IN BRIEF

THIS ISSUE
September 2013
Issue 121

Oregon State Bar
PROFESSIONAL LIABILITY FUND
www.osbplf.org

Malpractice Prevention Education for Oregon Lawyers

Business Associate, Esq.: HIPAA's New Normal

HIPAA Omnibus Rulemaking

On January 25, 2013, the Office of Civil Rights (OCR) released its revision of the Health Insurance Portability and Accountability Act's (HIPAA) Privacy, Security, Data Breach, and Enforcement Rules. The Data Breach and Enforcement Rules became effective on March 26, 2013, including the minimum penalties described below. Most of the rest of these rules are effective for business associates on September 23, 2013. An exception exists for most business associate agreements in effect on January 24, 2013: these agreements must be compliant with the new rules by September 24, 2014.

The significance for attorneys of this regulatory overhaul is the direct application of these new rules to them when they are either HIPAA business associates or the subcontractors of a business associate that receives protected health information (PHI). A business associate receives, creates, uses, stores, or transmits PHI on behalf of a HIPAA "covered entity" (i.e., a health care insurer or health care provider). For example, an attorney representing a provider in a malpractice action typically receives medical records from his or her client. This receipt and use of PHI makes the attorney a business associate and thereby subject to HIPAA regulation. Similarly, a business attorney who reviews or obtains information concerning payment for care usually receives PHI and is therefore also a business associate. The expert witness who is given medical records obtained from a physician or hospital client in preparation for trial or deposition is a subcontractor of a business associate who receives PHI and is therefore also a business associate.

Why We Care

Attorneys who receive PHI from their clients are almost certainly "business associates" under HIPAA. As such, they are subject to minimum penalties for "willful neglect" of their HIPAA obligations: $10,000 per violation, if the violation is corrected within 30 days; $50,000 per violation, if it is not. Lesser penalties are levied for negligent violations, greater penalties for intentional ones. Attorneys will likely be presumed to know their obligations under HIPAA, and therefore are more likely to be found willfully or intentionally neglectful of their HIPAA obligations than other business associates.

Violations are counted on a per person, per day, per standard basis. Annual liability under each standard is capped at $1.5M, but breaches of confidentiality or security typically involve the violation of multiple standards. Misuse or wrongful disclosure of PHI often produces a public relations nightmare, and is usually followed by a settlement with the OCR in which the offender agrees to periodic and random compliance audits. Soon, OCR will promulgate rules that will provide for sharing a portion of the fines and settlements it collects with whistleblowers.

Business Associates Must Comply With HIPAA

Just like a medical clinic or hospital, business associates must implement privacy and security compliance programs to protect the confidentiality, integrity, and availability of PHI. Policies and procedures must be documented and implemented in order to come into compliance. Failure to

put these programs in place, and to follow them, is a violation of HIPAA.

Security

The key duties of a business associate under the Security Rule are as follows:

- Ensure confidentiality, integrity, and availability of all electronic PHI.
- Protect against reasonably anticipated threats or hazards to the security or integrity of PHI.
- Protect against reasonably anticipated improper uses and disclosures of PHI.
- Ensure HIPAA compliance by its workforce.

Risk Analysis

Security compliance under HIPAA begins with a "risk analysis." This involves, first, an inventory of PHI held by the firm, in both paper and electronic form, and second, a description of the firm's information network and electronic repositories of PHI. Next, threats to the confidentiality or security of PHI, whether natural or manmade, must be evaluated in terms of their likelihood and their impact in the event of PHI's misuse or unauthorized disclosure. This analysis of vulnerabilities and risk will drive security plan design and the allocation of resources to mitigate, first, the most likely and impactful threats, and so on down the line to the least likely and least dangerous of threats. The first thing the OCR will ask for when it investigates a complaint, conducts an audit, or responds to notice of a data breach is the documented risk analysis conducted by the business associate. If your firm does not have a documented risk analysis, then the only real question is the amount of the settlement or penalty. OCR is not likely to be sympathetic to law firms that fail to understand and comply with their legal obligations.

This Is Not Y2K

Security planning and implementation is not a one-time event. Security programs must provide for periodic review and revision of their risk analysis and security measures. Both the firm and the threat environment are always changing. Security programs must change with them, and failing to reassess and revisit the firm's security program is in itself a violation of HIPAA. A recent $400,000 settlement by OCR with medical clinics run by Idaho State University was primarily the result of the University's failure to periodically revisit and revise its security program.

Training

A major HIPAA obligation is ensuring workforce compliance. This means training, and more specifically, documented training. It also means enforcing firm policies concerning the handling and protection of PHI with employee discipline, up to and including termination. The business associate firm's workforce, both attorneys and staff, need to be trained to recognize and respond appropriately to potential HIPAA violations. Training should be made a part of new employee orientation and be repeated periodically.

Data Breach

In the event of a misuse or wrongful disclosure of PHI, the business associate must determine whether the PHI has been compromised and then either document a determination of a low probability that the PHI has been compromised or provide notification of the data breach to affected individuals and the U.S. Department of Health and Human Services. If a data breach involves the PHI of more than 500 individuals, then notice of the data breach also must be provided to local media and be prominently displayed on the firm's website. Thus, it is the expectation of OCR that either you will document your determination that a data breach has a low probability of compromising PHI or you will provide notification to affected individuals and, if necessary, the media. This determination or notification must be performed without delay, but in any event in no more than 60 days from actual or constructive notice of the breach.

One Word: Encryption

For a data breach to occur, PHI that is misused or wrongfully disclosed must be "unprotected." As a practical matter, that means unencrypted. The encryption of electronic PHI is the single most effective security measure available to HIPAA-covered entities and business associates. Strongly consider using it for electronic PHI at rest or in motion. Whatever the investment required, encryption will pay for itself many times over if – or when – you have a data breach.

Misuse of PHI

A data breach can involve the misuse of PHI within an organization; it need not involve disclosure outside the firm. PHI is governed by a strict "need to know" principle, the "minimally necessary" provision of the Privacy Rule. Thus, attorneys or staff who are not working on a matter that involves PHI should not have that information given or available to them. "Role-based access" is the guiding principle, as both administrative and technical means should be used to avoid exposing PHI to workforce members without a "need to know" about the PHI in question.

Suggested Next Steps

These recommendations may sound like extreme measures. Attorneys are already bound by ethical obligations to protect the secrets and privacy of their clients. They are now potentially subject to a hugely burdensome and complex reg-

imen of privacy regulation. This is the new legal landscape – one that we ignore at our peril. So I suggest that you take these first few steps toward compliance without delay:

1. Identify Privacy and Security Officials. This is not only required by rule, it places responsibility with identified persons. So long as everyone is responsible, no one is.

2. Document a Risk Analysis. Again, this is required, not simply a good idea. The firm may wish to take this on, or may look to compliance professionals for assistance.

3. Focus on Mobile Devices. The OCR hates PDAs. Data breaches resulting from stolen or misplaced laptops, iPhones, or Blackberries with PHI on them or accessible through them are a recurring breach scenario.

4. Compile Existing Policies and Procedures. We all have policies and procedures for keeping files safe and secure. You may be surprised at how far along you already are. You won't know what is left to be done until you have all of your explicit materials in one place and can compare them to your legal obligations.

Kelly T. Hagan
Schwabe, Williamson & Wyatt, P.C.