HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Blue Cross Blue Shield employees charged with taking and sharing data screen shots

Eleven people have been charged after a Blue Cross Blue Shield of Michigan (BCBSM) employee allegedly printed and shared screen shots of more than 5,000 subscriber profiles. The 11 people are charged with identity theft and credit card fraud, in what some observers are calling an example of how criminals can get past even the best HIPAA security measures.

Noting the insidious nature of such breaches, one former federal prosecutor says there are only two types of organizations: those that have been hacked and know it, and those that have been hacked and don't yet know it.

In the BCBSM case, three of the accused used the stolen information to purchase more than $742,000 worth of merchandise at Sam's Club, U.S. Attorney **Barbara L. McQuade** announced recently in Detroit.

According to the indictment, BCBSM employee Angela Patton printed screen shots containing subscribers' profiles and gave them to other individuals who used that information to apply for credit in other people's names and purchase merchandise in stores across the country. Co-conspirators were arrested in Texas, Ohio, and Michigan in possession of BCBSM screen shots coming from Patton's work computer as well as counterfeit identification cards and credit cards in the names of individual subscribers whose personal information was included in those screen shots.

Agents recovered additional screen shots that included personal information belonging to thousands of BCBSM and Blue Care Network subscribers while executing search warrants at co-conspirators' homes in metropolitan Detroit. The information included individuals' names, dates of birth, and Social Security numbers. Counterfeit and re-encoded credit cards and gift cards also were recovered. The indictment alleges that three of the co-conspirators who used counterfeit credit cards at major stores and warehouses fraudulently obtained more than $742,000 worth of merchandise from Sam's Club alone.

More data and more threats

Former federal prosecutor **Thomas G.A. Brown** says the BCBSM case is typical of the way healthcare providers are likely to suffer a HIPAA breach. Brown ran the cybercrime unit in the U.S. Attorney General's Office of the Southern District of New York for 12 years. Until 2014, he was involved with investigating and prosecuting such notable crimes as the Citibank hack, the Silk Road billion dollar drug web site, and many healthcare data breaches. Brown is now senior managing director of the Global Risk & Investigations Practice with FTI Consulting in Washington, DC.

His experience gives him unique insight into how criminals breach data security. "I spent a lot of time in small rooms with hackers and got a very good sense of how they think, why they target things, what they look for, and how they exploit it," Brown says. "We're seeing a growth in the volume of sensitive data being collected by companies, and we're also seeing an increase in the ways that information is accessible through the Internet. That works in the favor of the hackers."

The BCBSM data breach was not the type most healthcare organizations expect, Brown says, but it also was not unusual. HIPAA breaches originate with employees more than most company executives think, Brown says. "Most companies think of data security as building tall walls to keep the hackers out," he says. "That overlooks a critical factor, which is the insider's improper use of permissions. That is just as much a threat as the outsiders."

Any healthcare provider's HIPAA security plan should

address the threat from insiders with systems that limit an employee's access to data, Brown says. The computer system should include "firebreaks" that make it difficult for insiders to easily traverse between different databases and have access to more data than necessary for their job duties, he says.

Other internal security features include cameras trained on computer workstations and lockouts that prevent the use of jump drives or copying to a disc. Insiders can be exceedingly difficult to stop, however. Brown recalls one case in which an employee was thwarted by security cameras and a system that would not allow him to copy the computer code he wanted to steal. His solution was to simply print the code on paper, stuff it in his backpack, and walk out.

"The Blue Cross Blue Shield case is similar. They may have all the bells and whistles for high tech control, but these guys just took screen shots," Brown says. Detecting a breach afterward sometimes depends on having good logs of activity, which Brown says might have helped BCBSM and law enforcement identify the accused employee. *(See the story on p. 3 for more on the importance of good logs.)*

Healthcare providers are paying more attention to cyber security in the wake of recent cases such as the Anthem breach, which involved the protected health information (PHI) of more than 80 million people, but Brown says the threat from cybercrime can never be eliminated completely. More so than in any other industry, Brown says, healthcare providers must assume that hackers and thieves are constantly looking for a way in.

"Healthcare data is particularly useful to bad guys, because not only does it contain health information; it contains names, addresses, phone numbers, and Social Security numbers," Brown says. "It can be used to steal identities, open fraudulent credit lines, all the things the hacker is hoping for when he gets into any business's data. Getting into a healthcare system's data pretty much guarantees they're going to be able to sell this data for top dollar and make a nice profit."

Insider threats on the rise

McQuade stated in her announcement that while technology has made it easier than ever for criminals to commit identify fraud, technology is also making it easier for law enforcement to catch them. An individual's personal information has significant value on the black market, which is why the threat of data breaches and identity theft remain at an all-time high, she said.

BCBSM also investigated the breach internally, and **Gregory W. Anderson**, vice president for corporate and financial investigations at BCBSM, praised the law enforcement effort. "Our company is determined to thoroughly investigate alleged fraud and work hands-on with law enforcement to bring perpetrators of fraud and identity theft to justice," Anderson said. "We salute the task force for these arrests and for their diligent efforts to help Blue Cross protect our members' personal information and privacy."

Affected policy holders will be notified by letter and offered two years of free credit protection services, the company reports.

The BCBSM identity theft ring is yet another example of how insider threats are on the rise, says **Eric Chiu**, founder and president at HyTrust, a cloud control company in Mountain View, CA. "Employees and their credentials are the number one way companies are being breached today, with many high profile examples over the past 18 months including Target, eBay, Home Depot, Sony, Anthem, and Edward Snowden," Chiu says. "Identity theft and credit fraud are a big business for these new cyber criminals, and data is the new currency. Companies need to place security as their number one priority, especially around insider threats. Otherwise, they will become the next target."

Brown agrees that healthcare organizations must be proactive in ensuring HIPAA compliance, and not only because hackers are unrelenting in their efforts. The plaintiffs' bar also is realizing that there is money to be made in civil suits following a breach, particularly with class action suits, Brown says.

Civil suits related to HIPAA breaches have gained little traction because in most cases plaintiffs had no damages, only the threat of future damages from a stolen identity. Plaintiffs' attorneys eventually will find ways around that issue, Brown says. Attorneys are pursuing different legal avenues, and there is no shortage of plaintiffs, especially now that the public is becoming better educated and aware of this threat, Brown says.

Any increase in liability risk will be accompanied by increasing efforts from hackers, Brown says. The threat is constant, he warns.

"Just because you haven't been hacked yet doesn't mean you can't be hacked, and it doesn't even mean you really haven't been hacked. Maybe you have, and you just don't know it yet," Brown says. "Data security is an arms race, and the hackers are sharing information about every weakness they find. Healthcare providers have to remain vigilant and not be lulled into complacency by the thought that they haven't had an incident yet."

SOURCES

- **Thomas G.A. Brown**, FTI Consulting, Washington, DC. Email: thomas.brown@fticonsulting.com.
- **Eric Chiu**, President, HyTrust, Mountain View, CA. Telephone: (408) 776-1400. ■

Good computer logs critical to detecting breach

A detailed record of who accessed data, when, and how often might be the only way an organization can trace the source of a HIPAA breach. Ensuring the thoroughness of those logs should be a top priority for any healthcare organization, says former federal prosecutor **Thomas G.A. Brown**, senior managing director of the Global Risk & Investigations Practice with FTI Consulting in Washington, DC.

"Companies often do not have adequate logs, and so they don't even know what they lost or how it happened," Brown says. "They might know they've been breached, but they can't figure out what data was accessed, much less who is responsible."

It is a mistake to focus only on defending the computer system from attack, from outside or within, Brown says. Criminals eventually will find a way around even the best security, and incidents such as the Blue Cross Blue Shield Michigan screen shots show that insiders can steal data without leaving an obvious trail. But the computer log should reveal all, he says.

Internal segmentation of the data system should slow thieves, which prevents easy access across databases, but employees always will have access to protected health information (PHI), so Brown says the computer log can be used to determine when and how an employee accessed that data.

"The key thing is figure out what you lost, which is really important in the healthcare field, because you need to provide adequate notice to victims and other obligations under HIPAA," Brown says. "If you know you lost something, but you don't know what you lost, that's going to complicate your efforts to comply with HIPAA's obligations once you're aware of the breach." ■

Anthem refuses audit by Office of Inspector General before and after massive HIPAA breach

After all the negative press that Anthem suffered when reporting a HIPAA breach that affected 80 million customers, one might think they would avoid more bad publicity. But the health insurer is under fire for refusing to let the Office of the Inspector General (OIG) of the Office of Personnel Management (OPM), the agency overseeing the federal employee health benefits program, audit its IT security.

OIG performed a partial audit of Anthem's IT security in 2013 and gave the company (which was WellPoint Health Networks, before Anthem and WellPoint merged) good marks ... in the parts of the system that Anthem let it see. Auditors were denied access to other parts. The OIG auditors wanted to use the same automated tools they use at other institutions to document configurations of a sample of servers, then manually compare results to the company's approved baseline.

The company told the auditors that corporate policy prohibited anyone outside Anthem from connecting to the network, according to a September 2013 report by the OIG. "We were initially provided a description of what appeared to be a thorough configuration compliance auditing program at WellPoint," the report said. "However, when we requested documentation to support this description, WellPoint was unable to provide any evidence that a configuration compliance auditing program had ever been in place at the company."

Without data to the contrary, OIG determined that Anthem had "not implemented technical controls to prevent rogue devices from connecting to its network" and might have neglected to perform vulnerability scans on several servers with federal employee data. The Anthem servers were hacked within a year. The incident is thought to be largest HIPAA breach by far.

OIG recently reported that it asked Anthem to participate in a vulnerability scan in the summer of 2015 but that Anthem again said no. Anthem has not issued any statements on why it refused the audit. The lack of cooperation looks especially bad after Anthem's huge breach, says **Tim Erlin**, security and IT risk strategist at Tripwire, a company in Portland, OR, that assists with cyber security. "Without facts to the contrary, it's hard not to interpret the motivation

behind Anthem's refusal as an attempt to avoid embarrassment," Erlin says. "Regardless of the motive, declining an audit from OPM for the second time, following a massive breach, makes headlines. Insurers providing services to federal employees should be subject to security audits by the government, and they shouldn't have a choice in the matter."

Anthem also is under criticism from the Senate Health, Education, Labor and Pensions Committee, which accuses the insurer of dragging its feet in informing the 80 million customers affected by the cyberattack. Chairman Lamar Alexander (R-TN) and ranking member Patty Murray (D-WA) claimed recently that 50 million of those affected customers have not been informed. In a letter to Anthem's chief executive, the senators said they were "concerned with your slow pace of notification and outreach thus far."

A spokesperson for Anthem points out the company has set up a website and a hotline for affected customers and accelerated mailings. With so many affected customers, the logistics are challenging, he says. At press time, about 2.4 million letters were being mailed daily.

Meanwhile, the lawsuits against Anthem are beginning. A Brunswick, ME, man has filed a $5 million class action suit against Anthem Health Plans of Maine, and he claims that the company failed to adequately protect the personal information of its clients. In a complaint filed in U.S. District Court in Portland, attorney Benjamin Grant wrote on behalf of his client, Brian Mason, that Anthem acted unreasonably by failing to encrypt clients' confidential information, including Social Security numbers and medical and financial information. In Connecticut, Wilma J. Peterman is seeking an unspecified amount from Anthem for damages and restitution in a lawsuit filed Feb. 20 in U.S. District Court — District of Connecticut. She claims the Anthem data breach could have been prevented and should have been detected earlier.

"There is little doubt victims of the Anthem data breach will suffer significant and persistent financial harm as a result," attorneys for Peterman wrote in the lawsuit. "This time the hackers got Social Security numbers. For cyber thieves, the Social Security number is the holy grail, providing access to confidential customer information."

The lawsuit alleges that Anthem was negligent, breached an implied contract, and violated the Connecticut Unfair Trade Practices Act. ■

No date yet for OCR's HIPAA audits

The Department of Health & Human Services (HHS) Office for Civil Rights (OCR) still has not set a date for when the next round of HIPAA audits, originally planned for fall 2014, will take place.

OCR Director Jocelyn Samuels spoke at the 23rd National HIPAA Summit in Washington, DC, recently and confirmed the delay. Linda Sanches, senior advisor for OCR health information privacy, also spoke at the meeting and explained that the audits were delayed to allow healthcare organizations to implement new technology.

The HIPAA audit protocols still are being developed, Sanches said, but they will focus on the privacy, security, and breach notification aspects of HIPAA. ■

Premera Blue Cross says 11 million records breached

Boston-based health insurer Premera Blue Cross announced recently that a cyberattack might have exposed medical data and financial information of 11 million customers.

The unauthorized data access was discovered on Jan. 29, but it might have been occurring as far back as May 2014, the company said. Premera said the attackers might have gained access to claims data, including clinical information, along with banking account numbers, Social Security numbers, birthdates, and other data. Premera did not release details on how the hackers gained access.

Unlike some recent HIPAA breaches, including Anthem's case involving 80 million customers, the Premera breach included health information, the company said. Cybercrime experts say medical records are especially valuable on the black market because they can be used for insurance fraud.

Premera spokesman **Eric Earling** says there is no apparent link between the Anthem and Premera breaches. Premera identified the breach and reported it to law enforcement, Earling says. The attack affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliated brands Vivacity and Connexion Insurance Solutions. ■