Insight

Primer: The Health Insurance Portability and Accountability Act

CHRISTOPHER HOLT, JAKE GRIFFIN | AUGUST 11, 2021

Executive Summary

- One of the most frequently misunderstood areas of federal health law, particularly right now with inquiries around vaccination status, is the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- HIPAA aimed to make health care delivery more efficient, increase the number of Americans with health insurance, and ensure employees would not lose health coverage when switching or leaving jobs.
- Since being enacted, there have been several major additions to HIPAA that have made it into the central regulatory framework dictating how protected health information (PHI) is protected against health care fraud and theft.
- Amid rapid advancements in health information technology, additional changes to HIPAA will likely be needed in the coming years if PHI is to continue to be appropriately protected and to allow for continued innovation.

Introduction

One of the most frequently misunderstood areas of federal health law is the Health Insurance Portability and Accountability Act (HIPAA) and its related regulations and succeeding legislation. As one reporter satirically summarized, "You may ask, Is this a HIPAA violation? The answer is always yes, and the answer is always no." These misunderstandings have multiplied during the COVID-19 pandemic, as individuals, politicians, and businesses have misconstrued and misapplied HIPAA, often with little knowledge of the law's actual mandates. Take the scenario of a grocery store manager asking a customer why he is not wearing a mask inside the store. While the customer may claim this question is a violation of HIPAA, the store has every right to ask the question, even if the reason is because of an underlying medical condition.

HIPAA is far more limited in scope than generally understood, only applying to specified covered entities and business associates that work with protected health information (PHI). PHI, as defined by HIPAA, is individually identifiable health information that includes demographic or health care information relating to the individual's past, present, or future physical and mental health. A business that does not handle PHI for its customers as a part of its function does not have to comply with HIPAA. For the same reason, asking customers for proof of vaccination is permissible for businesses not considered covered entities or associated businesses working with PHI.

A primary aim of HIPAA, enacted in 1996, was to revamp the way PHI is maintained by health care organizations and health care insurance companies by setting new standards to prevent health care fraud (although rules for doing so were not established until years later). Other objectives included making health care delivery more efficient, increasing the number of Americans with health insurance, and ensuring employees would not lose health insurance when switching jobs.

HIPAA's Objectives

The objectives of HIPAA are outlined in its five different titles.

- Title I protects health insurance coverage for those who have lost or are changing jobs. Group health plans are also prevented from denying coverage to those with pre-existing conditions, with some exemptions for long-term health plans and plans offered independently from a general health plan (e.g., dental or vision plans).
- Title II, the primary focus of this primer, directs the Department of Health and Human Services (HHS) to establish national standards for processing electronic health care transactions in an effort to make the delivery of care more efficient. It also requires health care organizations and individuals to follow privacy regulations created by HHS.
- Title III includes tax-related health provisions dictating how much can be saved per person in a tax-free medical savings account used to pay for qualifying medical expenses.
- Title IV specifies conditions in relation to the coverage of persons with pre-existing conditions in group health plans. It also clarifies continuation of coverage requirements for those who have left employment.
- Title V includes provisions that prohibit the tax-deduction of interest on life insurance loans for employers providing company-owned life insurance premiums. It also expands the expatriation tax to include those deemed to be giving up U.S. citizenship or permanent residence for tax-related purposes, while also making these ex-citizens' names part of public record through the publication of the Internal Revenue Service's "Quarterly Publication of Individuals, Who Have Chosen to Expatriate."

Who Must Comply?

HHS has identified two separate groups as responsible for complying with PHI protections of Title II and all of its subsequent regulations and legislative expansions.

Covered Entities: Individuals and organizations that provide medical or other health services and engage with PHI. This list includes providers (doctors, dentists, pharmacies), health plans (health insurance companies, Medicare, Medicaid), and health care clearinghouses that process medical claims. Hospitals and nursing homes are examples of covered entities because they are organizations that provide health services and work with PHI.

Business Associates: Individuals or businesses that perform a certain function for and have a Business Associate Agreement with covered entities that details what PHI they can access. Lawyers, information technology contractors, and independent medical transcriptionists are examples of potential business associates. Prior to the Health Information Technology for Economic and Clinical Health (HITECH) Act—enacted in 2009 as part of the American Recovery and Reinvestment Act—business associates only had a "contractual obligation" to comply with HIPAA, and enforcement of that obligation was minimal. Business associates could not be fined directly for violations, and many failed to meet standards established by the previously issued Privacy and Security Rules. Now, because of the HITECH ACT, business associates are directly liable for their own HIPAA compliance and face financial penalties for noncompliance, just like covered entities.

Timeline

Since enactment in 1996, there have been several major expansions of HIPAA's PHI protections through rulemaking and legislation, including the Privacy Rule, Security Rule, Enforcement Rule, HITECH Act, Breach Notification Rule, and Final Omnibus Rule.

Privacy Rule

An important milestone in the history of HIPAA was the establishment of the 2003 Privacy Rule. This rule sets out national regulations for the use and disclosure of PHI by covered entities in all forms of communication, including written, electronic, or oral. PHI comprises identifiable health information about an individual that relates to "the individual's past, present, or future physical or mental health condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual." Eighteen identifiers have been recognized as PHI under HIPAA and are included in the list below. This information, however, can be disclosed by covered entities without patients' written authorization when required by law, or for treatment, payment, and health care operation purposes.[1] The Privacy Rule also requires covered entities to disclose PHI to individuals within 30 days of request. While failing to do so can result in financial penalties, covered entities are often cautious about fulfilling individual requests due to concern about violating regulations, making it difficult for individuals to obtain their own medical records in some cases. For example, one study found that processing times for releasing requested medical records varied from same day to 60 days for the top 83 hospitals, with hesitancy about violating HIPAA through unsecure communications as one factor contributing to longer waiting times. Additionally, patient complaints about access to their own medical records is the third most frequent issue that the HHS Office for Civil Rights (OCR) received in 2019 and 2020. Efforts that ensure health care workers are thoroughly trained in HIPAA would go a long way in alleviating this fear about violation and improving patient's timely access to personal medical information.

The 18 HIPAA identifiers are as follows:[1]

1. Names;
2. All geographic subdivisions smaller than a state, including street addresses, city, county, precinct, and zip code;
3. All elements of dates (except year) relating to the individual, including birth date, admission date, discharge date, and date of death;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;

7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images; and
18. Any other unique identifying number, characteristic, or code.

Security Rule

Effective April 21, 2005, the Security Rule consists of a list of regulations designed to secure electronic protected health information (EPHI). Three types of security measures are required from entities to comply with the rule: administrative safeguards, physical safeguards, and technical safeguards.

Administrative safeguards constitute the largest portion of the Security Rule and are defined by HHS as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect EPHI." In simpler terms, covered entities need to design policies that ensure the protection of EPHI and periodically evaluate how effective these policies are.

Physical safeguards entail security measures to limit physical access to EPHI by preventing workstation access to unauthorized users and developing procedures for disposal of EPHI from devices and hardware storage.

Lastly, technical safeguards are designed to control computer system access and track the movement of EPHI across an organization's systems. Doing so makes it possible to determine who accessed EPHI, when, and for what purpose.

Enforcement Rule

In response to many covered entities failing to comply with the HIPAA Privacy and Security Rules, the Enforcement Rule was finalized in 2006. This rule gives the OCR the authority to examine HIPAA violation complaints and assess financial penalties for noncomplying covered entities. If OCR decides a complaint warrants investigation, both the person who filed the complaint and the alleged covered entity will be notified and asked to present information about the incident in question. OCR reviews the case and then decides if the covered entity was in compliance. If OCR determines the covered entity was not in compliance, it will then attempt to resolve the case with the covered entity through voluntary compliance, corrective action, or a resolution agreement. OCR may decide to impose financial penalties on covered entities not taking action to resolve the matter. As of June 30, 2021, over 267,000 HIPAA Privacy Rule complaints have been submitted for HHS review, with 98 percent of them being resolved. Out of the 263,598 complaints resolved by OCR, almost 70 percent of them have resolved in either a "No Violation" decision or the complaint has been determined to not be eligible for enforcement.[2] The number of complaints that have been rejected suggests continuing

confusion over what the Privacy Rule covers.

HITECH Act

Before the HITECH Act was enacted, only 10 percent of U.S. hospitals were using electronic health records (EHRs).[3] To promote widespread adoption, the legislation allocated HHS with a budget of $25 billion to encourage providers to adopt EHR by offering financial incentives. Before HITECH, business associates of HIPAA covered entities had a "contractual obligation" to comply with HIPAA, but enforcement of this obligation was nonexistent since business associates could not be fined directly for violations. Now, business associates are directly liable for their own compliance and can be punished for failing to comply with HIPAA Security and Privacy Rules.

Effects of the HITECH Act have been mixed, however. While annual adoption rates of EHR increased from 3.2 percent to 14.2 percent after HITECH, EHR implementation has been deemed a major cause of physician burnout and 63 percent of doctors considers EHRs to be inefficient. Inefficiencies voiced by physicians include excessive scrolling through pages of notes and navigating through multiscreen workflows to find information. These point-of-care inefficiencies force physicians to waste their time scrolling through medical records, limiting time that could be spent on face-to-face interactions with patients.

Additionally, the number of EHR vendors has been dwindling in recent years through numerous mergers and acquisitions, and many are concerned about the impact this EHR market consolidation will have on physicians. Together, vendors Cerner and Epic control nearly 54 percent of the acute care hospital market and 85 percent of the large hospital market, with Epic holding onto 58 percent and showing no signs of stopping as it added an additional 19,247 hospital beds in the 2020 pandemic year. Physicians forced to switch from smaller vendors could face unexpected costs and lost productivity as they learn to navigate newly adopted systems. There is also fear that continuous market consolidation may lead to near monopolies, resulting in decreased innovation in the electronic sphere.

Breach Notification Rule

The Breach Notification Rule, finalized September 2009, requires covered entities to notify HHS and affected individuals when a breach, or "impermissible use or disclosure of PHI," affecting over 500 individuals has occurred. Failure to do so within 60 days of breach discovery will result in financial penalties. Breaches affecting fewer than 500 people only need to be reported to HHS annually.

Though the Breach Notification Rule sets minimum federal standards for health care information, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have their own security breach notification laws. These state and territorial security breach notification laws do not pertain to just health care, or necessarily health care at all, and are instead general provisions dictating who must comply with the law, what is considered personal information, what constitutes a breach, and what is required for breach notices. In 2016, fewer than half of states included medical information in their data breach notification standards, but several states have made the addition in the past few years in an effort to better protect and secure personal information. So far in 2021, 22 states have introduced or considered measures that would amend their current security breach laws, with one major trend being expanded definitions of "personal information" to include both biometric and health information. Many state laws are actually stricter and account for more data than the federal Breach Notification Rule does. For example, covered entities in Tennessee are required to notify patients about compromised information even if it has been encrypted and must also disclose any breach within 14 days of discovery, as

opposed to within 30 days that the federal regulation requires. HIPAA covered entities and business associates need to ensure they are accounting for and compliant with both federal and state laws when handling PHI.

Final Omnibus Rule

The most recent addition to HIPAA came in 2013 with the Omnibus Rule that increased HIPAA violation penalties through a tiered system, as shown and described below. Further, it included additional prohibitions on the disclosure of genetic information for underwriting purposes and PHI for marketing purposes.

The types of violation are:

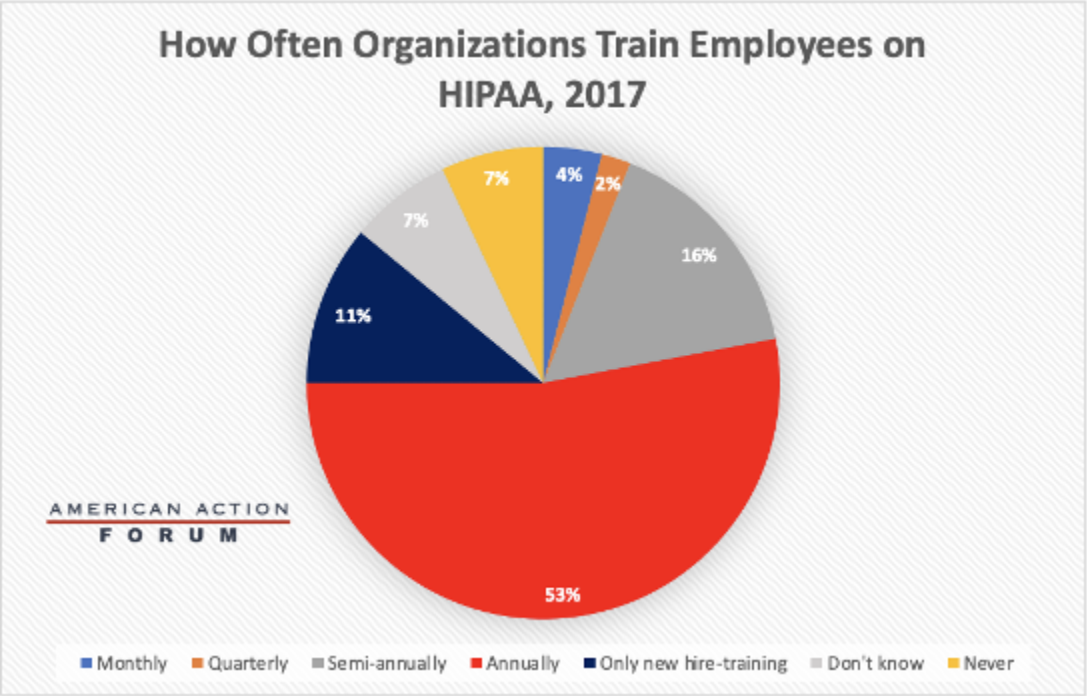
- Unaware of Violation: The covered entity or business associate did not know and should not have known the violation existed;
- Reasonable Cause: The covered entity or business associate knew or should have known, if reasonable diligence was exercised, that the violation existed but did not act with willful neglect;
- Willful Neglect – Corrected Within 30 Days: The violation was the result of intentional failure or reckless indifference to the obligation to comply with HIPAA but was corrected within 30 days of discovery; and
- Willful Neglect – Not Corrected Within 30 Days: The violation was the result of intentional failure or reckless indifference to the obligation to comply with HIPAA but was not corrected within 30 days of discovery.

Table 1: HIPAA Violation Penalties by Type.[4]

Type of Violation	Each Violation	Max Penalty of All Violations of the Same Type Per Year
Unaware of Violation	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected Within 30 Days	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected Within 30 Days	$50,000	$1,500,000

HIPAA Training

Covered entities and business associates are required to provide HIPAA training to employees who handle PHI. Although training is required, there is no detailed list of training requirements. Instead, the Privacy Rule states that training should be provided "as necessary and appropriate for members of the workforce to carry out their functions." This flexibility in training allows covered entities and business associates to design HIPAA training that is tailored toward risks that their own employees face rather than a one-size-fits-all approach that is less relevant or useful. HIPAA also does not specify how often training should take place, but typically training occurs annually. For new employees, the Privacy Rule requires training "within a reasonable period of time after the person joins the covered entity's workforce." This is usually interpreted as within a few weeks of joining. The chart below details how often organizations train their employees, with annually being the predominant timeframe.[5]



What's to Come

On December 10, 2020, HHS announced proposed changes to the HIPAA Privacy Rule designed to empower patients, improve coordinated care, and reduce regulatory burdens on the health care industry. Covered entities would be allowed to disclose PHI to social services agencies and other third parties that provide health-related services without the individual's authorization if the provider thinks it is a necessary component of improving the person's heath. This provision has drawn some scrutiny, as social service agencies are not considered covered entities and are not subject to HIPAA. Many fear that this sort of non-HIPAA protected information sharing may result in some individuals losing social services such as housing. To strengthen individuals' rights to PHI, covered entities would be required to disclose PHI to individuals within 15 days (from the current 30 days) of the request date. This tighter timeframe would likely generate new administrative burdens, especially in a time where health care organizations already are busy with COVID-19 cases and procedures.

Conclusion

Congress originally created HIPAA to help better regulate health insurance and make the flow of health care information more efficient. With additional amendments over the years, HIPAA has become the centerpiece of regulation dictating how PHI is to be maintained by covered entities and business associates in order to prevent health care fraud and theft. As technology continues to develop, additional changes to HIPAA will need to occur in tandem to maintain these protections.

[1] https://www.luc.edu/its/aboutits/itspoliciesguidelines/hipaainformation/18hipaaidentifiers/

[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[3] https://www.hipaajournal.com/what-is-the-hitech-act/

[4] https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf

[5] https://www.hhs.gov/hipaa/for-professionals/training/index.html