High stakes

How to keep your company safe from the risks posed by HIPAA and HITECH **Interviewed by Sue Ostrowski**

With penalties for violation of the Health Insurance Portability and Accountability Act soaring, companies need to make sure they are doing everything possible to protect themselves and make sure their employees and business associates understand the law.

And while it may seem obvious that HIPAA rules apply to health care providers such as hospitals and physicians, covered entities also include group health plans that are self-insured, says Patricia F. Jacobson, an attorney in the Health Care and Business Services Group at Stark & Knoll Co., L.P.A. The company itself is not a covered entity, but the health plan may be.

"You have to assume that, at some point, if you've got protected health information in your enterprise, a breach is going to occur, and you have to prepare accordingly," says Jacobson. "The best way to do that is to audit yourself and determine what mechanisms are in place and who's in charge of minimizing the potential for breaches."

Smart Business spoke with Jacobson about how your company may be at risk and how to take steps to minimize your exposure.

Patricia F. Jacobson
Attorney, Health Care and Business Services Group
Stark & Knoll Co., L.P.A.

What kinds of companies are subject to HIPAA compliance?

The scope of HIPAA has expanded. Any company that is a health care provider is considered a covered entity. If a company has a self-insured health plan — whatever the industry — that plan is also a covered entity.

Formerly, only covered entities were subject to penalties. However, with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the law now also applies to 'business associates,' defined as any company hired to do a job that exposes that entity to the protected health information of the covered entity's patients or employees covered by the health plan. This includes management companies, third party administrators, certain software vendors, debt collectors, law firms, accounting firms or medical billing companies. A plumbing, electrical or construction company hired to work in an office is not required to access Protected Health Information, so they are not 'business associates.'

How has HITECH changed the penalties for disclosing personal health information?

HITECH has dramatically increased the penalties for failure to comply with the law. When HIPAA went into effect, the penalties were $100 per offense up to a maximum of $25,000. The civil penalty that applies if a company had no way to know that information was released is a minimum of $100, but the maximum has risen to $50,000. The second tier, in which a company had reasonable cause for the disclosure, but no 'willful neglect' now starts at $1,000 per violation. Penalties for the next tier, where there was 'willful neglect' but a timely correction, start at $10,000. And if the breach resulted from willful neglect, which was not timely corrected, the penalty starts at $50,000 per violation. Multiple violations can entail civil penalties up to $1.5 million per year. Criminal penalties of up to 10 years in prison can also result.

And because the dollars collected by the Office of Civil Rights for offenses are used for further enforcement, you are going to see a lot more enforcement.

How can a covered entity or business associate protect itself?

Health care providers and health plans, and their business associates, must be vigilant about changes in HIPAA Privacy and Security Rules. For self-insured health plans, make sure that there is an impenetrable firewall between the employer's HR division and the people who run the health plan, so there is no chance of anyone using health information for employment decisions. To do that, maintain separate personnel and recordkeeping. Second, periodically educate your employees on the importance of the privacy and security of protected health information.

Third, implement strict policies and procedures. If your policies and procedures are lax, you could be accused of willful neglect if protected health information gets out. Once you have these in place for administrative purposes, physical purposes and technical security, make sure they are known to everyone who is concerned with this data and monitor it on a periodic basis.

Finally, conduct a self-audit with the help of a health care attorney. What you don't know can hurt you. Your legal adviser can help you determine if you are a covered entity or a business associate, what kind of information you use and have access to, and whether you have the required business associate agreements in place. It's all about measuring who you are, what you are, how you do it and then managing those aspects of your enterprise.

Will doing an audit and creating strict policies and procedures protect a business if a breach occurs?

You need to have compliance plans in place and adhere to them so you can point to them, and you can say you have a compliance officer and you have a HIPAA security person who are responsible for monitoring and keeping things ship shape.

It's very, very important that you not only have those things but that you actually use them. To ensure they are used, make sure your policies and procedures are simple and easy to follow. You don't want to go overboard and create a monster that you can't ever implement, because if you have policies and procedures and you don't comply with what you've put in motion, you're going to be in more trouble. And if they are simple and capable of being followed, it's far less likely that you'll ignore them.

Consult with a legal expert to get started on a self-audit and make sure your company is compliant. Whether you're an executive at a hospital or of a manufacturing firm with a self-insured health plan, you need to be cognizant of the risks and monitor your business practices periodically to make sure you are staying up to speed. <<

PATRICIA F. JACOBSON is an attorney in the Health Care and Business Services Group at Stark & Knoll Co., L.P.A. Reach her at (330) 572-1334 or PJacobson@stark-knoll.com.

Insights Legal Affairs is brought to you by Stark & Knoll Co., L.P.A.