The Impact of HITECH on Business Associates, Including Attorneys

By Suzanne D. Nolan

FAST FACTS:

Business associates now have a statutory obligation to comply with the Health Insurance Portability and Accountability Act and are liable for civil monetary penalties for failing to comply.

Among other things, compliance requires business associates to adopt written security programs to safeguard protected health information stored in electronic form and to limit disclosures of such information to the uses authorized in the required written business associate agreement.

Attorneys need to recognize when they or their clients are business associates.

The Health Information Technology for Economic and Clinical Health (HITECH) Act[1] has changed the regulatory landscape for "business associates." Under the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations,[2] a business associate is a service provider who, on behalf of a covered entity[3] (but other than as a member of the covered entity's workforce), performs or assists in performing a function or activity that involves the use or disclosure of protected health information (PHI).[4] Before HITECH, business associates had only a contractual obligation to comply with the HIPAA Privacy and Security Rules, through a business associate agreement with a covered entity. Now, all business associates have a statutory obligation to comply with both HIPAA and HITECH. For the first time, business associates are subject to statutory penalties for a failure to comply with HIPAA's Privacy, Security, or Breach Notification Rules.[5]

This statutory compliance obligation arises if a service provider performs activities that bring it within the definition of a business associate, even in the absence of a business associate agreement and irrespective of how the service provider and covered entity label their business relationship.

The proposed implementing regulations for HITECH[6] intend to extend this statutory compliance obligation to a subcontractor of a business associate by defining the term "business associate" to include a subcontractor who creates, receives, maintains, or transmits PHI on behalf of the business associate.[7] If a subcontractor hires someone on its behalf to assist it in handling PHI, the subcontractor's subcontractor also becomes a business associate. Consequently, under the proposed HITECH regulations, almost anyone who touches PHI on behalf of a covered entity, either directly or indirectly, will be subject to a statutory obligation to comply with HIPAA.

Clients such as accountants, IT providers, copy centers, medical record storage companies, and document destruction companies frequently have access to PHI in the course of providing services and will need guidance regarding their compliance obligations.

HITECH's expansion of HIPAA compliance obligations may take attorneys who do not concentrate in health care law and their clients by surprise. Many attorneys do not realize that using or accessing PHI in the course of representing a client can make them a business associate.[8] Many clients who are business associates are not aware that they are now subject to statutory compliance obligations in addition to any contractual obligations they may have under a service agreement with the covered entity. Moreover, clients who are subcontractors of business associates are apt to be completely unaware of the proposal to regulate them as business associates.

Attorneys should be mindful that clients such as accountants, IT providers, copy centers, medical record storage companies, and document destruction companies frequently have access to PHI in the course of providing services and will need guidance regarding their compliance obligations.

Evaluating Compliance Obligations

Attorneys must become familiar with HITECH and HIPAA to recognize when a client may be a business associate. Attorneys should determine whether activities performed by a client make that client a business associate and, if so, advise the client about compliance obligations including the requirement to enter into a business associate agreement, described in detail below. When representing a business associate, an attorney will need to determine if his or her representation of the client involves use of or access to PHI. If it does, then the attorney must enter into a business associate agreement with the client and otherwise comply with HIPAA.

Attorneys also should be mindful of when they are apt to encounter PHI during the course of representing a client. Attorneys tend to think of themselves as not being subject to HIPAA except when working with health insurance claims, billing information, or information directly describing a patient's health condition or treatment. However, because the definition of PHI is fairly broad,[9] attorneys are apt to handle PHI when they (1) represent a covered entity or a business associate in enforcing a restrictive covenant against an employee who is soliciting patients of the covered entity or who has disclosed patient data to a new employer, (2) provide representation in the sale or purchase of a covered entity or business associate and have access to a patient list or a detailed list of accounts receivable, or (3) represent a covered entity or business associate in audits or governmental investigations.

Regulation of Business Associates

To comply with HIPAA, business associates must implement written privacy and security programs, the requirements of which are specified in the Privacy and Security Rules. These two rules interact to protect PHI and regulate business associates. The Privacy Rule applies to all forms of PHI, whether oral, written, or electronic. It sets forth standards for determining under which conditions PHI can be used or disclosed. The Security Rule applies only to electronic PHI (ePHI), which is PHI created, received, held, or transmitted in electronic format (i.e., transmitted over or downloaded from the Internet or stored on a computer or portable computing device, including smart phones and PDAs, or computer media such as thumb drives, CDs, and DVDs). The rule sets forth the standards for ensuring the confidentiality, integrity, and accessibility of ePHI.

Business Associate Agreements

Both the Privacy and Security Rules require covered entities to enter into a business associate agreement (BAA) with their business associates.[10] The Privacy Rule sets forth the bulk of the requirements for the BAA, while the Security Rule adds specific requirements pertaining to ePHI.[11] The proposed regulations similarly regulate the business associate-subcontractor relationship, requiring that the business associate and its subcontractor enter into and comply with a BAA.

The BAA must restrict uses and disclosures of PHI by the business associate to those set forth in the BAA and required by law.[12] The BAA cannot authorize the business associate to use or disclose PHI in any manner that the covered entity could not, except for data aggregation and for the business associate's own administration and legal responsibilities.

In addition to the foregoing requirements, the BAA must provide that the business associate will:

- use appropriate safeguards to prevent unpermitted use or disclosure of PHI;
- comply with applicable requirements of the Security Rule;
- report to the covered entity known uses or disclosures of PHI not permitted by the BAA, breaches of unsecured PHI, and security incidents involving ePHI;
- ensure that its subcontractors and agents who work with PHI agree to the same restrictions (or a subset of such restrictions) and conditions that apply to the business associate;
- destroy or return PHI, if feasible, at the termination of the agreement, and if not feasible, use it only for the purpose that made it infeasible to return it;
- open its books and records to inspection by the U.S. Department of Health and Human Services; and
- make PHI available for access, amendment, and accounting of disclosures.

Additionally, the BAA must contain a provision permitting termination of the contract if a covered entity knows of a pattern of behavior by a business associate that violates the BAA.[13] The proposed regulations entail a similar provision requiring a business associate to terminate the BAA if it knows of such a pattern of behavior by a subcontractor.[14] A covered entity or business associate that fails to either cure the breach or to terminate the BAA under these conditions is in violation of HIPAA.

The responsibility for entering into a BAA is placed on the covered entity with respect to its business associate and, under the proposed regulations, on a business associate with respect to its subcontractors. Disclosing PHI in the absence of a HIPAA-compliant BAA or permitting a business associate (or, under the proposed regulations, a subcontractor) to create, receive, maintain, or transmit ePHI in the absence of a HIPAA-compliant BAA is a violation of HIPAA.

Requirement of a Security Program

HITECH requires a business associate, with respect to the ePHI it handles, to comply with the HIPAA Security Rule's administrative, physical, and technical safeguards; its organizational requirements; and its policies, procedures, and documentation requirements.[15] The Security Rule sets forth implementation specifications for the foregoing, some of which are required to be incorporated into the security program and some of which permit the use of a reasonable and appropriate alternative measure.

A business associate is required to develop a written security program that describes how it will meet each of the standards, safeguards, and requirements. Although technological controls such as passwords and firewalls and facility controls such as locks to restrict access to an office suite or server room are certainly important in protecting the security of ePHI, the majority of the standards are administrative and require (1) documented policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI; (2) the training of the business associate's workforce on those policies and procedures;[16] and (3) the updating of a security program in response to new security risks.[17]

Risk analysis is a required part of security-rule compliance and generally drives the development of a security program. Risk analysis is a comprehensive process that requires a business associate to inventory the PHI and ePHI that it holds or accesses, assess the risks to such ePHI that are present in the business associate's environment, assess the threats and vulnerabilities to such ePHI, assess the risk of and the extent of harm that could be caused by such threats, and consider the physical and technical security measures available to protect against and manage such risks. Such a risk analysis must be documented as part of the required written security program. Because the Security Rule does not generally require the use of specific security measures, business associates can adopt security practices consistent with the requirements of the Security Rule that are reasonable and appropriate given the resources of the business associate, its facilities and systems, and the manner in which it handles ePHI. A security program can be most effectively developed through consulting with computer security or IT experts who can conduct a risk analysis and recommend appropriate safeguards.

Given the risks associated with noncompliance, attorneys would be well advised to consult with health care attorneys and other HIPAA experts for advice on compliance obligations and the implementation of HIPAA-compliant privacy and security programs.

Breach Notification

HITECH also created a new compliance obligation for business associates, namely the obligation to report a breach of unsecured PHI. The Breach Notification Rule[18] requires a business associate to notify the covered entity of a breach of unsecured PHI. The proposed regulations require a subcontractor to report such breaches to the business associate on whose behalf it is performing services.[19] Both the Privacy and Security Rules specify that a provision requiring such reporting be included in the BAA.[20]

A breach of unsecured PHI means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI.[21] Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a methodology or technology specified by the secretary in the guidance.[22] Guidance by the secretary sets forth an encryption safe harbor based on using encryption methods described in various National Institute of Standards and Technology (NIST) publications.[23] Such guidance also sets forth a destruction safe harbor specifying shredding or destroying PHI in paper, film, or other media such that PHI cannot be read or reconstructed or clearing, purging, or destroying electronic media in accordance with NIST Special Publication 800-88.[24] Attorneys need to become familiar with the ways ePHI can be secured by rendering it unusable, unreadable, and indecipherable within the meaning of a safe harbor since the disclosure of ePHI so secured is not considered a breach.

Penalties

Penalties for noncompliance by business associates can be substantial and are based on the culpability of the business associate. Violations attributable to willful neglect, which is an intentional failure to comply with HIPAA or reckless indifference to a HIPAA compliance obligation, have a minimum penalty of $10,000 and can go as high as $50,000. Violations attributable to reasonable cause—the business associate knew or should have known through reasonable diligence that a violation occurred—have a minimum penalty of $1,000 per violation. Violations attributable to situations in which the business associate did not know or could not have known through reasonable diligence of the violation have a minimum penalty of $100.[25] Under the law of agency, a business associate can be held liable for a civil monetary penalty for the acts or omissions of its subcontractors.[26] These penalties are significant enough to encourage business associates to pay serious attention to HIPAA compliance obligations.

Concluding Comments

Attorneys need to review the HITECH final implementing regulations to determine if the proposal to regulate subcontractors as business associates is adopted. Attorneys also must recognize when they or their clients are business associates or the subcontractor of a business associate under HIPAA, and take the appropriate steps to comply with HIPAA. Noncompliance can lead not only to steep fines and government investigations, but also to the potential loss of an attorney's or client's reputation. Given the risks associated with noncompliance, attorneys would be well advised to consult with health care attorneys and other HIPAA experts for advice on compliance obligations and the implementation of HIPAA-compliant privacy and security programs. ■

Suzanne D. Nolan is a principal of Frank Haron Weiner. Her practice focuses on business and intellectual property transactions including trademark, patent, copyright licensing, and e-commerce transactions for all types of entities, with a focus on health care providers. She also advises health care clients on HIPAA, Stark, and Anti-Kickback Statute compliance and licensing matters.

FOOTNOTES

1. Title XIII of the American Recovery and Reinvestment Act of 2009, PL 111-5, 123 Stat 115 (2009).
2. The Health Insurance Portability and Accountability Act of 1996, PL 104-191, 110 Stat 1936; 45 CFR 160.103.
3. A covered entity is a health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. 45 CFR 160.103.
4. Pursuant to 45 CFR 160.103, "protected health information" is defined in part as individually identifiable information, including demographic information, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse and (2) 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.
5. The Privacy Rule is set forth at 45 CFR parts 160 and 164, subpart E; the Security Rule is set forth at 45 CFR parts 160 and 164, subpart C; and the Breach Notification Rule is set forth at 45 CFR parts 160 and 164, subpart D.
6. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed Reg 40868.
7. 75 Fed Reg 40912 through 40913 (proposed amendment to 45 CFR 160.103).
8. 45 CFR 160.103.
9. *Id.*
10. 45 CFR 164.502(e)(2); 75 Fed Reg 40919 (proposed amendment to 45 CFR 164.502(e)(2)).
11. 45 CFR 164.314(a)(2); 45 CFR 164.308(b).
12. 45 CFR 164.504(e)(2)(ii).
13. 75 Fed Reg 40920 (proposed amendment to 45 CFR 164.504(e)(5)).
14. 45 CFR 164.504(e)(2)(iii); 45 CFR 164.314(a)(2)(i)(D).
15. HITECH §13401(a), *supra*. HITECH did not directly state that business associates were required to comply with sections 164.306 and 164.314; such compliance was strongly implied. The proposed regulations state that business associates are required to comply with these sections.
16. 45 CFR 164.304(a)(5)(i).
17. 45 CFR 164.316(b)(2)(iii).
18. Subpart D of the HIPAA Regulations, 45 CFR 164.401 through 164.414.
19. 45 CFR 164.410(a)(1); 75 Fed Reg 40920 (proposed amendment to 45 CFR 164.504(e)(2)(i)(C)).
20. 45 CFR 164.504(e)(2)(ii)(C).
21. 45 CFR 164.402.
22. Guidance to Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information, 74 Fed Reg 19008.
23. *Id.* at 19009 through 19010, referring to NIST Special Publications 800-111, 800-52, 800-77, and 800-113.
24. *Id.* at 19010.
25. 75 Fed Reg 40914 (proposed amendment to 45 CFR 160.402).
26. *Id.*