Biggest Security Lapses for 2014-2015 and How to Handle Them

Save to myBoK

By Mary Butler

In the privacy and security world, whenever a big health data breach makes the news, HIPAA experts warn that it's only the beginning and the news will only get worse. Over the last year that has certainly been the case as the size and scope of breaches has climbed.

The last year has also seen some egregious cases of social media mishaps by healthcare professionals—and since social media channels aren't going away, the need to preach best practices is more important than ever.

As we approach the mid-point of 2015, it's time to regroup, look at what went wrong, and figure out how to prevent further embarrassment.

The Year of the Hacker

In August of 2014 Community Healthy System (CHS) announced that a group of Chinese hackers were to blame for a privacy breach affecting 4.5 million patients. Investigators believe that the hackers were looking for intellectual property of the system's networked medical devices, but when that wasn't available they went after patient names, addresses, birthdates, and phone and Social Security numbers instead.

Chris Apgar, CISSP, CEO, and president of Apgar & Associates, says the CHS breach was associated with the Heartbleed bug, making it the biggest breach resulting from the Heartbleed security bug, which struck servers and exposed weaknesses to hackers all over the Internet in April 2014. Apgar doesn't fault CHS for falling victim to Heartbleed that April, but he said the breach perpetrated by hackers that summer could have been prevented if the provider had taken the proper steps to patch the weaknesses the bug exposed. The fact that the hackers were looking for intellectual property was new—and alarming.

"Health IT greatly expanded as have medical devices that transmit data," Apgar says. "Hackers traditionally went after servers and other repositories where large amounts of data was stored. Now with the advent of the Internet of Things there's more data to grab and often it's easier to get to because of deficient security measures put in place by the developers."

To prevent criminals from doing greater damage during a breach, he recommends that providers take a hard look at the medical devices they are purchasing and make sure security is "baked in" or is sufficient for providers to feel comfortable that if the device is stolen or when it's transmitting data that the data is encrypted. He adds that only a handful of providers he's visited have do a really good job of doing this.

Apgar also says that foreign hackers will continue to target the US and other countries since the value of medical data on the black market is so high. If hackers are able to uncover the health records of VIPs and government officials, that becomes key information for foreign governments. Currently most foreign attacks are coming from Eastern Europe and China, says Apgar, but that may change given the value of the data.

When hackers compromised the data of 80 million consumers covered by insurer Anthem, Apgar says he was unsurprised by the difference in scope and the total number of people affected.

"The capability of storing larger and larger amounts of data in one place increases the risk significantly. If there are now hundreds and hundreds of terabytes stored on a server or appliance, it means if the hackers can get in, they will make off with significantly more data than in the past. Given the expanded use of big data over the past year or two I can easily see why the big jump. Hacker sophistication is becoming greater and greater," Apgar says.

Social Media #Fails

As attorney Ashley Trotto points out in a column for the *Knoxville News Sentinel*, the US Department of Health and Human Services has yet to issue formal guidance on how healthcare workers can and cannot use social media platforms with regard to patient information, employers must interpret HIPAA compliance on their own. She cites cases where nurses have been fired for posting shift change updates and Facebook. And in 2013, the *Journal of AHIMA* reported on the case of a Northwestern Memorial Hospital physician posting photos of a drunk patient to his Facebook and Instagram accounts.

Joanna Belbey, a social media compliance specialist at Actiance, suggests it might be difficult for the government to crack down on HIPAA compliance and social media.

"Given the fast moving social media landscape, explicit, rules-based social media guidance from HIPAA would become quickly out of date. A better approach is guidance that is principle based. In other words, focus on the outcomes—for example, protecting patient privacy—rather than how to achieve the outcomes," Belbey says.

Instead, organizations should focus on developing firm policies that are made abundantly clear to everyone. One way to do this is by establishing Social Media Working Groups within organizations comprising representatives from the compliance, legal, public relations, human resources, IT, marketing, and risk departments, as well as direct caregivers such as nurses and physicians. These groups should determine "dos and don'ts."

"Violations of these policies should be unequivocally spelled out as well, so that employees are aware of the ramifications of breaches of the policy," Belbey says. "Indeed, compliance with HIPAA necessitates that healthcare organizations make employees aware of the consequences of the inappropriate use or leakage of PHI and ePHI. This includes communicating in the policy any enforcement actions the organization would take against the employee if they are found in breach of the policy and mandating that employees read and sign acknowledgment of the organization's policies."

What HIPAA does do, according to Belbey, is call for the healthcare industry to monitor and supervise employee activities. On real-time communications platforms such as social media, users can easily create, edit, copy, and share information that could violate the security and privacy of patient records and cause the organization to be in breach of compliance with HIPAA.

"Putting in place a monitoring system that detects when certain key words or phrases are used, holds messages from being sent pending review and sends real-time alerts to managers, could be invaluable for avoiding important or confidential information is leaked. This would not only be a mechanism to ensure and prove compliance with HIPAA but could also protect the corporate brand and reputation," Belbey says.

Mary Butler is the associate editor at The Journal of AHIMA.

Original source:
Butler, Mary. "Biggest Security Lapses for 2014-2015 and How to Handle Them" (Journal of AHIMA), April 2015.
