Securing Cyber-Resilience in Healthcare Sector

Pankaj Kumar, Amit Singh, and Aritro Sengupta

1 Introduction

In recent years, we have seen a surge in cybersecurity incidents in the healthcare industry. These incidents mainly include ransomware attacks, malware infections, theft of patient data, and selling of the patient data in exchange for bitcoins or other monetary benefits. In the present scenario, the healthcare industry is understandably busy, caring for COVID-19 patients. Taking advantage of this situation, cybercriminals are trying to disrupt healthcare provider's systems and access sensitive medical records.

World Health Organization, United States Department of Health and Human Services, and UK-based Hammersmith Medicines Research facility have fought off cyberattacks recently. Other key healthcare organizations such as Medtronic, Fujifilm, Philips, Johnson and Johnson, GE Healthcare, and Siemens Healthineers [1–4] have also dwarfed many attempts to steal millions of medical records. Medical records contain valuable and sensitive personal data, including personal health records, ID numbers, addresses, contact numbers, and much more.

However, medical data records are not the only target in the healthcare domain. Wireless sensors network, Implantable Medical Devices (IMDs), medical imaging devices, and IT systems and processes in the hospital are the major target for cyberattacks. A report published by Greenbone networks [5] reveals that the WannaCry wave in May 2017 affected the National Health Service (NHS) in the UK. The ransomware encrypted data on numerous computers of the NHS. To do this, the attacker used a security gap in Windows systems. 81 of the 236 trusts were affected and 6912 appointments had to be rescheduled, including many critical operations.

In the U.S. in January 2018, the SamSam ransomware penetrated the network of the Hancock Health Hospital in Indiana and infected some of the hospital's IT

P. Kumar (✉) · A. Singh · A. Sengupta
Ministry of Electronics and Information Technology, Government of India, New Delhi, India

R. Agrawal et al. (eds.), *Cyber Security in Intelligent Computing and Communications*,
Studies in Computational Intelligence 1007,
https://doi.org/10.1007/978-981-16-8012-0_17

systems. The attacker exploited open/poorly configured Remote Desktop Protocol (RDP). Hancock Health paid the attackers around $60,000 to get its systems up and running again. Cyberattacks against hospitals have also been reported in Germany. In 2016, Klinikum Arnsberg and Lukas Krankenhaus in Neuss were victims of the Locky ransomware attack. Both systems were locked, and the attacker demanded ransom to make the system running again. Finally, Lukas Krankenhaus paid the ransom about €1 million.

As per another report published by Greenbone [6], medical data of more than one twenty million patients who underwent treatment in India have been leaked. These medical data are available on the Internet for free. One of the states, Maharashtra, have been affected the most by the medical data theft, with more than 69 million images of patients available online. The report also ranked the affected countries in terms of the action taken by their respective federal governments in stopping the data leak of patients. India is at number two in the ranking after the U.S. Apart from this, in the year 2019, several CVEs and research articles have been published which focus on vulnerable medical network, file-sharing formats, and access to the medical system framework [7].

We reviewed several research papers that discussed cyberattacks, challenges, and mitigations. The literature needs to be updated to cater to the evolving threat landscape. Based on new threats and cybersecurity dimensions, new mitigation strategies need to be prepared. Healthcare industry is complex and requires involvement of manufacturers, hospitals, and end users in reducing cybersecurity risks. This paper aims to bridge this gap and cover the latest cyberattack trends, including their mitigation policies. We also discuss cybersecurity challenges faced by the healthcare industries and end users in recent years.

The structure of the rest of the paper is as follows: Sect. 2 provides a detailed overview of a typical healthcare system and discusses its components that are vulnerable to cyberattacks. In Sect. 3, we explore different cyberattacks and vulnerabilities related to healthcare systems (implantable medical devices, wireless networks, data storage servers, hospital management systems) and measures to mitigate weaknesses. In Sect. 4, we discuss challenges and different risks related to cybersecurity. In Sect. 5, we discuss future directions and conclude the paper.

2 An Overview of a Typical Healthcare System and Its Major Components

A variety of network-connected devices are in use in the healthcare system. These devices vary from IoT-based hardware to a software-based hospital management system. In this section, we have discussed the popularly used devices and technologies used in the healthcare system.

2.1 Wireless Implantable Medical Devices (IMDs)

Implantable Medical Devices (IMDs) are electronic devices or artificial tissues that are implanted inside the body or on the surface of the skin of a medical patient.

These IMDs are linked to various communication networks which are known as "telemetry". These devices are aimed to provide more sophisticated computing competence. Medical representatives can access the implanted devices and control or configure them remotely. This has made the implants more intelligent and granted autonomy in controlling the health parameters of a patient. [8, 9]. The most common IMD devices include pacemaker devices, neurostimulators, drug delivery systems, biosensors, etc. The various IMDs are shown in Fig. 1.

Implantable cardioverter defibrillators (ICDs) and cardiac resynchronization therapy defibrillators (CRT-Ds) are two widely used **implantable pacemaker devices** [9, 10]. The physician uses these devices to monitor the heartbeat of the patient remotely. **Brain stimulator** devices work by transmitting electrical signals of low amplitude through electrodes placed in the brain of a patient. It is used in the treatment of diseases such as Parkinson, epilepsy, depression, etc. [11]. **Drug Delivery Systems (DDS)**, a pump, and a tube are implanted under the skin of a

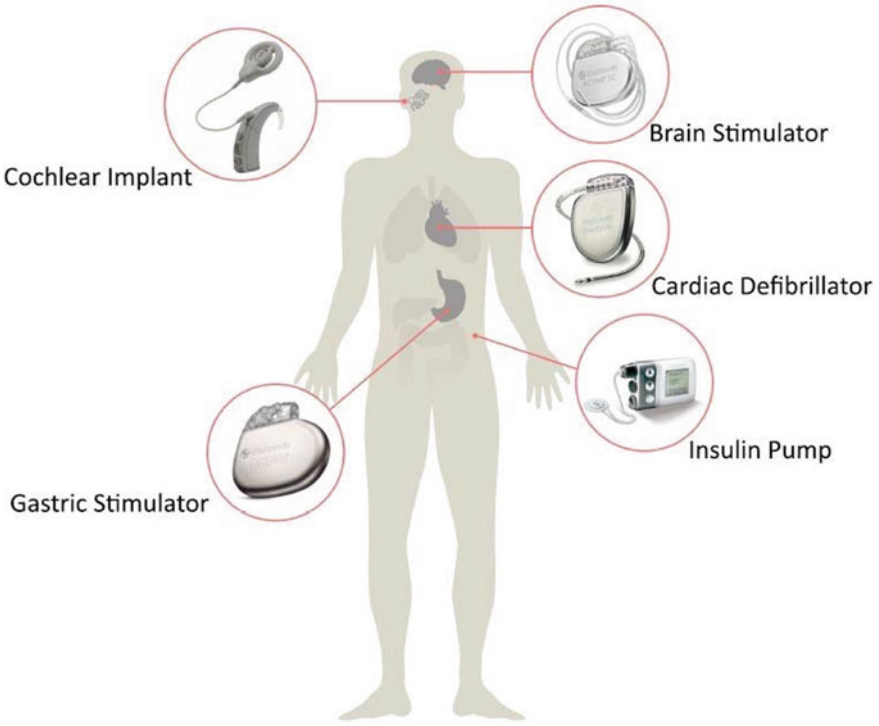

Fig. 1 Wireless implantable medical devices

medical patient. The purpose of the DDS is to supply medication to the patient in a measured, confined, and optimal way. **Biosensors are having** miniature sensors capable of sensing limited activities that are placed inside the body of a patient to monitor physiological parameters. Apart from the sensors, there exists a control node that communicates with the sensors and the controller. The sensors along with the central control node are termed as wireless biosensor networks. These IMDs are highly prone to cyberattacks as they are controlled through wireless network systems.

2.2 Medical Imaging Devices

These include devices that record medical images of the patient. For example, radiology devices that have imaging devices such as radiography, ultrasound, computed tomography (CT), nuclear medicine (positron emission tomography), and magnetic resonance imaging (MRI) which are used to diagnose or treat diseases. These machines record the medical images of the part of the body. The recorded image files are stored at the PACS/RIS server.

These devices are highly prone to cyberattacks. The medical images of patients are of high value to cybercriminals and they are selling it in the darknet at a towering price. Due to this, medical imaging devices are highly susceptible and are at the risk of being attacked by cybercriminals. In addition to the concern, most of the systems that are connected to these machines run outdated software versions that are vulnerable to various exploits. An attacker may use this loophole to exploit the vulnerability and gain access to the system.

2.3 Data Storage Server

These include the Picture Archiving and Communication System (PACS) server and Radiology Information System (RIS) server that store the medical image files of the patient. PACS is an Ethernet-based network which involves a server. The server receives scanned images from the imaging devices connected in the network, stores the images in the database for retrieval at a later point of time, and fetches the images for radiologists to analyze and prescribe. These support imaging modalities such as X-Ray, CT scan, MRIs, etc. [12, 13]. DICOM stands for Digital Imaging and Communications in Medicine and is a very old file format that is used for storing and sharing medical images. A DICOM viewer is used to view these files. A workflow diagram is given in Fig. 2.

These systems are responsible for collecting and storing sensitive data. These systems comprise a large number of software and hardware which are embedded in nature. Hence, if the systems are not patched from time to time, attackers may target these systems to exploit and gain access to the affected systems.

Fig. 2 PACS to DICOM workflow [14]

2.4 Hospital Management Network

As we know that hospitals have to collect patient's general information along with patients' medicine prescriptions, previous examination results such as X-Ray images, patient's documents of sterilization of surgical instruments, and other information about the stay. With the increasing number of patients, it is tedious and practically infeasible to store and maintain these data manually. To ease this, hospital management uses a dedicated software to store and manage these data. At the backend of the software, the storage servers (like SQL server) are connected to store the data. For example, patient management systems (PMS) are commonly used for admission and administration. Hospital information systems (HIS) support administrative processes in the hospital, such as in the areas of billing, controlling, order management, and care documentation. Radiology information systems (RIS) are used in radiology. These softwares are often found to be outdated as hospital managements fail to update the software patches on a routine basis. As a result, the vulnerabilities in the outdated software may be exploited by the cybercriminals, and subsequently they can get access to the patient's information. The information has enormous value in the black-market such as Darknet.

Cybercriminals have been using various types of cyberattacks such as DDoS, man-in-the-middle (MITM) attack, SQL injection, malicious code injection, phishing, ransomware, etc. to compromise integrity of healthcare devices and gain access to the systems. **DoS attack** is used to disrupt service and prevent users from getting access to service. This type of attack is done by flooding devices with unwanted and irrelevant requests. An attack where an attacker intercepts and alters the data sent between two nodes is known as **MITM** [15]. This is used to modify and gather data that breaches confidentiality. **SQL** is used by websites to manage their databases. SQL vulnerability may be exploited by an attacker to access the databases of healthcare organizations. In ransomware attacks, the attackers shut down the healthcare systems that may arise a severe issue for monitoring and caring/treatment of the patients. In

Table 1 Types of cyberattacks and affected healthcare systems

Types of attack	IMDs	Medical imaging devices	Data storage server	Hospital management network
Denial of service	✓			✓
MITM	✓		✓	✓
SQL injections exploit			✓	✓
Remote code execution and malicious software	✓	✓	✓	✓
Open SSH vulnerability	✓	✓	✓	
Ransomware	✓	✓	✓	✓
Phishing			✓	✓

Table 1, we have categorized different types of cyberattacks and relate to affected healthcare systems.

3 Recent Case Studies of Cyberattacks in Healthcare Systems

Currently, we are facing a global healthcare sector battle due to the ongoing COVID-19 pandemic. This has surged the number of cyberattacks in the healthcare sector. In this section, we shall discuss case studies related to recent cyberattacks observed in the healthcare domain (Table 2).

In coming sections, we shall also address vulnerabilities related to healthcare systems (implantable medical devices, medical image devices, data storage servers, hospital management systems) and steps to its mitigation.

3.1 Cyberattacks on Implantable Medical Devices

IMDs as discussed in Sect. 2.1 use wireless telemetry protocol, which enables them to communicate with each other and allows programmers and monitoring devices to do allotted tasks. The wireless telemetry protocol does not use basic security features such as encryption, authentication, or authorization. So this protocol has cybersecurity vulnerabilities. These vulnerabilities, if exploited, could allow an unauthorized individual to access and possibly manipulate the functioning of an implantable device, home-based monitor, or programmer. In recent years, multiple vulnerabilities

Table 2 Recent cyberattacks case studies

Organization	Type of breach	Month and year	No. of records	Breached devices/severs	Nature of lost data
Brno University Hospital, Czech Republic [16]	Ransomware	March 2020	20,000–30,000	IT networks	Name, date of birth, medical identification, address, and email
US Dept. of Health and Human Services	DDoS attack	March 2020	40,000–50,000	Network server	User credentials, medical information
World Health Organization [16]	Malicious code injection	April 2020	–	Email server	Login ID and password of users
Dominion National Insurer [17]	Information disclosure	April 2019	200,000	Network sever	Name, date of birth, medical identification
UK Healthcare Trust [17]	WannaCry attack	2017	30,000–35,000	Computer system	Login ID and password of systems

have been found in the IMDs. A summary of medical device vulnerabilities, along with their severity and impact, is shown in Table 3.

Steps to Mitigate

- Increase awareness among all stakeholders, including medical physicians and clinical IT teams about current and potential medical device vulnerabilities.
- Restrict unauthorized access to the network and networked medical devices through the implementation of AAA (authentication, authorization, and accounting) systems.
- An external device may be used that acts as a proxy between the device programmer and IMDs. Also, this proxy will perform the authentication process on behalf of the IMD. The proxy restricts the messages to/from the IMD and prevents attackers from decrypting them, while IMDs being able to decode them successfully [21].
- A pairing protocol may be enforced between the device programmer and medical devices to authenticate the communication. In this system, there is no need to share any prior key/password.
- A cryptographic key exchange may be used between the programmer and the medical devices through an auxiliary or Out-Of-Band (OOB) channel to authenticate the communication [22].
- Implement appropriate ACLs (access control lists) for IP addresses and/or port filters.

Table 3 Medical devices vulnerabilities and its impact

Medical devices	Vulnerability	Severity	Vendor	CVE	Vulnerability impact
Cardiac pacemakers, implantable neurostimulators, and implantable infusion pumps	Dropbear SSH server <2016.72 multiple vulnerabilities	Critical	GE healthcare, Animas, Bionet and Roche	CVE-2016-7407 [18]	It can disclose sensitive information held on the database server
MRI scanners and X-ray machines	Microsoft windows SMB server (4013389) security update (un-credentialed check) [19]	Critical	Carefusion and ReliOn	CVE-2017-0143** and CVE-2017-0144** [20]	Attackers can execute remote code on susceptible machines and run commands and gain access to the local machine
X-Ray machines	Denial of service (DoS)	High	Fujifilm	CVE-2019-10948 [20]	It allows an attacker to flood a network server with enormous traffic that requires a manual reboot of the device
CT scanners	OpenSSH vulnerability	High	Philips	CVE-2018-8853 [20]	It allows attackers to bypass authentication and gain access to sensitive patient information with the device
Blood gas analyzers	Remote code execution	High	Siemens Healthineers	CVE-2018-4845 [18]	Remote attackers access to the "Remote View" feature, may be able to gain privileges of the system

(continued)

Table 3 (continued)

Medical devices	Vulnerability	Severity	Vendor	CVE	Vulnerability impact
PET/CT and SPECT/CT medical imaging products	Remote code execution	High	Siemens Healthineers	CVE-2015-1635 [20]	It can access remotely and execute an arbitrary malicious program and gain access

- Medical devices should be designed in such a way that they have good communication competence and be more secure in a network system. The communication system should not depend only on external mechanisms like firewalls, intrusion prevention systems, or any other third-party solutions.

3.2 Cyberattacks on PACS Server

As on date 13.08.2020, there are 282 PACS servers available in India as per open-source intelligence (OSINT) feed as shown in Fig. 3.

Many systems are available without any restrictions or any access control mechanisms.
PACS servers allow direct access to patient data via DICOM viewer. This access is possible without authentication, and in most of the servers, the data is transmitted via HTTP, i.e., unencrypted in plain text. This may be targeted to access and alter a patient's DICOM imagery. In addition to this, PACS are not directly connected to the Internet but connected via health care's internal network. This may allow an attacker to exploit vulnerabilities through social engineering attacks, insider attacks, etc. [23]. A workflow of tempering the medical imagery between the investigation and diagnosis stage has been shown in Fig. 4.
Restriction of Malicious HL7 messages in the network: In a PACS environment, DICOM communicates using HL7 version messages. These are used to keep consistent information through all hospital information systems, RIS, and PACS server. Information of patients (like name, hospital ID, address, etc.) can be continuously updated without human intervention using HL7 messages across multiple systems. Unfortunately, the HL7 message protocol does not provide any way to prevent a malicious attack on the messages. An attacker can observe the network traffic of HL7 messages, learn about patient data, or modify the genuine messages during transmission [24].

A summary of the PACS server and DICOM file vulnerabilities along with its severity and impact is shown in Table 4.

Fig. 3 PACS server available in India as on date 13.08.2020.

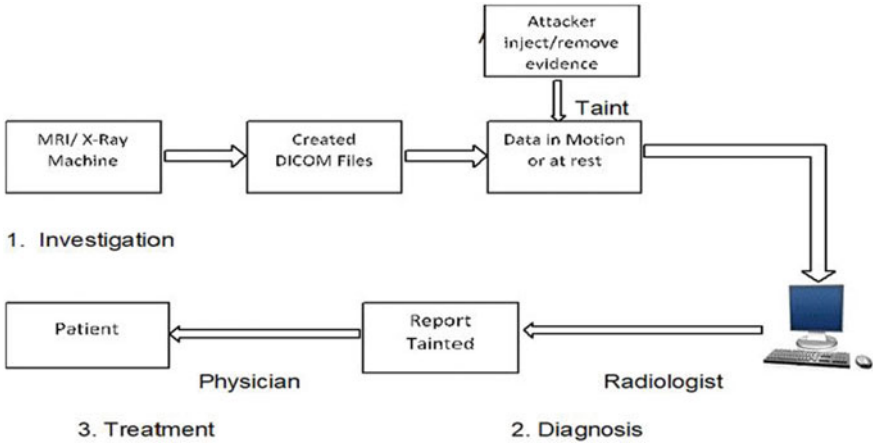

Fig. 4 Medical imagery between the investigation and diagnosis stages, both the radiologist and physician believe the fallacy set by the attacker

Table 4 PACS/RIS server and DICOM file vulnerabilities and its impact

Medical devices	Vulnerability	Severity	Vendor/organization	CVE	Vulnerability impact
PACS workstation 4.0 and 4.0.1	Information disclosure	High	GE Healthcare	CVE-2012-6694 and CVE-2012-6693 [20]	It has a password of 2charGE for the geservice account, which has unspecified impact and attack vectors related to TimbuktuPro
DICOM Part 10 file format	Portable executable (PE) malware	High	NEMA DICOM Standard 1995	CVE-2019-11687 [20]	It can execute a malicious file that is injected in the DICOM Part 10 File Format and manipulate the image stored in the PACS
Medical imaging system	Remote code execution	High	GE Healthcare	CVE-2017-14008 [18]	This may allow an attacker to bypass authentication and gain access

Steps to Mitigate

To prevent the injection of malware at the stage of the data-in-motion, the network administrator should encrypt the data communicated between the PACS network hosts using proper TLS certificate. To secure the data-at-rest, anti-virus software and servers running on end workstations should be regularly updated. Also, the exposure of the PACS server to the Internet must be restricted.

To prevent the spreading of malware embedded in the DICOM files through DICOM viewer, the vendors should test their applications through certified application tools at regular intervals. These application tools automatically update products based on third-party libraries when vulnerabilities become public, and employ, where possible, bitstream validators that identify distorted documents and restrict their processing and display.

To prevent malicious manipulation of medical images [23], digital signatures can be used to assure that any changes of an image cannot remain undetected at any point after image creation.

To protect the HL7 message exchange, TLS can be used to encrypt network traffic between the endpoints and the PACS server. This will thwart an attacker from analyzing the network traffic. Also, an MITM [22] attack can be averted if a bidirectional certificate exchange policy is implemented.

3.3 Compromising the Hospital Network

This can occur via access to a LAN port of the cabled network which is unprotected or misconfigured switches/routers, or if the encryption of the wireless network (WLAN) is compromised. After successfully compromising the network, the attacker intercepts the network traffic and analyzes the traffic through the Wireshark. Also, the attacker can learn about the network structure, available systems on the network, unencrypted user credentials, and the network protocols used. This enables the attacker unauthorized access to the network and gets a patient's sensitive information such as personal data, including personal health records, ID numbers, address, contact number, and much more. The hospital management system vulnerabilities, along with its severity and impact, are shown in Table 5.

Table 5 Hospital management system vulnerabilities and its impact

Management system	Vulnerability	Severity	Vendor/organization	CVE	Vulnerability impact
Monitoring systems, telemetry server, clinical information systems	Open SSH	Critical	GE Healthcare, ApexPro, Carescape	CVE-2020-6962 [18]	It can allow an attacker to obtain access to the SSH private key in configuration files
OpenClinic GA	Authentication bypass using an alternate path or channel	Critical	A product of open-source collaboration on Source Forge	CVE-2020-14485 [20]	It has bypass client-side access controls and may allow execution of admin functions such as SQL queries
Hospital management system in PHP v4.0	SQL injection	High	PHP Gurukul	CVE-2020-5192 [18]	It allows for the application's database and information to be compromised

To prevent the hospital network from cyberattack, we may take the following technical measures:

- Configure the network switches so that only the systems with known MAC address or previously bound MAC (i.e., serial numbers of network interface controller) address can connect [25].
- Switch off all unused ports. If required in the future, the ports may be opened by the administrator.
- Wireless networks should be reviewed and updated regularly. Also, the configuration must be audited periodically.
- Firewalls, routers, and network segmentation should be used to protect the systems that may be more susceptible to attacks.

4 Challenges and Risks Related to the Cybersecurity

- There are several cybersecurity challenges in evolving and expanding healthcare networks, inclusive of medical devices.
- The high cost of medical devices.
- Lack of skills and knowledge about how to use healthcare devices in a wireless network.
- In the market, there are a variety of medical devices and every medical device has its configuration and settings that may be a problem for medical practitioners.
- Lack of universal manufacturing standards and immaturity of existing standards.
- There should be a National level Medical Policy for data security and privacy issues.
- Hospital management should be held responsible for any data leakage as per the provisions of any regulation like the General Data Protection Regulation (GDPR).
- Non-updation of software by healthcare providers and medical practitioners.
- Lack of investment in technology, research, and personnel [26].

Safety risk of Patient

- Device function or performance gets changed that results in misdiagnosis or treatment error of the patient.
- Compromise of sensitive patient data like medical results or device-specific data like heartbeat rate.

Risks related to care delivery

- Hospital operations disruption.
- Reduced ability to properly deliver care.

Risks related to privacy

- Loss of critical information (patient healthcare information, credentials).
- Breach of data.
- Intellectual property (research, design, and trials data).

Table 6 Mitigation matrix for different devices in healthcare systems

Steps to mitigate	IMDs	Medical imaging devices	Data storage server	Hospital management network
Restrict unauthorized access	✓	✓	✓	✓
Pairing protocol between devices	✓	✓		
Cryptographic key exchange	✓	✓		
Disable unused ports			✓	✓
Digital signatures	✓		✓	
Updation of software	✓	✓	✓	✓
Isolation and segmentation of network			✓	✓
Use of security devices such as firewalls, IPS			✓	✓
Risk assessment and threat modeling	✓	✓	✓	✓

Risks related to finance

- Loss of reputation of organization.
- Revenue loss.
- Impact on corporate goodwill and stock value.

In Table 6, we have tabularized the mitigation matrix for different devices in healthcare systems.

5 Conclusion and Future Work

In the healthcare system, the safety of the patient will be a priority over cybersecurity needs. Closing the gap between the two objectives is the primary challenge. Minimizing data compromise and ensuring patient safety while being reactive to the cybersecurity threat environment are today's needs. Healthcare devices, wireless networks, and patient care management systems are now a vital part of healthcare networks. Thus, their security and privacy should be an essential component of cybersecurity defense. More coordination between the network administrative professionals and

medical physicists, as well as medical device makers and vendors, are required. Also, input from cybersecurity experts and government agencies at regular intervals are required. Cybersecurity vulnerabilities related to healthcare devices are very similar to any other system connected over the network. The need to mainstream the cybersecurity protection policy of healthcare devices is more visible because of the potential detrimental impact on patient safety after the exploitation of cybersecurity vulnerabilities of healthcare devices. This draws the difference between the importance of securing healthcare devices and other network environments. Given the current lack of governance and national level policy of networked medical devices, amalgamated with risk management, lack of knowledge of the security risks, reliance on medical device regulatory approval, and lack of preparedness by organizations to manage the risks, the need to protect the healthcare cybersecurity system is essential. While jurisdictional regulation has been the drive to enforce increased protection through privacy and security rules for medical data by a concerned government agency, the compliance to the same does not mean adequate security. Data breach regulation laws and compulsory reporting to government agencies have resulted in a proactive approach to secure cyberspace in the healthcare environment. To guarantee the protection of the healthcare system connected in a network, a coordinated, proactive approach including standard cybersecurity control and assessment, along with specific medical device data and workflow considerations, is needed.

References

1. Philips ultrasound authentication bypass vulnerability report published by NHS Digital. (2020)
2. Siemens security advisory by Siemens Product CERT 2019. (2020)
3. https://global.medtronic.com/xg-en/product-security/security-bulletins/conexus.html. Accessed 4 Jun 2020
4. K. Sheridan, A report: severe vulnerabilities discovered in GE medical devices. (2020)
5. Report published by Greenbone Sustainable Resilience: a German cyber security firm. (2018)
6. A report on medical data leak published by Greenbone.: Sustainable Resilience. (2019)
7. A follow report on medical data leak published by Greenbone: Sustainable Resilience (2019)
8. E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, H. Chen, Assessing medical device vulnerabilities on the Internet of Things, in *IEEE International Conference on Intelligence and Security Informatics (ISI)* (2017)
9. D.J. Slotwiner, T.F. Deering, K. Fu, A.M. Russo, M.N. Walsh, G.F. Van Hare, Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians, in *Proceedings of the Heart Rhythm Society's Leadership Summit*
10. E. Marin, On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them, in *ACSAC'16* (Los Angeles, CA, USA, 2016)
11. C. Camara, P. Peris-Lopez, J.E. Tapiadora, Security and privacy issues in implantable medical devices: a comprehensive survey. J. Biomed. Inf. **55**, 272–289 (2015)
12. D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark et al., Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-ower defenses, in *IEEE Symposium on Security and Privacy* (2008)
13. Z. Wang, P. Ma, X. Zou, J. Zhang, T. Yang, Security of medical cyber-physical systems: an empirical study on imaging devices, in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (2020)

14. https://www.softneta.com/wp-content/uploads/2019/02/SendToPACS-converting-files-to-dicom-workflow.png
15. M. Burhan, R.A. Rehman, B. Khan, B.-S. Kim, IoT elements, layered architectures and security issues: a comprehensive survey. Sensors (2018)
16. https://www.medicaldevice-network.com/features/cyberattacks-healthcare-covid-19/. Accessed 13 Sep 2020
17. L. Coventry, D. Branley, Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. 48–52 (2018). Maturitas. ISSN 0378-5122
18. https://nvd.nist.gov/vuln/detail. Accessed 4 Aug 2020
19. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. Accessed 11 Oct 2017
20. https://cve.mitre.org/. Accessed 4 Sep 2020
21. E. Marin, D. Singelée, B. Yang, V. Volski, G.A.E. Vandenbosch, B. Nuttin, B. Preneel, Securing wireless neurostimulators, in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy—CODASPY'18* (2018)
22. A.I. Newaz, A.K. Sikder, M.A. Rahman, A survey on security and privacy issues in modern healthcare systems, attacks and defenses. ACM Health **1** (2020)
23. M. Eichelberg, K. Kleber, M. Kämmerer, Cybersecurity challenges for PACS and medical imaging. Acad. Radiol. **27**(8), 1126–1139 (2020)
24. L. Pycroft, T.Z. Aziz, Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. Exp. Rev. Med. Devices **15**(6), 403–406, (2018)
25. P. Williams, A. Woodward, Cyber security vulnerabilities in medical devices: a complex environment and multifaceted Problem. Med. Devices Evid. Res. (Auckl) **8**, 305–316 (2015)
26. F. Luh, Y. Yen, Cybersecurity in science and medicine: threats and challenges. TIBTEC **1902** (2020)