Report on
PATIENT PRIVACY
Volume 14, Number 2 • February 2014

Practical News and Strategies for Complying With HIPAA

Despite Retail Setting, Target Breach Holds Lessons for CEs

Unless they've had their heads in the sand, privacy and security officers at HIPAA covered entities (CEs) and business associates (BAs) have no doubt heard about the massive data breach suffered by Target and other retailers; they may even have been among the tens of millions who got a letter or email from Target, or, more recently from Neiman Marcus or Michael's stores about their incidents.

While these breaches seem to be confined, at least for the moment, to retail establishments, CEs and BAs are vulnerable to similar, if not identical, sorts of attacks. Human error may have contributed to Target's breach, and the employees of CEs are often a source of vulnerability for organizations that must comply with HIPAA. (For strategies on reducing the risks that workers pose to PHI, see story, p. 1.)

"This could happen to any one of our hospitals," Mac McMillan, co-founder and CEO of CynergisTek, Inc. and chair of the HIMSS Privacy & Security Policy Task Force, told *RPP*. "What happened to Target may not necessarily have been a sophisticated attack" but might have been prompted by "mismanagement" of Target's information technology system, which created the perfect "opportunity" for lurking data hackers, he added.

According to Lisa Sotto, who heads the privacy and information management practice for the New York-based law firm of Hunton & Williams, LLP, "We take lessons from all security breaches that happen." Common themes include making sure HIPAA officials are "understanding the threats, observing [responses], and learning from the investigations and communications" that emerge from them.

Target first acknowledged a breach on Dec. 19, 2013, after it was revealed a day earlier by Brian Krebs, a former *Washington Post* reporter, on his blog. Since then, it's been tough to keep up with new information, but none of it has been very good for Target.

Number of Individuals Affected Has Ballooned

That first notice said "approximately 40 million credit and debit card accounts may have been impacted," but another issued on Jan. 10 by the company said "the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 million individuals."

An update issued in between those two, dated Dec. 27, 2013, said: "While we previously shared that encrypted data was obtained, this morning through additional forensics work we were able to confirm that strongly encrypted PIN data was removed." (To see all of the updates, visit https://corporate.target.com/about/payment-card-issue.aspx.)

It has not been clear whether these are two different sets of individuals; press reports have said the total number of people affected may be 110 million. And as far as what actually happened, the most recent information, coming from the "research lab" of Seculert, a firm that "provides cloud-based solutions that protect organizations from advanced malware," was that Target suffered a two-pronged attack that began at its card readers in stores.

"First, the malware that infected Target's checkout counters (PoS) extracted credit numbers and sensitive personal details. Then, after staying undetected for six days, the malware started transmitting the stolen data to an external FTP server, using another infected machine within the Target network," the firm said.

In addition, downloads of the stolen data began Dec. 2. "The cyber criminals behind the attack used a virtual private server (VPS) located in Russia to download the stolen data from the FTP. They continued to download the data over two weeks for a total of 11 GBS of stolen sensitive customer information," Seculert analysts said.

PHI May Have Been Exposed

Target is also a HIPAA covered entity by virtue of the bricks-and-mortar pharmacies housed in many of its stores, as well as its online shopping business. The company has said nothing to indicate whether the hackers penetrated its medical data files. But the kinds of information known to have been breached already meet the definition of "protected health information" (PHI).

RPP contacted Target and asked whether any HIPAA-covered information was in the breach, and spe-

Copyright © 2014 by Atlantic Information Services, Inc. Reprinted with permission from Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com

cifically whether pharmacy data were affected. But in two email responses, a spokeswoman did not provide an answer.

"At this point in the investigation, we have confirmed that payment card data and the partial personal information (name, email address, mailing address or phone number) were taken," Molly Snyder, a Target PR group manager, wrote on Jan. 27. She repeated that "the criminal and forensic investigation is ongoing." Snyder did not respond to a follow-up *RPP* email with additional questions.

RPP also reached out to Krebs, the journalist who first reported on the breach, who said he did not know whether any HIPAA-covered data were involved.

Confirmation of a PHI breach would come if Target were to post a breach notice to patients, but it could also be argued that the notices Target has already sent out qualify as a HIPAA breach notices. If it is a HIPAA breach, the incident will appear on the Office for Civil Rights Web page that lists breaches affecting more than 500 individuals.

OCR spokeswoman Rachel Seeger did not address *RPP*'s question of whether it had received a breach notification from Target stemming from this situation. "To the extent there is a breach of unsecured PHI of over 500 individuals, the CE has sixty days to report the breach to OCR," Seeger said. "Once the breach is reported, OCR would also have to verify the details of the breach with the CE before posting it to the website."

However, even that 60-day deadline is flexible: notice can be delayed if requested by law enforcement authorities or the CE needs more time to investigate. The FBI is now involved with Target's breach. So fervent watchers of OCR's so-called "wall of shame" page may have to be patient.

Where Are CEs Vulnerable?

Target's breach is a wake-up call for HIPAA covered entities and business associates, which shouldn't be complacent about their own security compliance, experts say. CEs and BAs should be "reviewing the technical vulnerabilities in their systems," said Jeff Drummond, a partner with Jackson Walker LLP in Dallas.

He adds that they need to shift their typical focus on securing PHI because a breach might be embarrassing or personally upsetting to patients to more of a recognition that data under their control are a valuable commodity that can be sold on the black market.

Such a shift doesn't mean CEs should ignore the common issues like inappropriate access and snooping by employees. But don't let that kind of worry "overshadow concerns about how you deal with credit cards, Social Security numbers and other financial data," Drummond told *RPP*. "What we need to be concerned about in health care is identity theft," Drummond said. "That's a bigger risk for us."

The staffs in large covered entities aren't as likely to be uninformed on security issues as those in smaller ones, but BAs and subcontractors of any size, particularly those that don't deal exclusively with health care data, may also lack current knowledge of data security practices. CEs would do well to share security updates with them whenever possible. Even messages that are seemingly as simple as making sure they are "really vigilant about using antivirus software" of a sufficient strength and that is updated can go a long way toward preventing problems in the future, Drummond said.

Don't Be a 'Bad Boxer'

"Bad things are going to happen, and HIPAA is not designed to punish you when the unforeseen happens," Drummond said. But CEs and BAs do need to take steps to reduce the possibility that known risks will become reality. He cautions against falling into the "bad boxer syndrome," referring to someone who "covers up where he just got hit," instead of predicting where the next one is going to come and taking action to protect himself.

McMillan concurs that Target and the other retailers' misfortunes should trigger CEs and BAs to look at their own practices. "The one take-away is that it is absolutely critical that we have good standards around our billing systems, good, solid disciplined processes for how we harden and patch our systems," McMillan told *RPP*.

Also crucial is making sure tests are run to ensure that all processes are operational and safeguards are working properly before a system is brought back on line after repairs or other changes have been made, he added.

Drummond and McMillan both said CEs and BAs need to be paying closer attention to their use of credit cards. Depending on the volume of their transactions, CEs and BAs may use everything from an old-fashioned metal card swiper, which essentially makes a rubbing of the raised characters and numbers on a card, to small, handheld devices that read the data on the magnetic stripe and can be connected to an IT system via a USB cord. The requirements of the privacy and security rules apply to the credit card data, of course, so safeguards — including physical and technical — are supposed to be in place.

Labs and other CEs that use credit card readers and have a particularly high volume of credit card transactions might take extra precautions as they may be targets for hackers like those who attacked the retailers.

McMillan said he advises his larger clients to completely outsource all credit card payment operations, which is better than trying to comply on their own with

Copyright © 2014 by Atlantic Information Services, Inc. Reprinted with permission from Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com

the Payment Card Industry Data Security Standard that is required of "merchants" who accept credit cards, which is a broad category that can include health care organizations.

Drummond and McMillan both say health care organizations also should not retain any credit card data for patients. There's no good reason to hang onto that information, they say, and no guaranteed way of securing it.

Sotto adds that the Target experience should also serve as a reminder to CEs and BAs to ensure they have an incident response plan ready, with all the people who will be needed identified in advance *(RPP 10/09 p. 5)*. They also should hold a drill with a mock breach to test how well the plan works, she recommended.

Stay Tuned — Literally

Some answers about what happened to Target, and perhaps ways to prevent future occurrences, may soon come to light. On Feb. 4, the Senate Judiciary Committee will hold a hearing, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." (See http://tinyurl.com/le7aynw.)

The hearing will feature two panels of witnesses, with the first person scheduled to testify being John Mulligan, Target's executive vice president and chief financial officer. Other scheduled witnesses include William Noonan, the deputy special agent in charge of the Secret Service's Criminal Investigative Division; the chair of the Federal Trade Commission; and a high-ranking official from the Department of Justice.

Mulligan will likely be limited in what he can say, given the investigation is ongoing, but the senators may have better luck in getting answers from Target than *RPP* did. To be broadcast live, the Feb. 4 hearing is expected to garner all the viewers, geeky though they may be, of a highly rated reality TV show.

It's anybody's guess as to whether Congress will take any action as a result of the Target breach, such as passing a federal privacy and security regulation that would include HIPAA CEs and provide a strong, national standard instead of the patchwork of HIPAA and state laws. Sotto told *RPP* she thought the time was right for passage in 2006, following the theft of a government employee's laptop and hard drive that had Social Security numbers and data for 26.5 million veterans.

On May 23 of that year, Sotto advocated for such a law when she testified before the Subcommittee on Regulatory Reform and Oversight at its hearing on "the regulatory burdens associated with state and federal data protection laws." She told *RPP*: "As a society we need to tackle this, because the problem is not abating. The bad guys are really motivated and talented — and creative."

Contact Drummond at jdrummond@jw.com, McMillan at mac.mcmillan@cynergistek.com, Krebs at krebsonsecurity@gmail.com, and Sotto at lsotto@hunton.com. ✧