Electronic Health Record, Patient Data, and Confidentiality

Andres Hernandez, Kazi Sabiha, Abbas Aslam, Jafren Rahman, Joshua Fung

York College

Biomedical Ethics

Professor McGarry

July 14, 2023

An electronic health record (EHR) is a digital version of a patient's comprehensive medical information. It includes medical history, medications, lab results, and many other data. The growth of EHR is supported by The Health Information Technology for Economic and Clinical Health (HITECH) Act passed in 2009 (Basil et al., 2022). Its usage has since grown significantly from 10% of the hospitals implementing it in 2008 to 95% in 2017 (Basil et al., 2022). EHR provides many advantages like reducing medical errors, creating an integrated health record system, and improving overall healthcare quality.

Despite the apparent benefits, EHR presents a few ethical issues along with its wide adoption. In addition to a patient's medical record, EHR stores sensitive patient information, such as the patient's name and address. While this helps clinicians to access patient records instantly, personal information is vulnerable to fraudulent use and provides financial incentives to third parties. Security concerns arise when this information is at risk of being manipulated. There is a growing trend of data breaches and can cost the healthcare industry as much as $6.5 billion annually (Basil et al., 2022). According to reports from numerous practitioners, between 2005 and 2019, approximately 249.09 million individuals were impacted by healthcare data breaches (Seh, 2020).

Unfortunately, as technology is advancing at a rapid pace, cyber attacks are becoming more dangerous and harder to be detected. For instance, phishing scams were calculated to create the greatest number of compromised health records due to poor human security (Yao & Banfield, 2022). The 2015 phishing scheme against Anthem Inc. was known to affect 78,800,000 records and remains the most significant cybersecurity breach in the healthcare industry (Yeo & Banfield, 2022). Phishing scams typically occur through deceptive emails, messages, or websites to trick individuals into revealing sensitive information.

A lack of adequate security for EHR creates more than just financial implications. When privacy and confidentiality are not protected, there can be a significant loss of trust from the patients. Patient privacy and confidentiality are closely related to other ethical principles as well. A data breach would undermine patient autonomy by disregarding their wishes to whom they wish to disclose their health information with. Patients would be less likely to share their health information and the patient-provider relationship can be negatively impacted (Basil et al., 2022). Because EHR is widely implemented today, patients may even lose trust in the overall healthcare system and refuse to seek care in any setting including clinics and hospitals.

Healthcare professionals have the obligation of safeguarding the confidentiality of their patients' medical information. In today's day and age, technology has become a prominent means through which patient health information is discussed. Emailing, faxing, and text messaging are common methods of communication utilized by health professionals to interact with each other as well as their patients. Although digital platforms may provide benefits such as increased efficiency, reduced expenses, and improved documentation, there is a potential risk of unintentional violation of patient confidentiality and privacy through the use of these communication methods. A total of 1,485 breaches in healthcare occurred from January 2015 to December 2020, with 73.1 percent caused by unintentional factors (Yeo & Banfield, 2022).

When communicating a patient's medical information through fax or email, there is a chance that a patient unintentionally provides an incorrect email address or fax number. If the wrong information is given, there is a risk that their personal health records may be sent to and accessed by unknown individuals (Lustgarten et al., 2020). 55.5 percent of the data breach incidents between 2015 and 2020 were caused by mistakenly mailing or emailing personal health information (PHI) (Yeo & Banfield, 2022). Furthermore, when two patients share the same date of birth, there is the possibility of confusion, resulting in the accidental transmission of one patient's records to the other. Ultimately, there are many possibilities where confusion or private patient information can be shared to the wrong person.

Similar situations can arise with text messaging. Texting is widely used amongst health care professionals to relay information to each other and to their patients. Healthcare providers may discuss information with each other about a patient that they share, or patients may receive reminders from providers about their upcoming appointments. However, there is a chance phones may be stolen or hacked, and private patient information can end up in the hands of unwanted individuals. It is important to consider that, when communicating over the phone, one may not always know who is on the receiving end. There is a possibility that someone else could gain access to the patient or provider's phone and communicate on their behalf (Lustgarten et al., 2020). Additionally, it is possible that a patient's or provider's phone number has changed, causing messages being received to unintended recipients.

Electronic medical record is a database that is accessible to all if not most of the healthcare professionals working in a facility (Lustgarten et al., 2020). There may be instances where a provider inadvertently leaves their computer unattended. Another provider may come by to use it and unintentionally view another patient’s personal information. Although these are considered accidental violations of patient health information, it ultimately jeopardizes a patient’s privacy and confidentiality. An insider's carelessness, negligence, or apathy can be accounted for as high as 26 percent of all human factor breaches (Yeo & Banfield, 2022). The trust between patient and provider is what enables the providers to effectively and efficiently care for their patients. Unintentional breaches of confidentiality may instill distrust in a patient and cause them to feel hesitant to share personal information with their provider, ultimately compromising their care.

In addition to breaches in private patient information due to human error, EHR may violate patients’ privacy in many other ways. EHRs are accessed by multiple individuals within healthcare organizations, including doctors, nurses, administrative staff, and IT personnel. If these records were to be accessed without authorization, patients' privacy and confidentiality could be compromised. Each access point within the EHR system poses a potential vulnerability where unauthorized individuals could gain access to patient records (Seh, 2020).

Alternatively, employees or individuals with authorized access to EHRs can also lead to breaches in patient privacy. For example, Broward Health experienced a data breach that originated from a compromised third-party medical provider with authorized access to its patient database. This incident highlights the vulnerability of healthcare organizations to breaches through their external partners. In this case, the breach occurred when the third-party medical provider's system was compromised, potentially granting unauthorized individuals access to Broward Health's patient database. Such breaches can have severe implications for patient privacy and data security, as the compromised information could include sensitive medical records, personal identifiers, and other confidential data. The incident underscores the importance of thorough vetting and regular security assessments of third-party vendors to mitigate the risk of breaches and ensure the protection of patient information.

Healthcare organizations must prioritize strong cybersecurity measures not only within their own systems but also when engaging with external partners who have access to patient databases. There is speculation that the compromised device owned by Broward Health's third-party provider did not have Multi-Factor Authentication (MFA) implemented. This absence of MFA is believed to have contributed to the vulnerability and subsequent data breach. By not employing MFA, an additional layer of security that requires users to provide multiple forms of authentication, such as passwords and verification codes, unauthorized access to the compromised device and, consequently, the patient data it contained may have been facilitated (Alder, 2023). Insider breaches can be particularly challenging to detect and prevent, as those individuals often have legitimate access to patient records.

A potential solution to counteract data breaches and issues seen in the use of EHR is the use of Blockchain. Blockchain is a network where blocks are considered units of data contained from a collection of interactions that are secure and cannot be accessed by anyone other than authorized users. It uses a decentralized and distributed nature to prevent data breaches. The data within each block is encrypted, so if an attacker gains access to the blockchain, they would not be able to access charts without the proper decryption keys (Pilares, 2022). Prevention from an attacker accessing files can eliminate phishing scams from continuing. The network contains multiple copies across each block, ensuring that if an unauthorized user tries to manipulate or compromise anything, no patient information would get lost. Blockchain can help enable secure messaging and data sharing, reducing the risk of PHI being sent to the wrong recipients, and implementing a system where providers have unique identities linked to their access permissions.

Besides the system itself, institutions should implement a requirement for strong passwords and secure login procedures. Additionally, institutions should develop a comprehensive plan for the next steps to be taken in the case of a data breach, including notifying affected patients and relevant authorities. The human element plays a significant role in electronic health record breaches as well. It is necessary for healthcare professionals to raise awareness about data breaches and change online habits to mitigate breaches caused by carelessness and phishing. Employees and staff should receive adequate training on the best practices for data security and privacy, such as faculty training workshops that discuss phishing scams. Faculty members should know how to identify suspicious behavior, unfamiliar emails, and verify the sender's identity. Moreover, warnings and retraining can be given to those who are careless with patient data, such as leaving their logged-in accounts unattended or discussing patient information in public. Repeated warnings may warrant faculty meetings and potential penalties, such as suspension, and in some cases, termination of employment.

Overall, while the electronic health record presents a revolutionary change in how patient data is stored, concerns regarding patient privacy and confidentiality should not be overlooked. Patient confidentiality and trust in the healthcare system are at risk if EHRs are not properly secured. This necessitates a collective effort at both the systemic and individual levels, including design changes and increased awareness among healthcare professionals. Ultimately, this will lead to strengthened patient-provider relationships and an improved overall healthcare system.

Works Cited:

Alder, S. (2023, April 26). *Broward Health notifies over 1.3 million individuals about October 2021 data breach*. HIPAA Journal. https://www.hipaajournal.com/broward-health-notifies-over-1-3-million-individuals-about-october-2021-data-breach/

Basil, N. N., Ambe, S., Ekhator, C., &amp; Fonkem, E. (2022). Health Records Database and inherent security concerns: A review of the literature. *Cureus*. doi:10.7759/cureus.30168

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. (2020). Digital privacy in mental healthcare: Current issues and recommendations for technology use. *Current Opinion in Psychology, 36*, 25–31. https://doi.org/10.1016/j.copsyc.2020.03.012

Pilares, I. C. A., Azam, S., Akbulut, S., Jonkman, M., & Shanmugam, B. (2022). Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. *Sensors,* 22(11), 4032. https://doi.org/10.3390/s22114032

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020, May 13). Healthcare data breaches: Insights and implications. *Healthcare* (Basel, Switzerland). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

Yeo, L. H., M.S., & Banfield, J., PhD. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, 19(2), 1-10. https://shorturl.at/cdezF