The HIPAApotamus in the Room: When Lawyers and Law Firms are Subject to HIPAA Enforcement, And How to Comply with the Law
by Leslie R. Isaacman, J.D., M.B.A.

The Omnibus Final Rule[1] of the Health Information Portability and Accountability Act[2] ("HIPAA") extended liability from covered entities[3] ("CEs") to business associates[4] ("BAs") for failing to safeguard protected health information[5] ("PHI") pursuant to the HIPAA Privacy, Security, and Breach Notification Rules. This change imposed, for the first time ever, direct accountability on business associates, with applicable civil and criminal liability, to comply with HIPAA rules. As a result, business associates are now required to protect PHI the same way that covered entities do.

In addition, the Health Information Technology for Economic and Clinical Health ("HITECH") Act[6] regulations have expanded the definition of business associates to include patient safety organizations, health information organizations, and subcontractors. Under HITECH's definition, attorneys who provide services for covered entities (or other business associates) and handle PHI are considered business associates.[7] Legal services fall squarely within the purview of HIPAA when a lawyer contracts directly with a covered entity.

Further, HITECH extended compliance obligations indefinitely to downstream subcontractors who provide services to business associates of covered entities. As a result, these so-called "subcontractor business associates" face the same obligations for compliance as first-tier business associates who contract directly with covered entities. Thus, even entities who may not realize it could face legal and enforcement risks and obligations under HIPAA and HITECH.[8]

Determining Whether You Are a Business Associate

Any person or entity, including any attorney or law firm, who receives PHI for purposes of doing something on behalf of a covered entity, business associate, or subcontractor, such as providing legal advice, is a business associate. Thus, even attorneys who don't technically practice in the field of health care law may be subject to HIPAA obligations when they receive PHI from their covered entity, business associate, or subcontractor clients.[9] Specifically, an attorney is considered a business associate when he or she, for example:

- Provides compliance support or defense to CEs, BAs, or subcontractors (whether or not in response to an enforcement action);
- Represents a CE, BA, or subcontractor in audits or governmental investigations;
- Represents a CE, BA, or subcontractor in any case involving individual patient diagnosis, treatment, or health benefits;

- Represents a CE, BA, or subcontractor in transactional work of any nature that involves access to any PHI (including, for instance, accounts receivable or payable information);
- Provides representation regarding health care professional discipline, payment or billing disputes, compliance advice, peer review, guardianships, informed consent, end-of-life issues, accreditation, licensing, administrative matters, risk management issues, or the like;
- Represents a CE, BA, or subcontractor in matters seeking to enforce restrictive covenants when PHI access is involved; and
- Responds to a subpoena requesting PHI in any form.

Notably, an attorney may unwittingly become a business associate by virtue of being hired by an existing business associate of a covered entity. For example, if a hospital's printing vendor, which receives and stores PHI, hires an attorney to provide legal services and then provides the attorney with access to the hospital's PHI, the attorney for the vendor becomes a subcontractor business associate.

As an attorney or law firm, it's your obligation to recognize when you are or could be considered a business associate and to then comply with the HIPAA Privacy and Security Rule provisions applicable to business associates. Non-compliance can lead to hefty fines and intrusive governmental investigations, and it can also lead to additional liability by your covered entity or business associate clients.

Complying with the Law as a Business Associate

Because of the HITECH Act, business associates are now directly and specifically liable for complying with the HIPAA Privacy,[10] Security,[11] and Breach Notification[12] Rules. To demonstrate compliance, lawyers and law firms must take specific actions under the law.

Lawyers must implement business associate agreements with their CE or BA clients and with their subcontractor BAs. Law firms must ensure that written policies and internal processes for compliance are established and reviewed, and firms should designate privacy and security officers who are responsible for compliance and training. In addition, lawyers and law firms are charged with actively protecting the confidentiality of any PHI they receive, create, or maintain electronically via encryption, and they must implement administrative, physical, and technical safeguards[13] for handling PHI. Further, law firms must conduct risk analyses, along with follow-up implementation of policies and procedures, to ensure compliance and detect potential vulnerabilities. Finally, lawyers and law firms must comply with the requirements and procedures for breach notification.

Business Associate Agreements

Business Associate Agreements ("BAAs") are contracts that specifically define how business associates can use and disclose PHI when performing services.[14] In general, BAAs should, at a minimum, include the following:

- A designation of permitted and prohibited uses of PHI by the BA;
- A requirement for the BA to implement "appropriate safeguards" to protect PHI;
- A requirement for reporting "security incidents" to the CE and for compliance with "breach notification" requirements;
- An agreement for BAs to properly establish that any subcontractor BAs are in compliance and report as required;[15]
- Allowances for access, amendments, and accounting of disclosures by the CE;
- Assurances that a BA's "internal practices, books, and records" are available for governmental review and audits;
- A provision for the return or destruction of PHI upon termination;
- Assurances that any PHI used or disclosed meets the "minimum necessary" standard of HITECH;[16] and
- An authorization for termination of the relationship upon any material breach of the BAA.

In addition, due to the potential exposure for liability under the Breach Notification Rule, CEs and BAs may want to consider including an indemnification provision in their BAAs.

Business associates have long been required to enter into BAAs with their covered entity clients. Under the law, covered entities are not allowed to disclose PHI to their lawyer business associates if there is no properly-executed BAA between them to ensure that PHI is appropriately safeguarded. Thus, as an initial step, attorneys and law firms representing covered entities must ensure that a proper BAA has been implemented.

Engaging Subcontractor Business Associates

In carrying out his or her duties as a business associate, an attorney may need to engage the services of a subcontractor business associate, such as software vendors, copy and printing services, document disposal services, expert witnesses, jury consultants, or billing services. These subcontractor BAs are equally subject to liability, and business associates should take active steps to ensure their subcontractor BAs are in compliance.

Under the HIPAA Omnibus Final Rule and the HITECH Act regulations, business associates must obtain "satisfactory assurances" that subcontractor BAs will safeguard any PHI in their possession. To do so, business associates must enter into BAAs with their downstream

subcontractors to monitor compliance. Just as it does with covered entities, the BAA provides the business associate with "satisfactory assurances" that its subcontractors will safeguard and protect any PHI in their possession.

Specific Privacy and Security Safeguards

Business associates are required by the HIPAA Privacy Rule to establish written policies and procedures that address the permitted uses and disclosures of PHI. BAs are also required to designate a "privacy officer" who is responsible for compliance and for training employees on HIPAA as well as internal privacy policies.

Under the HIPAA Security Rule, business associates must implement specific administrative, physical, and technical safeguards to protect against real and potential threats of disclosure or loss. BAs must also designate a "security officer" who is responsible for compliance and for training employees on HIPAA as well as the BAs internal security policies.

In addition, business associates must conduct an entity- and system-wide "risk analysis" to determine potential vulnerabilities to breaches, and they must effectuate policies to remediate risks. The law requires covered entities and business associates to conduct a risk analysis to assess "potential risks and vulnerabilities to the confidentiality, integrity, and availability" of electronic PHI ("ePHI").[17] Risk analysis is the first step in identifying and implementing safeguards for compliance with applicable law. Notably, enforcement agencies look first to risk analyses conducted by CEs and BAs, and the failure to perform such risk analyses is the main reason that entities fail governmental audits. Upon completion of a risk analysis, the CE or BA must then put into effect policies and procedures to mitigate or remediate any identified or potential risks or vulnerabilities.

Through the HIPAA Omnibus Final Rule and the HITECH Act regulations, the government has provided a clear message to covered entities and business associates that ePHI (*i.e.*, any PHI that exists or is stored in electronic media) should be encrypted.[18] Encryption is "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[19]

While all privacy and security risks cannot ever be fully eliminated, attorneys should take steps to determine how to ensure that exposure is minimal and risks are reduced as much as possible. Some key areas for concern for business associates to consider include:

- Encryption (or lack thereof);
- Unprotected internet, web browsing, and cookies;
- Network firewall protections;

- Hackers, phishing, ransomware, and other cybersecurity risks and threats;
- Mobile devices and password protections;
- Data sharing;
- Lack of physical security with files and documents containing PHI; and
- Staff training and compliance.

Business associates should consider all potential risks and then take steps to enact policies, procedures, and training with respect to any prospective vulnerabilities. For instance, a law firm that serves as a BA should maintain and enforce a policy and procedure on password requirements for all employees who have smartphones and other mobile devices that may contain PHI.

Breach Notification Rule

The Breach Notification Rule requires business associates to notify their covered entities following the discovery of any breach of unsecured PHI.[20] When breaches occur, business associates must perform additional risk assessments to determine the probability of data compromise, the nature and extent of PHI involved, details of the disclosure, and the extent to which the risk has been mitigated.

"Unsecured PHI" is useable, readable, or decipherable to unauthorized persons; in comparison, "secured PHI" is unusable, unreadable, or undecipherable.[21] PHI can become secured only through encryption or destruction; firewalls and access controls (such as passwords) are not sufficient for ensuring that PHI is secured.[22] A "breach" is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security and privacy of the information (except where an unauthorized person to whom the PHI is disclosed would not reasonably have been able to retain such information).[23] Pursuant to the HIPAA Omnibus Final Rule, unauthorized disclosures are presumed to be a breach unless the covered entity or the business associate can demonstrate, through a risk assessment, that there is a "low probability that the PHI has been compromised."[24]

A covered entity must provide notification of any breach within 60 days of discovery (*i.e.*, when the breach was discovered or reasonably should have been discovered). Notably, a

covered entity or a business associate is presumed to have knowledge on the day that any employee or agent has knowledge of the breach.

Penalties Applicable to Business Associates for Violations of HIPAA

HIPAA, through the Omnibus Final Rule, adopted significant civil and criminal penalties for enforcement. Following HITECH, there has been an increased emphasis on enforcement and an increase in fines and penalties issued by the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR"). Based on the updates in the law, business associates are now susceptible to direct criminal and civil liability.

The Omnibus Final Rule provides formal authority for bringing criminal charges against employees of both covered entities and business associates for failure to comply with HIPAA. The Rule invokes scaled criminal penalties for violations of HIPAA as follows:

- For knowing violations of HIPAA: fines of up to $50,000 per violation and/or up to 1 year imprisonment;
- For using false pretenses to violate HIPAA: fines of up to $100,000 per violation and/or up to 5 years' imprisonment; and
- For violations with intent to gain personally or commercially from the misuse of PHI: fines of up to $250,000 per violation and/or up to 10 years' imprisonment.

The Omnibus Final Rule also provides for civil monetary penalties through a tiered system based on knowledge and culpability:

- Lack of knowledge: fines of between $100 and $50,000 per violation;
- Reasonable cause: fines of between $1,000 and $50,000 per violation;
- Willful neglect (corrected): fines of between $10,000 and $50,000 per violation; and
- Willful neglect (not corrected): fines of $50,000 per violation.[25]

With these new penalties and fines available, OCR is substantially increasing its investigative staff in efforts to conduct additional audits to test the HIPAA compliance of both covered entities and business associates.

On March 21, 2016, OCR announced that it was implementing its next phase of audit processes. OCR plans to audit a broad range of covered entities and business associates of various types, sizes, and locations. This announcement marks the first time that business associates are being specifically targeted by the OCR for audits. Covered entities are being asked to provide information about their business associates, who could then become potential audit targets. Based on the results of the audits, OCR may pursue further compliance review and, potentially, enforcement actions against business associates.

Conclusion

Based on the HIPAA Omnibus Final Rule and the HITECH Act regulations, attorneys and law firms who receive PHI from their covered entity or business associate clients are now subject to audits as well as criminal and civil liability that had heretofore only been enforced against covered entities. As a result, lawyers and law firms now have a specific obligation to ensure compliance with the law. Under HIPAA, even non-health care attorneys can be considered business associates. Thus, all lawyers should be aware of the law and understand that it is the responsibility of the lawyer and the law firm to ensure compliance with the applicable and stringent requirements.

---

[1] 78 F.R. 5566 (2013).

[2] Pub. L. No. 104-191 (1996).

[3] Covered entities include health plans, health plan clearinghouses, or health care providers who transmit any health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted a standard. 45 C.F.R. § 160.103; 65 F.R. 82462 (2000).

[4] Business associates include any person or organization with whom the CE has an agreement to perform (or assist in the performance of) a function or activity involving the use or disclosure of individually identifiable health information. 45 C.F.R. § 160.103.

[5] Protected health information includes individually identifiable health information that is transmitted by or maintained in electronic media or any other type of media. 45 C.F.R. § 164.103.

[6] 45 C.F.R. §§ 160 and 164 (2013).

[7] 45 C.F.R. § 160.103(a).

[8] Notably, other privacy and security related federal and state laws may apply. See, e.g., Tenn. Code Ann. § 47-18-2107.

[9] Attorneys and law firms are specifically ***not*** subject to HIPAA requirements when they represent patients or are involved in workers' compensation cases. 45 C.F.R. § 164.512(1).

[10] Privacy is defined as the individual's right over the use and disclosure of his or her PHI, and it includes the right to determine when, how, and to what extent PHI is shared. The Privacy Rule grants rights to individuals for accessing and controlling the use or disclosure of their PHI. 45 C.F.R. § 164.502.

[11] Security is defined as the specific measures that an entity must take to protect PHI from any unauthorized breaches of privacy, and it includes measures taken to ensure against the loss of integrity of PHI. The Security Rule requires all CEs and BAs to develop and document a security program to guard against disclosure or loss, including policies and safeguards to protect electronic PHI. HIPAA requires general security measures that are both "reasonable and appropriate." 45 C.F.R. §§ 164.304, 164.306.

[12] 45 C.F.R. § 164.410.
[13] 45 C.F.R. §§ 164.308, 164.310, 164.312.
[14] 45 C.F.R. §§ 164.314, 164.504.
[15] 45 C.F.R. § 164.504(e)(2)(ii)(D).
[16] 45 C.F.R. § 164.502(b).
[17] 45 C.F.R. § 164.308(a)(1)(ii)(A).
[18] 45 C.F.R. § 164.312.
[19] 45 C.F.R. § 164.304.
[20] 45 C.F.R. § 164.410.
[21] 45 C.F.R. § 164.402.
[22] 45 C.F.R. §§ 164.304, 164.312.
[23] 45 C.F.R. § 164.402.
[24] 45 C.F.R. § 164.402.
[25] 45 C.F.R. § 160.404(b).