Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: How Access Controls And Employee Training Are Key To Preventing Breaches

Plus: Courts, states still unsure how to address data breach lawsuits.

Are the wrong people on your staff accessing protected health information (PHI) that they shouldn't or that they don't need to? If so, you could be at risk for an impermissible disclosure blunder.

Rady Children's Hospital in San Diego announced that it discovered two instances of impermissible disclosure of patient information, both of which arose from Rady employees sending more than 200,000 patients' PHI to job applicants, reported **Elana Zana** in a June 19 blog posting for the Seattle-based law firm **Ogden Murphy Wallace Attorneys**. The employees sent spreadsheets containing PHI to job applicants in order to evaluate the applicants' skill sets.

Zana highlights two HIPAA compliance flaws in particular that arose in this case:

1. Access Controls — The HIPAA Security Rule stresses the importance of both internal and external access controls. You must evaluate who within your organization actually needs access to PHI to perform their job functions. Determining whether access to PHI is appropriate is both a requirement of the HIPAA Security Rule and is a good mitigation tactic to avoid impermissible breaches, such as the one here.

2. Training — Under HIPAA, you are responsible for providing HIPAA Privacy and Security training for all members of your workforce. And the training does not stop with just the initial session; you must provide periodic refresher and update training as well. Providing periodic training updates and reminders, including examples of HIPAA breaches like this one, is very useful in driving home how easily HIPAA breaches can occur, and how expensive they are.

"Avoidance of HIPAA breaches altogether is nearly impossible, but proper access controls and training can help mitigate against breaches such as the one that occurred here," Zana concluded.

Failure To Allege Injury Could Nix A Data Breach Lawsuit Against You

If affected patients fail to allege actual injury resulting from a data breach, you might be off the hook for a class action lawsuit — at least, if you're in Illinois.

Back in July 2013, four unencrypted laptops containing PHI were stolen from **Advocate Health and Hospitals Corp**. After Advocate notified the affected patients of the breach, patients filed a class action lawsuit against the organization alleging negligence, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, invasion of privacy, and intentional infliction of emotional distress, according to a June 13 Privacy Alert from the law firm **Nixon Peabody LLP.**

The **Illinois Circuit Court** recently ruled against the plaintiffs, deciding to dismiss the case because the plaintiffs were unable to allege or provide evidence that the PHI contained in the laptops was actually accessed, used or sold, Nixon Peabody reported. Further, the court found that the plaintiffs did not satisfy the "injury in fact" requirement to pursue the claims, which meant that they had to allege actual injury.

"This case is in line with the majority of data breach cases, which require plaintiffs to allege actual injury in order to proceed," stated **Linn Foster Freedman**, a Providence, RI-based partner with Nixon Peabody, in the Alert. But as more plaintiffs pursue state law claims, "and more courts weigh in on the standing issue, the consistency in this area of law will be in jeopardy."

Hacker Incident: Better To Be Safe Than Sorry?

If you discover that your server has been hacked, but there is no evidence that a hacker actually accessed or used the PHI contained on that server, what should you do?

The **Montana Department of Public Health and Human Services** was in just such a situation, and it decided to notify 1.3 million individuals of the hacking incident "out of an abundance of caution." The notified population included individuals who have received services from the state, current and former Department employees, and contractors that have done business with the state, according to a June 27 **Nixon Peabody LLP** Privacy Alert.

An independent forensic investigation discovered that the Department's server had indeed been hacked after personnel noticed "suspicious activity," Nixon Peabody stated. The Department shut down the server on May 22 and reportedly took steps to strengthen security.

Not Ready? Get A Meaningful Use 'Hardship Exception'

If you're fretting over the looming meaningful use payment adjustments set for 2015, here's some good news: You might qualify for a hardship exception.

If you meet certain criteria, you could apply for and receive a hardship exception to avoid the meaningful use payment adjustments. According to a June 12 blog posting by **Elana Zana** for the Seattle-based law firm **Ogden Murphy Wallace Attorneys**, eligible professionals (EPs) may apply for a hardship exception based on the following reasons:

- **Infrastructure** — You are in an area without sufficient internet access, or you face insurmountable barriers to obtaining infrastructure, such as lack of broadband.
- **New EPs** — You are a newly practicing EP who has not had enough time to become a meaningful user. In this case, you can apply for a two-year limited exception to the payment adjustments.
- **Unforeseen Circumstances** — Examples may include a natural disaster or other unforeseeable barrier.
- **Patient Interaction** — You have a lack of face-to-face or telemedicine interaction with patients, or a lack of follow-up need with patients.
- **Practice at Multiple Locations** — You lack control over the availability of certified electronic health record technology (CEHRT) for more than 50 percent of patient encounters.
- **EHR Vendor Issues** — Your EHR vendor was unable to obtain 2014 certification or you were unable to implement meaningful use due to the 2014 EHR certification delays.

If any of these circumstances apply to you, you can apply for a hardship exception by submitting the 2015 Hardship Exception Application to the Centers for Medicare & Medicaid Services (CMS) (www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/HardshipException_EP_Application.pdf).

And CMS will automatically grant a hardship exception to certain EPs, Zana stated. If you meet the following criteria, you will receive a hardship exception based on your status with CMS — without having to submit an application:

- New providers in their first year;
- EPs who are hospital-based (spending more than 90 percent of your covered professional services in an inpatient or emergency department);
- EPs with certain PECOS specialties, such as anesthesiology, pathology, diagnostic radiology, nuclear medicine, and interventional radiology.

Posting Of PHI On Facebook Spurs Lawsuit

What are you posting on social media? Hopefully not protected health information (PHI).

A Facebook posting of Cincinnati-area woman's medical records has led to a lawsuit against a hospital, according to a June 4 news article on Cincinnati.com. In the lawsuit, plaintiff Shawntelle Turley claims that employees of the University of **Cincinnati Medical Center** (UCMC) posted a screenshot of her medical record to a Facebook group. The screenshot

showed her name and her diagnosis of syphilis.

The UCMC employees who posted Turley's medical record purportedly did so at the request of her ex-boyfriend. Turley is seeking more than $25,000 in damages for invasion of privacy, emotional distress, malice, and negligence.

Watch Out SNFs: HIPAA Penalties Will 'Set Records'

Now that the HIPAA audits are back in full swing, you need to be on your guard. And according to government officials, skilled nursing facilities (SNFs) are especially at risk for record-breaking HIPAA penalties.

The **U.S. Department of Health and Human Services**' chief regional civil rights counsel Jerome Meites warned that HIPAA penalties during the next 12 months should "set records," reported Christopher Froeb in a June 26 **Nixon Peabody LLP** blog posting. Meites made these comments during an **American Bar Association** conference in Chicago on June 12 and 13.

Meites urged SNFs and other providers to perform comprehensive risk analyses, particularly now that HIPAA audits have recommenced after the temporary suspension in 2012.

"SNF operators should take note of this increased enforcement and, if necessary, perform internal audits to confirm policies are in place regarding HIPAA compliance," Froeb advised.

You Could Get A Prison Sentence For HIPAA Violations

A relatively new development is terrorizing healthcare providers criminal charges stemming from violating HIPAA.

Case in point: A grand jury indicted a Longview, TX man, **Joshua Hippler**, on charges of Wrongful Disclosure of Individually Identifiable Health Information, stemming from HIPAA violations that occurred from Dec. 1, 2012 through Jan. 14, 2013, according to a July 3 press release from the **U.S. Attorney's Office, Eastern District of Texas.**

During that time, Hippler worked for an East Texas hospital and allegedly accessed protected health information (PHI) with the intent to use the information for personal gain, announced U.S. Attorney **John M. Bales.**

The criminal charges came about after **HHS Office of Inspector General** (OIG) agents conducted an investigation into the purported HIPAA violation. If convicted, Hippler could face up to 10 years in prison.