Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules

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

Doisy College of Health Sciences, Saint Louis University, St. Louis, Missouri

CE credit: For CE credit, you can access the test for this article, as well as additional *JNMT* CE tests, online at https://www.snmmilearningcenter.org. Complete the test online no later than December 2022. Your online test will be scored immediately. You may make 3 attempts to pass the test and must answer 80% of the questions correctly to receive 1.0 CEH (Continuing Education Hour) credit. SNMMI members will have their CEH credit added to their VOICE transcript automatically; nonmembers will be able to print out a CE certificate upon successfully completing the test. The online test is free to SNMMI members; nonmembers must pay $15.00 by credit card when logging onto the website to take the test.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 has made an impact on the operation of health-care organizations. HIPAA includes 5 titles, and its regulations are complex. Many are familiar with the HIPAA aspects that address 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 HIPAA, its history, its rules, its implications, and the role that imaging professionals play.

Key Words: HIPAA; security law; privacy law; patient rights

J Nucl Med Technol 2019; 47:269–272
DOI: 10.2967/jnmt.119.227819

Privacy and security laws are continually evolving to adjust to new challenges, new technologies, and the novel threats in the digital era. The laws of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 are more strictly enforced than ever before. Although periodic HIPAA training is mandatory for employees who 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 are imperative to protect health information confidentiality, privacy, and security. This article—part 1 of a 2-part series—is a refresher on HIPAA, its rules, and its implications. Part 2 will continue 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 *Code of Federal Regulations* parts 160–164. The law was passed by Congress and signed by President Bill Clinton on August 21, 1996, with the primary intent of ensuring 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 title 45 of *Code of Federal Regulations* part 164, and the regulations are complex and voluminous.

THE 5 HIPAA TITLES

Title I provides the ability to transfer and continue health-care coverage for American workers and their families who change or lose their jobs; it also limits the ability to deny health plan coverage due to preexisting conditions (*3*). Title II has an administrative simplification provision requiring that the U.S. Department of Health and Human Services (DHHS) establish national standards for electronic health-care 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, as well as guidelines for pretax medical spending accounts (*3*). Title IV specifies conditions for group health plans regarding coverage of

Received Feb. 25, 2019; revision accepted May 7, 2019.
For correspondence or reprints contact: Sarah Frye, Saint Louis University, Allied Health Building, 3437 Caroline St., Suite 3021, St. Louis, MO 63104.
E-mail: sarah.frye@health.slu.edu
Published online Jun. 10, 2019.

persons with preexisting 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 U.S. citizenship (*3*).

Health-care 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 health-care 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 access to health records (*1*).

The responsibility for implementing the new regulations that would help maintain the safety of health records was deferred to the DHHS, which established a schedule for this implementation (*4*). These rules and standards apply to covered entities, which DHHS defines as health-care providers, health plans, and health-care 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*). Lawmakers and health-care 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

Although HIPAA was signed into law in 1996, it was not until 2003 that HIPAA 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 HITECH Act in 2009 (*7*). The goal of the HITECH Act was to support the nationwide implementation of electronic health records to provide integrated medical data and information to providers as well as patients. HITECH offered incentive programs that helped to encourage the adoption of electronic health records 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 agreements be executed and maintained between the practice and all business associates (*4*). A business associate agreement is a contract that defines how the associates adhere to HIPAA along with the responsibilities and risks they accept. Because of 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 breaches among business associates (*7*).

PHI

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 from the provider, and information from 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 records, and other treatment records are also included. Medical images are also considered PHI (*11*).

Medical images exist in 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

Health-care 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 disclosed only to individuals or companies with a legal right to have it. Health-care professionals should use patient data only to perform specific job tasks and nothing more—that is, health-care professionals must use the minimum necessary information to accomplish the purpose of the request (*3*). When 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

In the context of PHI, the term *privacy* refers to the obligation 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, and Cigna), health-care clearinghouses (e.g., billing companies), and health-care providers (e.g., hospitals, clinics, and doctor's offices) and their business associates (e.g., attorneys and 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 d after such a request (*3*).

EXCEPTIONS TO THE PRIVACY RULE

An entity covered under HIPAA may not disclose PHI 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 under certain circumstances:

- For treatment, payment, or general health-care 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 2 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*).
- If the patient can agree to or object to a disclosure. For example, when a patient brings another person into the room with him or her, the patient automatically agrees that that person can hear the PHI (*6,15*).
- 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 applies only to hospitals in the disaster area for the emergency period identified in the public health emergency declaration and for up to 72 h after 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*).
- For public health activities and purposes, such as preventing or controlling the spread of disease or receiving reports of child abuse or neglect (*12*).
- If requested to do so by court orders (*3,12*).

SECURITY RULE

In the context of PHI, *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 physical access to PHI, including access to a location or physical object such as a building, office, secured area, computer, or file. Facility access must be authorized, created, and monitored, as well as terminated for individuals who are no longer with the organization. Incoming and outgoing equipment such as copiers and electrocardiogram machines must be inspected before 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 into place (*3*).

Technical Safeguards

Technical security refers to control of access to computer systems and protection of electronically transmitted PHI (*3*). Technical security addresses who has access to electronic medical records and how a person may access, view and use such records. PHI must be secured when it is being transferred to another location (*10*). Through encryption, data are always to be unreadable until a password is entered. Many entities use a third-party program that encrypts e-mail text. This protection goes above what password protection alone can do. As a general rule, free and public web e-mail services such as Outlook, Gmail, and Yahoo are not secure for the transmission of PHI. There are cloud-based e-mail platforms that host a HIPAA-compliant server (e.g., Office 365); however, this option does not control e-mail transmission from the cloud server to the e-mail recipient. Therefore, the best option is to avoid sending e-mails 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 nonsensitive 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 to train employees on their access rights and responsibilities in handling PHI; sanction policies to discipline employees who violate HIPAA; information access policies to grant appropriate access to computer workstations, health records, health 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; and contingency planning to ensure adequate preparation for emergencies such as cyber attacks, fire, vandalism, or natural disasters, including having policies and procedures in place to respond appropriately to such emergencies. All critical activities must have designated organizers so that each employee knows what is expected in the event of an emergency (*18*).

CONCLUDING RECOMMENDATIONS

Each facility is responsible for using the necessary safeguards to ensure compliance with HIPAA regarding the 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 business associate agreements. 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 that imaging technologists play.

DISCLOSURE

No potential conflict of interest relevant to this article was reported.

REFERENCES

1. Solove DJ. HIPAA turns 10. *J AHIMA.* 2013;84:22–28.
2. 45 CFR 164.530. Govinfo website. https://www.govinfo.gov/content/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec164-530.pdf. Accessed August 15, 2019.
3. Edemekong P, Haydel M. *Health Insurance Portability and Accountability Act (HIPAA).* Treasure Island, FL: StatPearls Publishing; 2018.
4. Morris K. Sing a song of HIPAA. *Ohio Nurses Rev.* 2013;88:12–14.
5. 45 CFR 164.104. Govinfo website. https://www.govinfo.gov/content/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-104.pdf. Accessed August 15, 2019.
6. Marting R. HIPAA: Answers to Your Frequently Asked Questions. *Fam Pract Manag.* 2018;25:12–16.
7. Yaraghi N, Gopal RD. The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: insights from an empirical study. *Milbank Q.* 2018;96:144–166.
8. Index for Excerpts from the American Recovery and Reinvestment Act of 2009 (ARRA). HeathIT.gov website. https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf. Published February 19, 2009. Accessed October 29, 2019.
9. 45 CFR 164.502. Govinfo website. https://www.govinfo.gov/content/pkg/CFR-2016-title45-vol1/pdf/CFR-2016-title45-vol1-sec164-502.pdf. Accessed August 15, 2019.
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. Updated June 16, 2017. Accessed August 15, 2019.
11. HIPAA Compliance & Medical Imaging. Quest International website. https://www.questinc.com/company/blog-posts/hipaa-compliance-medical-imaging. Updated October 2018. Accessed October 29, 2019.
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 August 15, 2019.
13. 45 CFR 164.501. Govinfo website. https://www.govinfo.gov/content/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-501.pdf. Accessed August 15, 2019.
14. Hilt RJ. HIPAA: still misunderstood after all these years. *Pediatr Ann.* 2014; 43:249.
15. 45 CFR 164.510. Govinfo website. https://www.govinfo.gov/content/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec164-510.pdf. Accessed August 15, 2019.
16. HIPAA privacy rule violation penalties waved in wake of Hurricane Harvey. NetSec. news website. https://www.netsec.news/hipaa-privacy-rule-violation-penalties-waived-wake-hurricane-harvey/. Published August 28, 2017. Accessed August 15, 2019.
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. Published February 18, 2009. Accessed August 15, 2019.
18. 45 CFR 164.308. Govinfo website. https://www.govinfo.gov/content/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-308.pdf. Accessed August 15, 2019.