Health Care Information Privacy

The HIPAA Regulations – What Has Changed and What You Need to Know

Note: Information provided to NCRA by Melodi Gates, Associate with Patton Boggs, LLC

Privacy and data protection issues, and related laws and regulations, are an increasing concern for NCRA members, especially when working with clients in highly regulated fields like health care. If you provide court reporting, CART captioning, or other services for health care providers or health care plans (*i.e.*, public or private health insurance plans), then you, your clients, and your subcontractors may be impacted by recent changes in federal regulations. Specifically, these regulations govern how many health care industry entities must act to protect patient information. So, if you are employed by or under contract with such organizations, then the regulations may also apply to you, especially if you will be interacting directly with or managing information about individual patients. If you are not employed by or under contract with such health care entities, then you may find it helpful to be aware of the requirements, even though they are unlikely to apply to you. This handout will provide you with high-level information and guidance regarding those regulations and recent changes. It also addresses potential issues with agreements that you may be asked to sign and steps that you can take now to meet your clients' expectations, ensure regulatory compliance, and lower risk for you and your business.

For example, if a client engages you to take a deposition in a matter that involves patient care, health care records, or other details regarding the relationship between a health care provider and one or more specific patients, then these regulations likely apply to you and any of your subcontractors who may perform the services. Similarly, if a health care provider hires you to provide CART captioning services in support of individual patient interactions, or other situations that involve communicating information regarding a particular patient or patients, then these regulations generally apply.

The **Health Insurance Portability and Accountability Act ("HIPAA")** was enacted by Congress in 1996 to standardize certain electronic transactions related to health care and make it easier for individuals to move between insurance plans. Several regulations intended to ensure the privacy and security of **protected health information ("PHI")** were issued in the following years. PHI is broadly defined to include data that can be reasonably used to identify an individual and "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." (*See* "Resources" below and 45 CFR 164.103).

More recently, the **Health Information Technology for Economic and Clinical Health ("HITECH") Act**, enacted in 2009, raised the bar for protecting such information, particularly in light of the financial incentives that it provides for certain healthcare providers to migrate to electronic records. In early 2013, the **U.S. Department of Health and Human Services, Office for Civil Rights ("HHS/OCR")** – the federal agency that promulgates and enforces the HIPAA regulations – issued a series of updates to the HIPAA regulations, under the HITECH Act, effective as of September 23, 2013.

HIPAA Roles & Relationships

The HIPAA regulations apply to health care providers, health plans (*i.e.*, public or private health insurance plans), and health care clearinghouses (*i.e.*, organizations that support specific types of electronic transactions). These three types of organizations are known as "**covered entities**," under the regulations. The regulations also apply to service providers that create, receive, transmit, or maintain PHI on behalf of covered entities. Such service providers are called **"business associates."** For example, court reporters or captioning service providers that work with health care providers and receive or interact with PHI would generally be considered business associates. The key consideration is whether the patient information is being used or disclosed by a covered entity, or a service provider who is acting on behalf of the covered entity. So, for example, a court reporter who is taking a deposition that includes questioning about the witness' health or health-related issues would only be considered a business associate if hired by a health care provider (or another business associate, such as an attorney, acting on the provider's behalf). The HIPAA regulations require that covered entities have a **business associate agreement ("BAA")** in place with each of their business associates, and the BAA must include a number of specific provisions, discussed in more detail below. The recent changes to the HIPAA regulations significantly increased the obligations for business associates and their subcontractors.

Recent Changes under the HITECH Act

HHS/OCR recently updated the HIPAA regulations to meet a number of new requirements put in place by the HITECH Act. Those changes were published in January 2013 and are effective as of September 23, 2013 (with an additional year available for covered entities to re-negotiate certain, existing BAAs). Most notable for NCRA members is that under the new regulations – sometimes referred to as the "HIPAA Omnibus Rule" – **business associates are now subject to direct regulatory enforcement**. Further, **business associates must now treat their subcontractors who create, receive, transmit, or maintain PHI in the same manner that covered entities treat their business associates** (*i.e.*, the business associate must execute a BAA with its subcontractors to flow down the obligations it has with the covered entity, and the regulations treat subcontractors in the same manner as business associates). Covered entities and business associates are responsible for their own workforces, including employees, volunteers, and others who are under their direct control. Typically, a business associate should treat its independent contractors as subcontractors for purposes of complying with the regulations. A covered entity or business associate may choose to impose specific requirements (*e.g.*, using a particular computer system or software) or provide training or other support to ensure that its business associates and subcontractors comply with the regulations. But ultimately, each business associate and subcontractor who signs a BAA is responsible for their own compliance with the regulations.

In addition, the HITECH Act provides for stepped up enforcement and imposes notification requirements, in the event that PHI is breached. Other notable areas of change in the regulations mainly impact covered entities and include restrictions on the use of genetic information; limits on marketing communications and the sale of PHI; the exclusion of data regarding those deceased for more than 50 years from the definition of PHI; support for simplified approaches to patient involvement in research studies; and relief for parents who wish

to permit covered entities to communicate with their children's schools regarding immunizations. Patient rights to receive electronic copies of their PHI and restrict access to certain data were also enhanced.

The HIPAA Regulations

The HIPAA regulations are organized into four key rules that each address a related set of duties and obligations for covered entities, business associates, and subcontractors:

1. The **Security Rule** (*See* 45 CFR 164.3xx) establishes requirements for **safeguarding electronic PHI** and is the **main focus for business associates and subcontractors**. Covered entities, business associates, and subcontractors must designate a security official, perform a risk assessment, meet organizational requirements (*e.g.*, establish appropriate BAAs), and implement and maintain administrative, physical, and technical safeguards to protect PHI. **The Security Rule recognizes the need to support "flexibility of approach" for implementing security measures, based on the size, complexity, infrastructure, and capabilities of a particular covered entity, business associate, or subcontractor, as well as costs and the level of risk to PHI.** So, NCRA members may customize their Security Rule compliance program, as is appropriate for their business. (*See* 45 CFR 164.306(b)).

   Examples of **administrative safeguards** include establishing security policies and procedures, risk analysis, risk management, reviewing information system activities, and establishing sanctions for those who violate security policies. Additional administrative safeguards include workforce training, managing access to PHI, and developing procedures to respond to security incidents and plans for contingencies such as system outages or other emergencies or disasters. **Physical safeguards** are simply measures to protect systems that store PHI from inappropriate access or use and include proper media disposal (*i.e.*, shredding or reliable data deletion/scrubbing). **Technical safeguards** encompass access controls, auditing capabilities, and other information technology measures such as data encryption that protect PHI and prevent unauthorized access or use.

2. The **Breach Notification Rule** (*See* 45 CFR 164.4xx) calls for covered entities to **notify affected individuals when PHI has been acquired, accessed, used, or disclosed in an unauthorized manner such that the privacy or security of the PHI is compromised**. The covered entity must provide information regarding breaches to the HHS Secretary on an annual basis, but in the event of a breach affecting 500 or more individuals, the covered entity must immediately notify the Secretary, and in many cases, the media. These large breaches are also listed on a HHS/OCR-maintained, publicly available website. While the regulations require the covered entity to notify affected individuals, business associates and subcontractors must notify their covered entities and business associates, respectively, according to the terms of their BAAs. **The new HIPAA regulations presume that an unauthorized use or disclosure of PHI is a breach, unless the covered entity, business associate, or subcontractor demonstrates that there is a low probability of compromise based on a formal risk assessment**. Certain situations are not considered breaches, such as unintentional, good faith access by a workforce member, inadvertent disclosure within a covered entity, business associate, or subcontractor organization, or disclosures where the

covered entity, business associate, or subcontractor has a good faith belief that the recipient would not have been able to retain the PHI.

3. The **Privacy Rule** (*See* 45 CFR 164.5xx) **limits the ways in which covered entities may use and disclose PHI, without patient authorization**. The Privacy Rule also requires that covered entities only disclose the "**minimum necessary**" amount of PHI to meet specific objectives, in most cases. So, for example, a covered entity should limit the amount of PHI it makes available to a business associate to only that required for the business associate to complete its tasks. Business associates should treat their subcontractors in the same manner. A business associate may perform a covered entity's duties under the Privacy Rule, such as responding to patient requests for access to certain records that contain PHI or supporting other patient rights. The services provided by NCRA members are unlikely to include these activities, but in the event that you do perform such functions, you must comply with the same Privacy Rule requirements as the covered entity. **If you are to provide patients with a transcript or other data that includes PHI, on behalf of a covered entity, then your BAA with that client should specifically permit you to make such disclosures.**

4. The **Enforcement Rule** (*See* 45 CFR 160.3xx-.5xx) specifies the processes and procedures that HHS/OCR uses to address potential violations of the HIPAA regulations. Civil money penalties, under the HITECH Act, may range from $100 to $50,000 per violation or a total of $1.5M for identical violations during a calendar year, based on the level of culpability.

The Business Associate Role – Why is My Client Asking Me to Sign a BAA? And, What Does It Mean For My Business?

The recent changes to the HIPAA regulations have caused most covered entities to review their compliance programs. Moreover, business associates such as lawyers and other service providers are now required to execute a BAA with their subcontractors. These factors make it much more likely that you are now being presented with BAAs, perhaps even for the first time. Under the HIPAA regulations, BAAs must include ten specific provisions, even if those terms do not apply to the particular services you may be providing to a covered entity (as a business associate) or to a business associate (as a subcontractor). Thus, you should expect a BAA to:

1. Establish the ways that the business associate (or subcontractor) is permitted to use and disclose PHI.
2. Provide that the business associate (or subcontractor) may not use or disclose PHI in any other manner.
3. Require that the business associate (or subcontractor) implement safeguards, consistent with the Security Rule.
4. Require the business associate (or subcontractor) to report any unauthorized use or disclosure of PHI, including breaches.
5. Ensure that the business associate (or subcontractor) supports patient rights, including accounting of disclosures (with proper data collection) and PHI access and amendment, under the Privacy Rule.

6. Obligate the business associate (or subcontractor) to comply with the applicable requirements, if it is carrying out any of the covered entity's duties or obligations under the Privacy Rule.
7. Require that the business associate (or subcontractor) make its internal practices, books, and records regarding its PHI-related activities and compliance with the HIPAA regulations available to HHS, in the event of a request or investigation.
8. Call for the business associate (or subcontractor) to either destroy or return any PHI at the BAA's termination, or if destruction is not feasible, to continue to safeguard the PHI.
9. Require that the business associate (or subcontractor) ensure any of its subcontractors agree to the same restrictions and conditions regarding PHI (*i.e.*, execute a BAA that flows down substantially similar provisions).
10. Authorize termination of the BAA, if the business associate (or subcontractor) violates a material term.

In addition to these required provisions, covered entities will often impose additional requirements on their business associates, in an effort to lower their own risk. For example, a covered entity may call for notification of any unauthorized use of PHI or a data breach within a specific, brief period of time, such as five or fewer business days. Covered entities also commonly seek indemnification from their business associates for any costs associated with breaches or other unauthorized uses of PHI. For instance, a covered entity may ask you to agree that you will take responsibility for any fines, litigation costs, or other expenses (*e.g.*, notifying affected individuals), if you or your workforce causes a data breach. Business associates often look to flow similar provisions down to their subcontractors. Before agreeing to any BAA provisions that call for narrow timeframes or other limits, or that go beyond the ten required elements described above, you should carefully review and consider the obligations, potential risks, and your available resources. In such circumstances, you should also consider seeking specific legal advice.

Keep in mind that as a business associate (or subcontractor), you must (1) comply with the HIPAA regulations; and (2) execute a BAA with any subcontractors who assist you in providing services that involve creating, receiving, transmitting, or maintaining PHI. For instance, you should have a BAA in place with independent contractors you hire to provide applicable services to clients with whom you have a BAA. You should also execute a BAA with vendors, such as information technology service providers, if they have access to the PHI that you create, receive, transmit, or maintain. To meet their HIPAA obligations, health care providers typically have specific controls in place to store and share documents that contain PHI in a secure manner. You should inquire with any such clients regarding how they would like you to store and share their information (for example, unsecured e-mail is typically not an appropriate way to transmit PHI, unless a patient specifically requests you to do so, after being warned of the risk that such information may be available to third parties). If you use cloud services to create, receive, transmit, or maintain PHI, then you will need to execute a BAA with them. Increasingly, cloud storage services, and other information technology providers, recognize HIPAA's requirements and will be prepared to answer your questions and take appropriate actions. You are also responsible for maintaining reasonable oversight and governance for your subcontractors.

Key Compliance Steps

Complying with the HIPAA regulations may seem daunting, but there are resources available to help you and some simple steps you can take now to get started:

- **Review BAAs**. Collect and maintain any BAAs that you have executed and periodically review them to ensure that you understand the requirements and maintain compliance.
- **Perform a risk analysis.** This includes documenting when and how you handle PHI, where it is stored, and how you protect it. Compare your safeguards to those required by the Security Rule and resolve any gaps that you identify.
- **Train your workforce.** Ensure that you and your employees understand your HIPAA obligations, and hold your subcontractors to the same standards.
- **Implement safeguards.** Recognize that the HIPAA regulations allow you to select an approach that is appropriate for the size and complexity of your business. For example, investigating the use of secure email, encryption for your mobile devices, proper access controls to limit who can access PHI, and cloud computing services that comply with HIPAA requirements are great places to start.
- **Manage your subcontractors.** Keep track of subcontractors who handle PHI and ensure that you have executed appropriate BAAs.
- **Develop a breach response plan.** Consider and document how you would handle a data breach that involves PHI *before it happens*. Who will you notify? How long do you have to respond? How will you mitigate risks? What other actions will you take to investigate and resolve the event?
- **Document your HIPAA compliance program.** Think like an auditor – what would you like to see to demonstrate your compliance program fitness? Put together a simple compliance notebook (online or on paper) that describes the steps you have taken and tracks your ongoing activities.
- **Seek advice specific to your business situation and needs.** Utilize available resources and seek specific legal advice when you have detailed questions or concerns.

Regulations pertinent to other industries, and some state laws, may also require that you implement certain privacy and data protection controls. For example, most states have a breach notification statute that applies in the event of unauthorized access or loss of certain personally identifiable information. Some states, like Massachusetts, also require that those who handle personally identifiable information have a written information security program ("WISP") in place. You can simplify your compliance programs by creating a single set of safeguards and documentation that address these various requirements, since such laws and regulations generally recognize the use of best practices for data protection.

Resources

- HHS/OCR provides a variety of resources for covered entities and business associates (including subcontractors) on their website at www.hhs.gov/ocr.

- The HITECH Act also called for HHS/OCR to implement a proactive HIPAA compliance auditing program. The initial audit protocols are available on the HHS/OCR website and provide a good checklist for performing your own self-assessment (*See*

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html). If you have a smaller organization, then you may need to simplify or adapt the protocols to your needs.

- The actual HIPAA regulations are codified in the Code of Federal Regulations, Title 45, Parts 160, 162, and 164. A combined version of the regulation text is available for download at http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html.