Healthcare Cybersecurity Vulnerabilities

Ryan DRAKE[1], Evan RIDDER[2]
[1] Arizona State University, United States
rdrake6@asu.edu
[2] Kansas State University, United States
eridder@ksu.edu

Abstract

The healthcare industry sector is often considered a soft target for malicious actors. Having a large attack surface coupled with a focus directed toward patient care rather than security, often health organizations haven't taken the necessary precautions to secure patient data or access to medical devices within their infrastructures. As the severity and the associated costs of cyber-attacks on entities within healthcare organizations continue to escalate, an increased effort within this industry to mitigate the risks associated with these vulnerabilities is necessary. This study seeks to present the most common types of healthcare attacks and their mitigation methodologies. Additionally, a discussion of how compliance with the GDPR in the European Union and the HIPPA regulation in the United States can positively affect a healthcare organization's defensive posture.

Index terms: Cybersecurity, GDPR, Healthcare, HIPPA, PHI, Privacy

1. Introduction

Beyond providing quality patient care, healthcare organizations must uphold ethical standards which include maintaining the privacy and confidentiality of patient health data [1]. To manage patient care, healthcare organizations process large amounts of sensitive data usually in the form of electronic health records which include patient personal health information (PHI), as well as financial and demographic data. This medical record data is a desirable target for cybercriminals as it is valuable for sale on the black market and it can be used for extortion purposes [2], [3]. Highlighting the extent of this issue, in 2021 over 45 million electronic medical records were stolen from healthcare providers in the United States. exposing sensitive patient personal, medical, and financial information [4].

Cybercriminals frequently attack medical providers due to the perception that the healthcare sector is a soft target [3]. Vulnerabilities in the healthcare sector can be attributed to many factors stemming from limited staffing resources, significant reliance on un-patched legacy systems which are no longer supportable, a large attack surface, and a lack of security awareness by care staff. [2], [3]. The number and complexity of attacks in the healthcare sector have risen over the last several years within the global community. As the severity and the associated costs of cyber-attacks on entities within healthcare organizations continue to escalate, an increased effort within this industry to mitigate the risks associated with these vulnerabilities is necessary [3].

This study seeks to present the most common types of healthcare attacks with mitigation strategies, along with a discussion of the concept of privacy in the context of the European Union's GDPR and the United State's HIPPA regulation.

2. Overview

As part of the ethical care of patients, the proper treatment of their personal and health-related data is essential. Privacy within the context of healthcare is associated with the handling of patient personal and healthcare data and is concerned with its collection, storage, processing, and use in a secure manner [1]. With the technological advances in the healthcare industry, patient-related data is recorded primarily in digital form and as such is vulnerable to information leakage due to unprotected information systems or through cyber attacks [2]. Care as to how these records are stored and processed, as well as securing the underlying IT infrastructure are fundamental steps necessary to reduce the risk of patient medical information leakage. However, as medical data is valuable to malicious actors, healthcare organizations provide attractive targets for an attack [3].

2.1. Personal Health Data

In the United States, more than 200 million patient records have been compromised since 2010 [4]. Most of these attacks were against electronic health records which contain patient personally identifiable information such as name, birthdate, addresses, and government identification numbers, however additional data such as medications, medical history, or test results can be part of this data [5]. Electronic health data is valuable on the black market as these stolen records usually contain a more complete identity profile beyond financial data. Health records often contain numerous aspects of demographic, financial, and potentially sensitive medical data which is appealing to the attacker since this PHI data can be sold and resold multiple times with stolen records often fetching $20 to $50 per record [5], [6], [7].

2.2. European Union - GDPR

The General Data Protection Regulation was enacted in 2018 in European Union (EU) as the main regulation that dictates the methods of how citizens' data is processed both in the EU and within its extraterritorial areas [8]. The GDPR applies to all data processing entities within the EU and as such, healthcare providers are also subject to the GDPR directives. GDPR compliance assists in the maintenance of privacy elements of healthcare data through regulations requiring strict compliance with patient consent rules for the collection, storage, and processing of personal data, eliminating patient consent by default [9]. Additionally, healthcare providers must adhere to the "right to be forgotten", allowing the patient to request their data be permanently deleted upon request. Security mitigations to maintain data security include encryption, the use of administrative, technical and physical controls, pseudonymization, redundancy, and intrusion protection mechanisms [8], [9].

2.3. United States - HIPPA

While the GDPR pertains to all business entities within the EU, the Health Insurance Portability and Accountability Act of 1996 (HIPPA) regulations only apply to healthcare providers within the United States. As opposed to the GDPR, HIPPA only applies to health care providers and processers within the United States and does not cover citizens outside of the bounds of the United States [10]. The HIPPA United States federal law protects the privacy of personal health information (PHI), giving rights to an individual regarding their data while imposing processing obligations to healthcare providers and processors. The basic principles of the HIPPA regulation include patient control of the release of their information, with strict boundaries put in place for the use and processing of PHI data. The use and processing of this data is for health purposes only and is not to be marketed or sold. Reasonable measures must be put in place to protect PHI from unauthorized access, disclosure, or use, where records can be either paper copies which must be physically located in locked areas, or electronic data records which must also be secured [6].

Similar to GDPR, healthcare providers within the United States must also comply with strict data security protocols and ensure compliance with the handling and disposal of PHI data. The HIPPA regulations are primarily centered around protecting patient records from a breach, however, HIPPA doesn't address the concept of patient consent to data use as GDPR does. Additionally, HIPPA does not give the consumer the right to data erasure as GDPR does, while both regulations have stringent penalties for organizations that violate the data processing and privacy laws [8], [9], [10].

3. Methods

As the healthcare industry remains an attractive target for cybercriminals, the identification of vulnerabilities associated with the healthcare industry and their associated mitigations can assist with the reduction of the risk associated with this industry silo. The methodology for this study included the following steps, identifying appropriate literature, the collection of data, the analysis and evaluation of the literature, followed by the categorization of the selected literature. The key terms "cybersecurity", "healthcare", "vulnerabilities", "GDPR" and "HIPPA" were used to search scholarly electronic databases which included PubMed, ProQuest, and Google Scholar. Additionally, websites associated with the reputable new sites were searched, as well as sites associated with the regulatory entities of GDPR and HIPPA. The literature review generated 57 sources, of which 9 were used as primary sources for evaluation and discussion. Exclusion and inclusion criteria were based upon the content of the abstract, level of research originality and the content of data presented. Broad themes of cyber vulnerabilities associated with healthcare emerged through the analysis and categorization of the reviewed literature which is discussed in Section 4.

4. Results

Four primary areas of the attack were identified through the literature review which include ransomware and malware, IT infrastructure, medical devices, and human-based exploitation which will be subsequently discussed.

4.1. Ransomware and Malware

Ransomware is a type of malicious software used by attackers to extort money from organizations. During a ransomware attack, the attackers first encrypt the target data to either block access or in some cases, exfiltrate the data. The attackers then message the organization with the monetary demands required to unlock the data [12]. These ransoms are usually paid in cryptocurrencies where the transactions are anonymous and non-reversible [2]. There is considerable debate as to if ransomware should be paid and if so, in what circumstances. Two issues concerning paying the ransomware are the incentivization of bad actors and the lack of guarantee that the attackers will honor their word [13]. Personal health data which has been encrypted by ransomware attackers should be assumed to be compromised, and as such would trigger breach notification obligations from a regulatory perspective [8], [9], [10].

As the most common attack mechanism for cybercriminals, ransomware attacks on the healthcare industry occur on a global scale [4]. The United States accounts for 60% of healthcare provider ransomware attacks followed by France, Brazil, Thailand, Australia, and Italy. Although these countries are the primary targets, other countries in the EU such as Germany and Romania have also had healthcare organizations such as hospitals, pharmacies, and medical centers attacked [11]. Some common malware associated with the ransomware attacks on healthcare entities includes Ryuk, DoppelPayer, LockBit, Hive, Maoloa, Phobos, WannaCry, Conti, Pysa, AstroLocker, Ragnarok, Vice Society, Groove, and CLoP [3], [4], [16], [11], [13].

4.2. IT Infrastructure Attacks

Large, complex data processing systems are required to manage healthcare ecosystems, and with that comes a large attack surface. Vulnerabilities in infrastructure elements such as firewalls, server applications, cloud storage, and processes can provide a means of attack to produce harm or exfiltrate sensitive data [6], [14]. As consumers interact with their health care providers over mobile and computer applications, ensuring web applications are hardened against attacks such as SQL injections or cross-site scripting is equally important [15]. Often infrastructure attacks provide the initial entry point for privilege escalation and subsequent takeover of systems to perform data exfiltration or for ransomware attackers [7].

Other attacks methods leverage vulnerabilities within the applications used by the medical staff such as the medical imaging and picture archiving and communications systems (PACS) used by the radiologists to evaluate various types of medical images obtained through patient CAT scans, MRIs, or ultrasound procedures [15]. Transmission of the images is done usually via DICOM, Digital Imaging, and Communications in Medicine which by default transmits messages in unprotected clear text that can be viewed through readily available packet analyzers such as WireShark [16]. Beyond obtaining the digital images, source and destination information used to further infiltrate the network can be obtained as well as sensitive patient healthcare information. Additionally, Health Level 7 (HL7) is set international standards which are used to promote the interconnectivity of medical devices from different vendors. Although HL7 version 3 is recommended level for use, many healthcare organizations are still using HL7 versions 1 and 2, which also by default transmit healthcare images, patient data, and network communications information in clear text by default which can lead to data leakage [15], [16].

4.3. Medical Device Vulnerabilities

As technology continues to be applied to the healthcare field, new medical devices which are both implanted, or wearable are becoming more available to a wider patient base. The ability to remotely monitor medical devices such as heart pacemakers or insulin pumps can potentially reduce the number of office visits while giving the patient greater control over their condition through the ability to better understand how their body is working [3]. Although these devices can provide improved patient care, their use does come with risks to their vulnerability to cyber-attack. Security vulnerabilities have been detected in implanted infusion pumps, cardiac pacemakers, and defibrillators, as well as the software used to access these types of devices. Frequently these devices were engineered and designed with the consideration of potential cyber-attack and often relied more on “security through obscurity” of proprietary protocols rather than a hardened attack surface [2]. The prevalent vulnerabilities include inadequate authentication mechanisms and access controls, with weak audit mechanisms. As many of these devices are similar to IoT there is frequently little storage with limited computational power and battery life. Attacks on medical devices can actively cause harm to patients by causing a malfunction of the device or through malicious device inputs or tampering with the device outputs. Attacks can also take place in the form of privacy loss due to data leakage of sensitive information [3], [7].

Beyond implantable devices, medical wearables also provide patients an ability to interact more directly with their health by allowing the continuous monitoring and recording of biometric data via the device sensors. These wearable devices can be compromised by pairing them between smartphone devices and virtual assistants [2.], [3]. As the FDA in the United States does not regulate smart devices used for medical purposes, the development of devices and apps are not subject to any restrictions which often can lead to serious privacy and safety issues [11]. Similarly, the European Union Medical Device Regulation (MDR) enacted in 2021 can view some types of wearables as borderline products where there is uncertainty over which regulatory framework applies [17].

4.4. Human-Based Exploitations

It is generally recognized that the human element presents the greatest threat to any organization either from malicious endeavors or through mistakes in configuration, lapses in security controls, or the unintentional introduction of malware through phishing campaigns [2], [5], [18]. The electronic data record is the chief target for malicious actors, who look for vulnerabilities within the systems used within the healthcare industry and its IT infrastructure or for exploitable human contacts contacted [6].

Security misconfigurations such as default passwords, improper configuration of firewalls, and server security or unsecured cloud databases provide an easy method for attackers to breach sensitive systems [3], [18]. With the plethora of available free vulnerability and penetration testing tools available, hackers can easily crawl through systems looking for open ports, default password configurations, or well-known vulnerabilities to exploit [2], [7].

Phishing uses targeted communications such as messaging or email to entice victims to either open an infected file or click on a malicious link to download malware. Phishing relies upon social engineering tactics to elicit a response from the victim to comply with the request, with the request often appearing to be from a trusted source such as the CDC, healthcare administrator, or IT staff [5], [18]. Once the file is downloaded or the malware installed from the malicious site, attackers can then continue their lateral movement and privilege escalation through the various systems to gain further footholds, leading to the exfiltration or encryption of that data to be used as ransom [13].

5. Discussion

Although an attack on medical devices themselves represents a way to directly impact patient care, the primary target for large-scale attacks is electronic data records that contain personal health information [4], [6], [11]. This data is attractive to the black market due to its longevity and multi-faceted nature which includes personal contact information such as addresses, government identification numbers, and financial records as well as medical information [6]. The securing of this information is an essential component of maintaining patient privacy and confidentiality. The application of compliance controls that are aligned with the GDPR and HIPPA regulations, coupled with the implementation of vulnerability mitigation strategies can enhance security protection efforts for healthcare providers.

5.1. Compliance

Regulatory compliance with the GDPR and HIPPA regulatory bodies provides a framework for healthcare organizations to apply security-based technical, administrative, and physical controls to provide security functions [19]. As part of the compliance process, healthcare providers must provide proof of the security controls they have in place, how they are operating, and depending upon the size of the organization an external verification must be done by a certified auditing company. Since there are strict fines for non-compliance to these security standards or if a breach occurs when basic security standards were not met, healthcare providers in both the United States and European Union countries are highly motivated to comply with the security requirements [8], [9], [10].

5.2. Mitigations

To mitigate the risks of unauthorized data disclosure or the tampering of devices, healthcare organizations must assume a zero-trust model for all systems and processes, with an assumption that their IT infrastructure could already be compromised. [20]. The central principle of zero-trust is that no device or network traffic should be considered trusted by default and with that, all traffic should be encrypted and subject to continuous monitoring to ensure the protection of data [21]. Beyond zero-trust enabling general cyber hygiene practices and security controls assists in protecting digital assets.

Industry-recommended cyber hygiene practices involve securing communications, protecting data, controlling access, proper authentication practices, ensuring patching is current, security training, and the implementation of security controls and data backups.[3], [5], [6], [7], [13], [14], [20], [21].

The securing of the communication system should be viewed from both an external and internal perspective. Externally the use of firewalls based upon the topology and use case is essential, coupled with the proper network architecture allowing for the segmentation of devices behind DMZs to help reduce the change of lateral movement of an attacker if a breach occurs. The use of intrusion detection systems (IDS) and intrusion protection systems (IPS) are also key to identifying possible attacks on the system [21]. Within the healthcare environment, data must be protected when in use, at rest, and in transit, and as such should be encrypted unless it is actively being processed [3], [6]. Storage systems, especially those on the cloud need to be encrypted and have access protections put in place [2]. Controls regarding access should be in place for both physical and data access, with strong authentication and authorization processes adhered to. It is crucial to maintain patch levels on all physical devices and software, as well as to be informed on emerging zero-day vulnerabilities such as Log.4 which could impact an organization's security posture.[21]. Staff training and mock drills help reduce the likelihood of unintentional internal security breaches through education regarding phishing and malware [5], [18].

Administrative security controls include enforcing least privilege where people are allowed access to only areas where they must have access to and no more, segregation of duties so that no one person can have unlimited access to a system, role, and rules-based access which allows for categorization of access privileges according to access requirements. Multi-factor authorization (MFA) should always be used if possible to help reduce the risk of stolen credentials being for system access [21]. Additionally, the strict management of any access or service account must be done. Beyond access control, the development of incident response plans is a central feature of the management of a data breach or cyber-attack, which should also include steps for disaster recovery if necessary. Backups should be monitored and periodically tested to ensure the ability to restore at set recovery objectives [2]. Detective security controls such as log collection and analysis vis SIEM systems are crucial elements to detect access attempts or potential breaches. Logs of servers, firewalls, gateways, and other communications must be monitored as well as the on the IDS and IPS devices. The scanning of emails and the use of data loss prevention technology should be used to assist in stopping scam emails before they reach the victim and data loss prevention software to stop the transmission of data that should not be shared [5]. Physical security controls should be put in place to ensure adequate protection of the data center and physical record access to only those who are authorized to do so [7]. Technical controls should include a wireless access policy that ensures that non-public access points are secured with WAP3 if possible [21]. Additionally, the use of anti-virus malware protection software should be mandatory for all end-user workstations and servers [20].

6. Conclusion

Traditionally, the healthcare sector has provided a soft target for malicious actors due to its broad attack surface and organizational priorities directed toward patient care rather than cyber security issues. Four general areas of cyber vulnerabilities were identified for the healthcare sector which included ransomware and malware, IT infrastructure attacks, medical device vulnerabilities, and human-based exploitations. These areas of attack can frequently be interrelated with attacks in one area leading to attacks in another, such as an attack on the IT infrastructure or a phishing scam that could lead to the installation of ransomware. The exfiltration of the electronic health data record is often the primary goal of attackers due to its value on the back market, while ransomware operators also often target healthcare providers. The GDPR and the HIPPA regulatory frameworks stipulate

security standards for securing patient data and leverage high fines for breaches due to non-compliance with their directives. Healthcare providers need to ensure that cybersecurity mitigations are followed to reduce the ability of malicious actors to cause harm within their organizations.

References

[1]. J. Mold, "Goal-Directed health care: Redefining health and health care in the era of value-based care," Cureus, vol. 9, no. 2, Feb. 2017, doi: 10.7759/cureus.1043.

[2]. S. Nifakos et al., "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," Sensors, vol. 21, no. 15, p. 5119, Jul. 2021, doi: 10.3390/s21155119.

[3]. F. Luh and Y. Yen, "Cybersecurity in Science and Medicine: Threats and Challenges," Trends in Biotechnology, Mar. 2020, doi: 10.1016/j.tibtech.2020.02.010.

[4]. December 2021 Healthcare Data Breach Report, HIPAA Journal, Jan. 18, 2022. https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/.

[5]. W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: threats, mitigation and approaches," BMJ Health & Care Informatics, vol. 26, no. 1, p. e100031, Sep. 2019, doi: 10.1136/bmjhci-2019-100031.

[6]. Conaty-Buck, S. (2017). Cybersecurity and healthcare records. Am Nurse Today, 12(9).

[7]. N. O'brien, G. Martin, M. Durkin, and S. Ghafur, "SAFEGUARDING OUR HEALTHCARE SYSTEMS A GLOBAL FRAMEWORK FOR CYBERSECURITY."

[8]. EU's General Data Protection Regulation Set to Disrupt the Medical Industry," www.healthitoutcomes.com.

[9]. "Who does the data protection law apply to?," European Commission, 2021. https://ec.europa.eu/info/law/law-topic/data-protection/.

[10]. O. for C. Rights (OCR), "Summary of the HIPAA Privacy Rule," HHS.gov, May 07, 2008. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[11]. K. Jercich, "The biggest healthcare data breaches of 2021," Healthcare IT News, Nov. 2021. https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021

[12]. A. H. Seh et al., "Healthcare Data Breaches: Insights and Implications," Healthcare, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[13]. L. Fernández Maimó, A. Huertas Celdrán, Á. Perales Gómez, F. García Clemente, J. Weimer, and I. Lee, "Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments," Sensors, vol. 19, no. 5, p. 1114, Mar. 2019.

[14]. G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?," BMJ, vol. 358, p. j3179, Jul. 2017, doi: 10.1136/bmj.j3179.

[15]. OWASP, "OWASP Top 10:2021," owasp.org, 2021. https://owasp.org/Top10/.

[16]. M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and Medical Imaging: an Overview," Journal of Digital Imaging, vol. 33, no. 6, pp. 1527-1542, Oct. 2020, doi: 10.1007/s10278-020-00393-3.

[17]. J. Gillum, J. Kao and J. Larson, "Millions of Americans' medical images and data are available on the internet. Anyone can take a peek," ProRepublica report, 2019, Online: https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet.

[18]. EMA, "Medical devices - European Medicines Agency," European Medicines Agency, Nov. 26, 2018. https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices#borderline-products-section (accessed Apr. 06, 2022).

[19]. S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social Engineering Attacks During the COVID-19 Pandemic," SN Computer Science, vol. 2, no. 2, Feb. 2021.

[20]. A. Marotta and S. E. Madnick, "Analyzing the Interplay Between Regulatory Compliance and Cybersecurity (Revised)," SSRN Electronic Journal, 2020, doi: 10.2139.

[21]. S. T. Argaw et al., "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," BMC Medical Informatics and Decision Making, vol. 20, no. 1, Jul. 2020, doi: 10.1186/s12911-020-01161-7.

[22]. D. Tyler and T. Viana, "Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture," Applied Sciences, vol. 11, no. 16, p. 7499, Aug. 2021, doi: 10.3390/app11167499.