Deep Science Publishing
https://doi.org/10.70593/978-93-49910-80-5_8

DeepScience
Open Access Books

Chapter 8: Cybersecurity and data privacy challenges in networked medical technologies

8.1. Introduction

The technological advances experienced in the last decades have brought us the so-called Internet of Things (IoT) and Human-Centered Internet technologies. By relying on the ubiquitous deployments of networked sensors, these technologies can enable an always-on connection with the physical and social world, supporting remote interactions on several aspects of our daily lives, such as work and healthcare, among others.

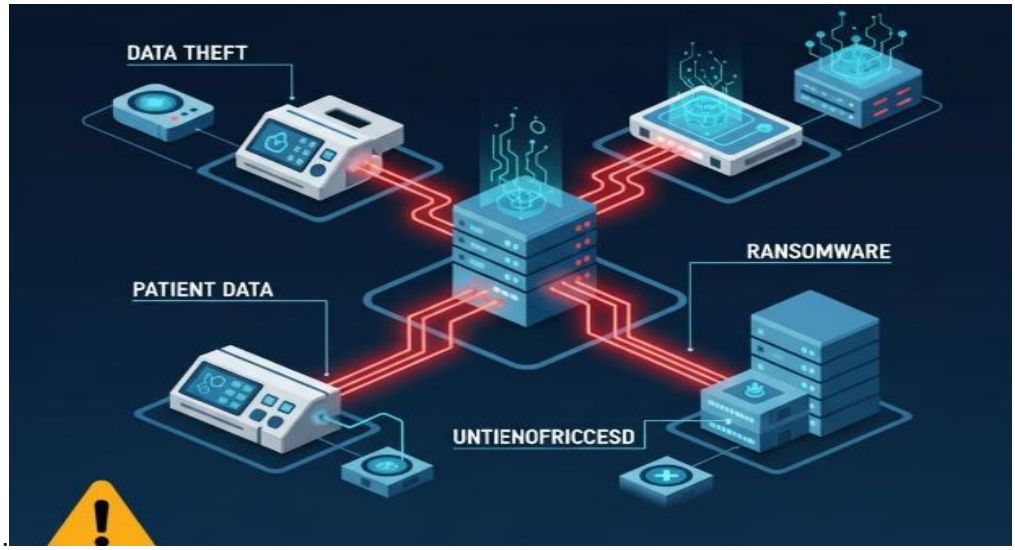

Fig 8.1: Cybersecurity and Data Privacy Challenges

The extensive utilization of wireless communication technologies has further enhanced the deployments and prospects for the IoT. In this context, the ubiquity of mobile devices

provides anytime access to local information, while cloud services provide virtually unlimited storage capacity and processing power. These near-universal technological infrastructures have promoted the data-driven society, a society where privacy-preserving data utilization models are essential to fully explore (Kumar & Silambarasan, 2019; Khan & Rehman, 2020; Ganaie & Kim, 2021).

There is a rapidly increasing reliance on networked technologies supporting remote medical treatments, that is, remote diagnosis, monitoring, and help for several types of medical conditions, namely chronic and mental health conditions, among others. The capabilities and prospects for these technologies have reached a promising maturity through the dissemination of wideband wireless connectivity quality and bandwidth, cloud computing solutions, and a wide range of wearable and implantable devices built with low-cost and high-performance sensors. These solutions are expected to improve the efficiency of healthcare systems, in addition to providing improved effectiveness for users that rely on remote technology-mediated medical interventions, helping to decrease waiting lists for diagnosis and therapy for health conditions, including mental health disorders (Tao et al., 2019; Wang & Cai, 2020).

8.2. Overview of Networked Medical Technologies

Networked Medical Technology (NMT) is a technology that is applied in health organizations to help solve specific problems, conducting independent anonymity by the patients by self-reporting their health information painlessly and continuously, using devices that sample health information and are interfaced with computer networks. NMTs include implantable medical devices, such as pacemakers, implantable cardioverter-defibrillators, implants for neuro-stimulation, and wireless transceivers; wearable medical devices, such as computer-enabled soles, inhalers, bandages, and wrist worn devices; and external monitoring devices, such as tele-monitoring systems for chronic diseases, home monitoring systems for home health care, and monitoring systems for mobile patients with ambulatory emergencies, including high-risk for heart attack, heart failure, stroke, and bronchial diseases.

Millions of patients every year rely on treated required NMTs, as they help treat and diagnose heart failure, neurological disorders, diabetes, chronic obstructive pulmonary disease, hypertension, asthma, and allergy rhinitis, and can help prevent or reduce the impact of patients' lives by emergency responses to high atypical measures of them. NMTs continuously monitor high-risk patients' critical health signals, increase the quality of telehealth, release the patients from required clinical testing, and allow the healthcare system to save economic resources. However, NMTs are a new entry in health organizations. More and more cyberattacks are being performed every year as they are a powerful access tool for cybercriminals, who are looking to steal the patients' sensitive

information or harm them. Both intentions jeopardized the patients' safety and security, damages patients morally and financially, can harm the reputability of health organizations, and wrecks trust in mechanisms predicted to help improve the health of patients, especially critical and chronic patients.

8.3. Importance of Cybersecurity in Healthcare

The increased use of Internet-enabled and -connected medical technologies is improving healthcare delivery, as well as expanding hospitals' operational efficiencies. Such technologies enable quick and anywhere access to patients' health records, which boosts the quality of discharge and outpatient care services. They also allow remote monitoring of unwell patients, the use of digital health assistants and online consultations, technological surgeries, and real-time health assessments. Continuous use of connected medical devices in healthcare services is expected to empower caregivers and make patient monitoring more efficient, which will boost their quality of life. The global telemedicine market is set to grow significantly. Despite the numerous benefits that networked medical devices bring to healthcare, security vulnerabilities that expose medical procedures, critical infrastructure, and patient data privacy challenges are increasing. Cybersecurity failures could deny hospitals' access to primary management services and critical data, help criminals pose as patients, manipulate treatments, or mutilate medical devices, take hostage patient data, disrupt or invade embedded control systems, leak sensitive private data, or risk patients' well-being and lives.

Additionally, healthcare services are also becoming rich target suppliers of biometric information related to individuals' physical and behavioral characteristics. Cybercriminals obtain such data through cyberattacks with identity theft purposes. Digital trends are making the information technology infrastructure of healthcare even more appealing to criminal and terrorist groups. The exploitation of minors' sensitive data, as well as the hacking of hospitals' and life-science organizations' payment systems to forge cybercriminal affiliates in order to finance illegal operations, are but a few examples of how patient-sensitive data could be used.

8.4. Data Privacy Regulations

Numerous evolving regulations have been implemented both nationally and internationally to protect data privacy within Networked Medical Technologies (NMTs) and offer guidance to researchers, medical practitioners, and developers. While these regulations pertain to the broader field of data privacy and do not explicitly mention NMTs, they serve as a springboard for practical implementations of data protection

measures that can be made specific for NMT applications. Violations against the regulations can result in substantial penalties.

The Privacy Rule was one of the earliest and focuses on the protection of health information. The main concern is to find a proper balance between the right individual data privacy and the need for sharing information for care provision and research. It establishes a set of national regulations to prescribe standards for data privacy and security regarding Protected Health Information (PHI). PHI is identified as information related to an individual and the individual's health status, provision of healthcare, or payment for healthcare. The main bodies covered are healthcare providers, health plans, and healthcare clearinghouses that maintain PHI. After developing specific standards under the Privacy Rule, NMT developers and healthcare providers must assess whether their service covered PHI data. If so, NMT developers must apply privacy practices, including providing users with privacy policies so that users know that their information is being shared. However, the rule leaves room for a number of exemptions with regards to de-identification. After the data is stripped from its identifiable elements, the PHI data is not classified as being PHI anymore, leaving NMT developers and healthcare providers outside of the scope of the defined privacy practices.

Fig 8.2: Data Privacy Regulations

8.4.1. HIPAA Compliance

Due to the privacy-sensitive nature of the health data that medical devices and their services handle, they may fall under the scope of the Health Insurance Portability and Accountability Act. This act mandates certain handling and protection requirements for PHI communicated, stored, or processed by Covered Entities and Business Associates. Covered Entities are defined as providers who transmit any health information in electronic form in connection with a transaction; health plans; and healthcare clearinghouses that process health information. According to the act, PHI refers to any individually identifiable health information within a Covered Entity's or Business Associate's possession or control, which is transmitted or maintained in any form or medium by a Covered Entity or Business Associate, or that is created or received by a Covered Entity on behalf of another Covered Entity. Business Associates are defined as "a person or entity who performs a function or activity on behalf of the covered entity that involves the use or disclosure of Protected Health Information."

Because the handling and protection requirements set forth by the act only apply to Covered Entities or Business Associates, a medical device manufacturer or health IT vendor providing a medical device or health IT application that provides a service to a Covered Entity that involves the use or disclosure of PHI must sign a Business Associate Agreement with that organization. In a Business Associate Agreement, the manufacturer or vendor agrees to comply with the act and requires specific measures to be in place to ensure compliance.

8.4.2. GDPR Considerations

GDPR has a strong influence globally and consequently the many global organizations investing in networked medical technologies will also need to be compliant with GDPR. For clarity and completeness, we begin with an explanation of what GDPR is, and when it is relevant to organizations. GDPR is the General Data Protection Regulation established by the European Union (EU) Parliament and Council in 2016. It governs the collection, use, and retention of personal data and creates a single legal-compliance framework applicable to all EU member nations. Any organization that collects or processes personally identifiable data of individuals located in the EU must comply with GDPR, regardless of whether they are based within an EU member country. GDPR applies to a broad range of entities, including those that offer goods or services, or those that monitor and maintain the behavior of individuals, located in the EU. Penalties for

non-compliance include heavy fines or a percentage, up to 4%, of global annual turnover, whichever is higher.

GDPR defines several data privacy principles that must be adhered to. Processing of personal data must be lawful, fair, and transparent. Personal data needs to be minimised and limited to that which is necessary for the stated purpose. It has to be accurate and kept up to date. Personal data will not be kept longer than necessary, and has to be in a form readily accessible to the individual. Processing of the data must be secure. Organizations that process personal data must comply and help individuals exercise their rights in respect of their own data, and must notify the individuals of any breaches involving their data. Data protection has to be considered, and when necessary implemented from the very beginning of any and all data processing activities.

8.5. Threat Landscape in Medical Technologies

Medical technologies are surrounded by a rich threat landscape that extends from classical shared public and private information threats, e.g., leaking health records, to novel technologies empowered information technologies but with a perpendicular medical workflow, e.g. falsifying a diagnosis. Healthcare, being a goal and a facilitator of information technology, intersects with both dimensions, thus creating a fertile ground for motivation of a cybercriminal and delivering a unique product, still manageable with cyber tools. Therefore, the medical information technology landscape forms such cyber threats as exploitation of security weaknesses in the design and implementation and hospital information technologies, e.g. EMRs beliefs, Medical Device Interoperability, device manufacturers and data analytics companies, which contain important sensitive, proprietary, and business valuable information.

Dangerous potential vulnerabilities exist during the data preparation stage of AI-aided analytics, and especially in data quality, as well as trustworthiness overall and AI failed consistency in performance. Data for clinical analytics are very heterogeneous and naturally exposed to data bias, noise, and compliance limits for data completeness. Medical decisions might challenge patients' lives and would be based on flawed models due to their poor predictive accuracy and explainability, therefore subjected to the AI-fraud link. Adversarial examples or data input/output must be addressed, as well as accuracy lapse in changing data distribution periods, which challenge an always-on AI-enabled surveillance. Cyber-related research emphasizes adversarial model examples or AI-fraud input data and the poor model guard mechanism typically aided with explainability algorithms. However, these approaches would not get priority over proper data-generation input rules addressing data bias, noise, feature space volume, and patients-related data incompleteness issues.

8.5.1. Common Cyber Threats

Medical technologies are used in many safety-critical applications. They often represent the first line in the diagnosis or therapy of critical diseases. Cyber threats to medical technologies that are networked or supporting data sharing face both traditional and new types of cyberattacks. Many of the cyber threats are similar to, or mirror, those applied against general IT platforms. Increasingly more types of cyberattacks have appeared for critical systems. Cyberattacks on traditional IT platforms have transformed over the years, employing different vectors, tools, and methodologies. In the early times, cyberattacks often played with vulnerabilities in software and no or weak security controls on access to the system platform itself and security for privileged commands. Break-ins, those in which the attacker gains remote access to the target system, upload malware for manipulation or exfiltration of local data or launching an attack on another system, are serious concerns. Modern cyberthreats are described by the terms “blended” and, now more than ever, “zero day.” These cybercrime activities could arise for profit or as a way of supporting organized hacking activities, espionage, disruption, vandalism, and theft. Over the years, cybercriminal organizations have supplied attackers with the necessary tools to exploit vulnerable systems.

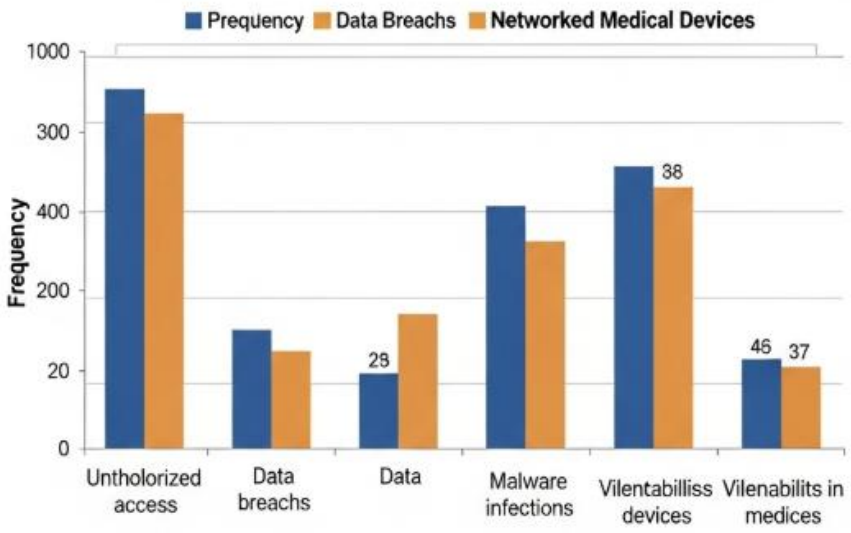

Fig 8.3: Cybersecurity and Data Privacy Challenges in Networked Medical Technologies

8.5.2. Emerging Threats

As networked medical technologies gain more capabilities and become widely used in many medical applications, they face greater challenges for cybersecurity and data

privacy. The vulnerabilities of networked medical technologies may be exploited by cybercriminals to achieve various malicious actions, resulting in damaging the technologies and putting affected patients in danger, and even affecting supply chains. This section mainly focuses on the specific aspects of cybersecurity and data privacy challenges and concerns that are faced by each type of networked medical technology including electronic health record, telehealth technology, medical imaging technology, Body Area Network, implantable medical device, and assistive health technology.

Cybersecurity and data privacy are especially critical for electronic health record systems due to the nature of the health information contained in the systems. Advanced technologies such as providing fake health information and connecting expert doctors from all over the world together and with the patients through telehealth to allow them to achieve teleconsultation especially without actual contact can be effective solutions to partially solve these challenges. Medical imaging technology solutions can also partially help deal with cybersecurity and data privacy challenges. In addition, doctors and experts can use Body Area Network nodes, devices, or wearable devices to monitor the patients and collect detailed patient health information continuously.

8.6. Vulnerabilities in Networked Medical Devices

Malware and exploits targeting medical devices may not be as heavily marketed as those targeting operating systems. Yet, cybersecurity vulnerabilities in medical devices could leave patients vulnerable to life-threatening exploits. Medical devices are becoming increasingly more versatile, flexible, and easily integrated in various medical environments, including homes, making them more susceptible to cyber threats. Medical systems often store sensitive and private information about individuals, some of which are only shareable with specific persons. Breaching medical systems may expose one to intimate and sensitive details about individuals. Moreover, devices such as voluntary cardioverter-defibrillators may be programmable to shock patients and can be used in exploits to forcibly shock patients for personal gain. Vulnerability research into medical devices has exposed myriad exploitable software and hardware vulnerabilities, including remote firmware update via USB flash drives, unencrypted communication channels, improperly protected Hospital Intranet, and unprotected data interfaces, accessible using verified authentication details.

Software Vulnerabilities

Since software can be remotely modified through updates and patches, software vulnerabilities pose an important threat to the safety of networked medical devices. Rather than using the secured method of signing firmware updates to prevent modified firmware from being uploaded to devices, some manufacturers use insecure methods,

allowing the upload of malicious patches. Moreover, many updates are installed over HTTP, using or without encryption, making the devices vulnerable to spoofing; unauthorized transmission of harmful patches is easy; and authentic patches can be intercepted and exploited, potentially risking human lives. Although not used in conventional computers, exploit kits, such as those targeting medical apparatus, can be used to exploit software vulnerabilities, thereby endangering patients.

8.6.1. Software Vulnerabilities

Vulnerabilities in networked medical devices can arise from many traditional software weaknesses, with old coding errors flowering anew in devices which may use decades-old versions of basic operating systems. In 2023, a significant percentage of all recorded vulnerabilities were found in networked medical devices. Traditionally, medical devices have been built on proprietary systems more or less untouched during seal-and-deliver timeframes that extended past the limits of ordinary coding errors. Security demands, adequacy of information transfer mechanisms, and overall usability considerations eventually brought discussion of the importance of cybersecurity to the deployment of medical devices. Traditional networked vulnerabilities, including Denial-of-Service weaknesses, Cross-Site Scripting weaknesses, Injection Payload variations, and Constructed Dynamic Code Execution vulnerabilities, while not always lethal in medical devices, can have dire and swift effects entirely unconsidered during the implementation phases of security regulations. Over time, an increased demand for software tasking, reduced overall security focus, and continued demand for speedy releases by manufacturers resulted in exploitable increases in software vulnerability.

Modern medical devices often utilize third-party code packages built by unregulated sources with no medical examination, seek out specialized storage solutions, use repurposed consumer electronics with no thought given to the additional workloads required, and have minimal testing and patching cycles. Attack vectors for these vulnerabilities already exist. The possible outcomes associated with years of non-regulation, neglect of software examinations, and legislative refusal to even consider addressing the associated security risks are manifest in already-achieved cyberattack results — Permanent Dream State of a Flow-Metrics Device, Reprogramming of Remote Control, and Ransomware. The survival of the stakeholder may depend on the utilization of mechanical tissues which define the abilities of the organism to perform within its environment.

8.6.2. Hardware Vulnerabilities

Security in traditional computing systems and applications is indeed vital since they are the source of many types of sensitive data for any users, companies or government. However, these systems are only a first step in focusing on security. Nowadays, a high number of computing devices, sensors and systems are embedded in our daily lives and are used to monitor and make decisions in a wide range of critical scenarios: smart buildings, wearables, medical devices, industrial control systems, autonomous and assisted vehicles, to mention a few. In these scenarios each type of device has defined its own level of restrictions and requirements: power consumption, communication protocols, determinism, confidentiality, safety, trust, security. All these restrictions are present during the entire life cycle of the device, mainly during development. The consequences of decisions taken during the design and development of these devices is what allows or not to keep the device/channel vulnerable or not vulnerable from outsiders when deployed and in the post deployment phase.

Networked medical devices, like all the above mentioned devices, are constrained systems that demand the development considering not only the specialized design to meet the functional requirements, but the security solutions that will prevent the device and network to be vulnerable both in the pre-deployment phase but also in the post deployment. It is therefore important to understand the potential vulnerabilities in order to apply the required security mechanisms at design time. The resource-constrained embedded systems, sensors and actuators are normally vulnerable to basic attacks due to the minimal cost budgets for the design. These attacks can be used to get information or cryptographic keys that allow other more elaborated attacks to the device or the entire network.

8.7. Conclusion

This chapter discusses fundamental cybersecurity and data privacy challenges associated with emerging classes of IT/OT/network edge and networked medical technology, elaborating on concepts related to health data privacy and lack of common cybersecurity safeguards found in today's ecosystem of health and medical devices. Topics presented in this chapter include challenges with shortage of workforce to combat these challenges, principles of modernized device development and deployment frameworks, and suggestions for additional research to better address these fundamental cybersecurity and health privacy challenges. Key findings of this chapter include that most connected devices rely on industry-specific regulatory safeguards that miss many dimensions of the cybersecurity problem, most connected medical technology devices that are far laterally exposed that use software for fast startup and recovery from turn-off states to become functional, have no inherent cybersecurity safeguards to protect confidentiality

and integrity of information and availability of services, and device-manufacturers invest in very lopsided protective measures that do not account for complete remaining risk that this device-persona issue introduces into systems-of-systems architecture. Secondary factors like overall cybersecurity economic insufficiency issues, and inefficient cybersecurity-policing structures are obstacles to promoting best practices in IoMT facility operators that procure these vulnerable devices in bulk. Based on these limitations provided by the present scenario discussed earlier, we present potential paths forward to address these IoMT ecosystem problems that will help create the conditions necessary for the ecosystem to become self-sustaining, beyond service policies for individual IoMT gadgets already mentioned: (i) make adequate talent available, (ii) develop secure by design concepts to systematize and incentivize secure designs and implementations by device manufacturers, (iii) develop deployment monitoring and electronic remediation decision-assist techniques to minimize dangerous weaknesses of deployed systems, and (iv) create service and support avenues to facilitate cybersecurity adjustment of older devices with weak defenses that have a very prolonged presence in IoMT facilities.

8.7.1. Future Trends

Research has been initiated to detect problems in networked medical devices and networks operated by these devices. However, the results available are purely academic. The medical devices used now are not upgraded in a short time. A medical device including an OS is normally considered for neglecting its update for twenty years. Cybersecurity and data privacy issues, incidents, events, and mechanisms will stay basic research and practice areas during these two decades. There are rather long-standing hopes that presently applied cybersecurity and data privacy techniques could be applied to networked medical devices and networks operated by these devices with full success. However, the devices appear to be too specific to allow appropriate adaptation and implementations of techniques and methods tested for a broad spectrum of infrastructures, such as confidentiality, integrity, and multiple access security, or digital forensics. In a way driven by blind optimism, techniques and methodologies that have been neglected for a long time are proposed to be applied to networked medical devices. They are basic cryptographic primitives or randomized testing for cybersecurity and data privacy assessment.

However, these primitives are applied in cryptographic or randomized frameworks that do not share similarities with tools that have been successfully implemented in a broad range of other applications closely cooperating on a particular task accessible for other participants. Tools whose implementations have been matured for decades may not need high-level cryptography, modular or trusted code distribution, or randomization to

become feasible for networked medical devices. Overly optimistic visions could become true with the proper amount of effort. In addition to the previous discussion on assessment methodologies, there are multiple active areas for research, innovation, and industrial implementation. Each of these areas could lead to significant improvements in the performance and safety of current networked medical devices.

References

Ganaie, M. A., & Kim, S. W. (2021). Intelligent healthcare system using emerging technologies: A comprehensive survey. SpringerLink. SpringerLink+1SpringerLink+1

Wang, X., & Cai, S. (2020). An exhaustive review on emerging healthcare Internet of Things technology. SpringerLink. SpringerLink

Khan, M. A., & Rehman, M. S. (2020). Applications of artificial intelligence and big data analytics in m-health: A healthcare system perspective. Journal of Healthcare Engineering. Wiley Online Library

Kumar, P., & Silambarasan, K. (2019). Enhancing the performance of healthcare service in IoT and cloud using optimized techniques. IETE Journal of Research. SpringerLink+1SpringerLink+1

Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2019). Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet of Things Journal, 6(1), 410–420. SpringerLink