HIPAA Changes Call for Revising BA Agreements

Save to myBoK

By Jan McDavid, Esq., JD

Business associates (BAs) of HIPAA-covered entities like hospitals and doctor's offices should already be intimately acquainted with HIPAA's privacy and security regulations. BAs should already have business associate agreements with every covered entity with whom they work and assume responsibility for everything they do with protected health information. So it seems improbable for BAs serving HIM professionals to be surprised or unaware that they are now-officially-on the hook for breaches of personal health information. Some may be surprised, however, because the new HITECH HIPAA modification "omnibus" final rule, released in January, has installed new and updated requirements for BAs and subcontractors.

New Rules, But Few Surprises

There were no real surprises, and little drama, surrounding the Department of Health and Human Services' release of the new HIPAA rule in January. In the past, if BAs were responsible for a breach, the covered entity could be fined. Typically following the incident, the covered entity would recover the cost of remediation from the business associate. Under the new HIPAA privacy rule, modified by the HITECH Act, the government can fine BAs directly. However, there was a slight variation from industry expectations. Many in HIM expected the new rule would require a breach notification letter to be sent to every patient in every instance of a breach. Instead, under the new rule, the HIPAA-covered entity must notify the patient after a risk assessment has been done and a determination has been made that there was, in fact, a compromise of personal health information. This change has made the risk assessment process ultimately more important to both covered entities and BAs.

Revamp Business Associate Agreements

So what's the benefit of covered entities reaching out to BAs during this transition? First and foremost, it's the law. Covered entities are required to change the terms of their BA agreements to reflect the changes created by the modifications to HIPAA. Here are three steps to begin the process:

- Evaluate one's portfolio of BAs
- Arrange contracts and existing BA agreements in expiration date order to evaluate risk and/or priority
- Schedule when each BA should execute a new agreement

Note that if a BA agreement carries over from a date prior to the rule's January 25 publication date, it is grandfathered in and covered entities won't have to update the BA agreement until September 2014. HIM professionals entering into a new agreement or renewal with a BA should immediately change the agreement to include the new provisions outlined within the omnibus rule to ensure full compliance with HIPAA.

Once aligned and scheduled, each BA agreement should be evaluated for the following:

- Evaluate current liability and indemnification details regarding breach incidents.
- Evaluate to include the new required elements.
- Determine if the BA is classified as an "agent." If so, include stringent requirements for security reviews and documentation of compliance. If a BA is an agent of one's facility, it is still liable for its actions.

Make Subcontractors Comply

A business associate's subcontracted companies and subcontractors are also now responsible for protecting any HIPAA-protected health information to which they are privy. BAs must have an agreement with their subcontractors, and subcontractors will now be held to the same standard as business associates.

This requirement has unique ramifications in HIM, where outsourced medical transcription or coding companies may subcontract work to a third party. Complete outsourcing transparency and business associate agreements with each party involved must be in place to fully comply with HIPAA.

Just like BAs, subcontractors must apply all security, privacy, and disclosure rules. They can only use personal health information as stated in the agreement, and they must be fully prepared to pay penalties if protected health information is breached.

Finally, healthcare organizations should emphasize to their BAs the importance of documentation. In the event of a breach, the covered entity will logically want to know what happened, to whom, when, and what was done to mitigate the incident. BAs must also document these same actions. This level of breach documentation may be new for some BAs.

Pieces of a Business Associate Agreement

Key components of a BA agreement include:

- Start date, expiration date, review dates, and signatures
- Terms and conditions of how to use or disclose PHI, data rights, security, etc.
- New language surrounding breach notification and the securing of data
- New disclosure-related requirements concerning EHRs
- Policies and procedures for retention and destruction of data, recording, and reporting of breaches

A sample business associate agreement provided by HHS is available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Important to Communicate Changes

Don't assume that your BAs understand the breadth of their new responsibilities. Communicate the changes, provide updated business associate agreements at the correct time, and eliminate any misinformation that might complicate business relationships. All in healthcare are working toward a common goal: accurate, secure, protected health information.

Jan McDavid (jan.mcdavid@healthport.com) is general counsel and chief compliance officer at HealthPort.

Article citation:
McDavid, Jan P. "HIPAA Changes Call for Revising BA Agreements" *Journal of AHIMA* 84, no.5 (May 2013): 42-43.