Putting It in Writing: Updating BA Agreements to Cover Breach Notification

By Beth Hjort, RHIA, CHPS, and Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA

When ARRA extended sections of the HIPAA privacy and security rules to cover business associates (BAs), it created a seismic shift in their contractual relationships with covered entities (CEs). Further, the changes became effective simultaneous with other ARRA amendments that require CEs and BAs to notify customers of breaches of their protected health information (PHI). Together the changes encourage BAs and CEs to jointly revisit their communication and work processes to meet the new regulations.

The focal point of their review will likely be the business associate agreement (BAA). At a minimum, covered entities, as the parties originating the PHI, should review each BAA with the guidance of their legal counsel.

Upon review, CEs may choose to retain existing agreements, or they may opt to add general contract terms such as the "business associate will comply with all present and future laws and regulations." However, those CEs that choose to modify their BAAs can use the opportunity to establish clear responsibilities and roles in breach prevention and management. Doing so will best position them to deter breaches, and should one occur, investigate and report it as necessary.

The Breach Notification Requirements

The breach notification requirements apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI. The provision appears in section 13402 of the act.

ARRA required the Department of Health and Human Services to promulgate rulemaking on the provision, which it did through an interim final rule issued by the Office for Civil Rights in September 2009. The rule became effective the same day, with full compliance beginning February 2010. OCR has yet to publish a final rule; at press time, no date had been announced.

Effective breach notification compliance is a coordinated, shared responsibility, though the CE holds the greater responsibility because it is the primary custodian of the data. The necessity for a formal coordinated response is even more significant considering that entities must notify affected consumers without unreasonable delay and within 60 days.

The BAA should avoid any ambiguity in roles by defining key terms in the agreement, and all definitions should be taken directly from the regulations. Clear understanding will help ensure compliance. Terms to define include covered entity, business associate (both as an agent and as an independent contractor), protected health information, and breach (including the definition of unsecured PHI).

Establishing an Ongoing Security Program

Through the agreement, the CE should set an expectation that the BA maintain an ongoing security program in line, at a minimum, with that specified in the HIPAA security rule. The BA should have in place security administration activities to assess, monitor, prevent, and mitigate security threats. The BA's security administration should be in compliance with the CE's program and approved by the CE. The program should include reasonable systems for discovery of breaches and a formal response plan should a possible breach be discovered.

As part of its risk assessment activities, the BA should:

- Inventory and prioritize assets
- Identify threats and vulnerabilities

- Review existing security controls
- Determine the likelihood of exposure
- Determine the impact of a security breach
- Prioritize and mitigate identified risks
- Establish a security incident response team

The plan of action for a potential breach should include an audit plan, harm threshold, response triggers, communication protocol, chain of command, contact information, back-up contact information for key responsible parties at the BA and CE, education, training, mitigation process, breach notification timeliness, content, and methods of the notice.

The BA should ensure that provisions of the BAA are contained in the agreements it holds with its subcontractors that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI.

Encryption

Under the regulation, a breach occurs only when PHI is unsecured. For this reason, CEs can consider requiring that the BA employ technologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals that are consistent with National Institute of Standards and Technology guidance.

The BA and CE shall jointly commit to establishing the necessary encryption technical requirements to allow for the secure exchange of encrypted PHI.

Workforce Training and Education

The BAA should require that BA workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.

The BAA can also commit the CE to ensuring its own workforce members and agents receive similar training and awareness. Furthermore, the CE can assist the BA in training workforce members and other agents on specific or unique CE processes.

Breaches Treated as Discovered

The breach notification rule requires that a breach be treated as discovered by a CE the first day it is known to the CE or should have been known by exercising reasonable diligence.

A CE is deemed to have knowledge of a breach if the breach is known or would have been known by exercising reasonable diligence to any person who is a workforce member of the covered entity, which by definition includes BAs.

The BAA can establish that the BA treat all breaches as discovered and allow the CE to set a limit on the number of days between when the BA discovers a potential breach and reports it to the CE. This will help ensure that the CE and BA can meet the requirement to notify consumers within 60 days of the discovery.

Establishing a System for Discovery of Breaches

Because a CE or BA can be liable for failing to provide notice of a breach, it is important that the BAA require implementation of reasonable systems for discovery.

BAA obligation begins at the discovery of a breach and continues as long as related activity continues, until all effects of the information breach are mitigated. Because the regulation provides for private right of action, the BAA should address the obligations of all parties.

The agreement must address all points of collaboration supportive of efficient resolution. It should establish agreed-upon mitigation timelines as well as clearly stated responsibilities for notification and mitigation.

The BAA should make clear that matters pertaining to PHI privacy and security shall be resolved to the satisfaction of the CE's compliance requirements.

The BAA should designate and provide a point of contact, back-up point of contact, applicable phone numbers, e-mail address, and other contact information both on and off business hours for the CE and BA. The designated point person could be the staff member serving as the entity's privacy official.

The BA can be expected to complete or participate in an investigation and risk assessment following a suspected information breach. The agreement should describe how the CE and BA will collaborate on the performance of a risk assessment to determine if an impermissible use or disclosure of PHI constitutes a possible information security breach.

The stated objective of the risk assessment should be to determine if a significant risk of harm to the individual exists as a result of the impermissible use or disclosure. The assessment should determine if a harm threshold has been crossed and a significant risk of financial, reputational, or other harm to the individual exists.

Should the assessment determine that a breach has occurred and a significant risk of harm exists, the BAA should establish how the BA and CE will work to notify individuals and mitigate the negative impact of the breach.

Resources

AHIMA. "How to React to a Security Incident." *Journal of AHIMA* 79, no. 1 (Jan. 2008): 66–70.

Department of Health and Human Services, Office for Civil Rights. "Standards for Privacy of Individually Identifiable Health Information." Available online at www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt.

Office for Civil Rights. "45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule." 2009. Available online at http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

Rhodes, Harry. "Letters of Agreement and Contract (Updated)." 2003. Available online in the AHIMA Body of Knowledge at www.ahima.org.

Beth Hjort is a former professional practice manager at AHIMA. **Harry Rhodes** (harry.rhodes@ahima.org) is director of practice leadership at AHIMA. This article is adapted from the paper "Healthcare Breach Management: Business Associate Agreement Addendum," originally published January 2010 online at www.ahima.org/advocacy.

Article citation:
Hjort, Beth M.; Rhodes, Harry B.. "Putting It in Writing: Updating BA Agreements to Cover Breach Notification" *Journal of AHIMA* 81, no.6 (June 2010): 52-53.