dbr DAILY BUSINESS REVIEW

Page printed from: Daily Business Review

Board of Contributors: Lawyers Must Get Hip To HIPAA: Avoiding The 'Wall Of Shame'

Mark A. Dresnick and Pamela I. Perry, Daily Business Review

March 31, 2014

Over the years, the legal and medical professions have often gone head to head.

These days, however, they share a common headache: the Health Insurance Portability and Accountability Act, better known as HIPAA, including amended federal laws and regulations called the Health Information Technology for Economic and Clinical Health Act, or HITECH. Unlike most headaches, however, this one requires a lot more than a few aspirin to manage.

As everyone knows by now, HIPAA is designed to safeguard a patient's protected health information, or PHI. Because HIPAA was designed to keep PHI confidential, health care information transmitted by health care providers often remains HIPAA-protected even after it leaves the hospital or doctor's office.

As a result, lawyers who receive medical records in the course of representing physicians, hospitals and health care plans (in HIPAA parlance, covered entities) must comply with HIPAA's stringent requirements or risk finding themselves on the wrong side of a federal inquiry.

HIPAA dubs lawyers who represent covered entities "business associates"—an innocuous phrase that gives rise to a significant mix of requirements and obligations.

For example, before a law firm representing a physician or a hospital can receive PHI in connection with a client's case, the firm must have a written business associate agreement with the client.

Among other things, the agreement must require that the law firm comply with various HIPAA privacy and security rules, and notify the client if the firm improperly discloses the health care information. Some agreements also require that the law firm indemnify the client for any HIPAA breaches, although this is not required by HIPAA.

In addition to entering into a business associate agreement, lawyers doing work for physicians, hospitals, and other covered entities must also have privacy and security policies in place to prevent the unauthorized disclosure of patient information.

Lawyer Liability

It may seem odd to remind attorneys and seasoned employees that loose lips (and unprotected chips) sink ships, but formal HIPAA training sessions can help deter HIPAA security breaches and may be strong evidence of due diligence and mitigation if things go wrong.

Equally important, if the lawyer needs to share the information with anyone not working at their law firm, including a medical malpractice defense expert, an information technology consultant or even a shredding company, the firm must have the third party (in HIPAA parlance, a subcontractor) sign a business associates agreement between the law firm and the subcontractor.

Notably, a subcontractor's carelessness can put counsel in harm's way. In some situations, a lawyer may become liable for the failure of the subcontractor to safeguard the PHI on an agency theory. Accordingly, if a medical expert misplaces his unencrypted laptop or leaves medical records at his favorite pub, the law firm that hired him might be on the hook for his loss.

Not surprisingly, reports of things going wrong abound. Laptop computers containing copies of medical records get stolen, employees lose iPads, and USB thumb drives containing medical records get misplaced.

Congress anticipated these hacking and other problems (ask former U.S. Rep. Anthony Weiner), and HIPAA requires that most losses of unencrypted PHI be reported by the business associate to the covered entity that entered into the agreement.

As a result, if your employee leaves an iPad containing unencrypted PHI on the Metrorail, or someone steals your laptop containing unencrypted health information from your car or hotel room, you must inform the covered entity—that is, your client—because your client must report the breach to the patients involved, the U.S. Department of Health and Human Services and even the media if the breach involves over 500 patients. This is a surefire way to turn a good client into a former client.

Big Breaches

In addition to creating a very unhappy client, a breach may also expose your firm and your health care client to civil fines. A HIPAA security breach may also expose your firm to indemnification issues concerning reimbursing your client for the costs of remediating the HIPAA security breach.

Further, a breach affecting over 500 patients will get your firm and your client listed on the infamous HHS "Wall of Shame"—the HIPAA website equivalent of the post office wall.

Finally, in addition to being embarrassing, a security breach may be expensive. HIPPA breaches are often not covered by standard legal malpractice insurance, although that void is increasingly being filled by separate cyber coverage policies.

At the end of the day, Congress has decided that when it comes to a person's health, privacy matters.

Although this adds risk to representing health care providers and carriers, the good news is that

there is a lot you can do to prevent a PHI malfunction.

Specifically, law firms should encrypt health care information, train employees and hire security savvy subcontractors. Further, counsel should securely destroy or return all PHI as soon as a case is over, and require that their expert witnesses and any other subcontractors do the same.

Physician practices and other health care providers that have been responsible for breaches have had to endure sanctions (including fines which can easily exceed $100,000) and have complained of other headaches no aspirin can possibly cure. But to a large extent, these maladies can be prevented. To paraphrase Ben Franklin (the Steve Jobs of his day), an ounce of encryption—and other safeguards—is worth a pound of cure. We urge you to get hip to HIPAA—and steer clear of the Wall of Shame.
