wiley

NEWSLETTER

HIPAA Privacy and Security for Beginners

July 2014

We hear lots about the Health Insurance Portability and Accountability Act (HIPAA) these days. Some of it involves new compliance challenges arising from recent developments in federal law. In other situations, HIPAA is a "problem," because it doesn't cover certain things or isn't being enforced aggressively enough, or causes some kind of difficulty in research or otherwise. For many, HIPAA is simply a long and confusing piece of paper handed to patients when they go to a doctor's office.

So, what is HIPAA, who needs to care about it, and what does it do? While we usually concentrate in *Privacy In Focus* on new developments or significant challenges, this time we'll go back to basics.

Background

The HIPAA era began in 1996, with the passage of the Health Insurance Portability and Accountability Act of 1996. While "HIPAA" now means many things to many people, at its foundation, the HIPAA law itself focused on "portability," the idea that individuals could "take" their health insurance coverage from one employer to the next, without having pre-existing health conditions acting as an impediment to job transitions.

When Congress passed HIPAA, it also added into the mix a variety of other topics related to the health care industry (such as creating large funding for what has now become an extended fight against health care fraud). One of the policy mandates adopted in HIPAA was to move toward standardized electronic transactions for the health care industry. The core idea was that certain "standard transactions"—such as the submission of a health insurance claim and the payment of that claim—could be "standardized" in mandatory electronic formats, and thereby create efficiency savings and more effective results. With these standardized transactions came a concern about privacy and security associated with health care information being put into electronic form, with the resulting requirements for the creation of the HIPAA Privacy Rule and the HIPAA Security Rule. So, now, for most people and in most situations, HIPAA has become shorthand for health care privacy and security.

Who Needs to Care about HIPAA?

First and foremost, the HIPAA privacy and security rules are designed to protect individuals, generally patients of health care providers and members of insurance or government health insurance benefit programs. From a policy perspective, lots of attention is paid to whether individual rights are protected appropriately under the HIPAA rules, balancing privacy interests with the overall operation of the health care system and significant

public benefits that arise from health care information.

From a compliance perspective, however, the focus is on those businesses that must comply with these HIPAA principles, and face potential enforcement if compliance problems arise.

So, who does need to comply with the HIPAA rules? HIPAA's history leads to much of this answer. Initially, driven by the primary focus of the HIPAA law on portability and standard transactions, the HIPAA privacy and security rules applied only to specifically designated "covered entities," health care providers, health plans, and health care clearinghouses. This includes a full range of health care providers, generally physicians, hospitals, pharmacies, and a wide variety of entities that provide direct health care services to patients.[1] It also reached to various "health plans," including government health care programs, private health insurers, and significantly, the health care benefit plans offered by employers. However, even from the start, HIPAA was not a general medical privacy law. It applied to certain entities in certain situations, for certain information. That meant that a large number of companies that obtain or use health care information are not within the scope of these rules, such as consumer-facing entities, many health care web sites, life and disability insurers, employers in their employment role, etc.

Because of this limitation to covered entities, the U.S. Department of Health and Human Services (HHS) (the agency tasked with writing these privacy and security rules) developed a creative solution to respond to a key fact about the health care system. While the covered entities are core participants in the industry, they rely on tens of thousands of vendors to provide them services, with many of these services involving protected patient information. Therefore, the concept of a "business associate" was born, *i.e.* an entity that provides services to the health care industry where the performance of those services involves the use or disclosure of patient information.

Because HHS originally had no direct jurisdiction over these "business associates," HHS imposed an obligation on the covered entities to implement specific contracts with these vendors that would create contractual privacy and security obligations for these vendors. The failure to execute a contract would mean that the covered entity violated the HIPAA rules. A business associate's failure to meet a contractual privacy standard would be a breach of that contract, but would not subject the business associate to government enforcement, because the business associate was not regulated under the HIPAA rules.

Now, as a result of the 2009 "HITECH" law and HHS regulations issued in 2013, these "business associates" must comply directly with significant portions of the HIPAA rules. Accordingly, while these vendors have had contractual obligations since the beginning of the HIPAA era, they now must meet many of the same standards as the covered entities, and face the same risks of government enforcement.[2] Although this legislation does not turn business associates into covered entities, it does impose—for the first time—direct accountability on these business associates, with potential civil and criminal liability for a failure to meet these requirements.

In addition, the HITECH regulations extended these "business associate" compliance obligations "downstream," to service providers of a business associate, and service providers to that downstream business associate, on indefinitely. These "subcontractors" face the same compliance obligations as a first tier business associate that contracts directly with a hospital or a health insurer.

Therefore, the following kinds of entities need to be concerned directly with compliance obligations and potential enforcement as a result of the HIPAA Rules.

- Health care providers, such as hospitals, physicians, and pharmacies;
- Health insurers and government health care programs;
- Any employer that provides health care benefits to its employees (with the employer's "health plan" being the covered entity);
- A service provider to any of these entities; and
- A service provider to a service provider of any of these entities (and on downstream, indefinitely).

Consequently, while HIPAA does not cover all health care information, it certainly applies to a large range of entities, many of whom may not realize that they face legal obligations and enforcement risks as a result of the HIPAA rules.

And, to be clear, the HIPAA rules also *affect* an enormous range of other entities that collect, rely on, use, and/or disclose health care information, because these rules have an impact on how this information can flow, even if entities are not covered directly.

However, it also is important to note that HIPAA, even with its recent expansion from the HITECH Act aside, is still not a general medical privacy law. While its scope has broadened, its protections still depend on where health care information starts, with a health care provider or health plan. That leaves enormous gaps in protection, particularly given recent technological and philosophical developments that are encouraging consumer involvement in their own health care and providing the technology to make this goal a reality.

What are the Core Principles of the HIPAA Privacy Rule?

Use and Disclosure

The HIPAA Privacy Rule consists of the "Standards for Privacy of Individually Identifiable Information," found at 45 CFR Part 160 and Part 164, subparts A and E. The core idea for most privacy rules involves the principles around how information can be used and disclosed. The general premise of the HIPAA Privacy Rule is straightforward. Information about individuals (called "Protected Health Information" or "PHI" in HIPAA) cannot be used or disclosed unless permitted by the rules or specifically authorized by the individual. The premise is that use and disclosure should be relatively easy for core health care purposes, and harder for everything else.[3]

Under the HIPAA structure, patient consent is provided by assumption, for particular categories of uses and disclosures. From the regulator's perspective, there are certain kinds of uses and disclosures of patient identifiable information that are essential to the operation of the health care system and for which patient consent is presumed under the regulatory structure. These purposes (known as "TPO" in the HIPAA system) are for (1) treatment; (2) payment for health care services; and (3) health care operations, essentially the administrative operations of running a health care business. For uses and disclosures that fit these categories, patient consent is presumed, and no further steps are needed. These TPO disclosures represent the overwhelming percentage of information use in the health care system, covering the core areas of treating patients, paying for this treatment, and operating health care businesses.

There also are certain categories of disclosures—known as "public priority" purposes—where patient consent is, essentially, irrelevant (from the perspective of those drafting the rules). These are areas such as public health disclosures, enforcement investigations, litigation, and a wide variety of other purposes where there is a public goal to be served in the disclosure, independent of patient consent. Disclosures in these areas can be made—consistent with specific limitations in some circumstances—without the need for patient consent.

For all other uses and disclosures, the disclosure can be made only with patient "authorization," a carefully defined and very specific document executed by a patient in a particular situation. Using an authorization, a patient can "authorize" any use or disclosure of the patient's information. So, if a patient wants his medical records disclosed to a future employer, or wants them sent to a financial advisor, or the covered entity wants to promote a patient's story in a newsletter, this can only be done with the patient's authorization.

Beyond these consent principles, there are various other core elements of the overall rules on use and disclosure. The "minimum necessary" principle provides a general overlay for most uses and disclosures (and is a good operating principle in all contexts). "Minimum necessary" means that an entity, even where a use or disclosure is permitted, should only disclose the "minimum necessary" information needed to perform the particular function. This is not a hard and fast rule, and companies do not need to spend an inordinate amount of time and energy scrutinizing each disclosure. But, it is important to develop general principles surrounding how companies determine what is the "minimum necessary" information to be disclosed, and employees should be trained to think about this principle in all settings.

Sale and Marketing

There also are specific rules related to the sale of PHI or the use of PHI for marketing. As with many privacy rules, using individual information for marketing purposes is highly limited. The HIPAA rules place substantial restrictions on how PHI can be used or disclosed for marketing purposes. Because the HIPAA restrictions apply to both use and disclosure, this means that companies are restricted in how they can communicate with their patients about marketing opportunities, in addition to placing restrictions on to whom this information can be disclosed. The recent HITECH rules limited this marketing even more, by precluding marketing (without a patient authorization) where there is remuneration (or payment) in connection with the marketing in most situations. As with all other areas, if a covered entity wants to do more than what is permitted by the HIPAA rules, then the entity must obtain the individual's authorization. For example, a health insurer that wants to

market its life insurance products, or those of a business partner, must obtain the individual's authorization.

The HITECH changes also included specific limitations on the sale of PHI. For some, this provision seemed unnecessary, since many "sale" situations would involve disclosures of PHI that were already prohibited by the HIPAA rules. Nonetheless, for those limited situations where a sale would be permitted in the context of the rules, the HITECH changes generally now require an authorization from the individual before information can be sold.

De-Identification

The HIPAA rules apply to individually identifiable information. The principle—set forth in significant detail in the HIPAA rules—is that if otherwise protected information has been "de-identified" according to the rules, this information is no longer "individually identifiable" and therefore there are no longer sufficient privacy interests at stake to justify regulation. The HIPAA rules set out a highly detailed formula for de-identification. If information is "de-identified" under these standards, then the information is no longer regulated by HIPAA, and can be used or disclosed for any purpose.

At the same time, it is important to understand that PHI remains PHI until it has been de-identified under these standards. Therefore, companies need to focus on these de-identification standards when making specific uses and disclosures. At the same time, something less than full de-identification is permitted in situations where a use or disclosure already is permitted by the HIPAA rules. If PHI can be used or disclosed in a specific situation, then removing a limited number of identifiers is an appropriate step (under a "minimum necessary" principle or otherwise), as no full de-identification is required. De-identification is required only for situations where PHI cannot be used or disclosed in a particular situation.

Individual Rights

The HIPAA rules also provide patients with specific individual rights, beyond the general rights conveyed through the use and disclosure limitations. Specifically, individuals have the following rights:

- The right to receive a notice of privacy practices (the one right that happens automatically, since notices must be provided by most covered entities);
- The right to "access" (receive a copy of) a "designated record set" about the individual;
- The right to amend information in certain situations;
- The right to an "accounting of disclosures" in certain situations; and
- The right to additional restrictions on use and disclosure of a confidential communication.

While these rights have been a significant element in all HIPAA discussions, few individual patients have exercised these rights since they went into effect in 2003.[4]

The individual rights have an impact on all covered entities, and some business associates. Covered entities, for example, provide privacy notices to individuals. Business associates, who often are invisible to these individuals, do not. Covered entities must develop means of responding to individual requests for a designated record set (even though few individuals will seek one), while only a small percentage of business associates maintain any element of a designated record set.[5]

Business Associate Contracts

While business associates now are covered directly by the HIPAA rules, HIPAA still requires contractual provisions defining how business associates can use and disclose PHI when performing services, along with various other requirements. While there is a real question as to whether these agreements serve a continuing purpose now that business associates must comply directly, the rules still require these contracts. Therefore, covered entities must execute these contracts with their service providers, and business associates must execute similar contracts with their downstream subcontractors. Negotiating these contracts in a reasonable and cost-effective way is a substantial challenge for both covered entities and business associates. While many of the provisions of these agreements are "standard," there are other provisions that typically result in significant negotiations between the parties.

General Policies and Procedures

Under the HIPAA Privacy Rule, there also is a requirement for covered entities to develop specific administrative procedures to ensure compliance with the overall rules. Under the precise language of the privacy rule, business associates do not appear to have a requirement to implement all of these procedures. However, for most business associates, it will be appropriate to develop these procedures as a means of both ensuring and documenting compliance with the rules.

The key topics for these procedures include:

- Designation of a privacy official;
- Training of employees;
- Development of "appropriate safeguards" for PHI (a "min-security rule" for all PHI);
- A complaint process;
- A sanction approach for employees who violate these rules;
- Appropriate mitigation procedures;
- Overall policies and procedures; and
- Record retention processes.

The HIPAA Security Rule

The second key component of HIPAA is the Security Rule, known formally as the HIPAA "Security Standards," set forth in 45 C.F.R. Parts 160 and 164, Subpart C.

The HIPAA Security Rule sets forth detailed requirements for the protection of electronic PHI. All covered entities and business associates must meet the requirements of the HIPAA Security Rule. Because it is process and documentation intensive, the Security Rule presents serious challenges for any health care company. While covered entities have had to comply with the Security Rule since 2005, business associates must now comply with these provisions as a result of the HITECH changes. For most business associates, this Security Rule compliance represents the single biggest challenge under HIPAA.[6]

In setting out the Security Rule requirements, HHS focused on four key goals/mandates for the protection of electronic PHI. To be in compliance with this Rule, a covered entity or business associate must:

- Ensure confidentiality, integrity, and availability of electronic protected health information created, received, maintained, or transmitted;
- Protect against "reasonably anticipated threats or hazards" to "security or integrity" of this information;
- Protect against "reasonably anticipated uses or disclosures" of this information that are not permitted under Privacy Rule; and
- Ensure compliance by its workforce.

In order to make this mandate feasible, HHS developed a "flexible" approach to compliance, by making the requirements "scaleable" based on the specifics of the organization. The provisions also are intended to be "technology neutral"—meaning that the rule does not dictate any specific technological solution. Instead, the rule focuses on process—how to evaluate a company's security risks and decide what steps should be taken.

Covered entities and business associates, therefore, must develop appropriate security measures based upon:

- The size, complexity, and capabilities of the business;
- The business' technical infrastructure, hardware, and software security capabilities;
- The costs of particular security measures; and
- The probability and criticality of potential risks to electronic protected health information.

In general, with this "flexibility," a covered entity under the Rule may use "any security measures that allow the covered entity to reasonably and appropriately implement the standards and specifications" of the Security Rule. This flexibility is both useful, by providing a range of appropriate options, and difficult to assess, as it is hard to tell when an entity has "done enough" under the Security Rule.

In addition, the Rule breaks down the regulatory provisions into "standards"—which constitute the general security topic which must be addressed, and "specifications," which are the particular safeguards designed to address the specific standard. All of these issues are designed to protect "electronic" protected health information—PHI from the Privacy Rule that is transmitted or maintained in electronic media. Some of the

specifications are "required," and must be implemented. Others are "addressable," meaning that a covered entity must review the issue and evaluate whether the particular step is "reasonable and appropriate" for implementation by the covered entity.

The Rule sets out a series of "administrative" safeguards that constitute the key provisions of an effective security program. In particular, the requirements for "risk analysis" and "risk management" set the stage for the remainder of the activities. In fact, most of the Security Rule describes an appropriate "process" that covered entities must go through in evaluating security options, broken down into technical, physical and administrative safeguards.

Under the Rule, "risk analysis" means to "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." Risk management, which involves the follow-up steps after a risk analysis, involves the obligation to "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule.]"

Also included in the administrative safeguards are requirements such as a sanction policy, assigned responsibility for security activities, security awareness and training, contingency planning, and "security incident" procedures (a "security incident" is an "attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system"). There is a separate administrative safeguard related to "business associates," which are vendors to covered entities (as defined by the HIPAA Privacy Rule). These security provisions will require specific provisions in business associate contracts.

"Physical" safeguards are less dramatic, but constitute an additional core set of safeguards. These include facility access controls (limiting physical access to information systems), workstation use policies, workstation security, and device and media controls (such as procedures for disposal of computer hardware in light of recent reports of privacy violations involving discarded computers that still retained PHI).

The "technical" safeguards also are relatively specific, involving access controls (such as unique user identification, automatic log-off, and emergency access procedures), audit controls, integrity (protection against improper alteration or destruction of PHI), person/entity authentication, and transmission security.

In addition to these safeguards, the Security Rule requires covered entities to develop security policies and procedures, and to maintain appropriate documentation of these policies and procedures.

In general, all covered entities and business associates must develop appropriate processes to identify locations of PHI, implement appropriate measures to protect the confidentiality of this information, and then develop policies and procedures that document and define how these protections are implemented across a company.

Breach Notification

The last "core" provision of HIPAA involves the new breach notification rule, the "Notification in the Case of Breach of Unsecured Protected Health Information" provisions, as set forth at 45 CFR Part 164 Subpart D. This regulation was required by the HITECH statute, and certainly has generated an enormous amount of publicity and discussion.

Essentially, the breach notification rule requires notification to individuals in the event of certain kinds of security breaches involving their PHI. In specific circumstances, notification also may be required to HHS and even media in specific geographic locations.

The primary notification obligations are placed on covered entities. Business associates must notify the affected covered entity in the event of a triggering breach.

Under the regulations, a "breach" means "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information. Certain situations are exempted from this definition, such as "any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under [the Privacy Rule.]"

For any other "not permitted" use or disclosure, notification to an individual is required unless the regulation indicates that notification need not be provided. In the final regulation, HHS made certain key changes to the notification standard. Specifically, HHS eliminated the "risk of harm" standard that was implemented in the interim final rule. There are two key steps in the changes implemented by HHS. First, HHS clarified that the "presumption" is that a breach requires notification to the affected individuals unless the covered entity "demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment." This change was designed to ensure that companies did not use the absence of clear information about a breach as a basis for a "no notice" decision. It is now explicit that notice is required unless a covered entity can conclude there is a "low probability" of "compromise" of the data.

Second, HHS has replaced the "risk of harm" threshold with a more precise "risk assessment" designed to determine whether there is a "low probability" of "compromise" of the data. While there is no longer a specific definition of this idea of "compromise," the set of factors for the risk assessment indicates that the analysis made by a covered entity will be very similar to what was done previously. Specifically, a covered entity or business associate, as part of its risk assessment, must review the following factors (along with any others that are appropriate):

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

This notification requirement has resulted in the reporting and notification of thousands of breaches, and a wide range of publicity about security issues in the health care industry. Ideally, this notification requirement also has encouraged health care companies to improve their overall security practices, to reduce the likelihood of having reportable security breaches.

Conclusions

For any health care company, whether a covered entity or business associate, the HIPAA Privacy and Security Rules require significant attention and impose realistic risks related to the protection of individually identifiable information about patients or health plan benefit members. *Keep in mind that these HIPAA requirements matter to your company if you are any of the following*:

- A health care provider (doctor, hospital, pharmacy, etc.);
- A health or long term care insurer;
- An employer to the extent you provide health care benefits to your employees;
- A service provider to any of these entities; or
- A service provider to a service provider (and on downstream).

While many of these provisions reinforce common sense confidentiality requirements, the HIPAA rules are complicated and detailed in part, and require meaningful attention to strategies and approaches for protecting personal information. Enforcement of these provisions, by the Department of Health and Human Services' Office for Civil Rights (along with state Attorneys General) has been modest, but is growing steadily. Enforcement sanctions range from corrective action plans to multi-million dollar penalties. Companies also face a wide range of HHS investigations, triggered by complaints, breach reporting or other public events. HHS also is developing a revised audit program that will involve proactive review of the privacy and security practices of certain health care companies.

With all of these issues, the health care industry faces a meaningful ongoing challenge from the HIPAA rules. While covered entities have been required to follow these provisions for many years, many companies either do not consistently do a good job or do not adequately engage in ongoing reviews of business activities to ensure compliance. For business associates, these requirements are much newer. Many business associates are still struggling with these requirements, particularly under the Security Rule, with a wide range of companies also unaware of the full range of obligations that have been imposed on them.

These provisions remain important to the health care industry and its individual consumers. Personal data has never been more important in the health care system, and there are a wide variety of societal benefits that stem from the use and disclosure of health care information. At the same time, these rules provide meaningful protections for the privacy and security of PHI, and the health care industry needs to make sure that it continues to take critical steps to protect the sensitive information of its core customers, the individual patients, and members.

---

[1] Because of the impact of the "standard transactions" rules, the HIPAA privacy and security rules do not apply to health care providers who do not utilize standard transactions. Therefore, it is possible (although increasingly unlikely) that doctors would not have to follow HIPAA simply based on how they conduct their business.

[2] For a broader analysis of the full range of HITECH provisions, see Nahra, "Summary of the New HIPAA/HITECH Omnibus Regulation," available at http://www.wileyrein.com/publications.cfm?sp=articles&id=8628 .

[3] Unlike many state health care privacy rules, all PHI is protected under the same standards in the HIPAA rules, except for the very limited category of psychotherapy notes.

[4] There has been significant debate in recent years about the HIPAA accounting rule. While it is likely that new regulations on this point will not be problematic, HHS initially proposed a substantial revision to the "accounting of disclosures" rule, which threatens (if adopted) to wreak havoc on a wide range of covered entities and business associates. This proposal—which should be withdrawn and replaced – demonstrates ongoing confusion about how many of these principles translate to the real world health care environment. See, e.g., Nahra, "The HIPAA Accounting NPRM and the Future of Health Care Privacy," BNA Health IT Law & Industry Report (July 4, 2011). See also Nahra, "Unfinished Business: Solving the HIPAA Accounting Rule Dilemma," *Privacy in Focus* (May 2013.

[5] A designated record set is essentially the core set of records about an individual's health care. Business associates will not be implicated unless they maintain some unique component of these records.

[6] While the Security Rule focuses on electronic information, all entities subject to HIPAA also must protect paper PHI appropriately. Many of the recent HIPAA enforcement actions have involved paper records.