Ensuring Your Business Associates Provide 'Satisfactory Assurances'

Save to myBoK

By Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA, and Kelly McLendon, RHIA, CHPS

HIPAA uses the term "satisfactory assurances" four times in the text of its Privacy and Security Rules. Each time the statement is used it describes a covered entity's (CE) responsibility to obtain satisfactory assurances from a business associate who creates, receives, maintains, or transmits electronic protected health information (PHI) that it will appropriately safeguard the PHI.

Unfortunately the definition of satisfactory assurances and the necessary steps business associates and subcontractors need to take to document their compliance with the HIPAA regulation is far from clear.

This article will explore the requirements that must be met by business associates and subcontractors under HIPAA and provide some considerations for covered entities to ensure that "satisfactory assurances" have been obtained.

A Patchwork of Regulations

Under the HITECH Act of 2009 and subsequent HITECH Omnibus Final Rule regulations, both business associates and subcontractors are now required to comply with the administrative, physical, and technical safeguard requirements of the HIPAA Security Rule and some provisions of the HIPAA Privacy Rule. Prior to the HITECH Act, the obligations for business associates were defined contractually through a business associate agreement (BAA) and the covered entity took full responsibility in the event of a violation of the HIPAA Privacy Rule. This all changed under the Omnibus Final Rule, where the responsibility for compliance shifted to business associates and subcontractors.

The BAA contract must address several areas of compliance. These include areas that are not clearly defined in regards to reasonable assurance of one's compliance up the chain from subcontractor to business associate to covered entity. The rule states:

- Business associates must implement appropriate safeguards to prevent unauthorized use or disclosure of protected information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information
- To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, the business associate must comply with the requirements applicable to the obligation
- The business associate must make available to the US Department of Health and Human Services (HHS) its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by, the business associate on behalf of the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule
- At termination of the BAA contract, if feasible, the business associate must return or destroy all PHI received from, or created or received by, the business associate on behalf of the covered entity
- The business associate must ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information

BAA Modifications May Be Necessary

To date, most meet the "satisfactory assurances" requirement through the use of the BAA between the covered entity and the business associate, obligating the business associate to protect the confidential health information. However, covered entities and business associates have increasingly begun to separately document key facts, policies, and procedures about their downstream entities. It has been noted that among larger hospitals and some savvy vendors, during the process of vetting their

downstream support organizations they have dramatically increased the demand for production of documentation illustrating the downstream organization's compliance, especially in the IT and security areas.

Although very comprehensive in scope, BAAs are usually not prescriptive in the details about how to implement and maintain the satisfactory assurances requirements. This leaves each covered entity with the challenge to determine whether their business associates and subcontractors are following the guidelines generally outlined in the BAA based upon satisfactory assurance.

What exactly are appropriate best practices for documentation of compliance that leads to a reasonable level of satisfactory assurance? Some might say that having the BAA is sufficient. Others say that it depends on the risk that the exposure might represent. HIPAA does not require the covered entity to "monitor" or validate the business associate. However, healthcare organizations are now seeking ways to strengthen the satisfactory assurances of business associate and subcontractor compliance.

Attestation Tools Facilitate Compliance

Attestation is a tool that can be utilized to validate BAA satisfactory assurances. Similar to the attestation healthcare organizations must do to prove they are meeting the quality measures called for in the "meaningful use" EHR Incentive Program, business associates would be asked to attest to their linked healthcare organization that they are compliant with the BAA and satisfactory assurance. Attestation tools can be developed by healthcare organizations or their consultants, and the tool itself can be flexible in design and customized to fulfill requirements associated with a covered entity or business associate expectation of compliance as outlined in the BAA.

The regulations as defined by HIPAA and the HITECH Omnibus Rule provide a framework that can be used to develop an attestation of compliance in the form of a self-assessment questionnaire. The content of this questionnaire might consist of a checklist or template that a business associate or subcontractor would complete to provide attestation for documented compliance. Questions could include elements such as:

- Have you formally designated a privacy and/or security official within your organization? Please provide their contact information.
- Do you have documented privacy and security policies and procedures designed to protect the confidentiality of protected health information? Yes or no?
    - Have you created security policies for safeguarding electronic protected health information per the HIPAA Security Rule (among others)? Please provide a list.
    - Have you created privacy policies for protecting and applying the HIPAA Privacy Rule? Please provide a list.
    - Have policies been reviewed and updated where appropriate within the past 12 months?
    - Do these policies address state breach laws?
    - Please provide us with a copy of your policies for risk management, encryption (data in motion, at rest, and e-mail), breach, sanctions, and workforce training.
- Do you conduct background checks on employees? Subcontractors?
    - Are these criminal, financial, or other types of checks?
- Do you have confidentiality agreements signed by all of your workforce members?
    - Please provide a copy of your confidentiality agreement.
- Do you have agreements with your subcontractors to ensure they comply with all of the requirements of HIPAA with regard to their access to and permitted use of PHI?
    - Please provide a copy of your subcontractor agreement.
- Do you limit access to PHI only to those who need it to fulfill their job responsibilities?

    - List safeguards, policies, and procedures to limit access to PHI.
- Do you provide ongoing HIPAA training and awareness for all of your workforce members?
    - List sources of training materials and subject matter expertise.
    - What is the frequency of HIPAA privacy and security training?
    - Please provide us with a description of the training provided within the last 12 months for employees and/or subcontractors.
- Have you completed a formal security risk analysis within the past 12 months?
- What framework (format) did you use to document your security risk analysis?
- Do you use external expertise to assist with security compliance? If so, please list.
- How do you monitor your workforce and their activities for compliance?
- If you manage PHI within an electronic system, does that system contain an audit log that can be used to review workforce member access to PHI?
- Do you routinely audit for appropriate access to PHI by your workforce?
- Do you have documented disaster recovery and business continuity plans?

Many times separate IT security questionnaires, some very complex, are used to determine a good view of the entire security infrastructure of a business associate or subcontractor. This is a prudent practice but is difficult for smaller organizations—both covered entities and business associates—to manage and can lengthen procurement deals. At all times the security questionnaires should focus on the actual access to and use of the PHI the subsequent business associate or subcontractor is obligated to protect. Typically the scope narrows as to what and how much PHI is used or accessed as the chain progresses downward, making the process slightly easier.

The attestation questionnaire might contain a simple phrase at the end such as, "As required by the standards of the Health Insurance Portability and Accountability Act (HIPAA), this certification provides satisfactory assurances that appropriate steps have been undertaken to comply with the requirements of contractual arrangements with the covered entity/business associate and the requirements of the HIPAA Privacy, Breach, and Security Rules." Attestation serves as a mechanism for proactive risk management and establishes the framework toward achieving satisfactory assurances under HIPAA.

Reference

Peterson, Grant. "Attestation: Strengthening 'Satisfactory Assurances' of the HIPAA Business Associate Agreement." *Risky Business - The Privacy Analytics Newsletter*. January 2012. www.privacy-analytics.com/files/january-2012.pdf.

Sample BAAgreements Online

The US Department of Health and Human Services has several sample business associate agreements that can be used as templates for providers and other covered entities. Access these templates at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Sharon Lewis (slewis@primeauconsultinggroup.com) is a principal at Primeau Consulting Group. Kelly McLendon (kmclendon@complianceprosolutions.com) is the managing director of CompliancePro Solutions.

Article citation:
Lewis, Sharon; McLendon, Kelly. "Ensuring Your Business Associates Provide 'Satisfactory Assurances'" *Journal of AHIMA* 86, no.10 (October 2015): 48-51.