AM I A "BUSINESS ASSOCIATE"? WHY SHOULD I CARE?

Paul F. Ebeltoft and Haylee Cripe Ebeltoft . Sickler . Lawyers

Complying with privacy and security rules protecting patient records set by the Heath Insurance Portability and Accountability Act (HIPAA) can be incredibly frustrating even for those directly involved in health care delivery and payment. However, it is critically important for attorneys, accountants, claim adjustors, billing service providers, medical expert witnesses, medical review consultants and many others who work only episodically within the health care industry to also know the HIPAA regulatory maze. The latest changes have opened the door for punishment of the unsuspecting.

WHAT IS A BUSINESS ASSOCIATE?

Merely providing services to a health care provider, health insurance plan or health care clearing house (covered entities) does not automatically make you a business associate. However, the federal Department of Health and Human Services (the Department) defines a HIPAA business associate in broad terms. If you are working with a covered entity in a way that involves the use or disclosure of individually identifiable health records or information, but you are not an employee of the covered entity, you are a business associate.[i] Outside counsel reviewing a threatened malpractice claim for a hospital, independent counsel on patient quality assurance reviews, insurance company claims personnel, utilization review consultants, benefits managers with access to health records, contract medical transcriptionist services and even independent medical record shredders are all business associates.

WHAT HAS CHANGED?

Until February 18, 2009, HIPAA placed the primary burden of privacy and security of protected health information on covered entities, charging them with ensuring that their business associates followed the statutory requirements. The means of doing so was (and remains) the requirement for a covered entity to maintain a written "business associate contract" with all of its business associates.

A business associate contract must identify the permitted uses of protected health information disclosed. It must set forth rules for permitted re-disclosure and must require the business associate to use certain safeguards to protect the health information. To view a sample business associate contract, visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

However, the Health Information Technology for Economic and Clinical Health Act, (HITECH), passed in February 2009, is materially changing the regulatory landscape. An interim final rule to implement portions of HITECH removed the safe harbor available for covered entities to avoid a monetary penalty for violation of HIPAA privacy and security rules by claiming lack of knowledge of the violation. Previously, a covered entity was liable under the federal common law of agency for civil monetary penalties for the actions of any of its agents acting within the scope of its agency relationship. An exception to liability allowed a covered entity to show that it had obtained reasonable assurances from its business associates regarding the safeguarding of protected information and either that it did not know about the unauthorized activity or that it took reasonable steps to end the violation. The interim final rule holds a covered entity accountable regardless of whether the entity knew of the business associate's pattern of activity.

The interim rule also imposes new reporting burdens on business associates requiring self-reporting of any safeguard breach. The report must be made "without unreasonable delay" to their covered entity and in no event more than 60 days from when the business associate or any of its employees knew or should have known of the breach. In general, a reportable breach is an impermissible disclosure of protected health information that significantly risks

financial, reputational or other harm to the individual whose records were disclosed. Covered entities then must report "upstream" to the Secretary of the Department, to those whose records were disclosed and in some cases to the media.

WHAT IS COMING?

The short answer is more changes that seriously affect business associates. In July 2010, the Department issued a Notice of Proposed Rulemaking (NPRM)[ii] covering the portions of HITECH not addressed in the interim final rules. Even though only proposed, the Department's website cautions against complacency. "Although the effective date (February 17, 2010) for many of these HITECH Act provisions has passed, the NPRM, and the final rule that will follow, provide specific information regarding the expected date of compliance and enforcement of these new requirements." Currently the Department intends to provide only 180 days from the final rule's effective date to come into compliance. It would be well for all business associates to be aware of what the NPRM proposes and to prepare.

Among many other things, the NPRM enables the Department to impose monetary civil penalties on business associates for violations occurring after February 18, 2010. The fine for breach could be in one of four tiers at the discretion of the Department, taking into account the nature of the violation and the harm resulting from it. The four tiers are: $100, $1000, $10,000, and $50,000 per violation. Each tier has a cap on the amount a business associate can be required to pay for violations of an identical requirement or prohibition in a calendar year. The caps for each tier are $25,000, $100,000, $250,000, and $1,500,000 respectively.

If the disclosing party did not know, and would not have known through reasonable diligence, of the breach, the fine will be at least in the $100 tier, but will not exceed $50,000 per occurrence. If the violation is due to reasonable cause but not willful neglect, the penalty will be at least $1,000 but not more than $50,000 per occurrence. If the violation is due to willful neglect, but corrected promptly after discovery, the fine is at least $10,000 but will not exceed $50,000 per occurrence. If the violation is due to willful neglect, but not corrected, the fine will be at least $50,000 per occurrence.

The NPRM also extends the scope of HIPAA privacy and security requirements. Previously, if a business associate properly hired a subcontractor to do the work of the business associate, the protections of the law could lapse, not extending to the subcontractor. The NPRM will close that loophole by making business associates responsible for compliance by an agent that performs functions for or provide services to a business associate, but is not a member of the business associate's workforce. Outside counsel (business associate) reviewing medical records created for an event from which a malpractice claim could arise against a client hospital (covered entity) will need a HIPAA compliant contract with a medical record reviewing service (subcontractor) that the lawyer employs to assist. The "downstream" subcontractor must comply with HIPAA privacy and security rule provisions regardless of whether there is a written contract with the business associate. However, since the business associate must take reasonable steps to ensure that the subcontractor is complying and immediately report any violations, a written contract is the only sensible course.

Interestingly, there is a whistleblower exception. A business associate does not violate the rules if the business associate discloses protected health information in a good faith effort to alert appropriate officials to conduct that violates professional or clinical standards or endangers patients, workers, or the public. However, this disclosure must be to an agency charged with health oversight or a public health authority authorized by law to investigate or oversee conduct or conditions the whistleblower believes are being violated. This can be a trap for the unwary however, so any business associate faced with the dilemma of disclosure should tread carefully and first seek advice concerning its legal obligations and options.

SIX STEPS YOU SHOULD TAKE NOW.

1. ***Determine whether you are a business associate or subcontractor.*** Do not rely on someone else to have made the determination for you. Review the type of information shared with you by covered entities or by third parties working on behalf of covered entities. If it includes protected health information, analyze existing rules and the NPRM. If you are a business associate of a covered entity, find and review your business associate contract. If you are a subcontractor, talk to your business associate. Get contracts in place if you do not have them.
2. ***Recheck your status.*** Establish a protocol to review newly developed associations with covered entities or business associates. Watch for the Department's final rules and use them to review again all existing customer/client relationships.
3. ***Develop your own contract.*** Preparing your own subcontractor contract will help you judge the fairness of contracts that covered entities or other business associates may ask you to sign. Be sure that the contract you develop appropriately mirrors your obligations under the contract with the covered entity for which you are working.
4. ***Use it.*** If you are a business associate who must outsource some of your work for a covered entity to others insist on putting a subcontractor contract in place. Do not forget third party computer technical support and off-site file and data storage vendors or those who may have access to protected health information indirectly while working for you.
5. ***Check your processes and procedures.*** A business associate or subcontractor is restricted to using protected health information for the purposes stated in the written agreement. Make sure that your protocols for privacy and security are HIPAA compliant and sound. Develop a decision-tree to determine who reviews a possible breach of privacy and security rules and who directs the course of action if a breach has occurred.
6. ***Check your current state law.*** HIPAA law and regulation will supersede less stringent state laws. If your state's laws exceed the federal requirements, you must comply with those requirements.

Paul F. Ebeltoft is President of Ebeltoft . Sickler . Lawyers. As a trial lawyer in North Dakota for more than 30 years, Paul is able to help all of his firm's practice teams, but he concentrates his efforts within its "Litigation Solutions" and "Alternatives to Litigation" teams.

Haylee Cripe is a law clerk at Ebeltoft . Sickler . Lawyers. She holds a Bachelor's of Accountancy from the University of North Dakota School of Business and Public Administration and is pursuing her J.D. from the University of North Dakota School of Law.

[i] 45 C.F.R. § 160.103 (2005).

[ii] Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40868-01 (July 14, 2010).