# Reduce BA Risk Through Due Diligence and Documentation

Save to myBoK

*By Mariela Twiggs, MS, RHIA, CHP, FAHIMA, and Sara Goldstein, Esq.*

Healthcare provider organizations rely on a variety of entities to help them carry out healthcare activities and functions. If these entities create, maintain, or transmit protected health information (PHI) on behalf of a provider organization, they are considered a business associate (BA) under HIPAA.

The broad definition of a BA under HIPAA encompasses many different types of vendors. PHI disclosure management vendors are examples of BAs, and often they can be trusted partners who offer valuable guidance and best practices to help providers stay compliant with the HIPAA Privacy and Security Rules. Other BAs may not be so obviously tied to privacy and security compliance, including food service companies, document shredding vendors, physician answering services, revenue cycle management subcontractors, and many others.

Regardless of the type of BA, provider organizations need to conduct due diligence and execute business associate agreements (BAAs), ensuring these partners have HIPAA-compliant policies and safeguards in place to protect the security and privacy of patients' PHI. Even with a BAA, breach risk and HIPAA compliance should be continually assessed as the provider organization conducts its own risk analysis.

## BAs Pose Risks to Provider Organizations

In recent years, BAs have come under greater scrutiny by the US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), which investigates and enforces reported HIPAA-compliance violations. With the enforcement of the HIPAA Final Omnibus Rule in 2013, BAs can now be held liable for violations of the HIPAA Security and Breach Notification Rules and certain provisions of the HIPAA Privacy Rule. New this year, BAs began facing OCR Phase 2 HIPAA audits.

This recent attention stems, in part, from the large amount of electronic PHI (ePHI) that BAs hold, which puts providers and their patients at risk. For example, North Memorial Health Care (NMHC) made a resolution agreement payment to OCR of more than $1.5 million this year after the theft of an unencrypted, password-protected laptop from a BA employee's locked vehicle impacted the ePHI of 9,497 individuals. NMHC did not have a BAA with its BA, which was performing payment processing for the provider.[1]

Similarly, Raleigh Orthopaedic Clinic, P.A. of North Carolina paid a $750,000 resolution agreement payment after it released more than 17,000 X-ray films to a BA without a BAA. The BA, which claimed it would digitize X-rays for the clinic, was actually a fraudulent company that sold the films to a recycler to be harvested for silver and never created the electronic images. [2] This example, in particular, highlights the importance of having BAAs and conducting due diligence of BAs.

## Conducting Due Diligence

Conducting due diligence of BAs is essential before the partnership begins, but also as part of the provider's ongoing risk analysis. The first step is to develop a questionnaire for the BA, or potential BA, to provide attestation or documentation of compliance. If red flags are identified, then a more in-depth review or assessment should be conducted. Some red flags, such as ignoring or inadequately responding to a questionnaire, should immediately disqualify the BA from consideration.

When deliberating these red flags, some may be riskier than others. The bottom line is provider organizations should only consider BAs who are willing to complete questionnaires and answer questions about how they protect PHI privacy and ensure its security. The BA should welcome site visits and demonstrations of their procedures and technology used to safeguard PHI—especially if it is highly integral to HIM processes, such as a PHI disclosure management partner. This includes quality assurance processes and tools, such as record integrity applications powered by optical character recognition

technology; internal management reports and benchmarks; privacy and security incident management processes; summaries from a data protection or similar committee; and customer focus updates regarding rules and regulations.

## Limiting Liability Through a BAA

The HIPAA Privacy Rule requires that a covered entity (CE) obtain "satisfactory assurances" from its BA, stating the BA will appropriately safeguard the PHI it receives or creates on behalf of the CE. Apart from the due diligence questionnaire, these satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the CE and the BA.[3]

The BAA should include HIPAA-mandated provisions, but can also offer enhanced protection for the provider. For example, if a breach is detected the provider can request notification within a shorter amount of time than is required under HIPAA or applicable state law. An organization can also protect itself through an indemnity clause that holds the BA liable if its actions resulted in a breach. Prior to a breach occurring, however, it is crucial that the provider obtain documentation of the BA attesting to HIPAA compliance in the BAA.

## Virtual Meeting on Advanced Business Associate and Subcontractor Management

Learn more about business associate agreement best practices during the "Advanced Business Associate and Subcontractor Management" session at AHIMA's Virtual Privacy and Security Academy Series, taking place online November 9. Attendees will earn three CEUs.

To register, visit www.AHIMA.org/events. Enter the event type "Meeting," and the domain "Confidentiality Privacy and Security."

## Enabling Transparency from the Beginning

To ensure compliance and breach protection for both the provider organization and the BA, both parties should encourage information and process transparency from the beginning of the relationship. Starting with thorough due diligence and establishing clear expectations in the BAA will ensure mutual openness and risk mitigation.

The best course for providers is to select BAs they can rely on for compliance knowledge, guidance, and best practices. This type of vendor offers value on top of its contracted service, and is likely both a long-term and trusted partner.

## Notes

[1] US Department of Health and Human Services. "$1.55 million settlement underscores the importance of executing HIPAA business associate agreements." HHS press release. March 16, 2016. www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html.

[2] Murphy, Kyle. "X-ray film scam exposes 17k patients to possible data breach." *Health IT Security*. May 7, 2013. http://healthitsecurity.com/news/x-ray-film-scam-exposes-17k-patients-to-possible-data-breach.

[3] US Department of Health and Human Services. "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524." www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/.

*Mariela Twiggs (mtwiggs@mrocorp.com) is national director, training and compliance, for MRO. Sara Goldstein (sgoldstein@mrocorp.com) is MRO's general counsel.*

**Article citation**:
Twiggs, Mariela; Goldstein, Sara. "Reduce BA Risk Through Due Diligence and Documentation" *Journal of AHIMA* 87, no.10 (October 2016): 56-57.