October 10, 2016

More health care organizations on HIPAA's hit list

To avoid penalties, facilities should step up risk management, including cyber insurance

FEATURED STORY **BY RODIKA TOLLEFSON, THIRDCERTAINTY**

When the Health Insurance Portability and Accountability Act (HIPAA) became law in 1996, the internet was an infant. Physicians walked around with paper charts. A tablet referred to a pill. And the typical cyber attack aimed to deface a website.

But with the evolution of the electronic age, the majority of the nearly 1.2 billion annual medical visits in the United States are documented, stored and shared in electronic form.

And the threat landscape has been evolving as well.

Kurt Roemer, Citrix chief security strategist

"Now that (the records) are online and connected across multiple providers and exchanges, there will be more breaches if nothing else is done (for security)," says Kurt Roemer, chief security strategist for Citrix, which provides security tools.

Related essay: *Why check-box HIPAA compliance is a bankrupt strategy*

In response, federal authorities have stepped up enforcement actions against health care organizations that violate patient privacy rules under HIPAA. As a result, the number of sanctions has reached record levels.

In August, Advocate Health Care Network agreed to pay a record $5.55 million HIPAA settlement for a series of 2013 data breaches affecting 4 million patients.

That case was the tenth closed this year by the Department of Health and Human Services' Office of Civil Rights (OCR), surpassing any previous year since HIPAA became law.

Settlements send a message

And the fines levied by OCR in 2016 have been hefty, averaging just over $2 million per sanction. This stepped-up enforcement is no doubt sending a message to health care providers.

Matt Mellen, Palo Alto Networks security architect

"There's a clear upward trend," says Matt Mellen, security architect for health care with Palo Alto Networks, which provides a next-generation cybersecurity platform. "Ten fines in one year is definitely enough to get the attention of health care organizations."

The trend also is reflected in the number of incidents reported by HIPAA-covered entities. OCR's database, which only includes incidents that impact 500 or more individuals, shows a steady growth each year.

In 2010, 198 incidents were reported to OCR, compared to 296 in 2014 and 269 last year. This upward trend has been documented in various cybersecurity reports, including IBM's 2016 Cybersecurity Intelligence Index, which put health care at the top of all other industries for the number of data breaches.

And according to Ponemon's recent "State of Cybersecurity in Healthcare Organizations in 2016," nearly half of the 535 respondents said their health care organizations experienced an incident in the past 12 months involving loss or exposure of patient data.

The sector is clearly struggling to keep up with the threats, but the problem is not the law itself, says Niam Yaraghi, a fellow at the Center for Technology Innovation at the nonprofit Brookings Institution.

Putting teeth into the law

"HIPAA is a fairly good law," he says. "The problem is that health care organizations consider it as the ultimate level of security that they have to implement, and they do not have any incentive to go beyond HIPAA."

Jodi Daniel, a key draft writer of HIPAA's Privacy Rule and Enforcement Rule

"When the rules first came out … the focus of enforcement was on education and promoting voluntary compliance," says Jodi Daniel, who worked for the Department of Health and Human Services for 15 years and was one of the key draft writers of HIPAA's

Privacy Rule and Enforcement Rule. The goal was to help the industry "get it right, as opposed to penalizing them for getting them wrong."

The first OCR settlement—$100,000—didn't come until 2008. And over the next three years, there were only a total of six. The pace picked up in 2012, as has the average amount of the settlements.

What happened in the meantime was the passage in 2009 of the Health Information Technology for Economic and Clinical Health Act. The HITECH Act dramatically expanded the penalties, based on "increasing levels of culpability," and increased the maximum to $1.5 million instead of $25,000 per identical violation. It also extended HIPAA to business associates.

The addition of business associates was significant, considering that a large number of breaches are attributed to third-party incidents.

Risk management more important

The increased OCR enforcement also is putting an emphasis on risk management. Of the 39 settlements to date, at least 14 included lack of risk assessments among the violations.

Palo Alto's Mellen says OCR's emphasis on risk management is a positive trend.

"The risk management process is designed to identify all the potential threats to patient data and allows you to define action plans to mitigate those risks," he says.

Cyber attacks, in particular, pose a bigger threat to patient privacy than other types of breaches. Yaraghi's report shows that nearly 120 million people were affected by about 150 incidents involving cyber attacks vs. a little over 20 million people affected by about 700 incidents involving theft (laptops, media, etc.).

And the number of hacking/IT incidents is seeing a dramatic increase. Those reported to OCR between 2010 and 2014 grew from nine to 32. In 2015 there were 57; this year through August there already have been 51.

Niam Yaraghi, Niam Yaraghi, fellow at the Center for Technology Innovation

Yaraghi is a proponent of a third-party HIPAA certification system to serve as a preventative measure. But a true economic incentive, he believes, would be cybersecurity insurance. He recommends every health care organization have a policy.

"Health care organizations will have to take security into account to reduce the cost of premiums," he says.

In the meantime, the increased OCR enforcement could create a stronger

incentive for health care organizations to step up cybersecurity. It will also get the attention of boards of directors, Citrix's Roemer says.

"It would make it more difficult for the health care institutions and their boards to casually say they aren't going to invest in security," Roemer says. "It will definitely drive some changes in behavior."

More stories related to HIPAA and health records:

Hospital hacks show HIPAA might be dangerous to our health
Encrypting medical records is vital for patient security
Healthcare data at risk: Internet of Things facilitates healthcare data breaches

Posted in Data Privacy, Data Security, Featured Story