J of Nuclear Medicine Technology, first published online June 10, 2019 as doi:10.2967/jnmt.119.227819

A Review of the HIPAA, Part 1: History, PHI, and Privacy and Security Rules

Wilnellys Moore, MS, RT (R)(N) (MR)(AART), CNMT, Sarah Frye, MBA, CNMT, PET, CCRP

Doisy College of Health Sciences, Saint Louis University

For correspondence contact: Sarah Frye, Allied Health Building, 3437 Caroline St 3021, Saint Louis, MO 63104 USA

Email: sarah.frye@health.slu.edu

Phone: 314-977-9038

Word Count: 2631

Key words: HIPAA, Security Law, Privacy Law, Patient Rights

Abstract

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has made an impact on the operation of healthcare organizations. HIPAA includes five titles and these regulations are complex. Many are familiar with the HIPAA aspects that address the protection of the privacy and security of patients' medical records. There are new rules to HIPAA that address the implementation of electronic medical records. HIPAA provides rules for protected health information (PHI) and what should be protected and secured. The privacy rule regulates the use and disclosure of PHI and sets standards that an entity working with health data must follow to protect patients' private medical information. The HIPAA security rule complements the privacy rule and requires entities to implement physical, technical, and administrative safeguards to protect the privacy of PHI. This article—part 1 of a 2-part series—is a refresher on the HIPAA, its history, its rules, its implications, and the role imaging professionals play.

Introduction

Privacy and security laws are continually evolving to adjust to new challenges, new technologies, and the novel threats in the digital era. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 laws are more strictly enforced than ever before. Although periodic HIPAA training is mandatory for employees whom have access to, or manage patient data, HIPAA rule violations continue to occur (1,2). Recent updates and modifications to HIPAA have strengthened its standards and broadened the inclusion of who must comply with HIPAA. Fortified by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and the Omnibus Rule of 2013, HIPAA emphasizes compliance with increased auditing, augmented penalties, and thorough enforcement of the laws. Staying abreast of these changes and complying with these laws is imperative to protect health information confidentiality, privacy, and security. This article—part 1 of a 2-part series—is a refresher on the HIPAA, its rules, and its

implications. Part 2 of the series continues the discussion of HIPAA with a specific focus on its limitations, privacy and security officers, enforcement, violations, and the role of imaging technologists.

History

In 1996, the federal government passed a law that created national standards to protect the confidentiality of medical records. HIPAA can be found at Title 45 of the Code of Federal Regulations (CFR) Parts 160-164. The law was passed by Congress and signed by President William Jefferson "Bill" Clinton on August 21st, 1996 with the primary intent of assuring portability and continuity of health insurance coverage for millions of Americans; however, HIPAA entails more than portability, privacy, and security. HIPAA consists of 5 sections called "titles" in 45CFR164 and the regulations are complex and voluminous.

The 5 HIPAA Titles

- Title I: Provides the ability to transfer and continue healthcare coverage for American workers and their families that change or lose their jobs. It also limits the ability to deny health plan coverage due to pre-existing conditions (3).
- Title II: This title's Administrative Simplification provision requires that the United States Department of Health and Human Services (DHHS) establishes national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data and helps prevent health care fraud and abuse (3).
- Title III: Provides changes to health insurance laws and deductions for medical insurance. It also provides guidelines for pre-tax medical spending accounts (3).
- Title IV: Specifies conditions for group health plans regarding coverage of persons with pre-existing conditions and modifies the continuation of coverage requirements (3).

- Title V: Includes provisions related to company-owned life insurance and to the treatment of individuals without United States citizenship (3).

Healthcare professionals are most familiar with the HIPAA title that addresses the protection of the privacy and security of patients' medical records. After all, this is the part of HIPAA on which healthcare professionals receive periodic training. Before the introduction of HIPAA, multiple federal rules and regulations addressed privacy in various forms, but these rules and regulations lacked clarity and consistency (1). State and federal requirements differed, and there was confusion as to which regulations were applicable in which situations. Congress recognized the need on a national level for privacy and security standards as the use of electronic technology surged. Patients' health data needed to be readily accessible to doctors, nurses, technicians, pharmacies, billing and coding companies, and administrative staff. There was a growing need to modernize the flow of medical data to facilitate and expedite the access to health records (1).

The responsibility for implementing the regulations that would help maintain the safety of health records was deferred to the DHHS which established a schedule for the implementation of these new rules (4). These rules and standards apply to covered entities, which DHHS defines as healthcare providers, health plans, and healthcare clearinghouses and business associates (5). Creating and enacting these general rules took time because private and government systems needed to be upgraded, policies and procedures had to be reviewed for adequacy and applicability, and personnel needed to be trained. Initially, HIPAA was met with skepticism and confusion (1,6). Law makers and healthcare professionals wondered about its cost-effectiveness, how meaningful the protections would be, and how these rules could interfere with efficient patient care (6).

New Rules

While HIPAA was signed into law in 1996, it was not until 2003 that it was fully implemented. By that time, the need for enforcement standards and additional rules addressing specific privacy issues had been identified (4). HIPAA grew in prominence after the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009 (7). The goal of the HITECH Act was to support the nationwide implementation of Electronic Health Records (EHRs) to provide integrated medical data and information to providers as well as patients. HITECH offered incentive programs which helped to encourage the adoption of EHRs by hospitals and other providers, while also penalizing those who were eligible for the incentives but chose not to implement them (7,8). Additionally, HITECH significantly increased monetary penalties for HIPAA violations (1).

The surge in medical records collected, archived, and transmitted electronically led to unprecedented challenges regarding patient privacy. As a response to these challenges, DHHS developed changes to HIPAA that addressed subsequent standards and rules. The Omnibus Final Rule was enacted on January 25, 2013 and expanded covered entities to include business associates, which consist of auditors, consultants, Information Technology companies, and others with whom facilities have agreements involving the use of protected health information (PHI) (4,5). HIPAA requires that updated business associate agreements (BAAs) be executed and maintained between the practice and all business associates (4). A BAA is a contract that defines how the associates adhere to HIPAA along with the responsibilities and risks they accept. Due to the Omnibus rules, both covered entities and business associates are subject to the full civil and criminal penalties for violations of the laws (1,4). The Omnibus rule is intended to strengthen the privacy and security safeguards of patient data. The enactment of these new rules significantly reduced the number of privacy breach incidents among business associates (7).

Protected Health Information

PHI includes all information that could be used to identify an individual. Any part of a person's medical record and payment history is considered PHI and may not be shared with unauthorized personnel. PHI is used within a medical facility and includes verbal and written communications. PHI can be found in computer files, paper medical records, information from insurance companies, information form the provider, and information legal offices. (9). Name, address, date of birth, phone number, social security number, medical record number, medical history, photographs, charts, health plan beneficiary numbers, license numbers, vehicle identifiers, Internet Protocol addresses, biometric identifiers (such as retina, voice, and fingerprints) and test results are all considered PHI (10). Physicians' and nurses' notes, billing and other treatment records are also included. Medical images are also considered PHI (11). Medical images exist in Digital Imaging and Communication in Medicine (DICOM) format, which combines sets of images with patient information and a description of the radiology modality. Under HIPAA, this type of DICOM data must also be protected and secured (11).

Need to Know Basis

Healthcare providers have the ethical and legal obligation to maintain the confidentiality of patients' PHI. It is also a responsibility to ensure that patient information is only disclosed to individuals or companies with a legal right to have it. Healthcare professionals should only use patient data to perform specific job tasks and nothing more - that is, healthcare professionals must use the minimum necessary information to accomplish the purpose of the request (3). When a there is not a specific rule to follow in a situation or a question arises, one should also rely on personal ethics and use the best judgement in deciding whether to disclose PHI.

Privacy Rule

The term *privacy* refers to obligations of authorized persons using PHI to keep such information secret. The privacy rule regulates the use and disclosure of PHI and sets the minimum national standards that every covered entity must follow to protect patients' private medical information. Under HIPAA guidelines, all PHI about an individual must remain private and confidential. The HIPAA privacy rule applies to health plans (e.g., Anthem, Medicare, Cigna), health care clearinghouses (e.g., billing companies), and health care providers (e.g., hospitals, clinics, doctor's offices) and their business associates (e.g., attorneys, consultants) that conduct health care transactions. This rule also gives patients the right to request their own radiographic images and a copy of their health records. By law, an individual must receive the requested PHI within 30 days after such a request (3).

Exceptions to the Privacy Rule

A covered entity under HIPAA may not disclose protected health information unless a patient authorizes its disclosure in writing. However, HIPAA outlines specific circumstances in which disclosure of PHI is allowed in the absence of an individual's written permission. PHI may be disclosed without authorization for the following purposes:

1. For treatment, payment or general healthcare operations. Providers can also share PHI with billing companies to receive payment for services rendered. PHI can also be used to perform system or compliance quality checks that improve health care operations (12).

   Under HIPAA, only two types of clinical care information cannot be shared between care providers without the patient's explicit consent: substance abuse records from a licensed abuse program and written psychotherapy notes (13,14).

2. If the individual can agree or object to a disclosure. For example, when a patient brings another person in the room with them, the patient automatically agrees that that person can hear the

PHI (6, 15).

3. During a natural disaster. For example, some violation penalties were waived during Hurricane Harvey in 2017 after the disaster protocol was implemented in Texas and Louisiana area hospitals. The waiver is granted by the U.S. president or a state official and it only applies to hospitals in the disaster area for the emergency period identified in the public health emergency declaration and applies for up to 72 hours following the implementation of a hospital's disaster protocol. The waiver does not apply to all elements of the Privacy rule and these provisions are usually stated in the official waiver. (3, 12, 16).

4. For public health activities and purposes, such as preventing or controlling the spread of disease or receiving reports of child abuse or neglect (12).

5. If requested to do so by court orders (3, 12).

Security Rule

Security refers to procedures designed to prevent unauthorized persons from accessing PHI. The HIPAA security rule complements the privacy rule and requires entities to implement physical, technical and administrative safeguards to protect the privacy of PHI.

Physical Safeguards

Physical security refers to the physical access to PHI. It includes access to a location or physical object like buildings, offices, secured areas, computer hardware, files, and so forth. Facility access must be authorized, created, monitored and terminated for individuals who are no longer employed by the organization. Incoming and outgoing equipment such a copiers and electrocardiogram machines must be inspected prior to removal from the facility and inventoried. Just like passwords, access badges should not be shared or left unattended. It is important to control and monitor personnel accessing secure areas, and security measures must be put in place (3).

Technical Safeguards

Technical security refers to the control of access to computer systems and the protection of electronically transmitted PHI (3). Technical security addresses who and how a person may access, view and use electronic medical records. PHI must be secured when it is being transferred to another location *(10).* Through encryption, data is always to be unreadable until a password is entered. Many entities use a third-party program that encrypts email text. This protection goes above what password protection alone can do. As a general rule, free and public web email services like Outlook, Gmail and Yahoo are not secure for the transmission of PHI. There are cloud-based email platforms that host a HIPAA compliant server (e.g., Office 365); however, this option does not control email transmission from the cloud server to the email recipient. Therefore, the best option is to avoid sending emails containing PHI altogether. Instead, use patient portals to relay information containing PHI. Many electronic health record systems can provide this service.

Technical safeguards require facilities to implement procedures, software, and equipment to protect PHI. Facilities should incorporate encryption and decryption in backing up, restoring, and transmitting electronic patient information (10). Policies and procedures must be set up to destroy PHI when it is no longer necessary to fulfill a job or function. Disposal of documents that contain PHI must be handled correctly. DHHS identifies shredding, burning, pulping or pulverizing as acceptable methods to render paper records unreadable and indecipherable (17). For electronic data, overwriting media with non-sensitive data, degaussing, shredding or incinerating are all acceptable and effective practices (17). DHHS encourages organizations to consider which methods are most practical and appropriate for each facility (17).

Administrative Safeguards

Administrative safeguards require facilities to create and update policies and procedures for employees to learn and follow to help ensure the security of PHI. Some examples of administrative safeguards are:

- Acceptable Use Policies - established to train employees on their access rights and responsibilities in handling PHI.
- Sanction Policies - needed to discipline employees who violate HIPAA.
- Information Access Policies - to grant appropriate access to computer workstations, health records and transactions, and other programs or processes.
- Security Awareness Training - to educate and remind employees of policies and procedures related to software updates, computer log-in monitoring, password updates, and other critical security measures.
- Contingency Planning – to ensure adequate preparation, policies and procedures are in place to respond appropriately to emergencies, such as cyber-attacks, fire, vandalism, or natural disasters. All critical activities must have designated organizers, so each employee knows what is expected in the event of an emergency (18).

Concluding Recommendations

Each facility is responsible for employing the necessary safeguards for HIPAA compliance for privacy and security of PHI. Employers should ensure that employees are adequately trained and following HIPAA requirements. HIPAA compliance includes more than just not talking about PHI in an elevator. Make sure business associates can be trusted and have updated BAAs. Remember that authorized personnel who handle PHI are responsible for protecting it. Each facility must be committed to developing a culture of HIPAA compliance. Organizations need to ensure a knowledgeable workforce

that understands the new HIPAA rules. It is important for employers to be proactive rather than reactive. Part 2 of this series, which will appear in a future issue of this journal, will go further into the HIPAA limitations, patient rights, compliance, violations, and the role imaging technologists play.

Financial Disclosures: The authors received no funding for this article.

Disclaimer: The authors have no conflict of interest.

References

1. Solove, D. J. (2013). "HIPAA turns 10." *J ahima* **84**(4): 22-28; quiz 29.
2. 45 CFR 164.530. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec164-530.pdf. Accessed August 3, 2018.
3. Edemekong, P., Haydel, M. Health Insurance Portability and Accountability Act (HIPAA) [Updated 2018 May 13]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2018. Available from: https://www-ncbi-nlm-nih-gov.ezp.slu.edu/books/NBK500019/
4. Morris, K. (2013). "Sing a song of HIPAA." *Ohio Nurses Rev* **88**(2): 12-14.
5. 45 CFR 164.104. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-104.pdf. Accessed July 3, 2018.
6. Marting, R. (2018). "HIPAA: Answers to Your Frequently Asked Questions." *Fam Pract Manag* **25**(2): 12-16.
7. Yaraghi, N. and R. D. Gopal (2018). "The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study." *Milbank Q* **96**(1): 144-166.
8. HITECH Subtitle A – Medicare Incentives Section 4101 p. 60 https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf
9. 45 CFR 164.502. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2016-title45-vol1/pdf/CFR-2016-title45-vol1-sec164-502.pdf. Accessed July 3, 2018.
10. Disclosures for Emergency Preparedness - A Decision Tool: Limited Data Set (LDS). Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/limited-data-set/index.html. Accessed September 2, 2018.
11. Marks, M. Medical Imaging and HIPAA Compliance. AAOS Now. American Academy of Orthopaedic Surgeons website.

https://www.aaos.org/AAOSNow/2017/Oct/Managing/managing02/?ssopc=1. Updated October 2017. Accessed June 10, 2018.

12. Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2013 and 2014. U. S. Department of Health and Human Services website. https://www.hhs.gov/sites/default/files/rtc-breach-20132014.pdf. Accessed July 4, 2018.
13. 45 CFR 164.501. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-501.pdf. Accessed July 8, 2018.
14. Hilt, R. J. (2014). "HIPAA: Still misunderstood after all these years." *Pediatr Ann* **43**(7): 249.
15. 45 CFR 164.510. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec164-510.pdf. Accessed July 3, 2018.
16. HIPAA Privacy Rule Violation Penalties Waved. Netsec.news website. https://www.netsec.news/hipaa-privacy-rule-violation-penalties-waived-wake-hurricane-harvey/ Accessed July 2, 2018.
17. What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information? Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html. Accessed September 14, 2018.
18. 45 CFR 164.308. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-308.pdf. Accessed August 4, 2018.