, and processed by healthcare professionals every day. At the same time, those who are dealing with the sensitive data the most are considered to be the weakest link in the organizational cyber-security chain. As a consequence, the healthcare professionals are considered to be the main facilitator of cyber data breaches that may have a significant impact on patients' private and personal life. Meanwhile, if trained appropriately they can act as the main shield against the cyber-threats.

---

[61] See Part I. 11 of the ESC: Everyone has the right to benefit from any measures enabling him to enjoy the highest possible standard of health attainable.

[62] IAPP suggest a LIA legitimate interests assessment, and provide a template. See Ref. [31].

[63] Art. 6(3) of the GDPR.

[64] Directive (EU) [16], available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L.2016.194.01.0001.01.ENG.

[65] Healthcare operators are subject to the NIS directive if they meet the criteria, laid down in its Article 5, and those in point (g) of Article 3 of Directive 2011/24/EU.

Traditional ways of ensuring cybersecurity within the organization do not pay enough attention to the human factor. One of the solutions to improve the cyber-knowledge of the healthcare professionals is to provide them with innovative trainings tailored according to their personal traits and habits in order to raise their awareness about cyber-threats, consequences that cyber-attacks may provoke, how to timely detect them and finally how not to fall victims to them. By deploying the cyber-training of its professionals, a healthcare operator may be in a position to better understand the current threats against it by measuring the actual risk and to find potentially effective and tailored countermeasures to mitigate the cyber-risk.

Acknowledgements The research leading to these results was partially funded by the European Union's Horizon 2020 Research and Innovation program as the **DOGANA project (aD- vanced sOcial enGineering And vulNerability Assessment)**, under grant agreement No. 653618 and **COMPACT (COmpetitive Methods to protect local Pub- lic Administration from Cyber security Threats)**, under grant agreement No. 740712.

References

1. Ariu, D., et al.: Social Engineering 2.0: A Foundational Work, Proceedings of ACM Computing Frontiers conference, 2017, available at: https://www.dogana-project.eu/images/PDFFiles/ComputingFrontiers17DAriufinal.pdf
2. Arndt, R.Z.: In Healthcare, Breach Dangers Come From In-side the House, Modern Healthcare 2018, available at: http://www.modernhealthcare.com/article/20180410/NEWS/180419999. For example, more than 20% of the reported data breaches are due to a human error. At the same time, around 13% of reported data breaches concerned celebrities healthcare records that are of particular interest to hackers
3. Article 29 Data Protection Working Party, Guidelines on Automated individual decision- making and Profiling for the purposes of Regulation 2016/679
4. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013
5. Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, WP260rev.01, adopted on 29 November 2017 and as last revised and adopted on 11 April 2018
6. Article 29 Data Protection Working Party, Guidelines on data protection officers (DPO), WP243, 13 December 2016
7. Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, [1]WP259 rev.01, adopted on 28 November 2017 and as last revised and adopted on 10 April 2018
8. Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250 p. 6
9. Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, adopted on 8 June 2017, 17/EN, WP249, available at https://ec.europa.eu/newsroom/article29/document.cfm?action=display&docid=51030
10. Bundesschutzgesetz.: For English Translation see https://iapp.org/media/pdf/resourcecenter/Eng-trans-Germany-DPL.pdf
11. Cain, A., Edwards, M., Still, J.: An exploratory study of cyber hygiene behaviors and knowledge, J. Info. Sec. Appl. **42** (2018). http://www.sciencedirect.com/science/article/pii/S2214212618301455
12. Custodio, F.: DOGANA D5.2 Legal Requirements for Privacy by Design, 2016 pp. 10–12, available at: https://www.dogana-project.eu/images/PDF Files/D5.2-Legal-Requirements- for-Privacy-by-Design.pdf

13. Court of Justice of the European Union, Case C210/16, Unabhngiges Landeszentrum fr Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, 05.06.2018
14. Court of Justice of the European Union, case C 582/14, Patrick Breyer v. Bundesrepublik Deutschland
15. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
16. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
17. ECSO, Cyber Security for the Healthcare Sector, WG3, Sectoral Demand, 2018
18. Boyraz, E.: v. Turkey, ECtHR judgment of December 2 2014, 54
19. European Union Agency for Fundamental Rights, Fundamental Rights Report 2018
20. European Convention on Human Rights
21. European Social Charter
22. European Commission.: GDPR Implementation: State of play in the Member States on 6 December 2017, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=9350
23. European Parliament.: Legislative train: Anti-discrimination directive, http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental- rights/file-anti-discrimination-directive
24. Finn, P., Jakobsson, M.: Designing ethical phishing experiments. IEEE Technol. Soci. Magazine Spring **26**(1), 46–58 (2007)
25. Gold, M.: Griggs' Folly: Essay on the Theory, Problems, and Origin of the Adverse Impact Definition of Employment Discrimination and a Recommendation for Reform, 7 Indus. Rel. L.J. 429 (1985)
26. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A.: Correlating human traits and cyber security behavior intentions. Comput. Sec. **73**, 345358 (2018)
27. Gutwirth, S.: Hildebrandt, Mireille. Some caveats on profiling, In: Gutwirth, S., Poullet, Y., De Hert, P. ((eds.) Data Protection in a Profiled World, 2010. Springer, Dordrecht, pp. 31–41
28. How to make your staff cybersecurity aware, https://www.telegraph.co.uk/connect/small-business/business-networks/bt/how-to-make-staff-cybersecurity-aware/
29. How Effective Is Security Awareness Training for Threat Prevention? https://securityintelligence.com/how-effective-is-security-awareness-training-for-threat-prevention/
30. IAPP: Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, https://iapp.org/media/pdf/resourcecenter/DPN-Guidance-A4-Publication.pdf
31. IAPP: EU Member State GDPR Implementation Laws and Drafts, https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/
32. Jones, M.L.: A right to a human in the loop. Soc. Stud. Sci. **47**(2), 216239 (2017)
33. Kamp, M., Krffer, B., Meints, M.: Profiling of Customers and Consumers Customer Loyalty Programmes and Scoring Practices. In: Hildebrandt, Mireille, Gutwirth, Serge (eds.) Pro- filing the European Citizen: Cross-Disciplinary Perspectives, pp. 201–215. Springer, New York (2008)
34. Konstantin Markin v. Russia, ECtHR Grand Chamber judgment of 22 March 2012, 127
35. Le-Khac, N.A., Markos, S., Kechadi, M.T.: Towards a New Data Mining-Based Approach for Anti-Money Laundering in an International Investment Bank. In: Goel S. (eds.) Digital Forensics and Cyber Crime. ICDF2C 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Tele-communications Engineering, vol. 31. Springer, Berlin, Heidelberg (2010)
36. Meisner, M,:Financial Consequences of Cyber Attacks Leading to Data Breaches in Healthcare sector, CJFA 2017, vol. 6(3), p. 70
37. Martnez-Prez, B., et al.: Privacy and Security in Mobile Health Apps: a Review and Recommendations (2014)

38. Regulation (EU): 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
39. Resnik, D.B., Finn, P.R.: Ethics and phishing experiments. Sci. Eng. Ethics **24**, 1241 (2018). https://doi.org/10.1007/s11948-017-9952-9
40. Schermer, B.: The limits of privacy in automated profiling and data mining. Comput. Law Sec. Report **27**(1), 45–52 (2011)
41. Selbst, A., Powles, J.: Meaningful information and the right to explanation, Inter- national Data Privacy Law, Vol. 7, Issue 4, 1 November 2017, p. 233242, https://doi.org/10.1093/idpl/ipx022
42. Wu, S.: A legal guide to enterprise mobile device management, ABA Section of Science & Technology Law, 2013, pp. 50–60, ISO/IEC27002:2013, Information technology. Security techniques. Code of practice for information security controls, 2013
43. Title VII of the Civil Rights Act of 1964
44. Veale, M., Binns, R.: Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data, Big Data & Society, 2017, available at: http://journals.sagepub.com/doi/abs/10.1177/2053951717743530
45. Verhenneman, G., et al: WITDOM D6.2 Legal requirements on privacy, data protection and security in WITDOM scenarios, 2016, available at: http://www.witdom.eu/sites/default/files/witdom/public/content-files/deliverables/D6.2LegalRequirementsv3.3final20161130.pdf
46. Van der Hof, S., Prins, C.: Personalisation and its Influence on Identities, Behaviour and Social Values. In: Hildebrandt, M., Gutwirth, S. (eds.) Profiling the European Citizen: Cross-Disciplinary Perspectives. Springer, New York (2008)
47. Vogiatzoglou, P., et. al.: DOGANA D5.3 Legal and Ethical Conditions for Cautious Organisations (2017)
48. Wachter, S., Mittelstadt, B., Floridi, L.: Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law, 2017, vol. 7, No. 2

Chapter 6
Device for mHealth

Paolo Perego

Abstract Nowadays, wearable technology is the most promising and market growing technology. Wearable can be considered the winning card up to the mHealth sleeve. Despite mHealth born around the 2000s, only in the last lustrum, it has seen a massive diffusion both for monitoring and diagnosis. Moreover, many existing devices and products have been equipped with data transmission technologies in order to improve the capability of communicating data over the Internet by means of mobile devices (smartphone or tablet) or direct connection. Data transmission allow for communicating health data directly to physicians. This permits to monitor the patient from a distance directly from home, increasing their life quality and, in the meantime, decreasing the welfare costs. This chapter wants to be a compendium of the existing solution in term of wearable, but also non-wearable devices for mobile health. The last paragraph of the chapter reports current and future development of wearable devices, with invisible technology, smart garments, and Wearable 2.0.

6.1 Introduction

Mobile health, or mHealth, is a term coined by Robert Istepanian as use of "emerging mobile communications and network technologies for healthcare" [1]. mHealth is a cross-intersection between Medicine and technology, between Health and Communication technology and especially between Electronic Health (eHealth) and Mobile Technology. It consists of all systems that include acquisition, processing, classification, transmission, and recording of health-related information. mHealth systems are usually composed of three different main subsystems:

1. *Biomedical Sensor:* it is the real interface between the body and the system; it can be of different nature: a smart textile sensor, a microphone, a light sensor; but commonly it is able to transform the variation of a physical quantity (temperature, brightness level, …) in an electrical signal.

P. Perego (✉)
Dip. di Design, Politecnico di Milano, via G. Durando 38/a, 20158 Milan, Italy
e-mail: paolo.perego@polimi.it

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_6

2. *Mobile device:* it consists of the "m" letter of the mHealth definition. Mobile devices (usually Smartphones) are the core part of the mHealth system: the hub where all data from sensors and devices are gathered, stored, processed, and transmitted.
3. *Cloud:* The Cloud consists of the final step of the mHealth system. It consists of a connected platform, where health-related data and information can be stored, visualized, and processed. Cloud system has various stakeholders (doctors, caregivers, insurance, relatives…), who can operate with health information and send back information or advice to the user's mobile device.

6.2 mHealth System Classification

In the past decade, thanks to the advancements in miniaturized electronics and mobile computing, mHealth has been gaining big success in different aspects (monitoring, health practitioner support, prevention…). Figure 6.1 shows the growth of mHealth market since 2012 and it is expected to grow at a CAGR of 33.5% during 2015–2020 [3]. Since 2009, the growth rate is mainly due to penetration and diffusion of mobile phones in healthcare segment. Currently, mobile diffusion is more than 100% in developed markets while is expected to increase in developing markets such as Asia-Pacific, Latin America, and Africa. Moreover, the diffusion of 5G technology will further add capabilities and increase the use of the mobile platform (near-zero latency, advanced quality-of-service capabilities, and data rates on the order of Gbps).

The first distinction in mHealth solutions is between mHealth devices and mHealth services.

mHealth devices are objects connected to mobile devices (like smartphone and tablet) or with connection themselves (3G/4G or WiFi connection), which are able to acquire information and send them over the Internet.

mHealth services are platforms that use health-related data from one or different sources (not necessarily devices), and aggregate, process, visualize, and deliver them. Figure 6.2 shows examples for these two mHealth categories.

Together with smartphones penetration and diffusion, mHealth market growth can be mainly attributed to the high revenue generated by blood glucose meters, cardiac monitors, and blood pressure monitors, which together accounted 70% of the global mHealth market [5].

Blood pressure monitors are the highest revenue generating segment in global mHealth devices market, while blood glucose monitors are the fastest growing segment. mHealth services are dedicated to:

- diagnosis;
- monitoring;
- treatment;
- prevention;
- wellness and fitness.

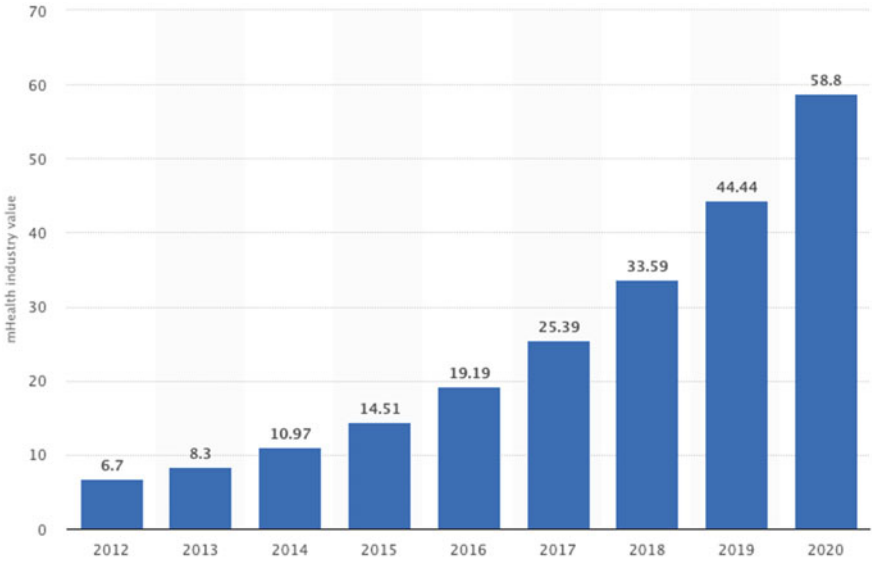

Fig. 6.1 mHealth market growth since 2012 (in billion U.S. dollars) [2]

Fig. 6.2 mHealth examples: **a** Blood pressure with smartphone data synchronization (iHealth BPM1); **b** AED service delivered by drones [4]

Mobile health services are still in the first growing phase because they are firmly related to mHealth devices. As for another market segment, also mHealth is undergoing a deep transformation passing from the product-centered strategy to a product-as-a-service strategy. The bigger growth is related to monitoring services, especially for chronic disease management, post-acute care management as well as aging population; but also awareness about fitness and general wellness, and government initiatives for welfare contribute to the growth of this segment.

6.3 Categories of mHealth Devices

mHealth devices can be clusterized in different categories according to different criteria. Franco et al. [5] report a first sub-categorization of mobile health devices by the application; from the most diffused one we can identify:

- Cardiovascular diseases;
- Diabetes;
- Respiratory diseases;
- Neurological disease;
- Others.

In these past years, monitoring of cardiovascular parameters is the largest segment of devices, which support most of the mHealth services. mHealth evolution goes hand in hand with wearable technologies. More and more wearable devices are entering the mHealth market thanks to their portability, invisibility, and great ease of use. For this reason, recently the mobile health systems can be divided into wearable and non-wearable device.

Wearable devices can be defined as a piece of technology that is worn on or put in contact with, the human body. They include one or more sensors, a processing unit, and a connection transceiver to exchange data with a host. This type of device has become a more common part of the tech world as companies started to develop different types of devices that are small enough to be worn and powerful enough to collect, by means of many kinds of sensors, information about the body and its surroundings.

Contrariwise *non-wearable* mHealth devices consist in technology, which can measure health information from the body but cannot be worn due to dimension and type of measurements.

An example for both types of device is the digital sphygmomanometer (Fig. 6.3); this could be either a wearable device or a non-wearable device, depending on the measurement method and related hardware solution which is implemented. It is obvious that wearable devices, except for some particular cases in which technology cannot be miniaturized, are the best choice for what concerns mobile health. In fact, they are linked by the same intrinsic characteristic that can be deduced from the definition of mHealth, that is mobility and portability.

6.3.1 Wearable Devices

Wearable devices allow for getting different kinds of data easily from the body without interfering with daily life activity. Moreover, thanks to small size and electronic miniaturization, wearables are almost invisible and permit to measure data in a more precise way thanks to the fact that the subject does not even realize that the measure is taking place [6]. There are five wearable categories:

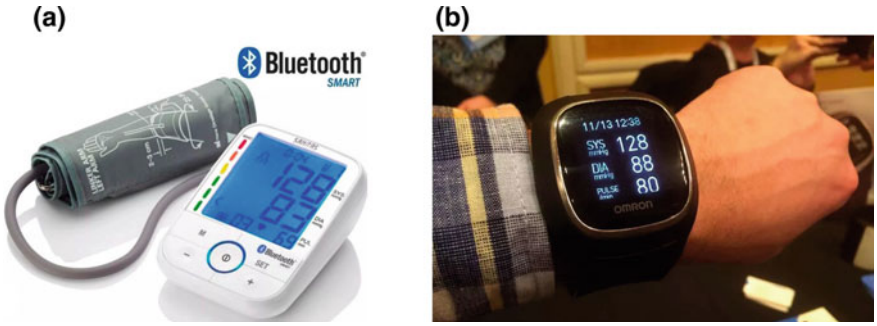

Fig. 6.3 Example for Non-Wearable **a** and Wearable **b** Sphygmomanometer for mHealth

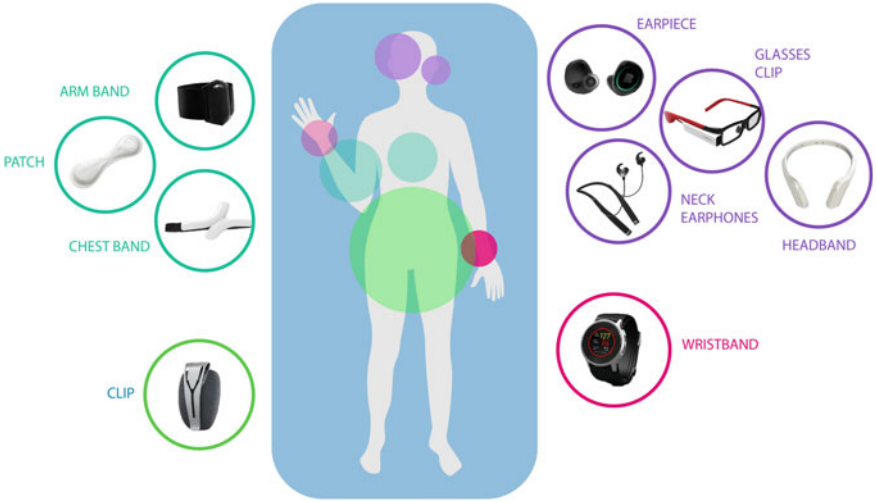

Fig. 6.4 Different positions for wearable placement on the body. Colors highlight the different positions for every kind of device

- *Wristbands:* Wearables worn around the wrist that might or might not integrate visual user interface.
- *Bands:* Wearables that use an elastic band to attach the monitoring device to the body.
- *Patches:* Devices attached by adhesives directly to the skin, in different areas of the body.
- *Head/hand accessories:* Devices worn on distal anatomical part (e.g., around the neck, on ears or fingers, on the head) and double as a fashion accessory.
- *Clips:* Devices attached to clothes by a mechanical fix, a magnet, or an adhesive.

Each class has different pros and cons, which are mainly related to the measurement technology and the miniaturization rate (Figs. 6.4 and 6.5).

Fig. 6.5 On the left, Empatica E4 wristband research device; on the right Empatica Embrace device with patented technology to continuously record physiological signals from multiple sensors and generate seizure alert

Wristbands are the most common wearable devices. With the launch of consumer smartwatch and activity tracker, these devices registered a market growth of 67.6% from 2014 to 2015. These devices can usually implement inertial measurement unit (IMU) for movement detection (e.g., steps, distance, exercises…), a microphone for environment monitoring, a flexible pressure sensor for cuff-less blood pressure measurement [7], optical sensor (PPG-photoplethysmography) for heart rate detection, temperature sensor. These allow for measuring a plethora of health data, but at the same time, the position on the wrist prevents the measurement of some variable such as electrocardiogram (ECG) or precise body segment movement monitoring. A particular example for wristband is the Empatica devices [9]. Embrace and E4, this is how the devices in 6.5 are called, integrate different sensors: accelerometer (for capturing motion-based activity), galvanic skin response sensor (GSR—for measuring the constantly fluctuating changes in certain electrical properties of the skin), infrared thermopile (for reading peripheral skin temperature) and PPG sensor (for measuring blood volume pulse—BVP—from which heart rate variability can be derived). With these sensors and optimized algorithm, Empatica devices are not only able to measure and transmit data to the physicians, but elaborate and aggregate them with the goal of generating seizure alarm. As described below, the main components of a mHealth system are clearly understandable in Empatica device: there are sensors, connection with the mobile device, algorithms and cloud system for alarm generation and data visualization.

Bands are the first wearable appeared on the market. BodyMedia Armband was launched in 2001 as a device for metabolic assessment able to measure energy expenditure with high accuracy [8]. Bands can be usually distinguished in armband and chest belt based on where they are worn.

Chest belt is usually known for heart rate monitoring, but can also include IMU for movement analysis. They are used mainly for sports (the first commercial one was

developed by Polar in the 90s), but in the past decade, they are used also in clinical for single lead ECG monitoring. A chest belt uses two electrodes for measuring cardiac signals: sports belts usually extract heart rate (HR) frequency from an average of 3/5 beats, while clinical belts directly process ECG signals and extract both beat-to-beat HR but also other characteristics of the cardiac signal (e.g., QRS morphology).

Armband can be equipped with different kind of sensors. Figure 6.6 shows three different types of armband for three different purposes. Figure 6.6a shows the BodyMedia Armband. It is closely related to Empatica technology because it used GSR and temperature sensors to compute daily energy consumption. The device shown in Fig. 6.6b is the Myo armband, wearable gesture control, and motion control device that lets the user takes control of the phone, computer touch-free. It includes 8 different bipolar EMG channels, a small battery and a microcontroller with Bluetooth technology for the communication with a computer or smartphone. The Myo, worn on the forearm, is able to record the muscular activation signals for each muscle during movement. A proper training of the algorithm allows for controlling computer or smartphone for different applications.

Figure 6.6c shows the Scosche Rhythm+ [11], a high precision heart monitor (very similar to the MioLINK [10]). It employs patented optical sensor technology for highly accurate monitoring and measurement. It can be placed on the upper forearm, but if it is snug enough, it cannot move on the arm and can be placed also on bicep and tricep. This kind of wearable includes optical different optical sensors which allow for a more accurate heart rate detection respect to wrist PPG.

Patches: Patches are usually the most invisible wearable devices. They can be attached directly to the skin, or to clothes. Figure 6.7 presents four examples of patches for different applications. Figure 6.7a is the Kenzen patch [12]; Kenzen device combines the depth of lab-based diagnostics with real time information from a wearable device to improve health and safety. It should (is not yet on the market) be able to monitor vital sign (heart rate), movement (by means of an internal accelerometer, environment (temperature), and, thanks to a patented system, analyze sweat. It consists of two parts—the first one is the main component which provides sensors for HR, movement and environmental temperature, the second one is the disposable sensor for sweat. Figure 6.7b is the Neurofen fever smart [13]. It is a smart thermometer for monitoring continuously fever status of newborns. Temperature-smart patches are the most diffused application for this kind of devices because are technologically simple and relatively cheap. These devices allow for monitoring the temperature of the baby in a continuous way; the mother can measure fever also when the baby is sleeping and automatically receives alert if the temperature increases. Figure 6.7c is the Spire health [14]. It is not properly a wearable device because it is attached to clothes and not to the body. Spire has an adhesive in order to be attached permanently to underwear. It includes a PPG sensor which is able to measure heart rate and heart rate variability and, with proprietary algorithms, monitors stress, activity, and sleeps to discover how they affect each other. Figure 6.7d is a prototype by L'Oreal for a UV detector. It can stick on nails and is a very simple sensor. Due to dimension, this device has no battery, neither Bluetooth or WiFi connection. Instead, it is NFC enabled so that it can be scanned with smartphone to retrieve the UV data collected.

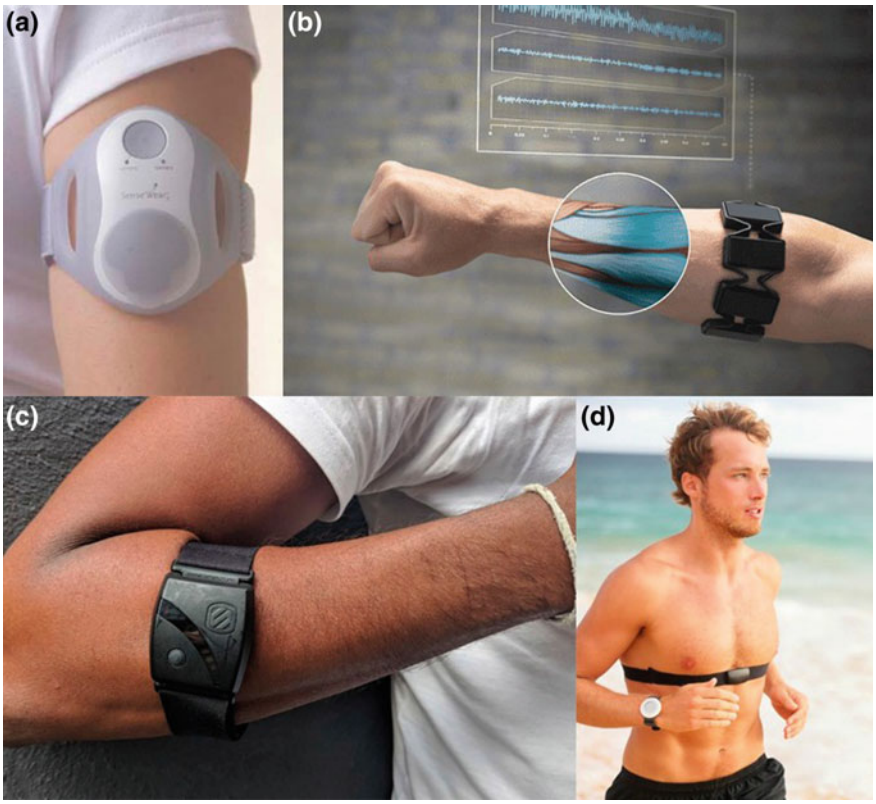

Fig. 6.6 Example for bands. **a** Bodymedia armband for metabolic assessment; **b** Myo armband for touchless control; **c** Scosche Rhythm+ and **d** chest belt device for heart rate monitoring

The UV Sense, as the company calls it, is meant to help people track how much time they spend in the sun without being overbearing. The UV Sense will determine how long the user has been outside, and once synced with the app, provides a score that says whether he/she is spending too much time in the sun (based on some initial questions about skin tone to set a baseline). Patches have more pros, they are small, invisible, versatile, but have also a big problem: the adhesive. Adhesive, in some cases, can cause irritation, rush and in some case also allergy. Moreover, it is very difficult to use them with elderly people because adhesive can cause irritation and even small wounds due to the fact that the skin of these users is often very dehydrated and fragile.

The categories of *head/hand accessories and Clips* are the most consumer ones. The first type includes earpieces, glass and glass clip, and headband. Most of these are not really medical devices, but they are able to monitor vital signs and, for this reason, they can be used for mHealth.

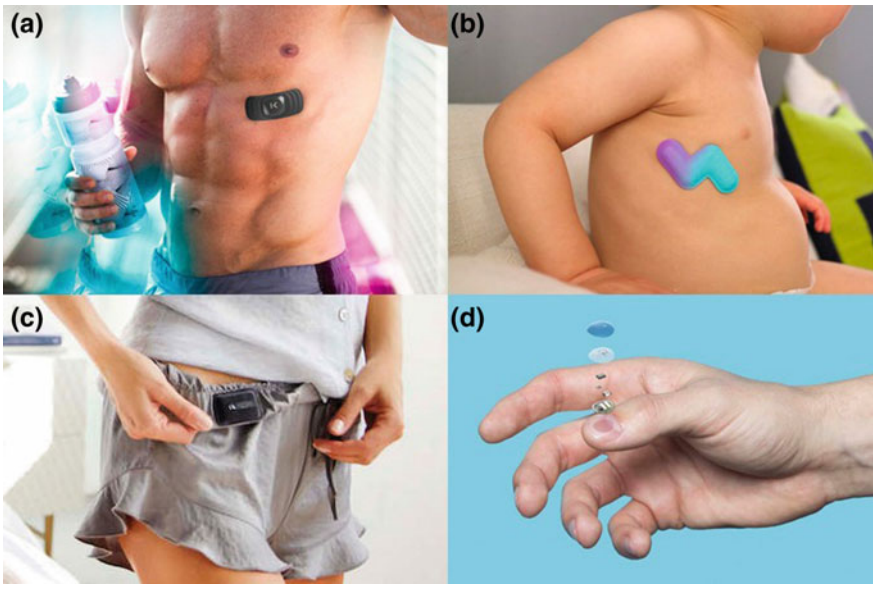

Fig. 6.7 Example for patches. **a** Kenzen smart device for vital signs monitoring and sweat analysis; **b** Neurofen fever smart thermometer; **c** Spire health tracker; **d** L'Oreal Smart UV detector

The most diffused earpieces are the Samsung Gear IconX [15]. As Bose SoundSport Pulse, Jabra Sport Pulse, and Under Armor Sport, they use in-ear photoplethysmography (PPG) for detecting heart rate and heart rate variability during physical activity. They can be also used for "almost daily" monitoring, except for battery duration on continuous monitoring (maximum 5 h) and needs to be recharged twice a day.

Google glasses are instead the most diffused example of smart glasses; they are at now out of the market, but they kicked off the market of smart glasses. They were designed as an extension of the smartphone. In fact, they can be used also for mobile health for retrieving heart rate from Ballistocardiogram [16]. This technology is most suitable for augmented reality: workers have the information they need for their jobs directly on the lenses, keeping their hands free and, at the same time, being monitored throughout the working day.

As for as the headband (or headgear) are concerned, they are controversial devices. Most of them are consumer devices, which monitor single or more EEG channels (especially Fp1 and Fp2 electrode for 10–20 EEG system [17]) for alpha and theta EEG pattern detection in order to give information and advice to the user against stress and to sleep better. The above criticism mentioned are related both on the wearability (these types of tools are not at all invisible and comfortable) and on their application (they are not used for medical purposes and their operation is not medically certified).

Clips are the simplest wearable device. They were the first and cheaper commercial wearables which include inertial sensors for movement detection. They are used for activity monitoring for elderly people thanks to their acceptance, compliance, and easy to use. With data recorded by clips, physicians can check how many steps and activity elderly people do during the day in order to fit their diet and physical exercises [18]. Despite their simplicity, their reliability is still under investigation.

In the previous paragraphs, a review of the most relevant device for mobile health has been reported. The paragraphs have shown the main categories for the wearable device and some example for each category. However, the purpose of this chapter is not to show all the possible wearable devices on the market, but report those which have been more widely used, and can be used, in the field of mHealth.

6.4 mHealth Future Perspective

Despite the development in the past decade, mHealth and especially wearable device are only in the first stage of their evolution. The market requires invisible technology which is able to record nonintrusively different biological signals, which are still a challenge because the size of wearable devices is inversely proportional to the number of signals that a wearable can measure.

In order to rebut this unwritten rule, in the past 5 years, some Wearable 1.5 solutions have been created. These devices use a new typology of sensors built on new sensitive material, which allow for integrating invisible sensors inside garments. Example are the sensorized garments from Pegaso Fit for Future European Project [19], which consist in a T-shirt and a bra with embedded conductive silver textile as ECG electrodes, and Sensoria smart device, socks with [20] built-in textile pressure sensors for step and balance detection.

Spire device shown in the previous paragraph is another example of wearable 1.5. Spire does not use new material for sensing but improve the wearability thanks to its soft case. The electronic part is covered by a textile case which allows for a better comfort 6.7C.

Figure 6.8 shows the Pegaso F4f system; the devices (like Sensoria, OMSignal, etc.), which use new materials and textiles for sensing, improve wearability, but they still need an electronic device for data collection. In the last years, the first attempt for wearable 2.0 has been done [21, 22]. Wearable 2.0 is a fully invisible device. They use a smart textile, flexible battery, and soft electronics in order to embed all the parts of the system directly in the garments; this dramatically improves wearability and comfort.

Mobile health solutions are becoming increasingly and medically relevant and important for patient care. Devices are becoming always more invisible and performant, but they are still only relegated to some areas of medicine (e.g., blood pressure monitoring). Nevertheless, also mHealth services are at the beginning of their development. With the logic of product-as-a-service, also mHealth is transmuting from

Fig. 6.8 Pegaso F4F system: it is composed of a smart T-shirt, smart bracelet, and apps

a product-centered system to a service centered system, in which products are only the instruments to gather data and access and support the service.

6.5 Conclusion

Despite this, many stakeholders are interested in mHealth, from healthcare providers to insurances. From the point of view of healthcare providers, mHealth solutions can improve the quality of care by moving the diagnosis and care path from hospital to home; at the same time, they can reduce the welfare cost thanks to immediate or early dehospitalization. Mobile operators and insurances see mHealth technology as black-box for humans; the device is able to assess user lifestyle by monitoring vital signs and activity H24. It will also recognize and classify the types of activity, food intake [23], etc. to build up a comprehensive profile of the users. This profile is used to give the users advice on how to improve their lifestyle and has a direct impact on the cost of your insurance.

Moreover, the value of mHealth devices and services in healthcare stems from and is being driven by, several factors, including one of the most difficult aspects to be taken into consideration during system development: the human factor. Patient proactivity to manage their health is the core coefficient in the formula of mHealth success.

References

1. Istepanian, R.S.H., Laxminarayan, S., Pattichis, C.S.: m-Health: Emerging mobile health systems. Topics in Biomedical Engineering. Springer, Boston, MA (2006)
2. Global digital health market from 2015 to 2020, by major segment (in billion U.S. dollars), Statista, https://www.statista.com/statistics/387867/value-of-worldwide-digital-health-market-forecast-by-segment/
3. mHealth market worth $23 billion in 2017 and estimated to grow at a CAGR of more than 35% over the next three years, https://www.reuters.com/brandfeatures/venture-capital/article?id=4640
4. Ambulance drone from TU-delft https://www.tudelft.nl/en/ide/research/research-labs/applied-labs/ambulance-drone/
5. Franco, J., Jeevane, Y: mHealth market (devices, applications, services & therapeutics)—global mobile healthcare industry size, analysis, share, growth, trends and forecast, 2012–2020. Hg. v. Allied Market Research (2015) http://www.alliedmarketresearch.com/mobile-health-market
6. Norman, D.A: The invisible computer: why good products can fail, the personal computer is so complex, and information appliances are the solution. MIT press (1998)
7. Luo, N., Dai, W., Li, C., Zhou, Z., Lu, L., Poon, C.C.Y., Chen, S.C., Zhang, Y., Zhao, N.: Flexible piezoresistive sensor patch enabling ultralow power cuffless blood pressure measurement. Adv. Func. Mater. **26**(8), 1178–1187 (2016)
8. Cole, P.J., LeMura, L.M., Klinger, T.A., Strohecker, K., McConnell, T.R.: Measuring energy expenditure in cardiac patients using the Body Media (TM) Armband versus indirect calorimetry: a validation study. J. Sports Med. Phys. Fitness **44**(3), 262 (2004)
9. McCarthy, C., Pradhan, N., Redpath, C., Adler, A: Validation of the Empatica E4 wristband. In Student Conference (ISC), 2016 IEEE EMBS International, pp. 1–4. IEEE (2016)
10. Mio Global: Mio LINK Heart rate wristband, https://www.mioglobal.com/en-us/Mio-Link-heart-rate-wristband/Product.aspx
11. Scosche Rhythm+, Armband Heart Rate Monitor https://www.scosche.com/rhythm-plus-heart-rate-monitor-armband
12. Kenzen patch https://www.kenzen.com/patch
13. Fever smart by nurofen https://www.kenzen.com/patch
14. Spire healthtag https://spire.io/pages/healthtag
15. Samsung Gear IconX https://www.samsung.com/us/mobile/audio/headphones/gear-iconx–black-sm-r140nzkaxar/reviews
16. Hernandez, J., Li, Y., Rehg, J.M., Picard, R.W.: Bioglass: physiological parameter estimation using a head-mounted wearable device. In: 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI, pp. 55–58. IEEE (2014)
17. Homan, R.W., Herman, J., Purdy, P.: Cerebral location of international 1020 system electrode placement. Electroencephalogr. Clin. Neurophysiol. **66**(4), 376–382 (1987)
18. Lauritzen, J., Munoz, A., Luis, J.S., Civit, A.: The usefulness of activity trackers in elderly with reduced mobility: a case study. Stud. Health Technol Inform. **192**, 759–762 (2013)
19. Perego, P., Andreoni, G., Tarabini, M.: Textile performance assessment for smart t-shirt development, mechanical and electrical study for conductive yarn. Proceedings of the eTELEMED (2016)
20. Dalsgaard, C., Sterrett, R.: White paper on smart textile garments and devices: a market overview of smart textile wearable technologies. Market Opportunities for Smart Textiles, Ohmatex, Denmark (2014)
21. Khan, Y., Garg, M., Gui, Q., Schadt, M., Gaikwad, A., Han, D., Yamamoto, N.A.D., Hart, P., Welte, R., Wilson, W., Czarnecki, S., Poliks, M., Ghose, K., Egitto, F., Turner, J., Arias, A.C.: Flexible hybrid electronics: direct interfacing of soft and hard electronics for wearable health monitoring. Adv. Func. Mater. **26**(47), 8764–8775 (2016)

22. Zamarayeva, A.M., Ostfeld, A.E., Wang, M., Duey, J.K., Deckman, I., Lechłne, B.P., Davies, G., Arias, A.C.: Flexible and stretchable power sources for wearable electronics. Sci. Adv. **3**(6), e1602051 (2017)
23. Fontana, J.M., Farooq, M., Sazonov, E.: Automatic ingestion monitor: a novel wearable device for monitoring of ingestive behavior. IEEE Trans. Biomed. Eng. **61**(6), 1772–1779 (2015)

Chapter 7
Big Data and Signal Processing in mHealth

Massimo W. Rivolta and Roberto Sassi

Abstract In this chapter, we present and discuss the state-of-the-art technology for the use of mHealth as a relevant source of clinical information. Then, we provide an overview of the signal processing pipelines that, up to date, are most suitable for the processing of data collected from sensors in unsupervised environments, as at home.

7.1 mHealth as Source of Clinical Information: Which Parameters Are of Interest?

mHealth has been defined as the emerging mobile communications and network technology for healthcare systems [1] and it represents the newest telemedicine paradigm. Despite telemedicine still being debated [2], the number of healthcare low-cost mobile applications is growing very rapidly and the increase of remote monitoring has led important market investments [3].

Another important key factor associated with the spreading of mHealth applications is the number of research investments (for example, in the European Union under the Horizon 2020 program) meant to reduce the costs of health care systems, which have been constantly increasing by the ageing of the population affected by chronic diseases. Indeed, based on forecasting reported in The World Population Ageing 2015 report [4], the number of old people (>60 years) will have a 50% increase in nearly all the countries of the world by the end of 2030. Moreover, the number of older people (>80 years) is growing even faster than the number of old persons overall. However, life expectancy comes with an increased number of elderly people with health-related issues at risk of permanent hospitalization, who might benefit from the use of mHealth applications for continuous monitoring at home. In fact, mHealth not only provides access to the Electronic Health Records anytime and

M. W. Rivolta (✉) · R. Sassi
Department of Computer Science, University of Milan, Via Celoria 18, 20133 Milan, Italy
e-mail: massimo.rivolta@unimi.it

R. Sassi
e-mail: roberto.sassi@unimi.it

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_7

anywhere but also might keep the patient aware of the risk factors and engaged to pursuit a better quality of life.

The main areas of interest for mHealth applications are given as follows:

- accessibility to Electronic Health Records by medical doctors;
- software infrastructures for improving assisted living technologies and resource management (e.g., scheduling of caregivers, big data health analytics);
- serious games for people engagement and awareness on health-related issues (e.g., active ageing for elderly, healthy lifestyle for obese teenagers, diabetes, smoking);
- monitoring of clinical variables using wearable and *non*-wearable sensors; and
- fitness and wellness.

Among all the possible applications, wearable sensors have become very popular in the medical field since they allow monitoring of relevant clinical information about a person's health over time, without the need for hospitalization [5]. Clinical variables or conditions usually quantified by wearables include cardiovascular status, sleep quality, temperature, physical activity, and quality of movement for fitness or risk of falling in elderly.

In this chapter, we focus only on technologies requiring wearable sensors for cardiovascular monitoring, sleep efficiency assessment, and risk of falling quantification.

7.1.1 Cardiac Monitoring with Wearable Devices: From Heart Rate Variability Assessment to Arrhythmia Detection

As stated in "Global Atlas on cardiovascular disease (CVD) prevention and control" [6], CVDs include diseases of the heart, vascular diseases of the brain and diseases of blood vessels and are the leading cause for over 17.3 million deaths per year, with no difference between men and women. Furthermore, 3 million of these deaths occurred before the age of 60.

The first five causative risk factors of CVDs are, sorted from the most relevant to the less, raised blood pressure, tobacco smoking, high blood glucose, physical inactivity, and overweight and obesity. Excluding the socioeconomical differences across nations [6, 7], these factors remain the most influential and are the consequences of sedentary life, unhealthy diets with high intakes of saturated fat, sugar, cholesterol and salt, and harmful use of alcohol or binge drinking. Therefore, CVDs might be largely prevented by performing regular physical activity and having a diet with fruits, vegetables and fish, and modest use of salt [6].

The main two cardiac events linked with death are heart attacks and strokes since they are responsible for over 7.3 and 6.2 million deaths per year, respectively [6]. Such deaths might be the consequence of cardiac arrhythmias. Cardiac arrhythmias are abnormal electrical activities in the heart involving atria and/or ventricles, manifested as altered speed or regularity of the electrical wave propagation.

Heart attacks might be caused by persistent ventricular arrhythmias, as a form of ventricular fibrillation (VF), and they might lead to sudden cardiac death. People at risk of VF requires the implantation of an electrical defibrillator that can promptly deliver an electrical shock capable of arresting the fibrillatory state. However, deciding which subject needs an implanted device is still matter of investigation [8] and currently, such devices are used as a secondary prevention [9]. Moreover, as stated in [6], the presence of external defibrillators in public spaces provides a marginal improvement on the survival and does not justify a widescale deployment.

Strokes are associated with another cardiac arrhythmia, i.e., atrial fibrillation (AF). It is characterized by irregular and uncoordinated atrial activation that leads to inefficiency of the functioning of the heart (i.e., less blood pumped into the ventricles). Indeed, the percentage of strokes due to AF accounts for about one-fifth of all strokes and the risk increases with age [6]. Because of its prevalence, AF management demands high costs for the health care systems worldwide and, therefore, a prompt diagnosis or intervention is required.

In the last two decades, CVD mortality inverted its trend between developed and underdeveloped countries [6, 7]. In fact, CVD is now more common in low-income nations and the reason is the combination of prevention and treatment interventions performed in developed countries. With such evidence, in order to reduce CVD risks and health care system costs, investments on prevention programs and technologies as mHealth represent a possible and feasible option.

Currently, the two main common mHealth applications for CVDs present in the market are those related to heart rate and blood pressure monitoring, respectively [10]. The former includes heart rate monitors integrated into elastic bands, portable or wearable electrocardiographic devices, photo-pleximographic-based sensors, contact or contact-less camera-based heart rate monitors [11–13]. These applications aim to quantify the heart rate variability (HRV), a well-known marker of autonomic regulation associated with many pathological conditions [14], and for arrhythmia detection. The latter mostly relates to cuff-less and continuous blood pressure monitors. They are based on mathematical models capable of estimating the blood pressure by means of the time necessary for a blood wave to reach the periphery from the artery (e.g., pulse transit time, pulse arrival time) [15].

7.1.2 Early Detection of Gait and Balance Disorders Through Wearable Accelerometers

Gait and balance disorders, unless associated with diseases (e.g., Parkinson), are the natural consequence of ageing and they usually worsen with time if not promptly treated. One of the main cause of injury in elderly due to such disorders are falls. Indeed, even though falls are caused by multiple reasons (e.g., environment), gait and balance disorders are the main predisposing factors [16].

According to the "Who global report on falls prevention in older age" report [17], approximately 28–35% of people aged 65 and over fall each year at least once. Moreover, falls account for about 40% of deaths related to accidents. The high proportion of falls, along with the increase in life expectancy, has led health care systems worldwide to an extremely unbearable burden in terms of costs and management. In such scenario, fall prevention might seem a feasible option and can be carried out through strategies for promoting healthy and active ageing [17]. However, prevention requires tools and technologies to early detect significant health changes as well as to promptly react.

Gait and balance disorders are clinically evaluated using movement analysis by means of instrumentation such as force plate and integrated multi-camera infrared settings. Although the clinical assessment of such disorders has extensively been used in practice [18], the role of movement analysis for monitoring is still controversial because of expensive instrumentation and impossibility to monitor and screen large populations over time. Therefore, fall prevention is limited since this technology cannot be used often and cannot be moved into a home environment.

In the context of fall prevention, since the 80s, an alternative approach widely investigated to assess the risk of falling is the use of a clinical scale (e.g., Tinetti test, Berg Balance Scale, Get Up & Go). A clinical scale is a test in which the subject is asked to perform movements (e.g., standing up, walking) and, for each of these movements, the physician assigns a "quality" score; then, the sum of the scores is supposed to be associated with the risk of falling. Even though clinical scales are inexpensive and typically easy to perform, they most require trained personnel. Consequently, clinical scales often suffer from inter-rater variability.

In order to compensate for the inter-rater variability, quantitative measures extracted from wearable inertial sensors, such as accelerometers and gyroscopes, have been investigated. Wearable sensors have become of common use for rehabilitation medicine and to assess balance and gait characteristics. Wearables are used to quantify trunk inclination, postural stability, step frequency, step symmetry, step and stride regularity, etc., and, moreover, to assess the risk of falling as well (e.g., [19–21]).

mHealth plays a role for fall risk assessment as well. Indeed, wearables in combination with clinical scales would be a feasible option for large-scale screening at home. The main challenges are building a technology that

- can be used at home;
- without the need of the physician observing the test;
- capable of providing clinical information regarding the quality of balance and gait.

In the last decades, several studies have reported promising results for automatic assessment of the fall risk using wearables. Of note, Narayanan et al. [22] demonstrated that the Time Up and Go test, Alternate-Step test and Sit-to-Stand with five repetitions test were reproducible at home using an accelerometer placed at the waist. Although these tests are not considered sufficient for a comprehensive evaluation of the fall risk because of their limited variety of movements, other more complex clinical scales have been investigated.

The Tinetti test is a complex clinical scale aimed to assess the fall risk by evaluating both the balance and gait [23]. Its score ranges from 0 to 28 and usually, a scoreless or equal than 18 is considered as high risk of falling (even though the threshold varies across studies). Senden et al. [21], Giansanti et al. [19], Rivolta et al. [24] have proven that Tinetti score might also be estimated automatically using wearables.

Although the current results are promising, there is still no evidence that automatic fall risk assessment at home using mHealth provides a reduced fall risk.

7.1.3 mHealth for Sleep Quality Tracking

Sleep is a dynamic process that significantly affects many physiological functions and contributes to the insurgence of different pathologies such as cardiac, neurological, and metabolic disorders. Sleep quality plays an important role in natural processes like memorization, learning, and concentration and moreover, when low, it might induce raised blood pressure or altered metabolic balance that could lead to CVDs.

Sleep quality is clinically assessed by means of polysomnography (PSG), which consists of one or more nights of sleep while the subject is instrumented with several electrodes. The usual setting comprises electroencephalogram, electromyogram, and electrooculogram and, sometimes, respirogram and electrocardiogram. The signals generated during the night are then manually analyzed by expert neurologists for each 30 s window (epoch is the correct nomenclature) and, according to the rules and guidelines defined by the American Academy of Sleep Medicine (AASM) [25], the sleep stage is assigned among wakefulness, rapid eye movement (REM), *non*-REM light sleep (NREM1 and NREM2), *non*-REM deep sleep (NREM3; also called slow-wave sleep, SWS).

Despite PSG is the current gold standard for sleep studies, it presents several disadvantages. It is expensive, labor-intensive, often inaccessible, and needs for specialized personnel. Therefore, long-term sleep monitoring requires more practical methods that can be used on a nightly basis. To this regard, in the late 70s, Kripke et al. [26] found that movements during sleep are most likely to be associated with wakefulness or light sleep of the subject when compared with PSG. The finding created a new research line on sleep medicine based on "movements" that it is still ongoing nowadays [27]. The instrument used for the detection of the movements is the actigraph: a device usually worn at the wrist as a watch.

Actigraphy is a valid technology for estimating sleep quality in healthy subjects and people with sleep disorders [27]. Moreover, being actigraphs small in size, inexpensive and comfortable for the user, actigraphy is considered a "cost-effective" solution for long-term sleep monitoring. However, it usually underestimates the waking stage since a person awake might stay still in the bed. In order to overcome the low detection of the wake stage, researchers have investigated on alternative methodologies such as the use of heart rate variability (HRV) or respiration [28] for automatic sleep stage classification.

Sleep particularly interacts with the autonomic nervous system, so that HRV presents different patterns across sleep stages. Several HRV features (e.g., powers in the VLF, LF and HF spectral bands, and the LF/HF ratio; see Sect. 7.2.1), have been found to have discriminatory power. However, being HRV highly variable within and between subjects and across nights, the overall accuracy for the automatic classification of sleep stages is about 0.7 with a balanced sleep and wake detection rate [29].

Recently, researchers have been investigating the combined use of actigraphy and HRV. The objective is then to verify whether their combination might retain the high sleep detection rate of actigraphy while increasing the wake detection rate. However, in the context of mHealth, in order to acquire the HRV signal, it would be necessary to use another wearable device (e.g., elastic band) that would lead to an undesired user experience. In order to overcome such issue, it has been questioned whether actigraphy measured at the chest would maintain similar performance to that at the wrist. The main rationale is that if they provide similar performances, then all sensors can be integrated on a single device, wore using a sensorized T-shirt or a chest-belt, capable of collecting both HRV and actigraphy. A recent study proved that it could be feasible [30]. The finding opens interesting possibilities in wearable device design and might facilitate long-term sleep monitoring at home.

7.2 Signal Processing for mHealth Sensor Data

7.2.1 Feature Extraction for Cardiac Signals

The autonomic nervous system regulates, through innervation, the heart rate in a continuous fashion. The quantification on how the heart rate adapts under external perturbations such as physical activity or emotions might be extremely important in detecting cardiac malfunctioning or abnormalities. The main cardiac signal employed to obtain insights regarding the autonomic regulation is the RR series. It is defined as a sequence of interbeat time intervals detected from the ECG. Since a complete heartbeat might last some hundreds of milliseconds, the commonly used reference of the time instant of the beat occurrence is represented by the peak of the QRS complex on the ECG, i.e., the R-peak. Therefore, the RR series is defined as the difference of two consecutive R-peak time instants, as in the following manner:

$$\mathrm{RR}_k = \mathrm{R}_k - \mathrm{R}_{k-1} \tag{7.1}$$

where k is the beat-index and R_k is the time instant of the kth R-peak.

The RR series and the information obtained from it are used as reference for alternative methodologies aimed to quantify the autonomic regulation: in other words, it is considered as "gold standard". Information is usually in the form of features directly or indirectly extracted from the RR series. RR features are typically categorized as time-domain, frequency-domain, and regularity features. For example, the standard

deviation of normal-to-normal beat intervals (SDNN) and the root mean square of successive differences (RMSSD) are time-domain features. The former evaluates the variability of the heart rate while the latter quantifies the variability of high-frequency components of the RR series. In a similar way, features can be extracted from the frequency domain by means of the power spectral density (PSD) computed on the RR series. For example, the ratio between the PSD area of the low frequency and high-frequency components is a well-known marker of the sympathovagal balance of the autonomic regulation. Finally, regularity features quantify the regularity or complexity of the RR series. For example, Sample Entropy (SampEn) or Detrended Fluctuation Analysis (DFA) are the most common tools to quantify regularity and long-term memory of the RR series, respectively. For a complete overview of the relevant RR features, please refer to [14, 31].

The main pipeline for the development and validation of alternative technologies aimed to quantify the autonomic regulation is the following:

1. raw signal acquisition;
2. signal preprocessing for RR series estimation;
3. feature extraction; and
4. comparison of the extracted features with the gold standard.

The major critical points of the pipeline are the raw signal acquisition and signal preprocessing because it is where the alternative technology usually pops up. Heart rate monitors integrated into elastic bands wore at the chest and cameras are widely investigated as feasible surrogate of the ECG for extracting the RR series. These two technologies rely on different assumptions. The elastic band captures small movements of the chest generated by the blood flux outgoing the heart while the camera detects different colors due to oxygenated or deoxygenated blood reaching the skin. Because of the presence of tissues such as vessels, muscles, and skin both methodologies present limitations in the frequency components, especially regarding the high ones, and are corrupted by several sources of noise when compared with ECG. Consequently, ad hoc signal processing algorithms need to be developed to remove the interferences.

Elastic bands are based on "wearable seismocardiography" that is the recording of body vibrations generated by the heartbeat. They contain a high-resolution accelerometer capable of detecting small movements and vibrations induced by cardiac valves and blood flux. The main limitation of seismocardiography is represented by the movement noise present on the raw signal. Indeed, chest movement such as voluntary contraction or respiration are constantly added to the periodic vibrations of the heartbeat. In this case, signal processing tools have to consider and implement ad-hoc filters.

The first generation of cameras for heart rate estimation using smartphone required the user to put the finger on the camera lens while the flash is on [32]. In this way, the skin surface reflects the light back to the camera lens based on the different absorption of the light by the oxygenated or deoxygenated blood. The major issue of this technology is twofold. First, the image acquired by the camera presents an inhomogeneous color because of the *non*-uniform pressure of the finger on the lens.

Second, the movements of the finger highly alter the image acquired. The technology requires the user to be as still as possible minimize pressure and movement artifacts. Moreover, the RR series is generated by aggregating the colors (or grayscale values) of each frame using a function such as mean, median or max [32]. In addition, the frequency content is limited by the low sampling rate (usually around 30 fps).

Cameras are used for contact-less facial heart rate estimation as well. Several problems arise with such technology. First, the selection of a facial region that maximizes the range of the color variations. In many studies, the forehead is employed because of its wide surface with no hairs. However, different portions of the forehead might have different blood vessel density and therefore, tracking of the face has to be performed to extract the RR series from the same region over time. Second, illumination and distance from the camera play a role on the signal quality and usually require standardized environments. Also, the cameras used in home environments are those present in smartphone which usually have low resolution and unstable frame rate; in this case, signal processing tools have to be developed keeping in mind such limitations.

7.2.2 Movement Analysis with Wearable Sensors

In this section, we provide an overview of several features extracted from a wearable accelerometer that are correlated with the risk of falling.

First of all, the location where the sensor is worn matters and the features change accordingly; the most used position is the waist close to the lower back. Since such position is close to the center of mass of the human body, it is less affected by quick movements. Another common position is the chest but this location is affected by instability of the upper trunk. Moreover, when using a triaxial accelerometer, the axis is approximately aligned to the three canonical axis named mediolateral, vertical, and anteroposterior, respectively. Therefore, two accelerometers measuring the same movement will have different values based on their orientation in the space. In order to have precise measurements, it would be necessary to project the data onto the canonical axes. However, the projection requires complex algorithms and calibration and therefore, it is not practically usable at home.

Features can be defined into two groups: (i) balance features; and (ii) gait features. Balance features require the use of quantities sensitive to the presence of movements. The root mean square (RMS) is a measure of variability and therefore, it is particularly suitable to differentiate between a stable position (e.g., orthostatic) and an unstable one. O'Sullivan et al. [20] found that the RMS of the vector magnitude (VM) during standing is correlated with the risk of falling. The algorithm was the following:

- collect a triaxial accelerometer signal $X_{k,}\ Y_{k,}\ Z_k$ (k is the time instant) with a fixed sampling rate;
- compute VM as follows:

$$\mathrm{VM}_k = \sqrt{X_k^2 + Y_k^2 + Z_k^2} \tag{7.2}$$

- compute RMS of 20 s of VM (N is the number of samples in 20 s)

$$\mathrm{RMS} = \sqrt{\frac{\sum_{k=1}^{N} \mathrm{VM}_k}{N}} \tag{7.3}$$

RMS has been found to be correlated with the risk of falling during a balance test in the orthostatic position while an accelerometer was worn at the lower back [20].

Regarding gait, Moe-Nilssen and Helbostad [33] defined step regularity, stride regularity, and step symmetry using the normalized autocorrelation function (NACOR) of the vertical acceleration collected from an accelerometer placed approximately on the center of mass during walking on straight walkway. Due to the periodicity of the movements, NACOR is a periodic signal as well. The first peak of NACOR is associated to the time-interval and regularity of steps while the second one to those of strides. Step regularity is defined as the amplitude of NACOR at the first peak (A_{d1} as in [33]) whereas stride regularity as the amplitude of the second peak (A_{d2}). Step symmetry is then derived by computing the ratio of the step and stride regularities (A_{d1}/A_{d2}). Consequently, step symmetry is 1 when A_{d1} and A_{d2} are similar between each other.

Other important features are step and stride frequencies. These two values can be extracted from NACOR as well. Indeed, the time-lags associated with A_{d1} and A_{d2} represent the average time-interval between consecutive steps and strides, respectively. Therefore, the inverse of such lags defines the average amount of steps and strides in the time unit.

7.2.3 Actigraphy and HRV-Based Methodologies for Automatic Sleep Quality Assessment

The main quantity measured by actigraphs is called activity count (AC) and it is supposed to be correlated with the "amount" of movement. However, the definition of "amount" is vague and each device manufacturer has its own closed-source algorithm. Such uncertainty relies on historical and technological reasons. Indeed, being the actigraph a device developed in the 70s, the low computational power and the battery required to be as much optimized as possible to be run for days. With time passing, during the years, technology progressed in such a way to have miniaturized triaxial accelerometers that can acquire accelerometer signals at fast rate for weeks. However, even with the new available technology, AC is still used and remains a valid candidate for automatic sleep classification.

AC can be computed in three common ways [27] assuming to have a signal proportional to the "amount" of movement: (i) time above threshold (TAT); (ii) zero-crossing (ZC); and (iii) digital integration (DI). First, time above threshold

counts how much time the signal remains above a predefined threshold. Second, zero-crossing counts how many times the signal crosses a predefined "small" threshold. Third, digital integration computes the area of the rectified signal. Each of these techniques has several characteristics, but mainly (i) sensitivity to the amplitude (DI); (ii) sensitivity to the time duration (TAT); and (iii) sensitivity to high-frequency components (ZC). In sleep studies, zero-crossing is the most widely used modality. However, the other two modalities work as well [34].

Here, we report a possible algorithm meant to compute ACs from a triaxial accelerometer using a ZC technique:

1. collect a triaxial accelerometer signal X_k, Y_k, Z_k (k is the time instant) with a fixed sampling rate;
2. compute VM (Eq. (7.2) of Sect. 7.2.2)
3. filter VM_k with a bandpass filter in the frequency band 0.25 and 3 Hz [27] (it removes gravity and most of the movements not associated with human activity);
4. rectify the filtered signal (e.g., absolute value);
5. count how many times the rectified signal crosses a "small" threshold (in single or double direction).

The "small" threshold has to be determined in such a way to be robust to the noise level when the actigraph is not moving or alternatively, it might be determined directly on the PSG data (e.g., ROC analysis).

For sleep studies, ACs are determined on either 30 s or 1 min epoch along an entire night. Such ACs are then injected into a classifier to provide an estimate of the sleep stage. In order for a classifier to estimate the sleep stage in a specific epoch, it is necessary to involve ACs of surrounding epochs. One of the most investigated classifier is in the following form:

$$P = \sum_{i=-B}^{A} \alpha_i \mathrm{AC}_i + \beta f(\mathrm{AC}_{-b}, \mathrm{AC}_{-b+1}, \ldots, \mathrm{AC}_a) \tag{7.4}$$

where P is the probability of having a sleep epoch, B and A are the number of previous and successive epochs to consider, α_i and β are model coefficients and f is a *non*-linear function involving the ACs. For example, Cole et al. [35] used a linear classifier (i.e., $\beta = 0$) with 4 min before and 2 min after the current epoch.

It is worth noting that the performance of the classifier highly depends on the model itself and on the total number of epochs considered. Other common classifiers for automatic sleep classification are support vector machine (SVM), linear discriminant analysis (LDA) and artificial neural networks (ANN).

Regarding HRV for sleep studies, the relevant features are substantially the same described in Sect. 7.2.1. However, to reduce intersubject variability, features might be modified. The strategy used in [30] divides the average RR series (inverse of the average heart rate) in a given set of consecutive epochs ($A + B + 1$ is the total number of epochs) by the average RR computed on the whole night. In this way, if

the subject is healthy, the ratio is likely to be heavily weighted by the total deep sleep time obtaining values close to 1 during sleep and far from 1 during wake.

Even in this case, the number of surrounding epochs has to be determined for each set of feature and classifier selected.

7.3 Future Challenges for Signal Processing in mHealth

In this chapter, we described the current state-of-the-art technology of mHealth used in combination with wearable devices for three different domains, i.e., cardiac monitoring, movement analysis and sleep quality assessment. Despite mHealth is a growing field that involves efforts from research institutes and investments from med-tech industries, it is still far from being widely utilized as a trustable option for health monitoring. The main reasons could be the widely spread presence of *non*-clinically relevant mobile applications [10, 36] or the social unacceptance of such technologies. Even though we respect such skepticism, we also believe that mHealth and wearable devices represent a new efficient way for long-term health monitoring and might revolutionize the health care system sectors worldwide.

Regardless of the applicative domain, signal processing in mHealth will play an important role in two areas. The first one refers to the engineerization of the products already available on the market. This means that signal processing algorithms will be optimized to achieve longer battery life and more precise measurements. The second one involves scientific research and, more specifically, being new sensors and wearables developed in a continuous fashion, it is necessary to understand whether such devices would have a clinically relevant role. In this context, signal processing in combination with feature extraction are the means to test the impact of the new mHealth technology on one's health.

References

1. Istepanian, R., Laxminarayan, S., Pattichis, C.S. (eds.): Emerging Mobile Health Systems. Springer US (2006)
2. Ekeland, A.G., Bowes, A., Flottorp, S.: Effectiveness of telemedicine: A systematic review of reviews. Int. J. Med. Inform. **79**(11), 736–771 (2010)
3. Silva, B.M., Rodrigues, J.J., de la Torre Díez, I., López-Coronado, M., Saleem, K.: Mobile-health: a review of current state in 2015. J. Biomed. Inform. **56**, 265–272 (2015)
4. United Nations: World Population Ageing. Technical report, Department of Economic and Social A airs, Population Division, 2015. ST/ESA/SER.A/390
5. Mukhopadhyay, S.C.: Wearable sensors for human activity monitoring: a review. IEEE Sens. J. **15**(3), 1321–1330 (2015)
6. Mendis, S., Puska, P., Norrving, B., World Health Organization, World Heart Federation, and World Stroke Organization (eds.): Global Atlas on Cardiovascular Disease Prevention and Control. World Health Organization in collaboration with the World Heart Federation and the World Stroke Organization, Geneva (2011)

7. NCD Risk Factor Collaboration (NCD-RisC): Worldwide trends in blood pressure from 1975 to 2015: a pooled analysis of 1479 population-based measurement studies with 19 1 million participants. Lancet **389**(10064), 37–55 (2017)
8. Deyell, M.W., Krahn, A.D., Goldberger, J.J.: Sudden cardiac death risk stratification. Circ. Res. **116**(12),1907–1918 (2015)
9. Borne, R.T., Katz, D., Betz, J., Peterson, P.N., Masoudi, F.A.: Implantable cardioverter-defibrillators for secondary prevention of sudden cardiac death: a review. J. Am. Heart Assoc. **6**, e005515 (2017)
10. Martinez-Perez, B., de la Torre-Diez, I., Lopez-Coronado, M., Herreros-Gonzalez, J.: Mobile Apps in Cardiology: review. JMIR mhealth and uhealth **1**(2), e15 (2013)
11. Gambi, E., Agostinelli, A., Belli, A., Burattini, L., Cippitelli, E., Fioretti, S., Pierleoni, P., Ricciuti, M., Sbrollini, A., Spinsante, S.: Heart rate detection using microsoft kinect: validation and comparison to wearable devices. Sensors **17**(8), 1776 (2017)
12. Iozzia, L., Cerina, L., Mainardi, L.: Relationships between heart-rate variability and pulse-rate variability obtained from video-PPG signal using ZCA. Physiol. Meas. **37**(11), 1934–1944 (2016)
13. Siddiqui, S.A., Zhang, Y., Feng, Z., Kos, A.: A pulse rate estimation algorithm using PPG and smartphone camera. J. Med. Syst. **40**(5), 126 (2016)
14. Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology: Heart rate variability: standards of measurement, physiological interpretation and clinical use. Circulation **93**(5), 1043–1065 (1996)
15. Sharma, M., Barbosa, K., Ho, V., Griggs, D., Ghirmai, T., Krishnan, S., Hsiai, T., Chiao, J.-C., Cao, H.: Cu-less and continuous blood pressure monitoring: a methodological review. Technologies **5**(2), 21 (2017)
16. Nordin E, Lindelöf N, Rosendahl E, Jensen J, Lundin-Olsson L.: Prognostic validity of the Timed Up-and-Go test, a modified Get-Up-and-Go test, staff's global judgement and fall history in evaluating fall risk in residential care facilities. Pubmed ref: https://www.ncbi.nlm.nih.gov/pubmed/18515291
17. World Health Organization (ed.): WHO global report on falls prevention in older age. World Health Organization (2008)
18. Wren, T.A.L., Gorton, G. E., Ounpuu, S., Tucker, C. A.: Efficacy of clinical gait analysis: a systematic review. Gait Posture **34**(2), 149–153 (2011)
19. Giansanti, D., Maccioni, G., Cesinaro, S., Benvenuti, F., Macellari, V.: Assessment of fallrisk by means of a neural network based on parameters assessed by a wearable device during posturography. Med. Eng. Phys. **30**(3), 367–372 (2008)
20. O'Sullivan, M., Blake, C., Cunningham, C., Boyle, G., Finucane, C.: Correlation of accelerometry with clinical balance tests in older fallers and non-fallers. Age Ageing **38**(3), 308–313 (2009)
21. Senden, R., Savelberg, H.H.C.M., Grimm, B., Heyligers, I.C., Meijer, K.: Accelerometry based gait analysis, an additional objective approach to screen subjects at risk for falling. Gait Posture **36**(2), 296–300 (2012)
22. Narayanan, M.R., Redmond, S.J., Scalzi, M.E., Lord, S.R., Celler, B.G., Lovell, N.H.: Longitudinal falls-risk estimation using triaxial accelerometry. IEEE Trans. Biomed. Eng. **57**(3), 534–541 (2010)
23. Tinetti, M.E., Williams, T.F., Mayewski, R.: Fall risk index for elderly patients based on number of chronic disabilities. Am. J. Med. **80**, 429–434 (1986)
24. Rivolta, M.W., Aktaruzzaman, Md., Rizzo, G., Lafortuna, C., Ferrarin, M., Bovi, G., Bonardi, D. R., Sassi, R.: Evaluation of the Tinetti score and fall risk assessment via accelerometry-based movement analysis. Pubmed ref: https://www.ncbi.nlm.nih.gov/pubmed/30195985
25. Iber, C., Ancoli-Israel, S., Chesson, A. L., Quan, S. F., et al.: The AASM Manual for the Scoring of Sleep and Associated Events: Rules, Terminology, and Technical Specifications, 1st edn. American Academy of Sleep Medicine, Westcherster, IL, U.S.A. (2007)
26. Kripke, D.F., Mullaney, D.J., Messin, S., Wyborney, V.G.: Wrist actigraphic measures of sleep and rhythms. Electroencephalogr. Clin. Neurophysiol. **44**(5), 674–676 (1978)

27. Ancoli-Israel, S., Cole, R., Alessi, C., Chambers, M., Moorcroft, W., Pollak, C.P.: The role of actigraphy in the study of sleep and circadian rhythms. Sleep **26**(3), 342–392 (2003)
28. Redmond, S.J., de Chazal, P., O'Brien, C., Ryan, S., McNicholas, W.T., Heneghan, C.: Sleep staging using cardiorespiratory signals. Somnologie **11**(4), 245–256 (2007)
29. Aktaruzzaman, Md, Migliorini, M., Tenhunen, M., Himanen, S.L., Bianchi, A.M., Sassi, R.: The addition of entropy-based regularity parameters improves sleep stage classification based on heart rate variability. Med. Biol. Eng. Comput. **53**(5), 415–425 (2015)
30. Aktaruzzaman, Md., Rivolta, M.W., Karmacharya, R., Scarabottolo, N., Pugnetti, L., Garegnani, M., Bovi, G., Ferrarin, M., Sassi, R.: Performance comparison between wrist and chest actigraphy in combination with heart rate variability for sleep classification. Comput. Biol. Med. (2017)
31. Sassi, R., Cerutti, S., Lombardi, F., Malik, M., Huikuri, H.V., Peng, C.K., Schmidt, G., Yamamoto, Y.: Advances in heart rate variability signal analysis: joint position statement by the e-cardiology ESC working group and the European heart rhythm association co-endorsed by the Asia Pacific heart rhythm society. Europace **17**(9), 1341–1353 (2015)
32. Peng, R.-C., Zhou, X.-L., Lin, W.-H., Zhang, Y.-T.: Extraction of heart rate variability from smartphone photoplethysmograms. Comput. Math. Methods Med. **2015**, 1–11 (2015)
33. Moe-Nilssen, R., Helbostad, J.L.: Estimation of gait cycle characteristics by trunk accelerometry. J. Biomech. **37**(1), 121–126 (2004)
34. Johnson, N.L., Kirchner, H.L., Rosen, C.L., Storfer-Isser, A., Cartar, L.N., Ancoli-Israel, S., Emancipator, J.L., Kibler, A.M., Redline, S.: Sleep estimation using wrist actigraphy in adolescents with and without sleep disordered breathing: a comparison of three data modes. Sleep **30**(7), 899–905 (2007)
35. Cole, R.J., Kripke, D.F., Gruen, W., Mullaney, D.J., Gillin, J.C.: Automatic sleep/wake identification from wrist activity. Sleep **15**(5), 461–469 (1992)
36. Ong, A.A., Gillespie, M.B.: Overview of smartphone applications for sleep analysis. World J. Otorhinolaryngol. Head Neck Surg. **2**(1), 45–49 (2016)

Chapter 8
mHealth Services: Examples and Future Perspectives

Gabriella Borghi, Loredana Luzzi and Cristina Masella

Abstract The potential impact of the adoption of mHealth solutions on the health care and social care sectors has become clearer and key stakeholders have been involved. Despite these improvements, mobile telemedicine remains a grey area: problems persist in the lack of interoperability between mHealth solutions and EU healthcare systems and liability for damages caused by the use of mHealth solutions are still unclear. However, some lessons emerge by the experiences developed so far.

8.1 An Overview of mHealth Initiatives Globally

In April 2014, the European Commission acknowledged the relevance of mobile health publishing the 'Green Paper on Mobile Health' and launching a public consultation in which EU [1] invited stakeholders to provide their views on barriers to the uptake of mHealth in the EU. In the Green Paper mobile health (hereafter 'mHealth') is defined as 'medical and public health practice supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices'. Few years before the World Health Organization published mHealth New horizons for health through mobile technologies [2], the results of a global survey aimed at studying four aspects of mHealth (level of adoption, types of initiatives, status of monitoring and evaluation, barriers to implementation) among 14 categories of mHealth services. The survey shows that at least one type of mHealth service was offered in the majority of Member States (83%) and that many countries offered four to six programmes. The four most frequent mHealth initiatives were health call centres (59%), emergency toll-free telephone services (55%), managing

G. Borghi
Cefriel Scarl, Politecnico di Milano, Viale Sarca, 226, 20126 Milan, Italy

L. Luzzi
University of Milano Bicocca, Piazza dell'Ateneo 1, 20126 Milan, Italy

C. Masella (✉)
DIG Department, Politecnico di Milano, Via Lambruschini 4B, 20156 Milan, Italy
e-mail: cristina.masella@polimi.it

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_8

emergencies and disasters (54%) and mobile telemedicine (49%). The use of mobile devices for emergency was reported by over 48% of Member States across all regions, except the African and Eastern Mediterranean Regions. The least frequently reported initiatives were health surveys (26%), surveillance (2%), awareness raising (23%) and decision support systems (19%). Most of the mHealth programmes were in the pilot or informal stage. The report also pointed out that higher income countries show more mHealth activity than do lower income countries. Countries in the European Region are currently the most active and those in the African Region the least active. mHealth is most easily incorporated into processes and services which historically use voice communication through conventional telephone networks.

In 2016, the WHO mHealth Technical Evidence Review Group published the Guidelines for reporting of health interventions using mobile phones: Mobile health (mHealth) Evidence reporting and assessment (mERA) checklist [3]. The purpose was to improve the quality of reporting of mHealth initiatives, defining a minimum set of information that should be collected. The authors state that through widespread adoption, these guidelines should standardize the quality of mHealth evidence reporting, and indirectly improve the quality of mHealth evidence (Fig. 8.1).

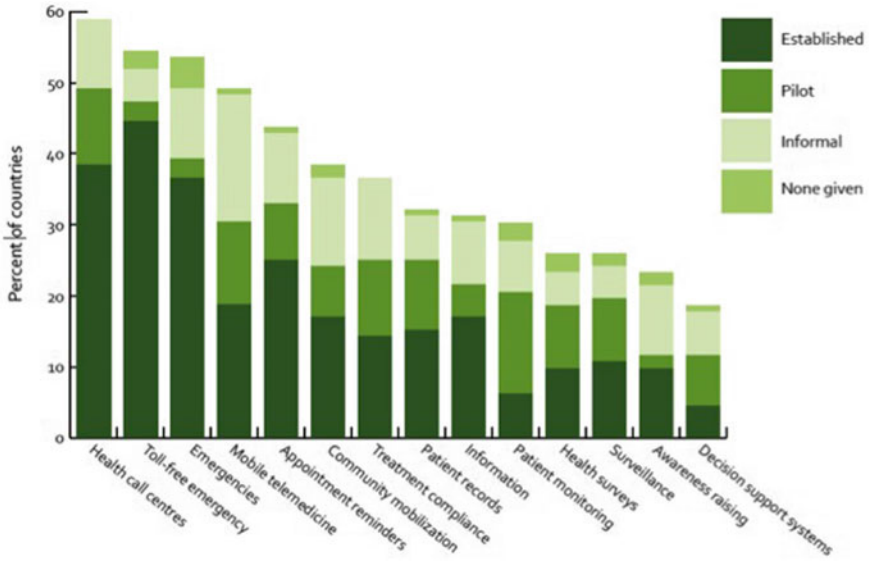

Fig. 8.1 Adoption of mHealth initiatives and phases, globally

8.1.1 *Adoption of mHealth Initiatives: From Small Pilot Programmes to Large-Scale Deployments*

Mobile surfing by smartphone has surpassed in Italy, by the end of 2014, desktop surfing by computer. In the world, 51.3% of Internet traffic comes from smartphones and tablets. This significant 'overtaking' show that smartphones, with more and more powerful models and ease of use, support citizens in many everyday situations. Thus, mHealth may potentially transform citizens' lifestyle and way of working of health and social workers and, consequently, may have a global impact on the care both in the rich and poor countries.

Already today, several are the examples of mHealth applications: text messages for administrative requirements (e.g. confirm reservations), Whatsapp for sending images, Point of Care Testing (POCTs) to carry out laboratory examinations, diffusion of wearable technologies and sensors to monitor clinical parameters. Moreover, a number of health apps have been developed, both for medical purpose and lifestyle management. They are usually available in the app stores, either free of charge or for hire, but also in specialized portals or public and/or private websites. It is estimated that 165,000 apps for health exist on the international market (in Italy about 5000). But in this case, just less than 25% are dedicated to the Disease and Treatment management, as can be seen from Fig. 8.2.

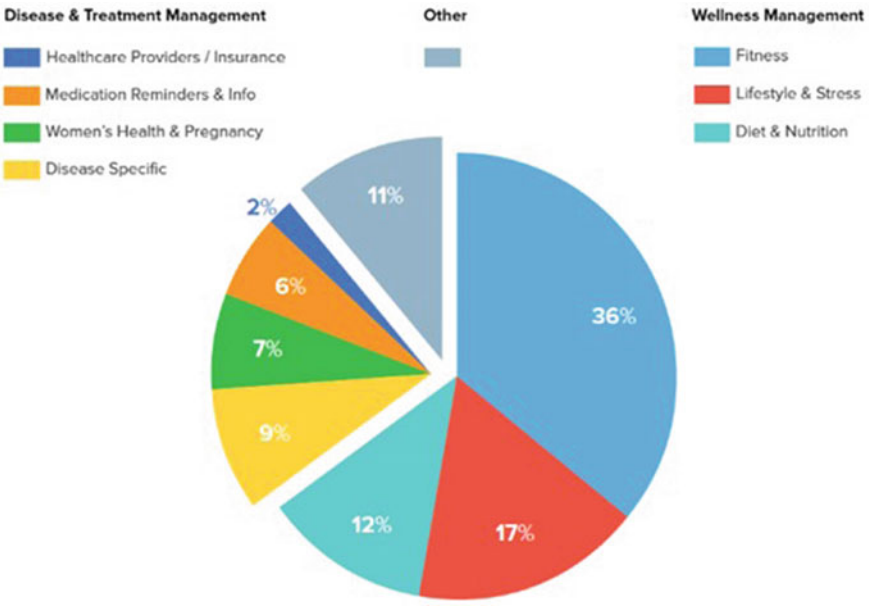

Fig. 8.2 mHealth apps by category—Mevvy, June 2015; IMS Health, AppScript, June 2015; IMS Institute for Healthcare Informatics, August 2015. *Source* Mevvy

8.1.1.1 Portals of Apps and Medical Device

The most popular health apps mainly concern wellness management (fitness, lifestyle and stress, diet and nutrition), but a growing number of more clinical apps are being developed: information both towards clinicians and citizens; treatment of specific diseases; chronic disease management; management of drugs (how to remember their uptake and where to find a pharmacy). Not all the extant apps are 'Mobile Medical Apps'. To be defined in such a way, apps should be comparable (and marked for conformance) to a medical device, according to the definition contained in the Directive 93/42/EEC.

In Italy, this context is studied by the Healthcare App Observatory, established in 2015 by a collaboration between the Ministry of Health and the Formit Foundation. The observatory provides a database for all the available apps, classified by pathology and reported with some essential information such as purposes and functionalities, operating systems and link to download the existing apps [4]. In December 2017, the number of apps in the database were 701 (but only 2% of them classified as medical device), out of them 102 were related to cardiology and 59 to internal medicine. Surfing on this portal is possible to find specific mHealth initiatives, using filters such as the medical branches, medical devices used, functionalities and target users. Some of these initiatives are described below to give a view of the complexity of the innovations in progress and to clarify the potential impact that these transformations are producing and will be able to produce in a short time.

The Open Smart Register Platform (OpenSRP) [5] is a software system that supports frontline health workers to electronically register and monitor their client's health. Using mobile phones or tablets, the system frees health workers from cumbersome paperwork and helps to ensure that every individual is reached with essential health interventions. Using emerging mHealth best practices automated reminders and reporting, decision support, multimedia counselling OpenSRP builds on the existing robust mobile technologies to deliver a powerful and dependable application to skilled health workers, empowering them to more effectively deliver and account for the care they provide to their clients [5]. The application has the support of WHO, UNICEF and several technology partners. It is used in several countries including Pakistan, Indonesia, Bangladesh.

Several are the projects on mobile health for tobacco control promoted by WHO (mSmoke-free, mCessation, mAwareness, mTraining, mIllicit) and many experiences borned at national level. For example, Maccabi Healthcare services, in Israel, developed a health app ecosystem using medical devices (mobile, wearable and home based) for health management. Kaiser Permanente in the United States carries out about one-third of meetings in 'primary care' by email, using mobile teledermatology. Some German insurance companies provide the reimbursement of the Medical Apps Caterna [6] and NeuroNation [7]. Caterna's therapy, initially developed at the University of Dresden and with the CE mark since 2011, is prescribed with the occlusion therapy, which is an eye patch worn over the child's strongest eye, in order to strengthen the weakest one. With Caterna, the child has regular training sessions. NeuroNation is a cognitive training website and the app is launched in

Fig. 8.3 Medical apps website

2011. NeuroNation's cognitive training content was developed in concert with psychologists of the Free University of Berlin and Technische Universitt Dortmund and is offered in eight languages. There is also an Italian reference: accessible to general public through a portal called MEDUSA (MEDicina Utenti Salute online), it was created by the Istituto Superiore di Sanit in collaboration with the Department of Clinical Medicine of 'Sapienza' University of Rome, in order to raise awareness and provide access to valuable and reliable sources of healthcare information.

On the website, it is possible to find a number of services designed for health professionals (doctors, nurses and physiotherapists). MedicalApps [8], for instance, is specifically designed for the doctors that use smartphones and tablets registered in the network who can download and activate apps (Fig. 8.3).

iMedicalApps [9] is 'the online publication for medical professionals, patients and analysts interested in mobile medical technology and healthcare apps. The editors lead a team of physicians, health professionals, medical trainees, and mHealth analysts in providing reviews, research, and commentary on mobile medical technology'. Coming from the experiences of iMedicalApps, it is developed iPrescribeApps.com, a platform that will enable providers to prescribe health apps to their patients (Fig. 8.4).

Mobimed.it [10] is an Italian blog, born in 2009 to provide doctors, nurses, pharmacists, students and health workers with a guide to applications, accessories and medicine resources for mobile device (smartphones and tablets). The site aims to recommend the best medical applications for smartphones and tablets and to update users with news, reviews, insights and links on the news of 'mobile medicine'. Refer-

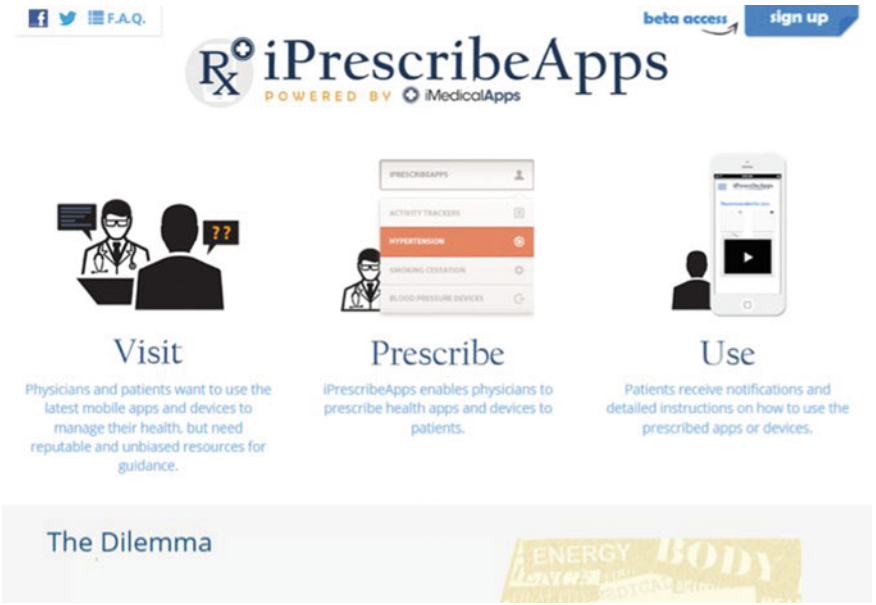

Fig. 8.4 iPrescribe apps

ring to portals for patients it is worth noting PatientView [11], which allows the user to search information about available apps filtering according to the pathology, to the mobile platform user have and also to his/her language.

8.1.1.2 Apps in the Italian Context

In Italy, there are some experiences that confirm the interest of using mHealth as an innovative way for the management of health. Booking an exam, paying it, collecting a medical report, but also checking the queue or the waiting time in the emergency department are the issues that some regions or companies have tried to address, improve and solve with apps. These are free solutions thought for citizens, but they often allow a saving also for the organizations.

TreC Project (Cartella Clinica del Cittadino—Citizen Clinical Record) is a research and innovation project in the field of Electronic Health (eHealth) of the Autonomous Province of Trento, developed with the support for the technical-scientific management of the Bruno Kessler Foundation. The project that aimed at creating a digital applications platform for citizens and started in 2012 with a basic module of online reports on the web, is now a service offered by the provincial health system to all citizens. It allows the users to: consult at any time all their online medical reports, keep diary of their health status, consult pharmaceutical prescripitions, pay on line—by credit card—and manage medical records of children.

In December 2017, more than 80,000 citizens were using the platform, more than 2000 payments and 60,000 online booking were made through the platform, thus demonstrating interest and capacity for use by citizens.

In the **Lombardy Region,** there are some apps accessible free of charge from the healthcare portal (www.crs.regione.lombardia.it/sanita) aimed at booking, checking waiting time of emergency departments and downloading medical record. The number of access to the portals is growing and new apps, targeted at specific topics such as vaccinations, medical prescriptions, gluten-free receipts, will soon be available (Table 8.1).

CAREGGI SMART Hospital is a free app for smartphones and tablets that allows the user to consult his/her health information and to interact with the hospital information system. The app helps people in orienting themselves when visiting the (large) Italian hospital, it provides social and health information for patients and family members, ranging from supportive actions such as diabetic risk calculations to timetable of public transport. Once registered, the user can consult real-time exam medical reports and book a blood sample using '#prelievo amico' which allows him to choose date and time and access directly (without queue) the laboratory. An innovative service is offered by 'AnticoagulanteAmico': a new app, integrated with the hospital system that provides, for patients that need an anticoagulant therapy, a personalized therapeutic plan and tricks to control adhesion and persistence, ensuring in this way hospital-territory integration and improving patients behaviour.

Qurami is the app used by Humanitas, an Italian private hospital, to better manage the waiting time: it allows patients to queue before they physically reach the reception. The app notifies patients when it is time to go to the reception because the call of their number is now close. Over 300,000 downloads in 4 years and 400 h of estimated saving of time are reported.

AMD Algoritmi per la terapia personalizzata (Personalized Therapy Algorithms) aims at simplifying the choice of a suitable therapy for a particular patient. The doctor, through the characteristics of the patient under review, is guided in the interpretation of AMD decision-making algorithms, in order to identify the best suited therapeutic approach. Intending to act as a practical tool to help to overcome

Table 8.1 Source LISPA latest data as at 7 June 2017

App	Date of release	Installations on android	Installations on iOS
SALUTILE Referti	9 May 2016	Total: 17,286 Active: 11,194	12,993(*)
SALUTILE Pronto Soccorso	6 June 2016	Total: 13,318 Active: 9316	9691(*)
SALUTILE Prenotazioni	15 May, 2015	Total: 29,004 Active: 13,273	20,912(*)

(*) users who agreed to share their information with App developers

therapeutic inertia, AMD algorithms are now available as an app, which can be downloaded for free by any doctor.

AIFA (Agenzia Italiana del Farmaco) updated the algorithm for the approach of type 2 diabetes mellitus therapy in collaboration with SID (Societ Italiana di Diabetologia) and AMD in June 2016. 'This algorithm represents a further evolution of the innovative online system to identify the glycemic target and calibrate the pharmacological treatment on the needs of the individual patient, reconciling the different and several hypoglycemic alternatives with the most up-to-date evidence available' said AIFA General Director, Director General. The application also contains other useful tools for the daily doctor's clinical practice such as Diabetes risk calculator (Toumiletho Questionnaire), HbA1c value converter, BMI calculator.

DID Plus Diario Interattivo del Diabete (Interactive Diabetes Diary) simplifies the daily management of insulin therapy and makes carbohydrate count easier. DID Plus helps to calculate the bolus of insulin and send all stored data to the diabetologist in order to check the progress of the therapy and, if necessary, modify it. Currently, the app has been downloaded 1908 times and it is active in 882 installations.

InfoStranieri per la Salute is a multilingual app dedicated to the prevention of infectious diseases and the promotion of vaccinations for foreign citizens. Thanks to the app, the user will be able to view information about the services provided by the Regional Health Service, to carry out a vaccination check-up for the all family members, to calculate a personal risk score for tuberculosis and contact the migrant friendly Prevention Services.

Viaggia in Salute is an app developed by ATS Milano (a local health authority) that offers advises and information to everyone is programming a travel abroad. Translated in several languages, it is focused on infectious risks and preventive measures, vaccine and travel kit of drugs that must be taken before leaving.

8.2 Constraints and Opportunity to Health Implementation

Patients agree that mHealth will improve the quality and cost of health care, but the common opinion is that there are still several obstacles to overcome before reaching a significant spread of these solutions.

The EU public consultation on Mobile Health [12] collected 211 responses from public authorities, healthcare providers, patients organizations and web entrepreneurs, both inside and outside the EU on 11 issues related to the spread of mHealth in the EU. According to the green paper, the factors that hinder the development of mHealth in Europe are privacy and data security, patient safety, a clearer and better legal framework, a clear evidence of cost-effectiveness and the interoperability and the standardization of technological solutions are. Nearly, half of respondents believe that in order to build user confidence, it is necessary to develop powerful tools for managing privacy and security (such as data encryption and authentication mechanisms), but someone warns against the risks of an excessive regulation. Web entrepreneurs ascribe the difficulty to access to the market to the lack of a

clear regulatory framework, interoperability standards and common quality criteria. Respondents suggest that EU countries should ensure the interoperability of the mHealth solutions with electronic medical records and adopt open standards. Evidence of cost-effectiveness of mHealth is still poor. Some data coming from Nordic countries state that mHealth can lead to a 50–60% reduction of nights in the hospital and re-hospitalization for patients with a chronic obstructive pulmonary disease, and a reduced expenditure of 25% in the overall care of elderly people. Following the diffusion of the green paper, a mHealth stakeholder meeting took place to address ongoing and potential future policy actions in the field of mobile health, in 2015 in Riga [13]. The EU Commission presented an initiative related to a Code of Conduct that has been finalized in 2016 [14]. The objective of this code is 'to foster citizens' trust in mHealth apps, raise awareness of and facilitate compliance with EU data protection rules for app developers'. Moreover a Working Group on mHealth assessment guidelines was established and a report, including few case studies on mHealth, was published in 2017 [15]. Unfortunately, although the Working Group put a considerable amount of work, no minimum level of consensus among the members of the Working Group has been reached: guidelines address a fast moving and evolving range of technologies and regulatory initiatives were not stable. In the meantime, two important regulations that impact mHealth apps (such as the new Medical Devices Regulation and the new General Data Protection Regulation) were issued and regulatory initiatives at Member State level have evolved significantly during the same period.

Moreover, as clearly pointed out by WHO, policymakers and administrators need to have the necessary knowledge to make the transition from pilot programmes to strategic large-scale deployments (WHO Report on mhealth 2011 [16]). As a matter of fact, mHealth interventions consist mostly of pilot projects or small-scale implementations that have been focused on studying feasibility and effects, with little attention paid to the infrastructure needed for scaling up and sustaining the mHealth product. This is the reason why a limited understanding of what may be required to translate these projects into large-scale deployments exists. The current literature surrounding scaling up mHealth offers many recommendations for addressing identified challenges; while important, such recommendations may not be readily actionable. In response to this need, WHO supported the design of the MAPS Toolkit 'to help project teams in conducting self-assessments, review progress and develop plans to improve their ability to scale up and achieve sustainability of their mHealth products' [17].

8.3 Conclusion

Over the last years, the potential, and some would argue disruptive, impact of the adoption of mHealth solutions on the health care and social care sectors has become clearer. The policy responses to these developments by key stakeholders have also evolved. Despite these improvements, as pointed out during the Conference "The

Future of Mobile Health in Europe", held Brussels in February 2017, mHealth is still a grey area, with unclear liability for damages arising from the use of mHealth solutions and problems caused by the lack of interoperability between mHealth solutions and EU healthcare systems.

Nevertheless, country appetite for mHealth has exceeded expectations [18] and some lessons emerged by the work done within 'Be He@lthy, Be Mobile', a WHO initiative to collect experiences within national health systems. The experiences are:

- start simple: a basic SMS programme which works will have better health outcomes and build a stronger case for adding other programmes in the future;
- political commitment is needed from government authorities: each mHealth service must be integrated into a countries broader strategy and action plan for the condition that it is targeting;
- user engagement is crucial: getting users to register in is one thing, but helping people to maintain their use of an mHealth can be challenging;
- robust monitoring and evaluation needs to be set up from the beginning because what gets measured gets done;
- mHealth is not a short term business case for mobile operators: benefits are more on long-term skills upgrading as a service provider.

References

1. Green Paper on mobile Health (mHealth) Brussels, 10.4.20114 COM(2014) 219
2. World Health Organisation: mHealth New horizons for health trough mobile technologies, Global Observatory for eHealth series, vol. 3 (2011)
3. Agarwal, S., Lefevre, A.E., Lee, J., L'engle, K., Mehl, G., Sinha, C., Labrique, A., Vasudevan, L., Tamrat, T., Kallander, K., Mitchell, M., Aziz, M.B., Froen, F., Ormel, H., Muniz, M., Asangansi, I.: Guidelines for reporting of health interventions using mobile phones: mobile health (mHealth) Evidence reporting and assessment (mERA) checklist. BMJ **352** (2016)
4. Database Health App: http://www.appsanitarie.it/banca-dati-app-sanitarie
5. Open Smart Register Platform: http://smartregister.org/
6. Medical Apps Caterna: http://www.mobihealthnews.com/31549/caterna-offers-prescribable-reimbursed-eye-strengthening-gaming-app-in-germany
7. NeuroNation: https://www.neuronation.com/
8. MedicalApps: https://www.medicalapps.it/
9. iMedicalApps: http://www.imedicalapps.com/
10. mobimed.it Italian Blog: http://mobimed.it/
11. PatientView Search Site: http://www.patient-view.com/-bull-directories.html
12. EU Public Consultation on Mobile Health: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-green-paper-mobile-health
13. mHealth in Europe: Next steps discussed at eHealth Week in Riga https://ec.europa.eu/digital-single-market/en/news/mhealth-green-paper-next-steps
14. Privacy Code of Conduct on mobile health apps. https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps
15. Report of the Working Group on mHealth assessment guidelines. https://ec.europa.eu/digital-single-market/en/news/report-working-group-mhealth-assessment-guidelines
16. WHO Report on mHealth. http://www.who.int/goe/publications/goemhealthweb.pdf (2011)

17. mHealth MAPS toolkit-mHealth Assessment and Planning for Scale. http://www.who.int/life-course/publications/mhealth-toolkit/en/
18. Using mobile phones to increase access to health services. https://www.itu.int/en/ITU-D/ICT-Applications/eHEALTH/Behealthy/Pages/BeHealthy.aspx

Chapter 9
The Healthcare System Perspective in mHealth

Alessia Paglialonga, Anisha A. Patel, Erica Pinto, Dora Mugambi and Karim Keshavjee

Abstract mHealth is gradually leveraging changes in the way health care can be delivered. This transformation is driven by increased mobile devices' penetration and capabilities, along with growing patient data demand. New opportunities arise in the areas of telemedicine and patient monitoring as conventional clinical services (including Electronic Medical Record systems) can be integrated with mHealth devices and applications at the patient level. The benefits of mHealth can be enhanced by patient segmentation strategies and customization of services, in a way that is intended to be patient centered to meet the individual needs. Current trends and developments in technology such as rapid advances in the use of blockchains, machine learning, and artificial intelligence technologies have the potential to open unprecedented opportunities in mHealth and healthcare services. For these opportunities to translate into real benefits, further research and multi-stakeholder efforts are needed, for example, to address the issues of interoperability, information governance mechanisms, regulation and certification, and the sustainability of mHealth over the long term.

9.1 Introduction

The future of mHealth goes well beyond the pervasive use of apps for medicine, health, and fitness and wellness by patients and consumers [14, 48]. mHealth is growing and changing along with healthcare needs and, thanks to its potential benefits in terms of remote monitoring and consultation, patient data management, and

A. Paglialonga (✉)
Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni (IEIIT), Consiglio Nazionale delle Ricerche (CNR), Milan, Italy
e-mail: alessia.paglialonga@ieiit.cnr.it

A. A. Patel · E. Pinto · K. Keshavjee
Institute for Health Policy, Management and Evaluation (IHPME), University of Toronto, Toronto, ON, Canada

D. Mugambi · K. Keshavjee
InfoClin Inc, Toronto, ON, Canada

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_9

customization of patient experiences, it has the potential to transform health care and the way it is delivered. The increased penetration of capable devices along with growing patient data demand are driving a paradigm shift, where the patient becomes a direct supplier of information through wearable devices and applications [37, 38, 44]. This opens new opportunities—and challenges—in terms of healthcare delivery, as conventional clinical services can now be integrated with tools and systems at the patient level. For example, how to take full advantage of mHealth for telemedicine and remote monitoring, or how to make Electronic Medical Record (EMR) systems and, in general, hospital services interoperable in this new context are only some of the main challenges that need to be tackled in clinical practice. Successful experiences in various contexts suggest that effective, informed use of mHealth can be advantageous. At the same time, there are still important barriers in the field, and still an urgent need for further research and multi-stakeholder efforts for effective implementation [15]. This chapter will outline some of the most promising trends in the area and discuss the major challenges as well as future opportunities and research needs.

9.2 Current Trends

The development of mHealth is still a work in progress as technology is continuously evolving and its degree of penetration and adoption into the healthcare workflow varies greatly across different settings and application areas. A report by the World Health Organization (WHO) [53] found that mHealth activities are spread throughout almost all countries, but with variation in adoption and awareness levels. The potential of mHealth is related to its ubiquitous, pervasive, easy to use, and flexible character, along with the increasing sensing and computation capabilities of mobile devices.

A key area which needs to be developed in the health sector is the customization of apps to the direct needs of individual patients. The rise of the digital age has expanded the amount of information that is collected, shared and used. Large advances have been made in mass customization in the business sector. Data regarding consumers needs, attributes, preferences, behaviors, and lifestyles have become more accessible, giving businesses the opportunity to analyze, and group customers into segments [49]. From this, customized segment-based marketing strategies have been developed to foster business growth, improve customer loyalty, expand branding and increase profits [49]. It has also lead to increased consumer engagement and satisfaction.

As such, mHealth can open unprecedented opportunities for addressing challenges in health care. Some of these opportunities are related to effective, successful integration of mHealth into healthcare services in clinical as well as in nonclinical settings. In particular, recent developments in mHealth have stimulated substantial interest in the field of telemedicine and remote monitoring, integration into EMR systems, patient segmentation, and patient-centered care.

9.2.1 Telemedicine and Remote Monitoring

With the help of mHealth devices and applications, now physicians can easily diagnose or treat their patients who live in remote areas or are not able to visit their clinics, by using remote patient monitoring techniques. This is especially promising in specific target populations, for example, in individuals with dementia or elderly patients, who live independently in their home and need to be monitored, as well as for those living in rural or underserved areas with lack of multispecialist hospitals and healthcare professionals [3]. Using broadband connections, patients can be examined, diagnosed, and treated in a timely manner. There are more than 5 billion wireless communication subscribers nowadays, and more than 70% of them are in low and middle-income countries. Moreover, commercial wireless signals reach 85% or more of the world's population, extending much farther than the electrical grid [44].

Managing complicated chronic conditions outside the hospital setting can be a challenging task for both patients and their caregivers. Successful implementation of telemedicine was proven, for example, in patients with extensive bowel disorders, such as Crohn's disease and colitis, who typically require a daily intravenous infusion of nutrients and frequent interactions with the healthcare system. The University of Kansas Medical Center School of Nursing and its Center for Telemedicine and Telehealth has been conducting research to determine how to provide more convenient care for these types of patients [47]. In their telemedicine program, clinicians conduct virtual visits with patients who have been supplied with video- and audio-enabled personal tablets and a 4G data plan. Visits include a review of medical history and nutritional status, home care education, and a visual examination of the patients' infusion insertion site and abdomen.

Studies such as the one mentioned here have shown that telehealth consults have reduced infection and depression rates, and increased quality of life for patients. Moreover, the mHealth approach can enable quicker diagnosis and treatment than if a patient were to set up an appointment for an in-office visit. Another important benefit of virtual visits is coordinated care as a multidisciplinary team can more easily discuss complex cases in virtual settings.

In addition to audio- and video-transmission for remote consultation, telemedicine programs can also take advantage of a very large range of sensors, data, and applications. For example, compact smart systems can be used remotely to monitor vital physiological parameters, blood pressure, oxygen saturation, photoplethysmography, blood glucose levels, EEG signals, body movements, and physical activity, fall detection, stress levels and mood assessment, sleep monitoring parameters, and so on [31]. As such, continuous patient monitoring and detection of abnormalities in real-time becomes possible. Several examples of smart, integrated, mHealth-enabled platforms for telemedicine and patient monitoring have been introduced recently. For example, the Mobihealth project is a platform that integrates the technologies of body area networks, wireless broadband communications, and wearable medical devices to enable remote management of chronic conditions and detection of emergencies [19]. Projects such as MyHeart [18] and WEALTHY [40] have developed

garment-based wearable sensors for general health monitoring of people at home and in community settings. A personal system using smartphones and wearable sensors was introduced by Gay and Leijdekkers [16], where a patient is monitored (including life-threatening anomalies) by using various types of off-the-shelf sensors (ECG, accelerometer, oximeter, weight scale, blood pressure monitor), whereas Ruiz-Zafra et al. [45] developed a scalable, interoperable platform to support mHealth systems that are based on open-source software.

In general, the provision of mobile-based telemedicine services is a promising area as demonstrated by the several platforms and services introduced in the past years. However, important issues exist in this area and need to be carefully addressed for effective, secure, seamless implementation of telemedicine programs. Some of the most challenging issues include, e.g., the need to integrate heterogeneous devices; the accuracy of vital signs and data estimation; the need to contextualize the data collected (e.g., with respect to patients conditions, status, and recent history); and, related to this, the accurate and reliable detection of abnormalities and critical events with a reduced false alarm rate [13].

9.2.2 mHealth-Enabled Electronic Medical Record (EMR) Systems

The growing field of mHealth has created ample debate on how to take advantage of mobile devices and applications (through sensing, recording, data capturing and processing, and transmission capabilities) for medical purposes. The market for health and activity tracking shows several examples of how major smartphone manufacturers have integrated health and activity tracking in the design of their mobile devices. Also, as sensors become increasingly reliable and accurate, and cloud-based services make computing capabilities virtually unlimited, health apps are also increasing beyond data recording and health tracking into prediction algorithms [29].

Further opportunities to expand the possibilities of such data to improve health outcomes come from the integration of these services with EMR systems. The integration of personal mHealth solutions with the patients EMR would facilitate monitoring, assessment, and decision-making, and contribute to ultimately improve quality of care. It could also contribute to decrease the burden on healthcare systems, which is high especially in developed countries due to an aging population, an increase of chronic diseases, the rise in healthcare costs, and the dwindling pool of healthcare professionals. Empowering patients to manage their own health and support, by tracking their health status and participating actively in treatment regimens and preventive strategies, can help address these challenges [33]. Integration of personal mHealth with EMR systems fulfills the objective of electronic health information exchange (HIE [23]) that allows doctors, nurses, pharmacists, other healthcare providers and patients to appropriately access and securely share a patient's vital medical information electronically improving the speed, quality, safety and cost of patient care

[46]. HIE envisages the creation of a health IT ecosystem in which data are securely exchanged among providers, patients can access their healthcare documents, and clinical research benefits of the aggregated data collected in clinical settings [51]. Integration of mHealth into the HIE framework would open the way to patients direct contribution to their own EMR, enabling two-way exchange from professional health information systems to patient-managed digital health systems or personal health records (PHR) [34].

The PHR is a tool to collect, track, and share past and current information about patients health. PHR records are often created and monitored by the patents themselves. PHR-based healthcare management systems can potentially improve patient engagement and data-driven medical diagnosis. A recent study demonstrated development of an EMR-tethered PHR app, named MyHealthKeeper, which allowed clinicians and patients to share lifelong data. The study showed the effectiveness of the patient-managed, clinician-guided health tracker system and its potential to improve patient clinical profiles. However, PHR adoption and acceptance by healthcare consumers are sometimes limited due to several barriers. Potential barriers can be related to technical issues (e.g., usability, work ow issues, and data security concerns), to the healthcare system (e.g., reimbursement, legal issues), or to the end user (accessibility, privacy concerns, complexity, and knowledge) [33].

To realize the full potential of mHealth-enabled PHR/EMR systems, infrastructure changes are needed to enable such personal data to synchronize with the medical records and integrate seamlessly into the healthcare system as a whole. This integration is challenging because key issues such as validation of technologies, standardization of data outputs and exchange, and integration into clinical decision-making have to be addressed [29]. Moreover, functional requirements which become particularly challenging in a mobile environment have to be fulfilled such as faithful exchange of information, data protection, interoperability, patient literacy and responsibility, clinicians attitudes, evidence for the benefits, and limitations [34].

Lack of interoperability is a major issue as it can result in decreased levels of quality of patient care and waste of financial resources. Interoperability covers different domains: technical interoperability, related to shared communication protocols for exchange of bytes; syntactic interoperability, related to shared data formats; semantic interoperability, related to shared ways to interpret the information; and organizations and services interoperability, related to shared business processes [28]. Therefore, for effective implementation of EMR systems and their integration with mHealth at the patient level, interoperability issues at the various levels have to be tackled. Significant efforts have been made to develop standards and recommendations for EMR development and integration. For example, the CEN/ISO EN13606 norm was designed for semantic interoperability in order to define a rigorous and stable information architecture for communicating an EMR among different systems or with centralized data repositories [27]. Health Level Seven International (HL7) is a non-profit organization involved in the development of international interoperability standards. HL7 messaging standards define the language and data structure required for information integration among systems [21, 22]. The openEHR is an international not-for-profit foundation, which issued a detailed and tested specification for

an interoperable, open platform for flexible electronic records systems. The SMART Health IT app platform provides a method for using open standards for integrating apps with EMRs [46].

Related to interoperability and usability of EMR systems and their exchange with personal mHealth, there is the issue of standardization of data outputs. Use of EMRs is becoming increasingly widespread and this is leading to more and more data being generated. However, these data are frequently not captured in a standardized manner and it is difficult to make them available for research and health care, thus failing to bring real-time impact on healthcare providers and patients at the point of care. Conceptual implementation models have been proposed for how structured data could be captured from multiple EMRs and used effectively by multiple stakeholders, e.g., healthcare providers, patients, researchers, public health policymakers, EMR vendors, legal officers, and not-for-profit organizations [17].

In addition to meeting the needs of a range of stakeholders, each with their own needs, for the purpose of creating meaningful information exchange systems, EMR design should also fulfill the need to manage individual and population health risk proactively. Integration with mHealth-mediated data collection at the patient level can be key to enable risk assessment and disease prevention. Collection of large amounts of data from multiple sources, and the possibility to monitor patient health form the basis for the creation of new knowledge that can be used to predict and not only to react to disease. In addition to remote sensing of physiological parameters, mHealth also facilitates the collection of individual lifelog data, e.g., on diet, exercise, and risk factors, all of which are extremely important for health and, typically, poorly captured in conventional EMRs. The same holds for interventions and outcomes data. Meaningful use of all the information collected from patients, along with advanced patient segmentation and predictive analytics can potentially pave the way to intelligent individual—and population—health management [30].

9.2.3 Patient Segmentation and Patient-Centered Care

In THINK Marketing [49], Tuckwell and Jaffey focus on the communication channels through which businesses engage with consumers. To achieve greater success in communicating with their customers, businesses may first conduct one or more of the following market segmentation techniques: Mass Marketing, Market Segmentation, Niche Marketing, and/or Direct Marketing. Each technique subdivides the target population and marketing approach. Mass marketing takes a broad marketing strategy that appeals to all consumers, while Direct Marketing is a one-to-one strategy that meets the specific needs and preferences of individual consumers. Segments can be created based on demographics (e.g. sex, income, education level), psychographics (e.g., interests, values, lifestyle), geographics (e.g., region, urbanity) and/or behavioral responses (e.g., occasion for use, the degree of brand loyalty, response to messaging). While segmentation techniques are widely known and used within the marketing realm, it is rare to see them adopted within the healthcare sector.

9.2.3.1 Applying Segmentation to Patient Care

Patient segmentation is a technique that has evolved recently in the healthcare sector, but awaits a successful approach that is applicable to a variety of contexts. Current practitioners take elements from market segmentation to direct care planning in a way that is intended to be patient-centered to meet patient needs [12]. Applications of patient segmentation include population health management; targeted messaging of healthcare information; distribution of segment-specific care services; policy or budget strategic decision-making; and development of new segment-focused products and/or services [5, 50]. These applications have the potential to be integrated to work alongside mHealth applications and programs to support patient care.

Patient segmentation has existed for quite some time, with Kaiser Permanente having segmented their patient population into subgroups (e.g., sick, well) based on health status in the 1970s [50]. However, technology and data analysis tools have increased segmentation opportunities. For example, it is now possible to predict which patients are going to lapse during treatments by analyzing existing data. This can lead to the creation of tailored interventions to meet the needs of these individuals and provide support when it is required. Developing personalized interventions for patient segments can offer more success with patient adherence to medical treatments and support patient self-management, particularly if offered through mobile technology [9, 35].

Multiple patient segmentation frameworks and applications have been explored in theory or in practice. Due to the variety and scalability of this developing field, validated approaches to patient segmentation are challenging to identify within scholarly literature. Some approaches are described below, along with their potential to be implemented on mHealth platforms and applications.

9.2.3.2 Patient Segmentation Frameworks, Approaches, and Applications

Behavioral Segmentation Models Van Dongens Patient Segmentation model proposes a dynamic, patient-centric segmentation strategy based on a 2×2 matrix of behavioral characteristics related to life events or disease stage subdivided into: readiness for change and coping status with the health condition [12]. The cross-section of each of these characteristics depicts patient illness perceptions and beliefs that may affect the degree of planning needed to address individual patient needs, thus improving health outcomes [12].

Psychographic Segmentation Models c2B solutions has developed a psychographic segmentation model that is aimed at increasing patient engagement. Psychographics considers a person's attitude, values, personality and lifestyle to segment populations based on shared motivations and preferences [5, 6]. c2B divides people into 5 categories: Self-Achievers, Balance Seekers, Priority Jugglers, Direction Takers and Willful Endurers. Self-Achievers are the most proactive, as they will attend check-ups and screenings and will research self-management practices

for their health. At the opposite extreme are the Willful Endurers, who live by the moment and avoid thinking or focusing on their future health status [6].

At TriHealth, a pilot segmentation program was implemented to engage patients with diabetes or musculoskeletal disorders with the management of their healthcare journey [5]. Each patient was classified into 1 of the 5 segments designed by c2B Solutions based on survey responses. Based on the segment, TriHealth coaches were able to tailor their coaching strategies when communicating with their patients. Results of the study demonstrated that patient segmentation used within this context improved goal attainment as well as overall patient and coach satisfaction [5].

The PATH Institute has designed a model to analyze and predict behaviors and attitudes by using psychographic segmentation to classify an individual into one of the PATHs nine Valuegraphic Profiles of healthcare consumers [26, 41]. According to PATHs studies, 90% of American adults can fit within one of their profiles, which can assist with predicting healthcare patterns (usage, risks, trust in clinicians, compliance, etc.). The nine Valuegraphic Profiles include: Clinic Cynic, Avoider, Generic, Family-Centered, Traditionalists, Loyalist, Ready User, Independently Healthy and Naturalist. By acknowledging the needs required within each segment, health services can be augmented to utilize resources more effectively.

Levels of Integration Segmentation Model Patient segmentation techniques could support integrated patient-centered care models by identifying and supporting specific patient care needs and tailor care delivery. Vuik et al. [50] propose a level of integration model based on macro-, meso- and micro-level integration and their associated population strategies. At the macro- or whole population level is the integration of care programs for all patients, such as Kaiser Permanentes integrated service model [50]. At the meso- or sub-population level, is the integration of care for a specific subpopulation based on chronic condition or other factors, such as in bundled care models. Lastly, at the micro-level, high-risk individuals are segmented for specific case management. Segmentation can help divide the population at these levels to target integrated care provision based on segment needs.

The Better Care Fund (BCF)—NHS England—How to Guide: The BCF Technical Toolkit The Better Care Fund (BCF) Task Force has a toolkit that helps healthcare organizations to perform population segmentation, risk stratification and information governance [4, 36].

BCF has recognized that the healthcare system is typically designed around conditions and clinical pathways. Consequently, individual patient needs are not addressed, and optimal resource utilization rarely occurs. Segmentation is encouraged as an approach to improving care. To perform segmentation BCF suggests that organizations divide local populations into groups based on care needs and the frequency of care that is required. There are four approaches for grouping; utilization risk (risk stratification), age and condition, social and demographic factors and behavior—however, each of these groupings carry both pros and cons. After the segmentation technique is selected and completed, healthcare organizations can determine which population segments should be targeted, and allocate funding accordingly [4].

The NHS (National Health Service) in England has also provided a list of risk stratification approved companies to assist each area within NHS to identify who

requires the highest level of care in each segment (NHS England, 2017 as cited in BCF NHS England 2014 [4]). Utilization risk identifies the possibility of the individuals using emergency services by using an algorithm (e.g. Combined Predictive Model) but this is typically only relevant to acute care. By using a risk stratification tool, people are divided into risk strata based on a risk score that can reveal where care should be targeted. This approach has been used by Care More and Kaiser [4].

Age and condition are another group that is easily outlined, but can be perceived as a generic approach. ChenMed and New York Care have been noted to use this technique. It incorporates clinicians and public perspectives on conditions, analysis of health data, and evaluation of international grouping models [4].

Patient Persona Approach Personas is a term used to describe a fictional representation of an ideal consumer [43]. Marketing companies vary in the key questions they use to create patient personas. For example, some may ask about the target audiences goals, demographics and challenges, while others will also gather information on psychographics, objections and what the organization can do to help [24, 32, 43]. Healthcare clinics can gather and analyze information regarding their patients in order to pinpoint similarities and trends [43]. Using this information, patient personas can then be created and used for creating customized care bundles.

9.2.3.3 Implementing Patient Segmentation in mHealth

Several patient segmentation frameworks and examples have been listed above. However, there are several other factors that may be key in the successful implementation of patient segmentation strategies when healthcare delivery is conducted in person or over mHealth applications.

Leveraging data from existing data sources such as EMRs or billing data can provide a foundation for future population segmentation purposes [5]. This data could be used to discern demographics, behaviors, geographics, or preferences, which can help inform care planning and delivery [5]. Additionally, it can be used to identify patterns in care delivery to support business decision-making to support health system transformation [5].

Patient activation, which is a patients capability and willingness to self-manage their own care [20], has been examined in some studies using the Patient Activation Measure (PAM) [2]. A correlation was found—higher patient activation is linked to more healthier behaviors. Thus patient activation should be possibly be considered during segmentation.

The KOPRA is a tool that is used to assess a patients communication preferences relative to age and stages of chronic disease. The KOVA tool was also developed to determine if the communication from the provider was in alignment with the patient's preferences. Together the KOPRA and KOVA tools could be used to identify top communication preferences that patients are receptive to during the patient-provider encounter.

Health literacy and numeracy can hinder the patient's ability to understand their care plan [2]. This barrier could be removed by using electronic tools to present health information in images or through the use of voice. However, the right balance (images vs. text) will be needed to be determined for each user [2].

Patient language, cultural norms, gender roles, and cultural preferences should also be taken into account when designing mHealth apps. Language and cultural norms can have a direct impact, for example, on what foods patients end up eating or what kinds of exercise they participate in.

Socioeconomic status is another major determinant of health. Patients in different social strata have different constraints, needs, and health issues. They may also not be able to afford mHealth apps, even if they do have a smartphone. App designers and publishers need to consider patients in this group if they are going to be successful in creating value for patients and for the insurers who are likely to pay for them in the future.

Before any work begins, the fundamental purpose of patient segmentation should be understood. Clayton Christensen discussed the Jobs to be Done Theory of Innovation in a Harvard Business Review IdeasCast [7]. He states that if a business focuses on the fundamental job they originally set out to accomplish, they are more inclined to grow and innovate. Within the healthcare sector, patient-centered care is highly valued but lost at times due to reporting and financial constraints. Patient segmentation could offer exciting returns to changing health behavior; however, if we lose sight of the patient, we could possibly lose the ability to innovate.

9.2.3.4 Limitations and Future Considerations for Patient Segmentation

Although market segmentation techniques have offered positive results in business, the same results may not occur in healthcare. In markets, typically once a consumer is attracted to a product and determines they want or need it, they will make a decision to purchase it. However, in healthcare, there are many complex variables that affect patient decision-making, some of which may be dependent on systemic changes that need to occur within the healthcare system itself [12]. This is a notable limitation of patient segmentation methodologies.

Most market segmentation approaches are designed to extract more value from customers. However, the concept of customer value may not translate well to the healthcare sector. In socialized medical settings and even in advanced market-driven ones, patients are rarely consumers. Rather, they depend on their healthcare providers to recommend or offer diagnostic testing and treatments and they depend on healthcare systems or insured services to pay on their behalf. So, in fact, the patient value may actually be more related to the risk of complications and use of the healthcare system and value is likely to accrue if patients receive better care. It is well known that the most vulnerable patients are most likely to be of the highest value, they are the sickest and have few resources to impact their own health.

In addition to the usual demographic, geographic, behavioral and psychographic approaches to segmentation, health system planners, app publishers, healthcare providers, and health program implementers need to consider some additional elements that are necessary for successful improvements to patient care and for enhancing the patient experience of and satisfaction with the healthcare system.

Ethical considerations need to be accounted for when creating patient segments. When utilizing patient segmentation techniques, data sources should be selected and reviewed to see if they will provide a fair representation of the target population. Different data sources and sets will determine how target groups are formed. Patient privacy, confidentiality, autonomy, and dignity need to be considered at all times when developing programs.

Users should be aware that datasets typically capture one moment in time. In fact, the BCF Technical Toolkit cautions users that the information gathered from segmentation is static nature and will not appropriately adjust for highly complex patients. Thus, it advised that whenever segmentation is performed, organizations should frequently revisit their segments and update them with the most recent data [4].

Additionally, if segmentation is encouraged by a higher authority, funding suggestions and information governance can possibly be communicated in a more standardized manner. For example, the BCF Technical toolkit provides the NHS with guidance on how to use the information gathered from segmentation to develop future funding plans. The toolkit also discusses security and privacy laws around aspects such as data storage, identified and de-identified data, alongside providing a Risk Stratification Information Governance Assurance Checklist [4].

Patient segmentation experts need to also discuss how data will be integrated within the healthcare landscape. As there are many frameworks available, each one will have to be vetted to determine the approach that best suits the target market groups needs (i.e. mHealth apps, clinical decision support systems, etc.).

Lastly, mHealth app publishers will need to address the push to use real-time/recent data. mHealth applications provide another source where data can be collected for segmentation almost instantaneously. This may assist with augmenting care delivery in a more timely manner that ultimately better suits the needs of the individual.

9.3 Opportunities for Future Developments

As the mHealth arena matures, we can expect to see the impact of a variety of trends that are already well underway, including a greater movement toward personalization of health advice through precision medicine, segmentation and behavioral interventions. As our understanding of what health consumers are looking for and how to engage them improves, we can expect increasing benefits, especially for patients themselves. Just as the alternative and complementary medicines are a huge industry

, we can expect useful mobile applications to be an increasingly trusted source for improvement of health and wellbeing.

Some trends to watch out for include rapid advances in the use of blockchains, machine learning, and artificial intelligence technologies, in situ clinical trials and better interoperability. Barriers that need to be addressed include, appropriate information governance mechanisms, the ability for researchers and vendors to work together more closely, a rapidly evolving regulatory arena and the sustainability of app publishers over the long term.

9.3.1 Trends

Distributed ledger technologies, more popularly known as the blockchain, have advanced rapidly in the last decade. The ability for patients to have greater control over secondary uses of their data could have widespread implications [10]. Certainly, patients have very clear preferences about who should and should not see their medical data [52]. However, the mechanisms available for patients to control their own data have been rather blunt. Fine-grained control exercised by patients was considered to be too difficult and potentially burdensome to patients. However, recent advances in technology and mobile applications are making it easier for patients to play a direct role in decision-making regarding their own data [25].

Advances in machine learning and artificial intelligence are being made rapidly and the costs of providing real-time insights using these tools are dropping significantly. They allow small publishing houses to use advanced technologies with very small investment and with their existing staff [1]. These technologies are likely to allow mHealth app publishers to analyze data faster, test hypotheses faster, and customize their offerings for their customers to create better engagement experiences for patients. The opportunity to use advances developed in other industries to problems in healthcare are increasingly available at a nominal cost and very shallow learning curves.

To gain more traction, mobile apps will need to meet demands from providers and patients for evidence that they actually work. Yet, traditional randomized controlled trials are too unwieldy and slow for testing mobile apps [42]. Better approaches are needed and will arise when the quality of mHealth apps is high enough that a heuristic walk-through or an expert review will no longer be sufficient to assess the quality of apps. One promising approach is to use adaptive clinical trials within the clinical practice, enabling more rapid patient enrollment and data collection within the circle of care. The adaptive randomized controlled trial allows more rapid assessment of whether an app is working and can quickly eliminate apps that are not performing well [42].

Interoperability, as outlined in Sect. 9.2.2, continues to be a difficult issue to tackle in health care. Although HL7 has been developing standards for over four decades, the problem is still open. The lack of business cases, lack of good data governance and lack of incentives to share data make interoperability difficult to

achieve. However, recently, HL7 has utilized industry standard technologies to move their so-called Fast Healthcare Interoperability Resources (FHIR) forward. They are seeing increased traction from this new approach. Work still needs to be done on identifying barriers and solving them early to enable integration with EMRs. The SMART Health App platform uses HL7s FHIR approach to enable EMRs to integrate with apps [46] and the Argonaut Project is developing the partnerships to enable more widespread use of the HL7 FHIR standards [21, 22]. Overall, there is hope that the interoperability will soon be solved.

9.3.2 Barriers

If data is to move seamlessly for easy patient access, much needs to be done in health information governance [11]. Data in socialized medicine settings continues to be stuck in organizational silos, inaccessible to most stakeholders. Data may flow to researchers and system managers, but it is still slow and inefficient. Data tends to flow in batches rather than as a continuous stream, which is what is required for mHealth.

The cost of conducting research in health care is very high. Asking app publishers to develop new evidence-informed apps and testing them in a rigorous manner may be too much to ask for. Researchers however are constantly developing new apps and testing them. Is it possible to develop a trusted, stereotyped relationship between researchers and app publishers so that app publishers have access to world-class R&D at a good price and researchers have access to partners that can commercialize their findings and enable knowledge translation of their work? Having good intellectual property agreements will be key to the success of any partnership between researchers and commercial entities. Universities need to look into the best intellectual property arrangements.

The app regulatory environment is constantly evolving. Recently, the Food and Drug Administration (FDA) in the US has invested significant resources to speed up the review of mobile apps and to make the process of app review as easy as possible for vendors. Attempts have been made, especially in the USA and in the EU, to develop regulation and recommendations but the road towards guiding principles and recommendations is still largely unpaved [39]. Any regulatory process, regardless of the ease and lightness of touch will incur significant expenses, which will need to be recouped at some point.

This begs the question of how app publishers expect to attain sustainability and profitability with the apps? Most apps never reach this stage. However, if patients and providers are expecting to get reliable and high quality service from their apps, app publishers need to have a reliable revenue stream to sustain operations and invest in new features, functions and updating the app in response to new medical knowledge, new finding from machine learning algorithms and patient and provider feedback.

Reimbursement is also an issue as healthcare systems or insurance companies will need to step up to the plate and pay for mHealth apps on behalf of patients so that the question of affordability does not come up and so that app publishers can attain some level of sustainability for their apps.

9.4 Conclusions

Recent advances in mHealth technology and capabilities opened for new opportunities in health care systems and service delivery. This is a timely topic and several successful experiences throughout the world show that mHealth enabled healthcare services can translate into benefits for the patients and the systems as a whole. This chapter outlined significant examples in the field of telemedicine, patient monitoring, and in general patient data management. Patient-centered customization of health care is also made possible by the use of mHealth and individualized services, also by translating segmentation strategies that can be borrowed from marketing theories and can function as an inspiration for future expansion for mHealth technologies. There is still much research needed, to translate these opportunities into real benefits. Multidisciplinary and multi-stakeholder efforts would be essential to define guiding principles for mHealth development and use in health care, and to tackle open questions such as interoperability, information and patient data governance, regulation, affordability, and sustainability.

References

1. Amazon Web Services, Inc.: Machine Learning at AWS. https://aws.amazon.com/machine-learning/ (2018). Accessed 30 Jan 2018
2. Balouchi, S., Keshavjee, K., Zbib, A., Vassanji, K.: Creating a supportive environment for self-management in healthcare via patient electronic tools. In: Househ, M., Borycki, E., Kushniruk, A. (eds.) Social Media and Mobile Technologies for Healthcare, pp. 109–125. IGI Global (2014)
3. Bastawrous, A., Armstrong, M.J.: Mobile health use in low- and high-income countries: an overview of the peer-reviewed literature. J. R. Soc. Med. **106**(4), 130–142 (2013)
4. Better Care Fund (BCF) NHS England: How to Guide: The BCF Technical Toolkit Section 1: Population Segmentation, Risk Stratification and Information Governance. https://www.england.nhs.uk/wp-content/uploads/2014/09/1-seg-strat.pdf (2014). Accessed 30 Jan 2018
5. Butcher, L.: Consumer segmentation has hit health care. Heres how it works. https://www.hhnmag.com/articles/6932-consumer-segmentation-just-hit-health-care-heres-how-it-works (2016). Accessed 30 Jan 2018
6. c2B solutions: Psychographic Segmentation—Changing Healthcare Consumer Behaviour by Engaging Their Motivations. https://www.c2bsolutions.com/psychographic-segmentation (2017). Accessed 30 Jan 2018
7. Caremichael, S.G. (Interviewer), Christensen, C. (Interviewee).: The Jobs to be Done Theory of Innovation [Interview transcript]. Retrieved from the Harvard Business (2016) Review Website: https://hbr.org/ideacast/2016/12/the-jobs-to-be-done-theory-of-innovation. Accessed 30 Jan 2018

8. Chindalo, P., Karim, A., Brahmbhatt, Saha, N., Keshavjee, K.: Health apps by design: a reference architecture for mobile engagement. Int. J. Handheld Comput. Res. (IJHCR) **7**(2), 34–43 (2016)
9. Cocosila, M., Coursaris, C., Yuan, Y.: M-healthcare for patient self-management: a case for diabetics. Int. J. Electron. Healthc. **1**(2), 221–241 (2004)
10. Cunningham, J., Ainsworth, J.: Enabling patient control of personal electronic health records through distributed ledger technology. Stud. Health Technol. Inform. **245**, 45–48 (2017)
11. Dong, L., Keshavjee, K.: Why is information governance important for electronic healthcare systems? A Canadian experience. J. Adv. Humanit. Soc. Sci. **2016**, 250–260 (2016)
12. Van Dongen, N.: The patient segmentation model. https://pharmaphorum.com/views-and-analysis/the-patient-segmentation-model/ (2014). Accessed 30 Jan 2018
13. Esposito, M., Minutolo, A., Megna, R., Forastiere, M., Magliulo, M., De Pietro, G.: A smart mobile, self-configuring, context-aware architecture for personal health monitoring. Eng. Appl. Artif. Intell. **67**, 136–156 (2018)
14. Federal Communications Commission (FCC). mHealth Task Force findings and recommendations. http://www2.itif.org/2012-mhealth-taskforce-recommendations.pdf (2012). Accessed 30 Jan 2018
15. Foster, K.R., Callans, D.J.: Smartphone apps meet evidence based medicine. IEEE Pulse **8**(6), 34–39 (2017)
16. Gay, V., Leijdekkers, P.: A health monitoring system using smart phones and wearable sensors. Int. J. ARM **8**(2), 2935 (2017)
17. Ghany, A., Keshavjee, K.: A platform to collect structured data from multiple EMRs. Stud. Health Technol. Inform. **208**, 142–146 (2015)
18. Habetha, J.: The MyHeart project-fighting cardiovascular diseases by prevention and early diagnosis. In: International Conference of the IEEE Engineering in Medicine and Biology Society 2006, pp. 6746–6749 (2006)
19. Van Halteren, A., Bults, R.G.A., Wac, K.E., Konstantas, D, Widya, I.A., Dokovski, N.T., Koprinkov, G.T., Jones, V.M., Herzog, R.: Mobile patient monitoring: the Mobihealth system. J. Inform. Technol. Healthc. **2**(5), 365–373 (2004)
20. Health Affairs. Health Policy Brief: Patient Engagement. https://www.healthaffairs.org/action/showDoPubSecure?doi=10.1377%2Fhpb20130214.898775&format=full (2013). Accessed 30 Jan 2018
21. Health Level Seven International (HL7). http://www.hl7.org/ (2018). Accessed 30 Jan 2018
22. Health Level Seven International (HL7) Argonaut Project Wiki. Argonautwiki.hl7.org. http://argonautwiki.hl7.org/index.php?title=MainPage (2018). Accessed 30 Jan 2018
23. HealthIT.gov. What is HIE? https://www.healthit.gov/providers-professionals/healthinformation-exchange/what-hie (2016). Accessed 30 Jan 2018
24. Hult Marketing. Know Your Audience: Building Patient Personas [Weblog comment]. https://blog.hultmarketing.com/blog/building-patient-personas (2017). Accessed 30 Jan 2018
25. Ichikawa, D., Kashiyama, M., Ueno, T.: Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth **5**(7), e111 (2017)
26. Institute for Healthcare Improvement (IHI). One Size Does Not Fit All: Think Segmentation. http://www.ihi.org/resources/Pages/ImprovementStories/OneSizeDoesNotFitAllThinkSegmentation.aspx. Accessed 30 Jan 2018
27. ISO 13606. http://www.en13606.org/. Accessed 30 Jan 2018
28. Kalra, D., Blobel, B.: Semantic interoperability of EHR systems. Stud. Health Technol. Inform. **127**, 231 (2007)
29. Kelli, H.M., Witbrodt, B., Shah, A.: The future of mobile health applications and devices in cardiovascular health. Euro. Med. J. Innov. **2017**, 92–97 (2017)
30. Keshavjee, K., Mirza, K., Martin, K.: The next generation EMR. Stud. Health Technol. Inform. **208**, 210–214 (2015)
31. Kher, R.K.: Mobile and e-Healthcare: recent trends and future directions. J. Health Med. Econ. **2**(3), 10 (2016)

32. Knight Marketing. Using Patient Personas for More Effective Healthcare Marketing. http://knightmarketing.com/blog/using-patient-personas-for-more-effective-healthcare-marketing/ (2016). Accessed 30 Jan 2018
33. Laxman, K., Krishnan, S.B., Dhillon, J.S.: Barriers to adoption of consumer health informatics applications for health self management. Health Sci. J. **9**(5), 1–7 (2015)
34. Marceglia, S., Fontelo, P., Rossi, E., Ackerman, M.J.: A standards-based architecture proposal for integrating patient mHealth apps to electronic health record systems. Appl. Clin. Inform. **6**, 488505 (2015)
35. McKinsey&Company. A 360-degree approach to patient adherence. http://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/a-360-degree-approach-to-patient-adherence (2017). Accessed 30 Jan 2018
36. NHS England. (2017). List of risk stratification approved organizations. https://www.england.nhs.uk/wp-content/uploads/2017/03/risk-stratification-approved-orgs-290317.pdf. Accessed 30 Jan 2018
37. Ozdalga, E., Ozdalga, A., Ahuja, N.: The smartphone in medicine: a review of current and potential use among physicians and students. J. Med. Internet Res. **14**(5), e128 (2012)
38. Paglialonga, A., Mastropietro, A., Scalco, E., Rizzo, G.: The mHealth. Chapter 2, this volume. (2019)
39. Paglialonga, A., Lugo, A., Santoro, E.: An overview on the emerging area of identification, characterization, and assessment of health apps. J. Biomed. Inform. **83**, 97–102 (2018)
40. Paradiso, R., Loriga, G., Taccini, N.: Wearable system for vital signs monitoring. Stud. Health Technol. Inform. **108**, 253–259 (2004)
41. PATH (Patterns of Adapting to Health) Institute. Patterns of Adapting to Health. http://www.pathinstitute.life/patterns-of-adapting-to-health.html (2017). Accessed 30 Jan 2018
42. Philpott, D., Guergachi, A., Keshavjee, K.: Design and validation of a platform to evaluate mHealth apps. Stud. Health Technol. Inform. **235**, 3–7 (2017)
43. Pyxl. Buyer Personas for Healthcare Digital Marketing. https://pyxl.com/articles/buyer-personas-healthcare-digital-marketing/ (2015). Accessed 30 Jan 2018
44. Roess, A.: The promise, growth, and reality of mobile health another data-free zone. N. Engl. J. Med. **377**, 2010–2011 (2017)
45. Ruiz-Zafra, Benghazi, K., Noguera, M., Garrido, J.L.: Zappa: an open mobile platform to build cloud-based m-health systems. In: Ambient Intelligence-Software and Applications, p. 8794 (2013)
46. SMART Health IT. SMART Health IT. https://smarthealthit.org/ (2018). Accessed 30 Jan 2018
47. Smith, C.E., Spaulding, R., Piamjariyakul, U., Werkowitch, M., Yadrich, D.M., Hooper, D., Moore, T., Gilroy, R.: mHealth clinic appointment PC tablet: implementation, challenges and solutions. J. Mob. Technol. Med. **4**(2), 21–32 (2015)
48. Steinhubl, S.R., Muse, E.D., Topol, E.J.: The emerging field of mobile health. Sci. Transl. Med. **7**(283), 283rv3 (2015)
49. Tuckwell, K.J., Jaffey, M.: Market segmentation and target marketing. In: THINK Marketing, 2nd edn. Chapter 6. http://www.pearsoncanada.ca/media/highered-showcase/multi-product-showcase/tuckwell-think-ch06.pdf 2014. Accessed 30 Jan 30 2018
50. Vuik, S.I., Mayer, E.K., Darzi, A.: Patient segmentation analysis offers significant benefits for integrated care and support. Health Aff. **35**(5), 769–775 (2016)
51. Williams, C., Mostashari, F., Mertz, K., Hogin, E., Atwal, P.: From the office of the national coordinator: the strategy for advancing the exchange of health information. Health Aff. (Millwood) **31**(3), 527–536 (2012)
52. Willison, D.J., Keshavjee, K., Nair, K., Goldsmith, C., Holbrook, A.M.: Computerization of medical practices for the enhancement of therapeutic effectiveness investigators. Patients' consent preferences for research uses of information in electronic medical records: interview and survey data. BMJ **326**(7385):373 (2003)
53. World Health Organization (WHO).: mHealth: new horizons for health through mobile technologies: second global survey on eHealth. WHO Press, Geneva, Switzerland (2011)

Chapter 10
Conclusion

Enrico Frumento

Abstract As discussed in Chap. 4 of the book, today we assist to a blending between private and professional lives due to the flexibility to work at any time from different locations. A blending facilitated by the diffusion of ubiquitous technologies that allows to merge seamlessly physical and virtual encounters. The recent global recession directly increased the dynamicity of the labor market fostering the adoption of more flexibility and more mobility. Thanks to mobile and ubiquitous terminals, a user could complete a task in any possible place, home, public spaces or company offices. From a technological point of view, this trend promotes the evolution of the so-called digital ecosystems: communities of people who interact, exchange information, combine, evolve in terms of knowledge, skills, and contacts, in order to improve their lives and meet their needs. The *mobilization* of our lives dramatically changed our behaviors in many ways, not only for the ubiquitous communication they support. This transformation crosses several domains and does not only interests the healthcare area. However, health care, being one of the crucial sectors for the correct functioning of a society, is heavily affected. The transformations undergoing in the healthcare domain affects not only the infrastructure but also the common habits of healthcare workers. This, as demonstrated in the book has economic, technological, and ICT security consequences.

As reported in the introduction of the book the four typical areas in which a hospital is organized (a sensing component, a processing unit, the software, and a cloud/web-based repository with analytical and interpretation capabilities) are equally impacted (see Chaps. 2 and 5).

As a matter of fact, Hospitals have evolved from a localized place of care to a *delocalized and extended network* of *care services*. This change of perspective has in effect created a "**Patient Ecosystem**", in which services are delivered to patients across a *wide variety of locations*, from hospitals to homes as well as "on-the-go". This transformation led to the phenomenon of mobile healthcare services or mHealth.

E. Frumento (✉)
Cefriel Scarl, Politecnico di Milano, Viale Sarca, 226, 20126 Milan, Italy
e-mail: enrico.frumento@cefriel.com

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5_10

mHealth services are, however, one aspect of a complex organizational infrastructure which includes by the hospital and its supply-chain.

As explained in Chap. 5, Mobile health, or mHealth, is a cross-intersection between Medicine and technology, between Health and Communication technology and especially between Electronic Health (eHealth) and Mobile Technology. It consists of all systems that include acquisition, processing, classification, transmission, and recording of health-related information. mHealth systems are usually composed of three different main subsystems: Biomedical Sensor, Mobile device, and Cloud.

Especially in mHealth, therefore, services involve a *diversity* of Healthcare professionals, channels, and technologies. This transformation has also modified the relationship between patients and the healthcare professionals, moving from a limited number of "*visits to the doctor*" to a *continuous mode* and a more permanent collaboration that has the potential to increase the quality, impact, and effectiveness of health care on patients. While the introduction of this evolution crossed over the past decades, its *adoption* is growing exponentially thanks to the evolutions of mobile services, the increased penetration rate of information technology to the complete healthcare supply-chain actors. Similarly, it has increased the number and coverage of *healthcare operators*, extending from operating hospitals to remote care services facilities, nursing homes, teleassistance, etc.

Across these different profiles, very different perspectives govern the role and uptake of information technology.

For *healthcare operators*, the deployment of information technology is a means to increase efficiency, required by the economic complexity of ensuring sustainable healthcare services toward a growing and increasingly aging population. It is also a mean for the *healthcare administrators* to face the challenge of expense expansions and funds contraction.

For *healthcare professionals (doctors, nurses,* etc.*)*, information technology is often *imposed* to them by the operators and /or public authorities, ranging from information exchange (electronic patient record, etc.) to monitoring (connected devices, etc.) and operational support (robotized interventions, etc.). Healthcare professionals are not the *drivers* of change but are the main users and adopters of the technology that is provided to them often without receiving a sufficient level of information to be fully aware of how best to use the technology.

But, however complex, healthcare services are always centered on humans; this means that healthcare infrastructures have to consider the impact of the new wave of "**moving to the humans**", referring both to the many technological developments, that have a common characteristic to "focus on" the user to ease his modes of interactions (through wearable systems, natural interfaces, and emotional design for user-centered innovation, etc.), and the way in which access to services is provided.

Moving to the patients or moving to the human is, therefore, the new mantra in health care. This concept opens up yet another problem connected to the healthcare supply chains. Some of the patients are familiar with information technology, and display a familiarity with, for instance, smart devices used in mobile wellness solutions [1]. Contrary to other domains in which a certain level of mistrust is per-

vasive, patients using health-oriented mobile devices tend to develop a high inherent level of trust and, as a consequence, they are often not aware of or they simply overlook the potential risks of their use [2]. For other patients, information technology is incomprehensible and they will also be unaware of the potential risks linked to health devices out of lack of understanding.

Health care and its mHealth counterpart is, therefore, a very rich and complex environment it is a critical infrastructure through its central societal role, and it is populated by huge numbers of *human profiles*, varying widely as to their role, level of interest and awareness of the vulnerabilities introduced by the use of information technology. They will also vary widely in terms of feeling (un)concerned about their own role in relation to these vulnerabilities.

As discussed mHealth affects the healthcare industry and all its surrounding elements: patients, healthcare operators, supply-chain, manufacturers, and lastly hospitals. At the European level, we can say that

- Homogeneity of healthcare organizations: healthcare organizations are relatively uniform around best practices, standards, and regulations and the homogeneity among them is higher than other sectors. This will facilitate the introduction of mHealth services in Europe (see Chap. 3).
- The healthcare operators have a unique mindset and culture: as discussed in Chap. 4 this poses a relatively higher risk, also looking at the evolutions of the threat landscape, of the human layer of security. It also differs in terms of the interconnectivity between healthcare operators that is driven by clearly identified needs (sharing patient information, sharing advanced research results, etc.) which has the benefit of scoping the type of interactions.
- EU Competitiveness: mHealth represents a very competitive opportunity for the European community, due to aging factors of its population and to the well-developed mobile infrastructure (also facilitated by the drop of roaming barriers and extra costs for the internet connection among the member states, in force since 2018).

References

1. HEALTHCARE SECTOR REPORT. Cyber security for the healthcare sector, ECSO, WG3 I Sectoral Demand, March (2018)
2. Frumento, E., Freschi, F.: How the evolution of workforces influences cybercrime strategies: the example of healthcare. In: Akhgar, B., Brewster, B. (eds.) Combatting Cybercrime and Cyberterrorism Challenges, Trends and Priorities (Advanced Sciences and Technologies for Security Applications), 1st edn, pp. 237–258. Springer (2016)

Index

G. Andreoni et al. (eds.), *m_Health Current and Future Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-02182-5