Health Information Compliance Alert

Enforcement News: How Data Breach Settlement Sets 'Unfortunate Precedent'

Plus: How your BAs can get you into a big breach mess.

Forget a class action lawsuit under HIPAA some plaintiffs are filing lawsuits (and winning settlements) against healthcare providers for data breaches under a variety of other federal and state laws.

After the billing vouchers of more than 13,000 patients went missing from an off-site storage vendor, plaintiffs filed a class action lawsuit against the **University of Miami Health System** (UMHS). The vouchers came from patient records from the health system's Department of Otolaryngology and included patients' names, dates of birth, Social Security numbers, physician names, insurance company names, medical record numbers, and procedure and diagnostic codes.

UMHS recently requested that a Florida judge approve a proposed settlement in the class action lawsuit, according to partner attorney **Linn Foster Freedman** in an Aug. 15 privacy alert posting for the law firm **Nixon Peabody LLP**. Under the settlement agreement, UMHS would pay $100,000 in individual claims, $90,000 in attorneys' fees, and $1,500 to the named plaintiff. UMHS would also conduct risk assessments and remediation.

What's especially curious about this lawsuit is that the plaintiff filed the action under the Fair Credit Reporting Act (FCRA) and Florida state law, alleging that she suffered financial harm because money was withdrawn from her bank account following the breach, Freedman stated. "This is the first time we have seen a settlement by a health system for a data breach under the FCRA, nor do we see how the FCRA can be relevant to the facts of this case."

Moreover, patients' financial information does not appear to have been included in the breached data from the billing vouchers.

Warning: "This settlement is an unfortunate precedent on two levels first, it appears to be a settlement under the FCRA, which is a first to our knowledge," Freedman stated. "And second, it is a settlement of a case where there does not appear to be any relationship between the data breach and the alleged harm and where the attorneys received almost as much as the settlement on the merits."

Bottom line: "Opening these doors in the data breach arena is discouraging," Freedman concluded.

Breach Risk: Keep A Close Watch On Your BAs

Using third-party vendors is always a concern when it comes to handling protected health information (PHI) and other personal or financial information. So here's yet another case to inspire you to make sure that your business associates (BAs) are keeping your patients' data safe and secure.

Hackers accessed the computer systems of Onsite **Health Diagnostics**, a third-party vendor that Tennessee uses to store information on its state employees, WSMV reported on Aug. 26. The hackers stole data on more than 60,000 state workers contained in a data table that included personal information belonging to members who participate in wellness screenings as part of the health plan.

Although the **Tennessee Benefits Administration** (TBA) claims that the hackers did not access any Social Security numbers, financial information or medical information, they did obtain individuals' email addresses, phone numbers, addresses, genders and dates of birth.

No identity thefts have occurred so far related to this data breach, but Onsite is offering affected individuals free identity

CPT® 2023 American Medical Association. All rights reserved.

theft protection. TBA blamed the breach on Onsite's "old computer system," but said that the vendor now has a new computer system in place with new securities, according to WSMV.

Hackers Attack 'Obamacare' Website

If hackers can attack a huge federal government website using relatively low-tech means, how can you be sure that your systems are safe?

On Sept. 4, the **Obama Administration** reported that a hacker had breached the Healthcare.gov website, reported the New York Times. Although investigators found no evidence that the hacker had taken or viewed users' personal data, this breach is nonetheless worrisome for the security of the online federal health exchange.

The Administration claims that the hacking incident was "an intrusion on a test server" that contained no consumer personal information and that the Healthcare.gov website was not even specifically targeted, according to the Times. The test server was connected to the Internet in error, its manufacturer-default password was unchanged, and it was not subject to regular security scans.

Federal employees noticed the breach on Aug. 25. Hackers downloaded malware onto the test server intended as a broader denial-of-service attack that would shut down other websites.

Telemedicine: Don't Forget About HIPAA Compliance

Policymakers are examining all aspects of telemedicine lately from promoting improved care coordination to ensuring proper reimbursement. But a recent telemedicine policy hasn't left out patient privacy either.

On June 11, the **American Medical Association** (AMA) released a list of "guiding principles" for telemedicine services. The list comes on the heels of a policy report from the AMA's Council on Medical Services addressing coverage and payment for telemedicine.

And although the AMA's guiding principles include a wide range of issues, including telemedicine payment rules and ways to improve health outcomes, they also address the unique challenges of maintaining patient privacy and HIPAA compliance while providing telemedicine services.

Links: To read the policy report, go to https://download.ama-assn.org/resources/doc/hod/x-pub/a14-cms-report-7.pdf. The AMA's June 11 announcement is available at www.ama-assn.org/ama/pub/news/news/2014/2014-06-11-policy-coverage-reimbursement-for-telemedicine.page .

Don't Let Terminated Employees Sneak Out With Patients' PHI

Yet another HIPAA breach reinforces all the crucial reasons why you should encrypt all mobile devices and portable data storage, as well as why you must keep a close watch over what employees and former employees take home with them.

A home burglary sparked a breach incident for **St. Elizabeth's Medical Center** in Brighton, Mass., after thieves stole a former employee's laptop and USB thumb drive that both contained 595 patients' protected health information (PHI), according to an Aug. 29 blog posting for the law firm **Nixon Peabody LLP** by attorney **Kathryn Sylvia**. The laptop and thumb drive were not encrypted and contained patients' dates of birth, medical history, diagnoses, test results and medications.

The patients received treatment at St. Elizabeth's **Center for Breast Care** or the hospital's hematology/oncology department sometime from May 14, 2011 through Jan. 31, 2014. The former employee was a physician at St. Elizabeth's.

St. Elizabeth's does not allow storage of unencrypted PHI. Although St. Elizabeth's has reported the theft to affected patients and officials do not believe that the thieves have misused the PHI, local police are still investigating the incident, Sylvia noted.

CPT® 2023 American Medical Association. All rights reserved.

Takeaway: "This should be a lesson for health care facilities and hospitals to ensure that, upon termination, all employees return electronic patient data and all hard drives or USB thumb drives are wiped clean to avoid situations like this," Sylvia stressed.

Why You Could Be Protected From State Law HIPAA-Breach Claims

HIPAA breach lawsuits are still in an uncertain territory when it comes to filing claims under state laws. But many states, like Illinois, are holding fast to the idea that if the plaintiffs cannot prove actual harm from a data breach, they don't have a leg to stand on.

Case in point: In August 2013, **Advocate Health & Hospitals** Corporation reported a large data breach after four laptops were stolen from an Advocate medical group administrative building. The laptops contained unencrypted protected health information (PHI) of more than 4 million patients.

Following the breach, two patients filed a class action lawsuit alleging negligence, violation of the Illinois Personal Information Protection Act, violation of the Illinois Consumer Fraud Act, invasion of privacy, and failure to take necessary steps to safeguard patients' PHI, according to a Sept. 5 Health Law Rx blog posting by healthcare attorney **Carolyn Metnick** for the law firm **Akerman LLP.**

But on July 10, the Kane County Circuit Court in Illinois granted Advocate's motion to dismiss the claims for lack of standing and failure to state a claim, Metnick reported. "The court held that the plaintiffs lacked standing because they could not prove that the information stolen had been accessed or used, and therefore, they could not prove that there had been actual identity theft or harm."

Although the court conceded that an increased risk of harm existed due to the laptops' theft and potential accessibility of the unsecured PHI, the thieves would actually need to disclose, sell or otherwise misuse the PHI for the lawsuit claims to be valid.

"This case is an example of the challenges in bringing claims under state law for HIPAA data breaches," Metnick explained. "Because most, if not all, states require that plaintiffs show actual injury to state a sufficient claim, plaintiffs often must overcome a high hurdle because they cannot show that their PHI was used to commit identity theft or other harm."

Caveat: "Even though state causes of action may be difficult to prove, covered entities and business associates face penalties under HIPAA," Metnick warned. "Also, although difficult, state causes of action are still a risk."

CPT® 2023 American Medical Association. All rights reserved.