

New HIPAA regs could bring more enforcement, lawsuits

By Leah Carlson Shepherd

April 30, 2009

New provisions to the Health Insurance Portability and Accountability Act that were included in the economic stimulus law signed in February could have broad implications for employers, their relationships with health insurers and their liability in protecting personal health information.

Kathy Reardon, an attorney with Bryan Cave, says: "It potentially could have a very big impact in a couple of fronts. You have a new administration that is very much committed to moving forward on an agenda of saving money, using electronic medical records, using electronic information."

For employers, the new rules could mean a greater HR administrative burden and a greater risk of privacy-related lawsuits.

"You're going to see a much bigger push toward enforcement by this administration than you saw by the former administration. There will be more enforcement activity on the state level and the federal level. There could be more lawsuits," Reardon confirms.

Key changes to the law include:

>> Employers and/or health plans must notify individuals and the Health and Human Services Department about any security breach where protected health information has been accessed, disclosed or acquired. This notification requirement applies to electronic and paper information.

>> The notifications must be sent within 60 days of the discovery of the breach. It must be sent by first-class mail, unless the affected person has indicated a preference for e-mail. If the mailing addresses are out-of-date, the employer and/or health plan must post a notice about the breach on its Web site.

If the breach involves protected health information for more than 500 people, the employer and/or health plan must notify prominent media outlets in the local area.

>> The notice should discuss the facts surrounding the privacy breach, the types of information that were involved in the breach and the steps that individuals should take to protect themselves.

>> Business associates, such as third-party administrators, consultants, actuaries, attorneys, pharmacy benefit managers, wellness program vendors and disease management vendors, must notify the employer and/or health plan when a privacy breach has occurred.

Civil and criminal penalties can apply to these business associates now.

The new HIPAA provisions must be incorporated into employers' and health plans' contracts with business associates.

>> The penalties for HIPAA privacy violations have been raised. Depending on the circumstances, penalties range from \$100 to \$50,000 for each violation, up to \$1.5 million total.

>> State attorneys general now can bring lawsuits in federal court on behalf of state residents who were impacted by a privacy breach.

Most of these changes will take effect in February 2010, but the new notification rules are scheduled to take effect in September 2009.

Enforcement

The new rules give state attorneys general new enforcement authority and enable them to contract with outside lawyers to file civil lawsuits with the full authority of the state attorney general and federal law.

It is "nothing more than a gift to the plaintiffs' lawyers," says Lisa A. Rickard, president of the U.S. Chamber Institute for Legal Reform.

"Allowing private law firms to litigate HIPAA enforcement is a recipe for vastly higher costs and increased regulatory complexity."

Rohan Beesla, a health care staff member for the ERISA Industry Committee, a nonprofit that represents employers and HR professionals, also objects to this provision, citing a concern about "overzealous prosecution."

Inconsistency could result from 50 different legal interpretations in 50 states, he notes.

Superseding state law

The HIPAA privacy rules take precedence over state privacy laws, unless the state law is more stringent.

Forty-four states, the District of Columbia, Puerto Rico and the Virgin Islands have passed legislation requiring notifications about security breaches involving personal information, according to the National Conference of State Legislatures.

"The difficulties are in identifying the state laws that are more stringent. The state law issue certainly is one that takes a lot of time for my clients to make sure they're in compliance when there's an incident," Reardon explains.

Beesla worries about legal and administrative complexity.

ERIC hopes to see upcoming regulatory guidance that will minimize obstacles to adoption of health information technology and will not make businesses grapple with 50 different privacy rules, he confirms.

He also says the new rules for accounting for lawful disclosures of protected health information could turn out to be quite burdensome for some employers.

Previously, covered entities did not have to account for disclosures that occurred for the purpose of treatment, payment and health care operations, but now those types of disclosures from electronic medical records must be tracked.

This requirement starts to take effect on Jan. 1, 2011, or the day the covered entity acquires the electronic health record, according to Joel Daniel, a lawyer with the firm Ogletree Deakins.

Beesla agrees there's a need for a required notification after a privacy breach. But, he says, "the statute was not airtight in excluding all good-faith errors.

"We hope, through the regulatory process, that they tighten that up a bit," so that a notice is not required after certain unintentional and limited disclosures of health information.

Helen Darling, president of the National Business Group on Health, warns that expanding HIPAA privacy protections could have unintended negative consequences.

"We are very concerned that expanding privacy and security standards that further restrict or go beyond HIPAA will hinder the ability to reap the full quality and efficiency potential of health information technology. For the past decade, the HIPAA standard has provided a workable framework for patients, physicians, hospitals, other providers, health plans and employers," she wrote in a letter to members of Congress before a hearing on health IT.

"Assuring patient privacy is a critical component of expanded use of health IT, but that privacy and security can and should be appropriately balanced with the need to promote safety, encourage medical research and save lives," Darling wrote.

"This balance can be struck if we take a 21st-century approach that both protects privacy and allows the sharing of information to improve quality."

Re-evaluating compliance

Because of the expectation of increased enforcement, "now is a good time to re-evaluate your HIPAA compliance efforts," asserts Reece Hirsch, an attorney with the firm Sonnenschein Nath & Rosenthal.

Covered entities should review the contracts they have with business associates to make sure the contracts incorporate the new privacy rules. "Health plans are going to have to be more diligent about knowing who their business associates are and who their business associates contract with downstream," Reardon says.

Likewise, employers "need to make sure that the health plans they contract with are prepared and ready to implement an appropriate breach response," Hirsch states.

Make sure your physical and technical safeguards for protected health information are effective and up-to-date, Reardon advises.

Employers also should review their liability insurance contracts to determine whether changes are needed to obtain coverage for potential HIPAA violations, according to a bulletin from The Segal Company, a consulting firm based in New York City.

<http://ebn.benefitnews.com/news/new-hipaa-regs-could-bring-more-enforcement-lawsuits-2672151-1.html>