Eli's Rehab Report

HIPAA: Learn From The Biggest HIPAA Breach To Date

Tip: You can still have a HIPAA problem, even if no medical information is taken.

Are you certain you've taken adequate precautions to prevent your patients' health records from being compromised? If you think you've pulled out all the stops think again. Cyberattacks become more sophisticated every day and you need to update how you guard against them just as frequently.

Background: On Jan. 29, health insurance giant **Anthem, Inc.** discovered a cyberattack on its IT system to gain unauthorized access and obtain personal information of its consumers. The suspicious activity may have occurred during several weeks in early December 2014, according to Anthem's Feb. 13 announcement.

Hackers obtained the personal information of an estimated 80 million beneficiaries covered by Anthem or other independent **Blue Cross** and **Blue Shield** plans that work with Anthem. These individuals include both current beneficiaries and past members of Anthem's affiliated health plans, dating back as far as 10 years.

Hackers may have accessed beneficiary information such as names, birth dates, Social Security numbers, healthcare ID numbers, home addresses, email addresses, employment information, and income data, Anthem reported. There is no evidence that the hackers accessed credit card or banking information, nor medical information such as claims, test results, or diagnostic codes.

Is This Really a HIPAA Breach?

Myth: Some major news outlets, such as USA Today, reported that because no actual medical information was stolen, the breach did not in fact fall under the HIPAA rules. But this isn't true.

Reality: "Anthem has stated that member health ID numbers, including Social Security numbers, were breached," wrote Milwaukee-based attorneys **John Barlament** and **Jennifer Rathburn** in a Feb. 9 analysis for the law firm **Quarles & Brady LLP**. "Under HIPAA, this information generally is 'protected health information' (PHI)."

And if PHI was involved, the unauthorized access was a breach under HIPAA. The question of whether medical information was compromised doesn't indicate whether a breach occurred, according to a Feb. 10 blog posting by **Mary Beth Gettins** of **Gettins' Law LLC.** "If the information held by a medical provider or health plan or business associate that identifies an individual is compromised, a HIPAA breach has occurred." The stickier question may involve not whether a HIPAA breach occurred (clearly it did), but instead whether "there was a HIPAA violation occurrence or liability," Gettins explained.

Beware of Phishing

Phishing may have been the cause of Anthem's cyberattack, Gettins said. "Phishers either tricked Anthem tech workers into revealing their password or induced the tech workers into downloading malicious software."

Further, Anthem is warning beneficiaries about phishing emails and telephone calls, with phishers posing as Anthem representatives and asking for beneficiaries' personal information.

Remember: "The black market for personal information is a thriving one," warned **Thomas Lewis,** partner-in-charge of **LBMC Security & Risk Services,** in a Feb. 10 analysis. "And the data stolen from Anthem is evergreen: names, birthdates, Social Security numbers, and income."

You can cancel credit cards, but names, birthdates and Social Security numbers don't change, Lewis noted. So although

you can offer free monitoring services for a year following a breach, "thieves can simply lie low for 12 months and reemerge in month 13 when the coast is clear."

Tip: Because phishing and similar types of breach incidents can be so detrimental, Gettins advised including phishing in your privacy and security staff training. Include a narrative in your training "about security risks like phishing and tutorials about what to do in the event of phishing or other security occurrences."

What Anthem Did Right

Anthem's response to the breach offers a few lessons on what you should do in a similar situation. First, discovery of the breach itself was certainly one of the most important things that Anthem did correctly.

"What the public may not appreciate is how the breach was discovered, and what it says about Anthem," Lewis noted. "Apparently, a suspicious query to the database alerted someone in the IT department. Frighteningly, this type of anomaly often goes undetected in many healthcare entities, and the company's swift response indicates that Anthem takes monitoring seriously, a commitment that many don't have."

Second, Anthem reached out to the FBI upon discovering the breach. "We've seen cases where the company only learns they've been breached when the FBI or another outside entity notifies them," Lewis lamented. Anthem also released a public statement, notified members, and launched an informational website (www.anthemfacts.com) immediately following discovery of the breach.

Anthem is also providing free identity protection services to affected individuals for two years and has created a dedicated toll-free hotline that consumers may call with questions relating to the breach incident.

Bottom line: "No one can ensure that their data is 100-percent safe," Lewis stated. "Anthem is a good example of this: they likely have a highly sophisticated control environment, but they still fell victim to a serious breach. That said, if the industry at large would tighten controls, monitor systems and draw up comprehensive response plans, we can all let the thieves know that we mean business, too