

COMPLIANCE PERSPECTIVES



Stephen R. Bentfield

The HITECH Act: Is Your Organization Ready for Implementation?

While widespread adoption of interoperable electronic health records (EHRs) is still several years away, the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act of 2009 (ARRA)¹ is expected to facilitate use of EHRs by ensuring their privacy and security.

To that end, the HITECH Act expanded the privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by (1) broadening the scope of business associates to include organizations instrumental in EHR adoption, (2) applying certain HIPAA standards previously applicable only to covered entities to business associates, (3) establishing notification requirements for security breaches involving unsecured protected health information (PHI), and (4) strengthening penalties for HIPAA violations.

Because laboratories qualify as both covered entities and business associates under HIPAA, laboratories must understand the HITECH Act and assess its impact on existing information privacy and security policies, procedures, and practices.



Dianne J. Bourque

New Business Associate Obligations

HIPAA business associates face significant new obligations under the HITECH Act. In addition to the breach notification requirements discussed below, business associates are now subject to certain HIPAA privacy rule requirements and the entire HIPAA security rule, which previously applied only to covered entities.²

For the first time, HIPAA business associates are directly responsible for complying with HIPAA's implementation specifications for business associate agreements.³ If a business associate knows that the covered entity is improperly using or disclosing PHI in violation of the business associate agreement (BAA), the business associate now must take "reasonable steps" to stop the violation.⁴ An improper disclosure could occur if, for example, the covered entity repeatedly transmitted the wrong PHI to a business associate over the Internet. If the business associate cannot stop the covered entity's violation, it can terminate the BAA, or it must notify the secretary of the Department of Health and Human Services (HHS) if termination is not feasible.⁵

Although, The HITECH Act also expands the scope of business associate status to capture several types of organizations expected to be instrumental in the widespread adoption of EHRs.⁶ Examples include health information exchange



Karen S. Lovitch

Stephen R. Bentfield,
Dianne J. Bourque,
and Karen S. Lovitch
are attorneys with
the law firm of Mintz
Levin.

¹ See generally Title XIII of Pub. L. No. 111-5 (Feb. 17, 2009), 123 Stat. 115, 258.

² ARRA §13401(a).

³ ARRA §13404.

⁴ See 45 C.F.R. §164.504(e)(1)(ii) as modified by ARRA §13404(b).

⁵ ARRA §§13401, 13403.

⁶ ARRA §13408.

organizations, regional health information organizations, e-prescribing gateways, or contract vendors that allow covered entities to offer personal health records to patients as part of EHRs.

Federal Breach Notification Requirements

Covered entities and business associates should take note of the HITECH Act's breach notification requirements because the associated administrative, financial, and reputational costs can be substantial. Before enactment, covered entities had no affirmative obligation under federal law to notify a patient if his or her PHI was lost or stolen or if the privacy and security of the PHI was otherwise compromised. However, a covered entity (and a business associate in specific instances) now must provide notification of such activity in certain circumstances.

How Is a Breach Defined?

HIPAA defines a breach as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the privacy rule] which compromises the security or privacy of the protected health information" and that poses a "significant risk of financial, reputational, or other harm to the individual."⁷ HHS has provided minimal guidance on how to determine whether significant risk exists. HHS has only observed that improper disclosure of a name and the fact that the person was a patient at a hospital may not pose the requisite risk under this standard of harm.⁸ In contrast, if the disclosure included the type of services received (e.g., oncology treatment), the type of facility (e.g., drug and alcohol rehabilitation), or information that increased the risk of identity theft (e.g., Social Security number), then the probability is higher that significant risk could result.

There are three exceptions to the definition of "breach." A breach does not occur:

- ❖ Where an unauthorized person to whom such information was disclosed would not reasonably have the ability to retain such information;⁹
- ❖ The acquisition, access, or use of PHI by an employee acting under the authority of a covered entity or business associate was unintentional; or
- ❖ Disclosure from an individual authorized to access PHI at a covered entity or business associate to another person at the same facility was inadvertent.¹⁰

In these latter two instances, the PHI cannot be further used or disclosed without authorization.

When Is Notification Required?

If a breach occurs, notification is required only if it involves "unsecured" PHI. A covered entity can render PHI secure through one of two methods identified by HHS in guidance issued in April 2009.¹¹ First, electronic PHI is secured if it is encrypted in accordance with certain National Institute of Standards and Technology (NIST) specifications. Second, PHI, regardless of format, is secured if the media on which it is stored has been physically destroyed. Securing PHI through one of these methods allows a covered entity to avoid notifying affected individuals.

What Steps Must Be Taken When a Reportable Breach Occurs?

If a breach involves unsecured PHI, the covered entity must notify affected individuals without unreasonable delay, and in no event no more than 60 calendar days

⁷ See *id.*

⁸ See *Breach Notification for Unsecured Protected Health Information; Interim Final Rule*, 74 Fed. Reg. 42,740, 42,745 (Aug. 24, 2009).

⁹ ARRA §13400(1)(A).

¹⁰ See ARRA §13400(1)(B).

¹¹ See 74 Fed. Reg. 19,006 (April 27, 2009).

after discovering the breach.¹² The notice must include:

- ❖ A brief explanation of the event;
- ❖ The date of the breach and of its discovery;
- ❖ A description of the types of PHI involved;
- ❖ The steps that affected individuals should take to protect against potential harm resulting from the breach;
- ❖ A brief description of the covered entity's response, including steps to investigate and mitigate harm, and to prevent future breaches; and
- ❖ Contact procedures for follow-up questions and additional information.¹³

The method of notification varies depending upon the number of affected individuals, and the financial burden can be substantial.¹⁴ At a minimum, written notification must be given by first-class mail to the individual's last known address or to next of kin (when applicable).¹⁵ If a covered entity has insufficient or out of date contact information for 10 or more individuals, it also must conspicuously post notice of the breach on its Web site or in major media outlets in the affected area and maintain a toll-free breach information hot line.¹⁶

Breaches affecting more than 500 individuals may require two additional—and potentially costly—notification requirements. First, public notice must be provided via “prominent media outlets” of a breach affecting more than 500 residents of a state or jurisdiction.¹⁷ Second, covered entities must notify HHS of security breaches affecting 500 or more individuals, which HHS must publish on its Web site.¹⁸ The HHS Office of Civil Rights (OCR), which is responsible for HIPAA privacy enforcement, recently posted the initial list of breaches affecting 500 or more individuals,¹⁹ and most of the reported breaches resulted from the theft of unsecured hard copy or electronic PHI.

Luckily, not every incident amounts to a reportable breach under HIPAA. To determine whether reporting obligations apply, a covered entity should determine the answers to the following questions:

- ❖ Has a breach involving unsecured PHI occurred?
- ❖ How many patients' PHI was accessed, acquired, or disclosed, and what were the circumstances surrounding the incident?
- ❖ Does the disclosure fit within an available exception?
- ❖ Does the breach pose a significant risk of financial or reputational harm to the individual?

¹² ARRA §13402(d)(1). A breach is considered discovered by a covered entity as of the first day on which such breach was known, or by exercising reasonable diligence would have been known, to the covered entity. See ARRA §13402(c). Business associates are held to the same notification deadline as covered entities, but the relationship to the covered entity affects when the covered entity must provide notice. ARRA §13402(b), (d) (1). If a business associate is an agent, the date on which the business associate discovered the breach is imputed to the covered entity, and the notice deadline is based on the date the business associate discovered the breach. However, if the business associate is an independent contractor, then the notice deadline is based on the date the business associate notified the covered entity of the breach. See 74 Fed. Reg. at 42,754.

¹³ ARRA §13402(f).

¹⁴ A recent *BusinessWeek* article reported on a theft of 57 hard drives from a BlueCross BlueShield of Tennessee training center that has cost the carrier over \$7 million to resolve. Robert McMillan, “Data Theft Creates Notification Nightmare for BlueCross,” *BusinessWeek*, March 2, 2010.

¹⁵ ARRA §13402(e)(1)(A).

¹⁶ ARRA §13402(e)(1)(B).

¹⁷ ARRA §13402(e)(2).

¹⁸ ARRA §13402(e)(3) and (4).

¹⁹ See <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html> (accessed Feb. 23, 2009).

Do Federal and State Breach Notification Requirements Differ?

In some instances, additional steps may be necessary to comply with state data breach laws. For example, state data breach laws often apply to Social Security numbers and certain financial information maintained electronically. In contrast, HIPAA applies more broadly to PHI and does not distinguish between hard copy and electronic PHI. Similarly, state data breach laws may impose tighter deadlines or different notification procedures or may be triggered only if the breach affects a certain number of residents.

As a business associate as well as a covered entity, a laboratory should consider its reporting obligations if a breach occurs. If the laboratory was acting as a business associate, its obligation is to the covered entity, and the laboratory must comply with any notification requirements imposed by it. Absent any contractual obligations to the contrary, the covered entity must perform the risk assessment and provide notification. However, if the laboratory was acting as a covered entity, it must take all actions required by law.

Enhanced Enforcement and Penalties

The HITECH Act also expanded HIPAA enforcement powers and penalties. Covered entities therefore can expect more active HIPAA enforcement through increased civil monetary penalties (CMPs) and expanded authority for state attorneys general to bring civil HIPAA enforcement actions. HHS previously could impose CMPs ranging from \$100 to \$25,000 per HIPAA violation, but a covered entity now may face escalating CMPs of up to \$1.5 million per calendar year.²⁰ The new violation categories require penalty determinations to be based on the nature and extent of the resulting harm:²¹

Violation Category	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
Covered entity did not know of the violation	\$100-\$50,000	\$1,500,000
Software Violation due to reasonable cause and not willful neglect	\$1,000-\$50,000	\$1,500,000
Violation due to willful neglect but corrected within 30 days of discovery	\$10,000-\$50,000	\$1,500,000
Violation due to willful neglect but not corrected within 30 days of discovery	\$50,000	\$1,500,000

The HITECH Act also authorized state attorneys general to bring civil actions in federal district court on behalf of residents who have been threatened or adversely affected by a HIPAA violation.²² Under this authority, an attorney general can seek an injunction or damages of \$100 per violation, not to exceed \$25,000. Although these numbers may seem insignificant, related adverse publicity carries its own cost. Connecticut Attorney General Richard Blumenthal was the first to exercise this new authority in bringing suit against Health Net of Connecticut Inc. for allegedly failing to secure patient medical records and financial information involving 446,000 Connecticut enrollees.²³ This case is still pending.

²⁰ ARRA §13410(d) (amending 42 U.S.C. §1320d-5(a)(1)).

²¹ 74 Fed. Reg. at 56,124.

²² ARRA §13410(e).

²³ See Connecticut v. Health Net of the Northeast, Inc., et al, No. 3:10-00057 (D. Conn. Filed Jan. 13, 2010).

Recommended Response to the HITECH Act's Changes

All covered entities, including laboratories, should review and revise their current business associate policies, identify all arrangements requiring a BAA, update template BAAs, and amend current BAAs. Given the increased liabilities associated with breach notification, covered entities and business associates likely will negotiate BAAs more actively than in the past, and some suggested revisions are discussed below.

BAAs should specifically address the new federal breach notification obligations and clearly establish which party bears the associated costs and responsibilities. Absent specific contract terms, the covered entity would be saddled with the entire cost and responsibility (not to mention adverse publicity) associated with a breach notification caused by a business associate. By revising BAAs to clarify which party bears the costs and responsibilities, a covered entity can equitably allocate this risk to the responsible party.

Additionally, BAAs should require business associates to report the discovery of any breach involving PHI to the covered entity promptly and to take appropriate steps to investigate and mitigate any harm. Because covered entities must give specific information to affected individuals, BAAs should require business associates to at least identify the affected individuals, describe the relevant facts and the type(s) of PHI involved, and explain the steps taken to investigate the breach and mitigate potential harm.

Finally, before contracting with a business associate, a covered entity should obtain adequate assurances that the business associate has implemented, or will implement, administrative, physical, and technical safeguards in accordance with the HIPAA security rule. Such assurances could come in the form of representations and warranties in the BAA, review of the business associate's HIPAA security policies and procedures, or both.

When acting as a business associate, a laboratory should carefully review any BAA received from another party and consider whether the laboratory functions as a business associate. For example, a laboratory should not execute a BAA received from a customer with which it no longer does business. A BAA is necessary only if one of the contracting parties is a covered entity, and the services or functions furnished by the business associate involve the use or disclosure of PHI. In addition, laboratories serving as business associates should keep track of various reporting obligations imposed by customers who are covered entities.

Conclusion

The HITECH Act and accompanying regulations are complex and far-reaching, and the potential penalties can be high for companies that fail to take appropriate steps. The HITECH Act therefore warrants careful review of existing privacy and security policies and procedures.

Stephen R. Bentfield, Dianne J. Bourque, and Karen S. Lovitch can be reached at Mintz Levin. Bentfield and Lovitch are in the firm's Washington, D.C., while Bourque is based in the firm's Boston office. Bentfield phone: 202-585-3515, e-mail: SRBentfield@mintz.com; Bourque phone: 617-348-1614, e-mail: DBourque@mintz.com; Lovitch phone: 202-434-7324, e-mail: KSLovitch@mintz.com. 