Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: How You Can Overcome HIPAA Lawsuits Based On 'Speculative' Claims

Plus: Breach impact grows by leaps and bounds over time for Cedars-Sinai.

More and more courts are dismissing lawsuits involving HIPAA breaches when the plaintiffs cannot prove that their personal information was actually used. Here's yet another case with a similar outcome.

In 2012, **Alere Home Monitoring Inc**. suffered a data breach when a password-protected laptop was stolen from an employee's vehicle, according to an Oct. 10 blog posting by partner attorney **Linn Foster Freedman** of the law firm **Nixon Peabody LLP**. The laptop contained 116,000 patients' names, addresses, birthdates, Social Security numbers and diagnosis codes.

Following the breach, patients filed a putative class action lawsuit against Alere, alleging negligence and unjust enrichment, as well as violations of the Fair Credit Reporting Act (FCRA), the Unfair Competition Law and the California Medical Information Act, Freedman reported. Alere asked the California court to dismiss the claims.

The court agreed with Alere, dismissing the claims because the plaintiffs couldn't prove that Alere is a credit reporting agency under the FCRA and that the information release constituted a loss of property. Alere claimed that the only damages alleged were for risk of identity theft and wrongful use of medical information, and invasion of privacy all of which were "speculative" claims, Freedman noted.

Bottom line: "This decision is consistent with many other similar cases, so it appears that this area of the law is becoming more and more well-settled," Freedman said.

Breach Aftermath: Time Is Not Always On Your Side

As the months tick by after a HIPAA breach, you might think that you're getting more and more breathing room from a bad situation. But that's not always the case the passage of time can actually reveal that a breach was in fact much bigger than you first thought.

Case in point: When **Cedars-Sinai Medical Center** reported a data breach of patient records this past summer, the count of affected individuals was at least 500 patients. But after recently consulting a data forensics firm, the hospital has increased the number of affected patients to a whopping 33,136, according to an Oct. 1 article in the Los Angeles Times.

The breach occurred when burglars stole a laptop from a Cedars-Sinai employee's home. Although the laptop was password-protected, it didn't have additional encryption software to further protect the patient data contained on the laptop. The laptop was never recovered and law enforcement hasn't made any arrests in connection with the burglary.

Don't Let Your Patients' PHI Blow In The Wind

If you needed another reason to ensure that your business associates are HIPAA-compliant in the face of a breach incident, here's one for you.

On Oct. 23, potentially thousands of medical records flew out of the back of a truck in southwest Omaha, NE, according to KETV Omaha. The truck, owned by Lincoln, NE-based **Medi-Waste Disposal**, was carrying paper medical records to a disposal and storage site. The back door of the truck wasn't latched and the papers flew out the back as the truck traveled down the road.

Good Samaritans and volunteers attempted to retrieve the records as the papers blew around the roadside, and Medi-Waste believes they recovered all documents, KETV reported. Medi-Waste has promised to establish new checks and balances to secure documents better in the future.

Get Ready For More HIPAA Security Scrutiny From OIG In 2015

The **HHS Office of Inspector General** (OIG) has released its annual Work Plan for fiscal year (FY) 2015, and HIPAA security is on its "hit list."

The OIG's Work Plan lists items like analyzing the IT security of community health centers and reviewing controls over networked medical devices at hospitals. The OIG wants to determine whether the Centers for Medicare & Medicaid Services' (CMS) oversight of hospitals' security controls over networked medical devices is sufficient to effectively safeguard electronic protected health information (ePHI).

"Computerized medical devices, such as dialysis machines, radiology systems, and medication dispensing systems that are integrated with electronic medical records (EMRs) and the larger health network, pose a growing threat to the security and privacy of personal health information," the OIG states in its Work Plan. "Such medical devices use hardware, software, and networks to monitor a patient's medical status and transmit and receive related data using wired or wireless communications."

Link: To view the OIG Work Plan for FY 2015, go to http://oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf.

Why EPs Are Failing MU Audits

If you're wondering how providers are doing with their meaningful use (MU) compliance, you might be surprised at the results so far from the new MU audits.

Centers for Medicare & Medicaid Services (CMS) audit results of MU compliance are beginning to emerge, and so far eligible hospitals (EHs) are faring much better than eligible professionals (EPs). Only 4.7 percent of EHs failed the audits, while EPs had far higher rates of failure, stated associate attorney **Elana Zana** in an Oct. 8 blog posting for the law firm **Ogden Murphy Wallace Attorneys**.

Approximately 21.5 percent of EPs subjected to prepayment audits did not meet MU standards. According to CMS, there were two reasons for this failure:

1. Failure to use a certified EHR; and
2. Failure to meet MU objectives and associated measures.

And most of those EPs who failed the audits (92.9 percent) did not meet the appropriate objectives and associated measures, while only 7.1 percent of those audited failed to use a certified EHR when attesting, according to a Sept 19 analysis by **Steve Spearman**, founder and chief security consultant for **Health Security Solutions** in Central, SC.

As for post-payment audits, approximately 24 percent of EPs failed to meet MU standards, for the same two reasons as the prepayment failure, Spearman reported. Most of the EPs who failed their post-payment audits (98.9 percent) did not meet the MU objectives and associated measures.

Cost: And for those EPs who failed the MU audits, providers will need to return their incentive payments to CMS the average returned incentive payment was $16,862.81, Spearman noted. Of course, providers who fail the MU post-payment audits can appeal the audit outcome, and won't need to return incentive payments if the appeal is successful.

But Spearman warned that for EPs "counting on incentive payments to cover EHR start-up costs and associated business expenses, returning thousands of dollars could be devastating." And both pre- and post-payment audits are occurring on a regular basis, indicating that the question of an EP or EH being audited is not "if" but "when."

Pay attention: Because MU incentives can play such a vital role in organization finances, it is important to make every

effort to satisfy all MU objectives and associated measures, Spearman stressed.

"More audits are coming, and making sure that you have double-checked your numbers before attesting and performed your security risk analysis, including an implementation plan and completion dates, is necessary," Zana concluded.