SECURITY ISSUES OF ELECTRONIC MEDICAL RECORDS

Muminova S.Sh.

Senior Lecturer, Nurafshan branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract: *This article examines common healthcare data security and privacy issues to provide insight into the context, challenges, and types of cybersecurity threats faced by healthcare organizations. It also highlights recent research related to two key solutions for protecting healthcare data.*

Keywords: *healthcare data security, HIPAA, cybersecurity, access control*

The widespread adoption of technologies such as Electronic Medical Records (EMRs), along with the integration of various devices and health applications, has led to the collection of vast amounts of health-related data. These data are now critical for direct patient care and for advancing the field of healthcare. However, the continuous use of identifiable data for patient-tracking and the secondary use of medical data have raised serious security and privacy concerns. Research in this area shows that the number of security incidents is growing significantly, with a fifteenfold increase in reported data breaches between 2010 and 2016.

Therefore, healthcare institutions, as part of the digital health ecosystem, must implement risk management strategies to handle these issues effectively. The U.S. National Institute of Standards and Technology (NIST) identifies two core elements in risk assessment: the impact of a negative event and the likelihood of its occurrence.

Once an institution understands its risk profile, it must set a risk tolerance threshold to meet its business goals and legal requirements. This threshold defines the acceptable level of risk and helps prioritize cybersecurity measures such as reconfiguring vulnerable systems and implementing critical security controls.

The NIST Cybersecurity Framework is one of the most respected models and offers an approach to managing cybersecurity risks based on the principles and best practices of risk management. To provide better context, this article explores cybersecurity in the medical field, common risks, challenges in medical data usage, and the legal constraints that must be considered.

As shown in Table 1, different types of threats compromise each of the six desired characteristics of a secure system. These threats were later formalized into the STRIDE threat model, which analyzes potential threats and vulnerabilities in a system and proposes ways to mitigate them.

Table 1: STRIDE Threat modeling and corresponding cybersecurity attributes, threat examples, and mitigation measures

STRIDE Threats	Description	Attribute	Example	Mitigation Method
Spoofing	Imitating another person or using a fake identity	Authentication	Failing to protect or sharing account credentials in public; someone impersonating an account (e.g., social engineering and phishing attacks)	Strong authentication, encryption, cryptographic protocols like TLS/SSL
Tampering	Malicious modification of data or processes	Integrity	System administrators or healthcare staff accidentally modifying data due to improper access control	Reliable authorization, hashing and signing of data, secure communication channels
Repudiation	Ability to deny that an action or event occurred	Non-repudiation	Patient or medical professional denies accessing, recording, or editing the data	Strong authentication, secure audit trails
Information Disclosure	Data leakage or breach of information security	Confidentiality	Eavesdropping; stolen or lost devices; unauthorized access due to weak access control	Encryption, secure communication channels, strong authorization
Denial of Service (DoS)	Making a service or network resource unavailable to intended users	Availability	DoS attacks, ransomware attacks, full disk space, memory, or CPU exhaustion	Regular backups, load balancing, use of firewalls and security gateways
Elevation of Privilege	Gaining access rights without proper ownership	Authorization	Unauthorized access via stolen or shared credentials; staff having unauthorized access	Proper validation, application of least privilege principle

			to patient records	

Depending on the system's purpose and the type of data it processes, some attributes may be more critical than others. According to the General Data Protection Regulation (GDPR), "processing" of medical data can pose serious privacy risks and should be strictly regulated. Any unrecorded changes in a patient’s medical record—such as deleting information about severe allergies or a Do-Not-Resuscitate (DNR) order—can lead to severe consequences.

Patient data must be made available to authorized individuals in a timely manner. A data breach can lead to the loss of critical patient information, resulting in a decline in the quality of care or incorrect treatment. Such breaches cause not only social but also economic losses for both healthcare facilities and patients. For example, in 2020, a ransomware attack on the Düsseldorf University Hospital in Germany rendered data inaccessible, forcing the hospital to halt emergency admissions for a time. According to reports from major agencies like the Associated Press, ambulances had to be diverted, resulting in at least one patient's death and delays of over an hour in treatment.

Even today, healthcare institutions of all sizes continue to face serious security incidents.

The long-distance delivery of medical devices often introduces the risk of receiving tampered hardware or software that could later be exploited to gain access to the organization’s infrastructure.

One of the main threats is malware. Malicious attacks—such as phishing, ransomware, and social engineering—are intentional and dangerous. Phishing remains a primary method of compromising systems and networks because users unknowingly click on malicious links, leading to malware infection. Once compromised, attackers can access victims’ systems. According to the Norwegian Office of the Auditor General, phishing accounted for 39% of email-based attacks on medical institutions.

REFERENCES:

1. Safran C, Bloomrosen M, Hammond WE, et al. Towards a national framework for the reuse of health information: A white paper of the American Medical Informatics Association. J Am Med Inform Assoc 2007;14:1– 9. doi:10.1197/jamia.M2273

2. Meystre SM, Lovis C, Bürkle T, et al. Reuse or secondary use of clinical data: current status and future developments. Yearb Med Inform 2017;26:38–52. doi:10.15265/IY-2017-007

3. Marco-Ruiz L, Beale T, Lull JJ, et al. Towards open process models in healthcare: open standards and legal aspects.. In: Fernandez-Llatas C, ed. Interactive Process Mining in Healthcare. Cham: :Springer International Publishing 2021. 81–99. doi:10.1007/978-3-030-53993-1_6

4. Bellika JG, Makhlysheva A, Bakkevoll PA. Significant increase in the risk of health data disclosure in the United States: an analysis of findings from the US data breach registry. In: Proceedings from The 15th Scandinavian Conference on Health Informatics 2017 Kristiansand, Norway, August 29–30, 2017. Linköping University Electronic Press 2018. 55–9.

5. NIST Cybersecurity Framework. NIST.

2013.https://www.nist.gov/cyberframework.

6. Kohnfelder L, Garg P. Threats to Our Products. Threats Our Prod. 1999.https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx.

7. Shostack A. Threat Modeling: Designing for Security. John Wiley & Sons 2014.