Health Law Daily Wrap Up, STRATEGIC PERSPECTIVES: Attorneys are business associates, too; PHI must be kept safe, (Nov. 24, 2015)

Click to open document in a browser

By Sarah E. Baumann, J.D.

The Health Information Portability and Accountability Act's (HIPAA) (P.L. 104-191) Omnibus Final rule (78 FR 5566, January 25, 2013) extended liability for failing to safeguard protected health information (PHI) pursuant to the HIPAA Privacy, Security, and Breach Notification Rules from covered entities (CEs) to business associates (BAs). The rule, which implemented provisions of statutory amendments contained in the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (P.L. 111-5), had a significant impact on BAs and CEs, who were expected to be in compliance with the rule by September 23, 2013, and, in limited circumstances, by September 23, 2014. Attorneys for BAs and CEs were forced to reevaluate the entities' relationships with one another and their plans for safeguarding PHI. One overlooked aspect of the Omnibus rule, however, is the liability it extended to attorneys acting as BAs. This Strategic Perspective will examine the classification of attorneys as BAs, provide examples of scenarios in which attorneys serve as BAs, and offer tips for compliance.

HIPAA liability

An understanding of the Omnibus rule requires knowledge of basic HIPAA terminology. CEs are health plans, health care clearinghouses, or health care providers that transmit any heath information in electronic form, in connection with a transaction for which HHS has adopted a standard (45 C.F.R. sec. 160.103; *Final rule*, 65 FR 82462, December 28, 2000). A BA is essentially a person or organization with whom the CE has an agreement to perform, or assist in the performance of, a function or activity involving the use or disclosure of individually identifiable health information (45 C.F.R. sec. 160.103). Protected health information (PHI) is individually identifiable health information that is transmitted by or maintained in electronic media or any other type of media.

HIPAA privacy standards establish guidelines for CEs and BAs concerning the release of PHI to other organizations and individuals and provide rules that CEs and BAs must follow in evaluating and responding to data breaches, including breach notification procedures. The HIPAA Security Rule requires CEs and BAs to comply with certain administrative, physical, and technical safeguards to ensure the security of electronic PHI (ePHI). Prior to the implementation of the Omnibus rule, CEs were liable for failure to comply with HIPAA privacy and security regulations. The Omnibus rule extended liability to BAs. It required CEs that engage BAs to have contracts in place, known as BA agreements (BAAs) to ensure that the BAs will safeguard PHI. CEs must also obtain "satisfactory assurances" to ensure that the BAs safeguard ePHI and use and disclose information only as protected by the Privacy Rule (see *Covered entities warned to manage exposure to business associate liability*, April 17, 2014). Failure to comply with the rule and regulations can lead to the imposition of tiered civil monetary penalties (CMPs) by the HHS Office for Civil Rights, as well as potential prosecution by state attorneys general and criminal penalties.

Attorneys as BAs

The regulatory definition of a BA includes a non-employee who provides legal services to or for a CE, where the service involves the disclosure of PHI, by either the CE or a separate BA, to the non-employee providing legal services (45 C.F.R. 160.103). The HHS Office for Civil Rights (OCR), which oversees HIPAA compliance, lists as an example of a BA, "an attorney whose legal services to a health plan involve access to protected health information." In listing this example, the agency makes clear that an attorney can be a BA in certain circumstances—but how can an attorney be sure of his or her role and the relevant obligations?

Ericka L. Adler, Partner at Roetzel & Andress, noted to *Health Law Daily*, "It was not initially clear whether lawyers were 'Business Associates' since they already have attorney-client privilege." However, the January 2013 Final rules "were a real wakeup call for lawyers." Kerry L. Moskol, Partner at Quarles & Brady LLP, broke the analysis down to two questions: (1) is the client a CE?; and (2) "is the law firm going to receive patient

information in the course of that representation?" If the answers to both questions are 'yes,' the attorney is a BA. "If the attorney works for a law firm," Moskol emphasized, "it is the law firm that becomes the business associate under the law, not just the individual attorney, and the law firm will need to ensure compliance with HIPAA."

Moskol provided several scenarios in which attorneys can be considered BAs, including attorney representation of health care providers dealing with informed consent, end-of-life, guardianship, peer review, and corrective action issues, along with instances involving of breaches of medical information. However, she was careful to point out, "Non-health care attorneys may also find themselves functioning as a business associate." She provided examples such as benefits attorneys who obtain patient information while representing health plans, labor and employment attorneys helping providers investigate employees, and litigation attorneys representing CEs in cases dealing with insurance coverage. Adler noted that malpractice and personal injury attorneys would be considered BAs, as would attorneys representing practices that are responding to insurance company audits or patient bill disputes. "There can even be an issue with a physician leaving a practice who has a right to take/solicit those patients that he or she brought to the practice, so a list of such patients is generated." Moskol noted that firms representing patients, however, will not be considered BAs if they obtain PHI because they are performing services on behalf of the patient and not a CE.

In order to carry out its duties as a BA, an attorney may need to develop a relationship with another BA, often referred to as a subcontractor BA. The attorney will need to enter into a BAA with that individual or entity. Moskol indicated that where a CE is responding to allegations of overpayment, the attorney representing that CE may need to hire a billing consultant who will have access to PHI, making the consultant a BA. Furthermore, the attorney may wish to hire that consultant directly, in an effort to maintain attorney-client privilege. In this situation, the attorney BA would need to enter into a BAA with the consultant BA. In other instances, an attorney might become a BA by virtue of being hired by an existing BA. For example, Moskol noted that a software vendor BA that stores a hospital's (CE's) patient information may hire an attorney to provide legal services, providing the attorney with access to PHI and making the attorney a subcontractor BA.

Penalties. Attorneys who serve as BAs and fail to comply with the HIPAA Privacy, Security, and Breach Notification rules are subject to the same penalties as other BAs. Specifically:

- For a person who did not know (and by exercising reasonable diligence would not have known) that he or she violated a HIPAA provision—$100 to $50,000 for each violation; maximum $1,500,000 total penalty in one year;
- For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect—$1,000 to $50,000 for each such violation; maximum $1,500,000 total penalty in one year;
- For a violation in which it is established that the violation was due to willful neglect and was timely corrected—$10,000 to $50,000 for each such violation; maximum $1,500,000 total penalty in one year; and
- For a violation in which it is established that the violation was due to willful neglect and was not timely corrected—$50,000 for each such violation; maximum $1,500,000 total penalty in one year (45 C.F.R. sec. 160.404(b)).

Moskol stated that the OCR has engaged in "minimal enforcement" against BAs to date, focusing mostly on CEs. Specifically, it began conducting "Phase 1" audits of CEs in 2011 to determine whether they were generally compliant with HIPAA; the agency made adverse findings for 89 percent of audited CEs. However, the OCR is expected to begin Phase 2 of its auditing program, when it plans to perform Security Rule audits of a limited number of information technology-based BAs, focusing on risk analysis and management, and Breach Notification Rule audits, focusing on breach reporting (see *OCR Phase 2 audits to focus on specific HIPAA rules*, July 17, 2015). Although originally planned to begin in 2014, Phase 2 audits were postponed, and are now expected to begin in 2016.

BA duties. The Privacy Rule requires BAs to establish policies and procedures addressing, in part, the permitted uses and disclosures of PHI. BAs must also identify a privacy officer who is responsible for compliance and train employees on HIPAA and firm privacy policies. The Security Rule specifically covers the protection of ePHI

and outlines specific administrative, physical, and technical safeguards that BAs must put in place. The Rule requires BAs to perform a risk analysis to determine vulnerabilities to breaches and then, importantly, to put into effect a policy to remediate those risks. The failure of BAs and CEs to perform risk analyses is the main reason that entities fail OCR audits. This failure is so widespread that Abby Bonjean, an investigator in the OCR's Midwestern Regional Office, referred to it as "the root of all evil that we see," (see *No risk analysis? That's the root of all evil*, July 2, 2015).

A thorough risk analysis should be enterprise-wide; cover all electronic protected health information (ePHI) that the organization creates, maintains, or transmits; apply to all places in which information is stored, including mobile devices, medical devices, and servers; cover risk to the ePHI during both use and disposal; and be updated when major changes, such as a merger, occur within an organization. The Rule also calls for the identification of a Security Officer responsible for compliance and employee training on HIPAA and firm policies. The Breach Notification Rule requires BAs to perform risk assessments when breaches occur to determine the probability of compromise, including the nature and extent of the PHI involved, the unauthorized person or person who used the PHI or to whom the disclosure was made, whether the PHI actually was acquired or viewed, and the extent to which the risk to the PHI has been mitigated, and outlines guidelines for notifying the HHS Secretary, the affected individuals, and the media of the breach.

Compliance tips. How can attorneys serving as BAs comply with HIPAA rules? Adler outlined basic steps attorneys should take to keep PHI secure. She recommended maintaining a locked storage area for medical records stored in an attorney's office; encrypting email that contains PHI; requiring passwords on computers where PHI is stored, or, alternatively, storing PHI in special electronic files to further limit access; shredding unnecessary PHI; and, when it is necessary to send physical documents containing PHI, utilizing courier services rather than regular mail. She also noted that some attorneys that represent health care practices "take the precaution of having every such client sign a Business Associate Agreement immediately just in case a situation arises. However, only if the lawyer comes into contact with PHI do they step into the BA role." Moskol cautions attorneys to read BAAs carefully, as CEs "are imposing heightened compliance requirements." "Law firms," she said, must ensure that "they do not agree to terms beyond those required by HIPAA unless they are prepared to comply with those additional requirements."

Risk. Are attorneys subject to greater risk than other BAs? Adler does not think that's the case. "There is certainly risk if basic safety precautions are not taken. However, even with those precautions, systems can be hacked and information stolen so lawyers face the same risk as health care providers in many ways. Additionally, errors can happen." However, "Where there is no real resulting harm, this should not result in large risk for a law firm but lawyers need to be aware of the steps to follow should an error occur." Moskol agrees that attorneys are subject to the same risk as CEs and other BAs. "However, from a practical standpoint, the most immediate risks that attorneys face in terms of a HIPAA violation are usually more likely to be reputational damage and the costs associated with a breach of their clients' PHI."

Conclusion

Attorneys with access to PHI should have been safeguarding that information even before the publication of the Omnibus Final rule, but that rule extended HIPAA liability to the firms that employ such attorneys, when acting as BAs. Attorneys should err on the side of caution and act as if they are BAs with respect to the safeguarding PHI. Attorney-client privilege does not protect attorneys from liability, and even non-health care attorneys may be considered BAs under HIPAA. Although the OCR is not expected to target attorney BAs with audits in the near future, attorney BAs should take this opportunity to ensure that they are fully complying with HIPAA so that they may be confident of their compliance if subjected to future audits, protect the individuals whose PHI they handle, and protect their own reputations.

Attorneys: Ericka L. Adler (Roetzel & Andress). Kerry L. Moskol (Quarles & Brady LLP).

MainStory: StrategicPerspectives HIPAANews AuditNews CMPNews ConfidentialityNews EHRNews HITNews ProviderNews RiskNews