Health Information Compliance Alert

Enforcement News: How PHI Disclosure By Employees Earned HIPAA Whistleblower Exception

Plus: Illinois courts want to see real injury when considering breach lawsuits.

One of the few exceptions under HIPAA for disclosing protected health information (PHI) without express consent is when an employee or former employee "whistleblower" furnishes PHI to his attorney. But before you disclose patients' PHI to a lawyer, you should make sure you meet four important criteria to qualify as a whistleblower.

Two former employees of the **Arkansas Children's Hospital** (ACH) claimed their employment was terminated in retaliation for raising questions about the ACH's billing practices, reported Providence, RI-based appellate attorney **Steven Richard** in a July 13 blog posting for the law firm **Nixon Peabody LLP**. (See case: Howard ex rel. United States v. Arkansas Children's Hospital, No. 4:13-cv-310 (E.D. Ark. July 1, 2015).)

The former employees disclosed large amounts of PHI to their attorney in anticipation of bringing a whistleblower lawsuit against the ACH, Richard explained. The plaintiffs obtained the PHI during their employment and retained the information after their termination. The plaintiffs sued the ACH for wrongful termination, as well as for retaliatory discrimination in violation of the False Claims Act's whistleblower protection provision.

The ACH countered that the former employees' disclosure of PHI to their attorney violated HIPAA, Richard said. But the **U.S. District Court for the Eastern District of Arkansas** disagreed, ruling that the plaintiffs did not violate HIPAA and instead fell within HIPAA's whistleblower exception.

Pay attention: To show that the plaintiffs qualified as whistleblowers under the HIPAA regulations, they had to prove the following four factors:

1. The ACH is indeed a covered entity;

2. The plaintiffs acquired the PHI in the course of their duties with the ACH when they were workforce members or business associates;

3. The plaintiffs believed that the ACH behaved unlawfully, violated professional or clinical standards, or was endangering patient safety; and

4. The plaintiffs made the PHI disclosure to legal counsel for the purposes of determining their legal options regarding their concerns.

Why Courts Are Still Reluctant To Allow Breach Suits With No Injury

Good news: When a HIPAA breach occurs but the plaintiffs cannot prove an actual injury due to the breach, many state appellate courts are ruling that the plaintiffs have no standing to file the lawsuit. And if this trend continues, you'll be a little safer from a deluge of expensive litigation following a data breach.

After two lower courts dismissed several privacy breach cases, an appellate court has consolidated the cases and made another ruling: the **Second District Illinois Appellate Court** affirmed the lower courts' decisions in the HIPAA breach

lawsuits against **Advocate Health and Hospitals Corporation** d/b/a **Advocate Medical Group**, an Illinois network of affiliated physicians and hospitals (Maglio v. Advocate Health).

Two different lawsuits arose from a breach case in which thieves stole password-protected computers containing the protected health information (PHI) of about four million former and current Advocate patients, according to a July 7 blog posting by **Carolyn Metnick**, a healthcare attorney for **Akerman LLP**. The plaintiffs alleged that Advocate's negligence in failing to follow best practices regarding information security led to the theft of their personal data. The plaintiffs also alleged that Advocate did not secure or encrypt the computers and failed to provide timely breach notification.

"Notably, the plaintiffs did not allege that anyone had improperly accessed or used the information or that they had been the victim of identity theft or fraud," Metnick noted. "On appeal, the plaintiffs argued that the trial courts improperly dismissed their complaints for lack of standing."

But the appellate court shot down the plaintiffs' appeal, calling their claims of injury "speculative," and as such, lacking standing, Metnick said. The plaintiffs also argued that the nature of the data as medical information warrants an implicit finding of harm, but the appellate court again disagreed.

"[The plaintiffs'] claims that they face merely an increased risk of, for example, identity theft are purely speculative and conclusory, as no such identity theft has occurred to any of the plaintiffs," the appellate court wrote. Also, the plaintiffs failed to show "a distinct and palpable injury."

'Overshare' On Social Media Leads To HIPAA Violation

Just because someone is a public figure doesn't mean that their protected health information (PHI) also belongs in the public domain. And with the insatiable lure of sharing everything social media, you may be tempted to "overshare" when it comes to a celebrity's medical information.

Case in point: The popular social media site **Twitter** was the scene of the latest "overshare" of a celebrity's PHI when an ESPN reporter tweeted part of the medical records of **New York Giants** defensive end **Jason Pierre-Paul**. The football player had allegedly seriously injured his hands with fireworks during the July 4 holiday.

Although HIPAA does not regulate reporters and other news media like ESPN, because they aren't typically considered covered entities or business associates under HIPAA, the Miami hospital where Pierre-Paul received treatment and its employees may face penalties of up to $50,000 for each violation and even jail time, according to a July 13 analysis by the law firm **Nixon Peabody LLP**. Florida privacy laws may also levy additional penalties against the hospital, not to mention the potential for a civil lawsuit from Pierre-Paul.

In this case, a worker at the hospital allegedly leaked the PHI to Pierre-Paul's friend, who shared the information on Twitter. As a result, the Giants pulled their $60-million contract offer to Pierre-Paul because of the severe hand injuries.

This is, of course, not the first time that a celebrity's PHI has been leaked. But unauthorized access to, and disclosure of, a public figure's PHI "emphasizes the need for healthcare providers to ensure that their workforce is adequately trained on HIPAA and state information privacy requirements," Nixon Peabody stated. Although providing medical care to a celebrity may generate favorable publicity for the facility, proper training should help providers to avoid drawing the attention of the **HHS Office for Civil Rights** (OCR).

Bottom line: "Providers should clearly inform personnel that unauthorized access of [PHI], even without disclosure, can be enough to violate HIPAA," Nixon Peabody stressed. "Hospitals and other providers also may want to remind personnel, particularly when a public figure is receiving treatment, that electronic record systems typically have an audit function to track who accessed which records."

What You Must Do When Your BA Has A Data Breach

If you are a covered entity (CE) and your business associate (BA) has a breach involving your patients' protected health information (PHI), what are your responsibilities and liabilities versus those of your BA?

On July 23, **Medical Informatics Engineering** (MIE) reported to the **HHS Office for Civil Rights** (OCR) a massive breach affecting nearly four million individuals. According to OCR, the breach was a "hacking/IT incident" involving electronic medical records. Based in Fort Wayne, Indiana, MIE is a business associate (BA) with clients that include the major health systems and physician networks across the state.

Under the HIPAA BA Agreement (BAA), MIE must notify its clients (the CEs) of the breach and HHS, according to a July 2 analysis by attorney **Mary Beth Gettins** of **Gettins' Law**. MIE is also liable for any violations, but the CEs are not liable for the BA's actions under HIPAA.

Caveat: If a HIPAA violation occurs, CEs must demand that the BA correct its wrong practices or violations, Gettins explained. If a BA fails to correct its improper privacy or security practices, the CE must terminate the relationship with the BA.

The CEs, however, are responsible for notifying the affected individuals of the breach. "That means the providers must go to their patients and say there has been a breach in writing. That is the bad news for providers," Gettins noted.

The other bad news is that although CEs aren't liable for their BAs under HIPAA, that doesn't mean that patients won't still hold CEs responsible, Gettins added. "With increasing frequency, affected individuals are filing complaints naming healthcare plans and healthcare providers in cases involving data breaches caused by [BAs]."

Big Breaches: Theft Down, Unauthorized Access/Disclosure Up For July

There were 20 reported breaches affecting more than 500 individuals in the month of July, according to the **HHS Office for Civil Rights'** (OCR) "Wall of Shame," and most (10) of those breaches were due to unauthorized access and disclosures.

Unlike June, which saw mostly theft-related breaches, July yielded only two reported theft incidents. Loss and hacking/IT incidents caused four breaches each. Healthcare providers reported the most breaches (13), while health plans reported six and only one was reported by a business associate (**Medical Informatics Engineering)**.

Also in July, reported HIPAA breaches mostly involved paper/films (seven), while electronic medical records followed close behind with five breaches. Network servers (three), email (three), desktop computers (two), and other portable electronic devices (two) were also noted as locations of breached information.

Link: To keep track of reported large HIPAA breaches, you can go to the OCR's "Wall of Shame" at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.