LTT LAW TECHNOLOGY TODAY

April 17, 2015

WHAT HIPAA COMPLIANCE MEANS FOR LAWYERS AS BUSINESS CONSULTANTS

BY JOE KELLY

While many lawyers strive to become true business partners with their clients, law firms that deal in sensitive health information may need to become actual "business associates." Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Omnibus Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH), lawyers may qualify as business associates, which carries a whole host of obligations and compliance measures—and serious penalties for failing to meet those standards.

HIPAA, Law Firms, and PHI

When law firms handle work that involves "protected health information" (PHI) for covered entities under HIPAA, they generally fall under the business associate classification. PHI includes items such as medical history or records, laboratory results and insurance information. This can affect firms in a variety of practice areas, such as medical malpractice cases or eldercare law. When accepting such clients, law firms need to understand if they become regulated by HIPAA and will be liable for any violation under the act.

Designed to make health care delivery more efficient and provide more people with health insurance, HIPAA's main provisions revolve around information portability, tax issues and simplifying administration. When the final HIPAA Omnibus Rule became effective in 2013, it involved major changes to the act's privacy and security rules that extended to business associates, such as law firms, and subcontractors of business associates.

According to the U.S. Department of Health & Human Services (HHS), the HIPAA Privacy Rule applies to covered entities, which it defines as health plans, health care clearinghouses, and certain health care providers. Covered entities often need to work with other organizations to carry out functions and activities. The Privacy Rule allows providers and health plans to share PHI with these so-called business associates, if the business associates provide appropriate assurances that they will only use the information for the purposes for which they were engaged, will safeguard the information and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Generally, covered entities and their business associates must sign "business associate agreements" (BAA) to ensure compliance.

As an example, HHS points to a complaint alleging that a law firm hired by a pharmacy chain improperly disclosed the PHI of a pharmacy's customer. HHS's Office for Civil Rights investigated the allegation and found no evidence that the law firm had impermissibly disclosed the customer's PHI. The investigation

did reveal that the pharmacy chain and the law firm had not entered into the required BAA. To resolve the matter, the firm and its client had to execute a BAA.

Not only do law firms need to comply with HIPAA, they may need to make sure their vendors, or subcontractors, do so as well. That means law firms must take a hard look at their relationships and contracts with cloud service providers, expert witnesses and others to ensure those organizations are HIPAA-compliant. The chain of liability extends infinitely. When a subcontractor works with another organization to receive, maintain or transmit PHI, those contractors and subcontractors become business associates.

Complying as Business Associates

If law firms take on covered entities as clients that give them access to PHI, attorneys must comply with all the relevant regulations. That involves performing a risk assessment to ensure that law firms meet the standards imposed by HIPAA, which include:

Physical safeguards

As a business associate, law firms need to physically secure their offices, networks and data. This involves controlling facilities and electronic information to limit access to those who have the necessary authorizations. Law firms must also secure the area where computers are kept, as well as the computers themselves. Firms must also properly handle the electronic media that contains PHI. In other words, leaving a laptop that contains PHI in a car represents a violation of HIPAA.

Technical safeguards

These standards include controlling access to systems that contain electronic PHI. Encryption and password protection need to be a key aspect of this. Firms also must use software that tracks activity in systems that contain protected information.

Administrative safeguards

These include implementing policies and procedures to prevent, detect, contain and correct security violations. The standards require law firms to identify a security official. Firms must also ensure that only authorized attorneys and staff can access electronic PHI and that firms have policies that limit access to electronic PHI. Law firms must also provide security training for all attorneys and staff, including creating passwords and addressing security breaches. Firms must establish procedures to identify, respond to, mitigate and document security incidents. They also need to create emergency response procedures for data backup and recovery in case of natural disaster, system failures, deliberate attacks or other incidents. Law firms must also have systems in place to determine if information has been altered or destroyed, and that whoever attempts to access information is the person they claim to be.

In case of a data breach, business associates must follow guidelines on disclosure, such as notifying the covered entity.

The penalties for violating HIPAA can be serious. Under the act's tiered penalty structure, the amount of fines increases with the level of culpability, with a maximum of $1.5 million per year for the same violation. The different levels are:

- Violation due to reasonable cause and not due to willful neglect
- Violation due to willful neglect but is corrected within the required time frame
- Uncorrected violation due to willful neglect

Develop an Action Plan

Once law firms have determined that they are business associates under HIPAA, they must figure out where they fail to comply with all the rules and regulations. Then, they need a plan to address those holes. That requires creating customized policies and procedures, training everyone appropriately and regularly updating the risk assessment plan.

While each firm is unique, there are several areas that present common challenges. Encrypting PHI is a must. Encryption and security policies are two of the best ways to keep data secure.

When working with cloud providers and vendors who handle data, attorneys must be assured that those companies are HIPAA-compliant, too. This should involve creating and executing business associate agreements. Firms also need to determine whether PHI may be stored in less-obvious places such as copiers.

HIPAA compliance is extremely complex and failing to comply can be expensive. Law firms should consider turning to partners who understand what's at stake and have the resources to ensure all regulations are being met. This is particularly true for smaller firms that may lack some of the on-staff compliance specialists that larger firms have.

By working with a trusted, knowledgeable partner who has turnkey products, firms can stay out of trouble while improving their peace of mind and freeing themselves from issues that distract from serving their clients.

Joe Kelly, founder and CEO of Legal Workspace, formally launched the company in 2010. In 2006, he first saw the potential for the Legal Workspace solution because of his broad exposure to how law firms operate. The evolution of virtualization, connectivity and hosting technologies made Legal Workspace a commercially viable solution, and it went live with its first client firm in 2008.

Originally published April 17, 2015 by ABA Law Technology Today ABA Law Technology Today