Health Information Compliance Alert

Enforcement News: Why Hospital Isn't Liable For Employee's Facebook Posting Of Patient's PHI

Plus: Senators want HHS to clear up confusion over medical identity theft and HIPAA.

Yet another judge ruled that a healthcare entity is not liable for an employee's HIPAA violation when those actions were outside the scope of the staffer's job duties. And although this ruling points toward a growing trend of opening the litigation doors to HIPAA-related lawsuits against individuals, it's also a relief for healthcare entities.

An Ohio court judge ruled that the **University of Cincinnati Medical Center** (UCMC) is not liable for a former employee's HIPAA violation in divulging a patient's protected health information (PHI) on Facebook, according to a Nov. 24 **Nixon Peabody LLP** blog posting by partner attorney **Rebecca Simone**.

While working for the UCMC's financial services department, the employee allegedly accessed patient medical records for personal viewing and posted a screenshot of the records on the social media site (see "Posting Of PHI On Facebook Spurs Lawsuit," HICA Vol. 14, No. 7, page 55). The screenshot revealed that a certain patient had a sexually transmitted disease.

As a result, UCMC fired the employee and the patient pressed charges against both the former employee and UCMC. In the case against UCMC, however, the court decided that "the hospital is not liable for employee actions outside the scope of their job duties," Simone noted. "The court reasoned that a hospital cannot be responsible when [it] had a privacy policy in place and an employee individually chose to disregard and violate that policy."

Impact: "This is a big win," noted attorney **Mary Beth Gettins of Gettins' Law** in a Dec. 7 blog posting. Because UCMC had proper employee training, policies, and disciplinary code/sanctions, the court found UCMC not liable.

"Yes, having the right things in place and doing the right things made all the difference," Gettins added. "Employees were given the education about what was okay and not okay under HIPAA and other privacy laws."

Should You Worry About Violating A Medical Identity Thief's HIPAA Rights?

You and your patients may soon see more support from the federal government when it comes to preventing and mitigating the effects of medical identity theft especially with new pressure to do so coming from Congress.

In a Nov. 10 letter to the **Centers for Medicare & Medicaid Services** (CMS) and the **HHS Office for Civil Rights** (OCR), the Chairs and Ranking Members of the Senate Committee on Health, Education, Labor, and Pensions and the Committee on Finance expressed their concerns with what HHS is doing to support and protect victims of medical identity theft.

Citing many large health information breaches lately, the senators raised fears regarding the surge in major cyberattacks on large insurers like **Anthem BlueCross BlueShield** and healthcare providers like the **UCLA Health System**. "We are concerned that data theft will continue to rise and will result in an increase in medical identity theft," the senators wrote.

Medical identity theft can have serious financial repercussions for victims, as well as adulteration of victim's medical records, which can have dangerous health consequences, the senators pointed out. And although the HIPAA Privacy Rule grants patients the right to view and request corrections to their medical records, "there is widespread confusion about how this rule applies in the case of a thief's information being comingled with that of his or her victim's."

Truth: In fact both HHS and the **Federal Trade Commission** (FTC) have addressed this very issue partner attorney **Adam Greene** in a Dec. 1 analysis for the law firm **Davis Wright Tremaine LLP**. The HIPAA Privacy Rule grants individuals the right to copies of their medical records maintained by covered healthcare providers and health plans. If you give victims of medical identity theft copies of their own records, you're not violating the thief's HIPAA privacy rights even if the thief's information is mixed with the victim's.

The senators posed a list of specific questions regarding medical identity theft to CMS and OCR, including (for example):

- What support does HHS provide to federal, state, and local law enforcement officials to aid their response to medical identity theft?
- What services does CMS offer to Medicare and Medicaid beneficiaries who suspect they are victims of medical identity theft?
- How do OCR and CMS coordinate medical identity theft prevention and mitigation efforts?
- Does HHS believe that the HIPAA Privacy Rule gives a victim of medical identity theft the right to access his or her health record if it contains a thief's health information? Has HHS encountered confusion on this matter previously? If so, what steps has HHS taken to address the confusion over the meaning of the Privacy Rule on this matter?

Link: To read the senators' letter to CMS and OCR, go to www.help.senate.gov/imo/media/doc/Medical Identity Theft Letter--final.pdf.

Healthcare Providers Take The Brunt Of Breaches In November

At least for November 2015, reported HIPAA breaches seem to come from all types of causes and affect all forms of protected health information (PHI) storage and transmission. Here's what you need to know about the latest breach trends.

Of the 10 total HIPAA breaches affecting 500 individuals or more reported to the **HHS Office for Civil Rights** (OCR) in November, only one was from a health plan and the rest were from healthcare providers. Three breaches involved theft, another three stemmed from unauthorized access/disclosures, another three involved hacking/IT incidents, and one stemmed from loss.

The cases involved various locations of breached information: paper/films (three cases), laptops (two), email (two), network server (one), and desktop computer (one).

One case involved multiple locations, including a desktop computer, laptop, network server, email, and other portable electronic device. This was the largest breach in November, reported by **OH Muhlenberg LLC** in Kentucky, stemming from a hacking/IT incident and affecting 84,681 individuals. You can visit the OCR's "Wall of Shame" at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

New York Providers: AG Is Fed Up With HIPAA Breaches, Putting You 'On Notice'

Not all healthcare entities get off the hook for an employee's HIPAA violation, especially if the entity plays a role in breaching its own patients' protected health information (PHI).

So goes the case of the **University of Rochester Medical Center** (URMC), which agreed to pay a $15,000 fine as part of a settlement with the **New York State Office of the Attorney General** (AG). The settlement agreement also requires URMC to train its workforce on policies and procedures related to PHI and notify the AG of future breaches, according to a Dec. 2 announcement by the AG **Eric Schneiderman**.

Watch out: "This settlement strengthens protections for patients at URMC, and it puts other healthcare entities on notice that my office will enforce HIPAA data breach provisions," Schneiderman said in the announcement. "Other medical centers, hospitals, healthcare providers, and healthcare entities should view this settlement as a warning, and take the time now to review and amend, as needed, their own policies and procedures to better protect private patient

information."

The data breach occurred in April 2015, when a URMC nurse practitioner who was planning to leave the medical center's employment and join a private practice allegedly asked for and received files of 3,403 patients she had treated, without patient authorization. She then purportedly gave that list of patient names, addresses, and diagnoses to her future employer, **Greater Rochester Neurology** (GRN), which then mailed letters to the patients informing them that the nurse would be joining the practice and advising them on how to switch to GRN.

URMC learned of the breach when patients began calling with complaints about the letters. URMC terminated the nurse, sent notification letters to the affected patients, and alerted the media of the breach. The AG's office launched an investigation into the breach incident, which then led to the recent settlement agreement with URMC, which you can read at www.ag.ny.gov/pdfs/URMC_Letter_ Agreement_Fully_Executed_11_30_2015.pdf.