Journal of Health, Medicine and Nursing
ISSN 2422-8419 An International Peer-reviewed Journal
Vol.112, 2023

Patient Information Privacy and Security Policy: A Brief Analysis

Victoria Abimbola Akintade
American National University, 4205 Dixie Highway, Loisville, KY 40216
akintadev@students.an.edu

Abstract
This review provides a summary of the patient information privacy and security policy. Covered entities are entrusted with the responsibility to safeguard the integrity of patient information, with a particular emphasis on protecting Protected Health Information (PHI). HIPAA's rules play a crucial role in ensuring the protection of PHI through strict enforcement. The review also highlights certain limitations to the HIPAA rules. Furthermore, an assessment of the patient information privacy and security policy is conducted using the "Five E Model" of policy analysis.
Keywords: policy, PHI, HIPAA, HITECH, privacy rule, security rule
DOI: 10.7176/JHMN/112-03
Publication date: December 31st 2023

1. Introduction

When a patient walks into a healthcare organization, certain information is collected as well as medical history and these need to be kept safe and secure. What is HIPAA? HIPAA is Health Insurance Portability and Accountability Act and it was created in August 21, 1996, to help keep protected health information confidential, authentic, safe, private, and secure (OCR, 2022). HIPAA was also established to ensure anyone who breaches the terms of patient's information privacy and security faces the full extent of its law (Edemekong, Annamaraju, & Haydel, 2022). Since HIPAA has been created, in addition to the advancement of technology, modifications and adjustments have been made to this policy to ensure more strictness and adherence to it. Patient information privacy and security policy via HIPAA guides healthcare professionals and organizations involved in the management of patient information (Solove, 2013; Moore & Frye, 2019).

2. HIPAA's Rules

Healthcare generates large amount of data in the form of patient information, however, if not adequately mined, secured, and protected, some of these data can fall into the wrong hands. Part of the data generated from healthcare is Protected Health Information. Protected Health Information (PHI) is the information that can identify an individual or used to identify an individual, such information include medical record number, patient's medical history, social security number, name, phone number, address, date of birth, patient's medical charts among other (Brown, 2022; Alder, 2023). PHI is also regarded as part of individual's health information. PHI can be in paper (hard) copy or electronic format also knowns as e-PHI. After its creation, HIPAA provides certain regulatory guidelines to the "Secretary of the US Department of Health and Human Services" on how to protect and keep electronic protected health information (e-PHI) secure (Nass, Levit & Gostin, 2009). The "Department of Health and Human Services" then established the HIPAA security rule and privacy rule. In the HIPAA security rule, it is paramount that everyone involved in handling or transacting e-PHI otherwise known as "covered entities", provide adequate security physically, technically, and electronically, to protect the privacy, confidentiality, and authenticity of the e-PHI (Nass, Levit & Gostin, 2009). Under the security rule, in using heath information technology such as the electronic health record to access electronic protected health information, certain guidelines were provided to healthcare professionals and organizations, to further enhance its security, prevent data breach and ensure the integrity of patient's data is protected (Edemekong, Annamaraju, & Haydel., 2022). Technology, through the use of health information technology seemed to enhance caregiving, promote better patient outcomes in healthcare organizations, and the purpose of the security rule was to ensure technology does not predispose e-PHI to attack, fraud, and other breaches, hence the "technical safeguards" provided by HIPAA in its Titles (Sims et al., 2019; Edemekong, Annamaraju, & Haydel 2022; OCR, 2022). The privacy rule imposes stringent measures on the sharing or disclosure of PHI; without permission from a patient, his/her PHI must not be disclosed to anyone; covered entities handling PHI were also required by HIPAA privacy rule to provide full protection on the PHI in their possession. The standards established in the privacy rule gives only the patient the authority to disclose their PHI to another party (Hass, Levit & Gostin, 2009). In the past, before HIPAA of 1996 was established, with regards to the privacy and protection of health information, only the federal government and its agencies had the sole responsibility of protecting health information and keeping it private and secure. This was the policy under the privacy act of 1974 (Theodos & Sittig, 2020). The federal government also had some guidelines to follow to ensure data's data are protected. The medical team and other workers in the healthcare organization were not under any law or mandated requirements

to keep health information private and secure but ethically they were mandated to do so (Solove, 2006).

3. HITECH and HIPAA

In addition to HIPAA's policy on keeping health information private and secure, the digital age also came around and the invention of health information technology brought a new dynamic to healthcare like never before. Examples of health information technology are Computerized Physician Order Entry, The Electronic Health Record, and Decision Support System (AHRQ, 2019). The Health Information Technology for Economic and Clinical Health (HITECH) Act was passed in 2009 to build up on the policy of HIPAA to further ensures the security of electronic PHI. While using health information technology, HITECH Act and HIPAA work together to ensure data breaches are prevented, protocols are followed in the event of a breach, the appropriate quarters are notified, and investigations are carried out to know how to prevent similar breach in the future (Burde, 2011). Also, HITECH allowed HIPAA to make some adjustments in their privacy policy and it provided reimbursement in Medicare and Medicaid to healthcare organizations that provided meaningful use of the electronic health records (Jha, 2010). The purpose of providing reimbursement for healthcare that provided meaningful use of the electronic health records is to provide incentive and encourage the use of the health information technology (Jha, 2010; Slight et al., 2015). Meaningful use of the electronic health records includes patients accessing their own health records via the creation of patients' portal, this in part promotes the idea that patients are part of the medical team, are actively involved in their own healthcare and should be encouraged to partake in decisions concerning their own health (Glenn & Monteith, 2014). Sequel to this and coupled with the wide acceptance of health information technology, certain standards and guidelines that must be followed to prevent breaches in patient's data (information) (Kruse, Bolton, & Freriks 2015; Rosenbloom, 2019). For healthcare organizations and professionals to qualify for reimbursement from HITECH, HITECH has specifically requested that only electronic health records that are "certified and qualified" are used in healthcare organizations (Burde, 2011; HITECH Act, 2009). This means that the electronic health record must have gone through HITECH quality control and the appropriate evaluation to confirm it is fit to use and PHI are safe and protected on it (HITECH, 2009).

4. Covered Entities

Individuals who are covered under HIPAA policy include all healthcare professionals, medical care team, health plans, associates and everyone who works with a healthcare organization and handles patients' information electronically within the organization or across other organizations (OCR, 2016; Rosenbloom, 2019). These people are also called "covered entities" and they would be punished if they violate the privacy and security policy outlined by HIPAA (Rosenbloom, 2019). For strict adherence to the regulation of HIPAA concerning PHI, the federal government has tasked the Department of Health and Human services, specifically the Office for the Civil Rights (OCR) with the responsibility to enforce HIPAA policy, conduct investigations, ensure violator of HIPAA policy are brought to books and upholding the guidelines of HIPAA (OCR, 2016).

5. Limitations

Some limitations have been discovered about HIPAA's policy in protecting patients' information. For instance, it has been found that HIPAA policy only applies to PHI obtained from a healthcare setting, while information obtained from settings aside healthcare such as public/social media platforms or blogs are not protected even if it includes PHI (Cohen & Mello, 2018); this is an aspect HIPAA might want to re-evaluate critically because of the amount of data being generated. Organizations and companies aside healthcare and covered entities are grouped as "non-covered entities" and as such, HIPAA policy does not apply to them, neither does HIPAA provides them with some kind of regulations of their activities (Kim, Lee & Choe, 2019). It is also worthy to note that these non-covered entities generate and manage PHI (Kim, Lee & Choe, 2019). HIPAA policy does not cover law enforcement agents. These agents are not excluded from accessing PHI, in healthcare organizations without a warrant, and there is no regulation or policy in place to serve as guidelines to these agents in accessing PH, this further expose PHI in an unsecured manner (Solove, 2022).

6. "Five E Model"

The purpose of policy analysis is to review the current policy with the information at hand, extract new information and re-evaluate the policy for possible changes and amendments which will address the issues that have been raised (Porche, 2019). In addition, policy analysis addresses issues of concerns from the policy and proffers ways to improve on the existing policy (Porche, 2019). The privacy and security of PHI falls under the meso-policy level analysis because it will include the healthcare organizations, the healthcare professionals and all individuals involved in the policy making and implementation (Porche, 2019). Under the meso-level of policy analysis, using the "Five E Model" to analyze the health information security and privacy policy, the components of the policy to be evaluated are:

A. “Effectiveness”: This is the success rate of health information privacy and security policy over the years since its establishment.
B. “Efficiency”: How competent is the policy in ensuring PHI are always secure and protected.
C. “Ethical considerations”: keeping PHI private and secure is ethically right and one of the responsibilities of healthcare professionals (Tariq & Hackert, 2023).
D. “Evaluations of alternative policy options”: in case of using a patient’s information for teaching and medical research purposes, de-identification can be considered which allows some information that can identify the patients to be removed from the patient information (OCR, 2022).
E. “Establishment of positive recommendations for change and what is feasible to be established”: because of technological advancement and the widely use of health information technology by healthcare professionals, recommendations and evaluations on patient information privacy and security policy will generate better ideas to further support the policy and improve patient’s safety (Kirst-Ashman, 2016).

7. Conclusion

In sum, in this technological age, patient information privacy and security policy through HIPAA, in addition to HITECH, has made it possible for everyone to safely access their medial information through the patient portal with minimal risks. Further, HIPAA has one of the most compelling healthcare policies that ensures adequate privacy and security for patients, it also grant patients the authority over their medical records and full accessiblity whenever they want it. However, HIPAA might not keep up with the technological innovation that the future may experience and that could pose some threats to the big data being generated in healthcare and across technological devices and also to patient satisfaction (Lee et al., 2016).

References

Agency for Healthcare Research and Quality (AHRQ), (2019). Health Information Technology Integration. Content last reviewed August 2019. Agency for Healthcare Research and Quality, Rockville, MD. https://www.ahrq.gov/ncepcr/tools/health-it/index.html

Alder, S. (2023). What is Protected Health Information? *The HIPAA Journal*. Copyright 2014-2023. The HIPAA Journal. https://www.hipaajournal.com/what-is-protected-health-information/

Brown, J. T. (2022). “*Dynamic De-identification Policies for Pandemic Data Sharing”,* Doctoral dissertation, Vanderbilt University.

Burde H. (2011). “The HITECH Act: An overview”, *American Medical Association Journal of Ethics*. Copyright 2023. The American Medical Association. https://journalofethics.ama-assn.org/article/hitech-act-overview/2011-03

Cohen, I.G. & Mello, M.M. (2018). “HIPAA and Protecting Health Information in the 21st Century,. *JAMA.* 320(3):231–232. doi:10.1001/jama.2018.5630

Edemekong, P.F., Annamaraju, P. & Haydel, M.J (2022). “Health Insurance Portability and Accountability Act”, [Updated 2022 Feb 3]. In: StatPearls [Internet]. Treasure Island (FL): *StatPearls Publishing*. 2023 Jan- . Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/

Glenn, T., & Monteith, S. (2014). “Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections”, *Curr Psychiatry Rep.* 16((11)):494.

HITECH Act, (2009), 42 USC sec 139w-4(0)(2) part 2, subtitle C, sec 13301, subtitle B, sec 3014: Competitive Grants to States and Indian Tribes for the Development of Loan Programs to Facilitate the Widespread Adoption of Certified EHR Technology.

Jha, A.K (2010). “Meaningful Use of Electronic Health Records: The Road Ahead”, *JAMA.* 304(15):1709–10.

Kim, Y., Lee, B., & Choe, E.K (2019). “Investigating Data Accessibility of Personal Health Apps”, *J Am Med Inform Assoc*. 265: 412–9.

Kirst-Ashman, K. (2016). “Introduction to social work & social welfare: Critical thinking perspectives”, Empowerment series. Independence, KY: Cengage Learning.

Kruse, C.S., Bolton, K & Freriks, G. (2015). “The Effect of Patient Portals on Quality Outcomes and Its Implications to Meaningful Use: A Systematic Review”, *Journal of Medical Internet Research.* 17((2)): e44.

Lee, B.S. et al., (2016). “Transparent Electronic Health Records and Lagging Laws”, *Ann Intern Med*. 1653: 219.

Moore, W., & Frye, S. (2019). “Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules”, *Journal of Nuclear Medicine Technology*. 47 (4) 269-272

Nass, S.J., Levit, L.A. & Gostin L.O. (2009). *“The HIPAA Privacy Rule. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research”,* Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information. Washington (DC): National Academies Press (US); *2009. 4, HIPAA, the Privacy Rule, and Its Application to Health Research. Available from: https://www.ncbi.nlm.nih.gov/books/NBK9573/*

Office for Civil Rights (OCR), (2016).“Individuals’ Right under HIPAA to Access their Health Information”, Health Information Privacy Division. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

Office for Civil Rights (OCR) (2022). *“Health Information Privacy: Summary of the HIPAA Security Rule”, US Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html*

Office for Civil Rights, (2022). *“Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule”, US Department of Health and human services. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale*

Porche, D. J. (2019). *“Health Policy: Application for Nurses and Other Healthcare Professionals*”, *[VitalSource Bookshelf]. Retrieved fro*m https://online.vitalsource.com/#/books/9781284157512/

Rosenbloom, S. T., et al., (2019). “Updating HIPAA for the Electronic Medical Record Era”, *Journal of the American Medical Informatics Association: JAMIA*, *26*(10), 1115–1119.

Sims, M.H. et al., (2019). “Legal and Ethical Issues Surrounding the Use of Crowdsourcing Among Healthcare Providers” *Health Informatics J*. 25(4):1618-1630

Slight, S.P. et al., (2015). “Meaningful Use of Electronic Health Records: Experiences From the Field and Future Opportunities”, *JMIR Med Inform.* 18;3(3).

Solove, D.J. (2013). “HIPAA Turns 10: Analyzing the Past, Present, and Future Impact”, 84 Journal of AHIMA. *Research Paper No. 75. Pg 21-28. Available at SSRN: https://ssrn.com/abstract=2245022*

Solove, D.J. (2022). “A Brief History of Information Privacy Law” *GW Law Scholarly.*

Tariq, R.A. & Hackert, P.B. (2023). “Patient Confidentiality”, In: StatPearls [Internet]. Treasure Island (FL): *StatPearls Publishing;* Available from: https://www.ncbi.nlm.nih.gov/books/NBK519540/

Theodos, K. & Sittig, S. (2020). “Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply”, *Perspectives in Health Information Management*, *18*(Winter), 1l.