Cecily Wang/Munoz-Pastrana

DS 380

Professor Wildman

24 April 2024

Word count: 2561

Safeguarding Privacy in Digital Healthcare: Ethical Imperatives and Policy Proposals

### Abstract

The ethical principles now at stake go far beyond what one imagined and are more long-lasting and damaging than a futile patient’s information on paper– what once used to be the analog past. Currently, healthcare organizations and corporations are facing a data security emergency as the revolution of digital platforms melds into healthcare systems and exposes sensitive patient information to more risks. After reviewing the United States of America v. Easy Healthcare Corporation and Howard University Hospital’s data breaches and violations of patient trust and privacy, the concluding efforts that must be realized to support and protect patients’ ethical rights to autonomy, justice, and maleficence are to be strengthened with stricter and more technologically secure policy add-ons via mandated encryption and routine data analysis into the existing Health Breach Notification Rule and ONC’s Cures Act Final Rule.

### Problem Background

Originally, the Health Insurance Portability and Accountability Act (HIPAA) was created in 1996 as a national standard to protect patient information, specifically known as protected health information (PHI) which are unique identifiers such as name, social security, address, etc. (Hussain et al. 2020). However, the transition to digital healthcare has officially outpaced the development of corresponding ethical and privacy guidelines that have been followed in the analog past (Rezaei et al. 2024). Before the current "experience age," characterized by mobile screens and IoT (internet of things), past approaches to patient data privacy like HIPAA were enough to protect sensitive patient information; however, due to technological advancements like AI and the expansion of electronic health records (EHRs), it now barely covers the surface in addressing the complex privacy concerns that arise in today's digital health landscape (Ozair et al. 2015). This became evident during the COVID-19 pandemic, which saw an increase in digital healthcare such as telehealth and therapy apps (U.S. Department of Health and Human Services 2023).

In the discussion of the ethics that go along with the expansion of digital healthcare, it is important to highlight the multiple stakeholders involved in the dilemma. At the core, patients face potential invasions of privacy and autonomy as their sensitive health data is passed across digital platforms beyond the protective scope of HIPAA. Healthcare providers are also having to balance the learning curve of technology against the ethical obligation to protect patient confidentiality. Meanwhile, digital health technology firms need to navigate the area of legal compliance and innovation to figure out how to integrate an honest and equitable algorithmic system into healthcare (Zarif 2021). This shows the need for strengthening existing regulatory measures so that these stakeholders are more protected and can better understand their place and rights in the new age of healthcare.

### Problem Analysis

The existing clinical ethical principles that face significant threats from inadequate digital privacy protections are patient autonomy, justice, and nonmaleficence–the commitment to not cause harm (Rezaei et al. 2024). The biggest concern that endangers these principles revolves around the risk to patient privacy posed by mobile and portable digital healthcare technologies. For example, wearable devices and mobile applications that collect health data tend to fall outside the protective sphere of existing federal regulations like HIPAA (Theodos and Sittig 2021).

The extent to which HIPAA can reliably protect digital patient health information is not the only concern when it comes to data privacy in healthcare. A higher-level view that incorporates this concern is the increased prevalence of data breaches in the healthcare sector (The HIPAA Journal 2024). As healthcare systems have digitally transformed—adopting EHRs, the Internet of Medical Things (IoMT), and cloud services—their vulnerability to data breaches has significantly increased (Hussain et al. 2020). A report by IBM Security states that the average cost of a data breach in healthcare is currently the highest of any industry, at approximately $10.93 million per incident which goes to show the need for better cyber security measures (IBM Security, 2023). While incorporating technology can improve patient care and operational efficiency, it can also lead to corruption or destroy personal health information during breaches. This issue uncovers the tunnel vision augmented by dangling new and advanced technology in front of healthcare organizations and companies which creates blindspots when it comes to protecting sensitive patient data. Studies have shown that hacking and IT incidents have become the leading cause of these data breaches, with unauthorized internal disclosures also becoming contributors to the risk profile (Smith et al., 2020). Additionally, the financial implications of these data breaches add another level to the challenge at hand since these breaches can cost the healthcare sector more than any other industry—the Ponemon Institute, a research center dedicated to technological privacy, has described the severe financial damage alongside operational and reputational hits that follow breaches (Jones et al., 2020). Furthermore, the delayed detection and notification of breaches complicated timely responses and can increase the risks associated with the exposure of sensitive information (Smith et al., 2020). This shows a need for improved security protocols and systems within healthcare organizations to safeguard against such vulnerabilities.

### Ethics

The ethical issue of the “invisibility of data collection”, is that patients are kept in the dark about how their data is tracked and utilized (Grande et al. 2020) which then leads to the question of what companies and healthcare organizations do with such sensitive data that is not encompassed by HIPAA regulations, and the commercial value attached to such data making it a sought-after digital asset to private companies who want to market it for profit (Kwon et al. 2015). This along with the quick adoption of AI into healthcare technologies can also lead to the issue of data inaccuracy because of how data can be flawed and misinterpreted which leads to inaccurate health predictions and thus, transcend into physical harm to an individual. The implications of not just HIPAA violations in the digital wild, but the immortality of such information that is commercialized and abused because of the blurred boundaries between digital information and the healthcare system all come together to call for a reevaluation of HIPAA and create regulatory measures needed to address the challenges posed by the digital health footprint (Grande et al. 2020).

As previously referred, one of the most important corresponding ethical issues is the impact on patient autonomy which has been long-standing in clinical ethics. For example, when EHRs are shared or linked without patient knowledge, autonomy becomes automatically compromised as patients lose control over their medical information (Williams and Mostashari 2015). Further complicating this issue is the possibility of patients withholding information from their healthcare providers due to fears of data leaks or security breaches, which can in turn negatively impact the quality and individuality of care they receive. The complexity of managing digital systems also places a burden on healthcare providers because it can push them into routines that may reduce the time available for patient interaction and thus weaken the quality of care.

### Real World Implications

Howard University Hospital experienced issues when its patient data was not encrypted. This led to unauthorized access when passwords were compromised (Williams and Mostashari, 2015). Not only is this a violation of patient rights, but it also simultaneously permits the healthcare system, as an institution, to lose credibility when it comes to caring for its patients. These institutions are here to improve quality of life, act as an educational space for future nurses and doctors, and ultimately, save lives. But when the sheer reputation of a hospital loses credibility and security, the people who lose the most in this scenario are the patients.

A separate case relating to the violation of privacy recently occurred last year. On June 2023, the United States of America filed a lawsuit against Easy Healthcare Corporation accusing them of sharing users’ private health data from their fertility app, Premom, with third parties without user consent and failing to notify their users about the unauthorized use of their PIH (Federal Trade Commission 2023). Notably, Premom also encouraged its users to link their Apple Health to the app. According to a press release, Premom disclosed identifiable health information to marketing firm AppsFlyer and Google. They also failed to encrypt adequately the data it shared with third parties, including those in China, subjecting this data to potential interception or seizure, and did not limit how third parties could use the data. This legal action demonstrates the ethical imperative to safeguard patient data amidst the complexities of digital healthcare. The court order imposed a comprehensive privacy and information security program, emphasizing not only the prevention of unauthorized disclosure of health information but also the accurate representation of privacy practices to consumers. As aforementioned, Apple’s Health Records app collects users’ everyday information along with lab results and medications and can be linked to other health-related apps (NYT 2021). At first glance, this may seem like a helpful cross-section between technology and health for the user, however, companies who provide these products are aware of the marketability and lack of federal regulation of this sensitive data and are racing to use it as seen with the Premom case study (Singer 2019).

Applications like Premom are just scratching the surface when it comes to health data. It is equally important to look at the base of electronic health records (EHR). The largest EHR vendor, Epic Systems Corporation, which services around 38% of U.S. hospital installations, emphasizes HIPAA compliance and has allegedly integrated many safety features into its platforms (Definitive Healthcare 2024). Except, after looking through the Epic Systems website, there appears to be an absence of explicit information on the broader ethical implications of digital health technologies on their platforms, such as how these technologies impact patient autonomy and privacy (EHR in Practice 2024). A piece of their content that sparked a red flag for digital ethical concerns and data breaches was how they described their system as a “Digital Front Door: Patients drive their healthcare by connecting…all online. No accounts of logins required” (Epic Systems Corporation, n.d.). This makes it seem like the biggest EHR distributor either overlooks or brushes off the importance of digital privacy, especially since they have been increasingly marketing new AI into their digital healthcare products (Kwon et al. 2015).

Overall, the regulatory gap shown through the analysis of various cases where PHI is misused and user rights are violated, and how EHRs are distributed, threatens the ethical principle of autonomy, as people have lost the ability to control the whereabouts of their information. The thinning line in health data privacy due to greater advancements and integration of digital technology in healthcare highlights the need for more integrated policies and regulations for current and future technologies that will become a part of the healthcare system so that the fundamental ethical principles of clinical practice are preserved. Because of this, it is clear that effective security programs should not only focus on preventing breaches but also function as part of broader market-based brand-building initiatives. This approach emphasizes the importance of viewing data security not only as a technical issue but as a central part of healthcare strategy and patient trust.

### Policy Proposal

Two recent policies that have addressed the issues this report has analyzed are ONC’s Cures Act Final Rule (Health IT 2024) and the Health Breach Notification Rule (FTC). The ONC Act (2020) emphasizes secure access to health information through the enforcement of standardized APIs and greater patient and provider access to EHI (ONC, 2024). Albeit its careful address to strengthen health information privacy, some additions could be made to reinforce the effectiveness of these measures including regular security audits. Introducing regular audits for healthcare providers using digital technologies to ensure compliance with encryption and data protection standards would add a secondary protective layer to the policy. The second act is the Health Breach Notification Rule which “requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information” (FTC 2022). This act is a huge step in strengthening patient autonomy by supporting their right to privacy at the federal level.

After examining current acts in place, the following are proposed policy add-ons that should be enforced at the federal level to initiate a good descent towards preserving patient autonomy, justice, and maleficence:

1. Standardize mandatory encryption to further protect patient data.
2. Incorporate data analytics by using machine learning algorithms to analyze patterns that highlight data breach risks.

Just by implementing these measures, one can confidently say that these policies will significantly enhance the security of digital health technologies. A study by the Cybersecurity and Infrastructure Security Agency (2023) found that encryption reduces the risk of data breaches by up to 60%, mitigating potential harm and financial losses (McLeod et al. 2018). Also, predictive analytics can identify vulnerabilities 70% faster than traditional methods which decreases the likelihood of successful data breaches (Jones et al., 2024). Research published by the Ponemon Institute in their 2021 Cost of Data Breach Report indicates that organizations with fully encrypted data systems experienced 50% fewer breaches compared to those without encryption. This emphasizes encryption as a critical component of data security frameworks that significantly diminish the risk of unauthorized data exposure (Ponemon Institute, 2021). According to the same Ponemon report, organizations that leveraged AI and analytics for threat detection and response shortened the time to identify and contain a breach by over 27%. This accelerated response time is crucial in minimizing the impact and cost of breaches (Ponemon Institute, 2021)

### Anticipated Critiques

The Health Breach Notification Rule requires only HIPAA-covered organizations to comply (FTC 2022). This limitation poses risks as private businesses that are not primary healthcare providers or entities may evade HIPAA regulations. To address this, it is essential to mandate that any entity handling Protected Health Information (PHI) adhere to the Breach Rule. While mandatory encryption enhances data security, it also complicates data sharing for legitimate research, potentially hindering medical progress. There are concerns that enforcing these policy add-ons may be financially and educationally burdensome due to the rapid advancement of technology. Despite the effort and investment required initially, the long-term benefits, including the prevention of costly data breaches and strengthened patient trust, justify these initial challenges.

To alleviate these concerns, the policy could suggest phased implementation and offer financial incentives for compliance, such as tax breaks or federal grants, to assist healthcare providers in upgrading their security systems. Additionally, there are concerns about the complexity of these technologies and their impact on the daily workflow of healthcare professionals. Nevertheless, as technology and digital security become increasingly crucial to society, it is important to begin training and supporting healthcare providers early in their careers. Continuous education and training programs are vital for equipping them to ethically use these technologies and develop critical thinking for future technological advancements. Another critique is the steep costs associated with implementing such policies. Integrating digital healthcare technologies requires initial investments and ongoing maintenance costs, which could increase healthcare expenses for minority populations and exacerbate health disparities (Williams and Mostashari, 2015). To address these ethical concerns, healthcare organizations could consider integrating technology ethics committees, similar to the clinical ethics committees (Cossit 2020). These committees would uphold principles of transparency, accountability, and inclusivity in the deployment of new technologies (Hassan and Schuklenk, 2021). These bodies could derive technology ethics from the IEEE Code of Ethics and fine-tune them to cater to the healthcare sector while still staying generalizable enough so that they remain just as relevant in the future.

### Conclusion

In conclusion, the challenges seen by the digitalization of healthcare systems need immediate and decisive actions to protect the foundational ethical rights of autonomy, justice, and nonmaleficence. As seen by recent high-profile breaches and ongoing vulnerabilities that were analyzed, it is clear that just simple compliance with existing standards is insufficient due to the workarounds that private corporations and software distributors are able to do to get past full HIPAA compliance. The integration of stricter encryption protocols and data analytics into existing healthcare frameworks is is necessary, especially as society runs towards greater incorporation of AI and technology into everyday systems. This step will help renew an environment of trust and security that supports and actively protects patient privacy. In now and the near future, it is crucial for all involved—from tech developers to government regulators—to commit to these measures and make sure that the policies involved are versatile and applicable to many new technologies to come. In the end, being able to do this will influence our collective capacity to manage and mitigate the risks inherent in the digital age of healthcare.

Works Cited

Cossitt, Alan. “Why Health Care Organizations Need Technology Ethics Committees.” *The Hastings Center*, 5 February 2020, https://www.thehastingscenter.org/why-health-care-organizations-need-technology-ethics-committees/. Accessed 23 April 2024.

Definitive Healthcare. “Top EHR Systems by Market Share | U.S. Inpatient EHR Vendors.” *Definitive Healthcare*, https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems. Accessed 23 April 2024.

EHR in Practice. “Epic EHR Software - Pricing, Features, Demo & Comparison.” *EHR in Practice*, https://www.ehrinpractice.com/epic-ehr-software-profile-119.html. Accessed 23 April 2024.

Epic Systems. “Artificial Intelligence | Epic.” *Epic Systems*, https://www.epic.com/software/ai/. Accessed 23 April 2024.

Federal Trade Commission. “Complying with FTC's Health Breach Notification Rule.” *Federal Trade Commission*, 21 January 2022, https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0. Accessed 24 April 2024.

Federal Trade Commission. “Health Breach Notification Rule.” *Federal Trade Commission*, https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule. Accessed 24 April 2024.

Federal Trade Commisson. “Easy Healthcare Corporation, U.S. v.” *Federal Trade Commission*, 2023, https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v. Accessed 24 April 2024.

Grande, David. “Health Policy and Privacy Challenges Associated With Digital Technology.” *NCBI*, 9 July 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7348687/. Accessed 23 April 2024.

“Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC.” *Centers for Disease Control and Prevention*, https://www.cdc.gov/phlp/publications/topic/hipaa.html. Accessed 24 April 2024.

HealthIT. “Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule | HealthIT.gov.” *Office of the National Coordinator for Health Information Technology*, 7 March 2024, https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program. Accessed 23 April 2024.

Hussain, Adil, et al. “Healthcare | Free Full-Text | Healthcare Data Breaches: Insights and Implications.” *MDPI*, 13 May 2020, https://www.mdpi.com/2227-9032/8/2/133. Accessed 23 April 2024.

IBM Security. “Cost of a data breach 2023.” *IBM*, 2023, https://www.ibm.com/reports/data-breach. Accessed 24 April 2024.

Kwon, Juhee, and Eric Johnson. “The Market Effect of Healthcare Security: Do Patients Care About Data Breaches?” *WEIS*, 2015, https://econinfosec.org/archive/weis2015/papers/WEIS\_2015\_kwon.pdf. Accessed 23 April 2024.

McLeod, Alexander, and Diane Dolezel. “Cyber-analytics: Modeling factors associated with healthcare data breaches.” *Science Direct*, April 2018, https://www.sciencedirect.com/science/article/abs/pii/S0167923618300368?casa\_token=6W8kda5diOgAAAAA:UQjtD7vmxqzVkX5XJQ7AWbK8m3CBTlqZ0zsaAkeVe5Ydy8rM7fuV4YFRGa5XOyqLh6drxNNQ. Accessed 23 April 2024.

Ozair, Fouzia, et al. “Ethical issues in electronic health records: A general overview.” *NCBI*, April 2015, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4394583/. Accessed 23 April 2024.

Ponemon Institute. “Ponemon Institute.” *Ponemon Institute: Home*, https://www.ponemon.org/. Accessed 24 April 2024.

Rezaei, Mojtaba, et al. “Key indicators of ethical challenges in digital healthcare: A combined Delphi exploration and confirmative factor analysis approach with evidence from Khorasan province in Iran.” *Science Direct*, 5 March 2024, https://www.sciencedirect.com/science/article/abs/pii/S0040162521001566. Accessed 23 April 2024.

Singer, Natasha. “When Apps Get Your Medical Data, Your Privacy May Go With It (Published 2019).” *The New York Times*, 3 September 2019, https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html. Accessed 23 April 2024.

Theodos, Kim, and Scott Sittig. “Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply.” *NCBI*, 7 December 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7883355/. Accessed 23 April 2024.

U.S. Department of Health and Human Services. “HIPAA and Telehealth.” *HHS.gov*, 18 October 2023, https://www.hhs.gov/hipaa/for-professionals/special-topics/telehealth/index.html. Accessed 23 April 2024.

Zarif, Azmaeen. “The ethical challenges facing the widespread adoption of digital healthcare technology.” *NCBI*, 29 October 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7612237/. Accessed 23 April 2024.

I think this may be irrelevant to add on here, but I put it just in case since the three sentences it highlighted that made it 17% were essentially bullet points as noted below:

