Business Associates and Satisfactory Assurances: A Simple Security Tool

Save to myBoK

By Dana DeMasters, MN, RN, CHPS

Covered entities are sharing vast amounts of electronic protected health information (ePHI) with business associates (BAs)—from outsourcing entire information technology and patient billing departments to participating in health information exchanges and population health studies.

Of the breaches involving over 500 individuals reported to the Department of Health and Human Services from 2009 to December 31, 2018, BAs were responsible for 16 percent, affecting 35,668,305 individuals. Although BAs are now directly accountable to the Office for Civil Rights (OCR), covered entities may still suffer monetary losses and reputational damages when one of their BAs is involved in a breach.

Covered entities are generally required to obtain "satisfactory assurances" that a BA who creates, receives, maintains, or transmits protected health information on their behalf will appropriately safeguard the protected health information (PHI). This is completed through a written BA agreement (BAA). However, any additional satisfactory assurances the covered entity may want to undertake, and how extensive those assurances should be, is not prescribed by HIPAA and remains the decision of each covered entity and what may work best for each organization.

The purpose of this article is to provide an example of a simple tool to assist covered entities in obtaining additional satisfactory assurances specifically related to the security of ePHI (download PDF form). In lieu of or in addition to this tool, covered entities may also request independent verification and validation from a third-party auditor, or proof of certification such as HITRUST or SOC 2 Type 2.

Before implementing this tool, the covered entity must dedicate a resource to manage, review, follow up on, and approve the security questionnaires once they have been completed. This resource is key to obtaining satisfactory assurances. Simply sending the questionnaire to the BA and hoping for a quick return will not be successful. A qualified resource must have an information security background and feel comfortable discussing and clarifying technical issues with the business associate—for example, an information security analyst or security officer.

It is important that the security questionnaire is completed before sharing any ePHI with the BA. For example, during the contract process the security questionnaire may be sent along with the BAA. The covered entity's resource will follow up with the business associate and ensure the questionnaire is completed and sent to the contract administrator. By policy and education, staff will understand that no ePHI is shared with the BA until the BAA and security questionnaire are signed and filed with the contract administrator.

The completed security questionnaire is centrally stored in the contract management software for easy reference. This document, as well as providing additional assurances about the vendors' security practices, records how the ePHI will be used, shared, transmitted, and stored. A sample security questionnaire is available at the end of the article.

Specific contact information is listed to assist with questions that may occur at a later time and specify who is responsible for vendor user provisioning. This easy reference is helpful for various departments such as information technology, compliance, risk management, and administration, who may need to access this information if a security issue or breach occurs, and for updates. Keep in mind that if the same vendor has a different project in the future and transmission or storage of ePHI will change, for example, a new or revised security questionnaire may be needed.

HIPAA does not require a covered entity to obtain satisfactory assurances for a BA's subcontractor. However, it is important to be aware of what subcontractors the BA may use and, if needed, request a copy or confirm that a BAA exists between them. How ePHI is shared between the business associate and the subcontractor may be documented on the security questionnaire.

As breaches involving ePHI increase, covered entities have a great responsibility, compounded by limited resources, to ensure their BAs will appropriately safeguard their patients' ePHI. Implementing a simple tool and dedicating a resource for the management of the tool will assist in successfully obtaining these assurances.

References

Department of Health and Human Services. "Uses and Disclosures of Protected Health Information: General Rules: Minimum Necessary" 45 CFR 164.502. April 4, 2003. www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf.

Department of Health and Human Services. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 78, no. 17 (January 25, 2013).

Department of Health and Human Services' (HHS) Office for Civil Rights. "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

t-w Security. "By the Numbers, Q4 2018." www.tw-security.com/pdfs/news/ByTheNumbersQ4-2018.pdf.

Dana DeMasters (dana.demasters@libertyhospital.org) is the privacy and security officer at Liberty Hospital in Liberty, MO.

Article citation:
DeMasters, Dana. "Business Associates and Satisfactory Assurances: A Simple Security Tool." *Journal of AHIMA* 90, no. 5 (May 2019): 26-29.