Codify
BY AAPC

Health Information Compliance Alert

Enforcement: Feds Ramp Up As Year Winds Down

If you ignore your HIPAA risks, expect to pay the price.

Over the past year, HIPAA enforcement has been spotty at best. But the **HHS Office for Civil Rights** (OCR) pulled no punches in November with a hat trick of cases for the ages.

Settlement Highlights the Importance of Encryption

Mobility drives healthcare today; it's just that simple. Handy devices promote efficiency and are easy to use. But, laptops, cell phones, and tablets are ripe for the taking and easy to lose - and that's become a big problem for covered entities (CEs), amounting to big penalties and hefty settlements for the loss of electronic protected health information (ePHI).

Details: In 2013 and 2017, the **University of Rochester Medical Center** (URMC) in New York filed breaches for a lost unencrypted flash drive and stolen unencrypted laptop respectively, according to an OCR release.

Upon investigation, OCR uncovered a laundry list of compliance issues, including risk analysis fails, security measure snafus, lackluster mobile device management (MDM), and encryption problems. Additionally, URMC was already on OCR's radar after a 2010 investigation showed the organization had previously failed to implement encryption on its mobile devices.

Result: In order to rectify its substantial compliance issues, URMC settled potential violations with OCR for $3 million. The large teaching hospital system, which employs over 26,000 individuals, also agreed to a corrective action plan (CAP) and two years of OCR monitoring, notes the release.

"Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk," says OCR director **Roger Severino** in the brief. "When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect."

Read more about URMC's settlement, CAP, and monitoring at www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html.

Internet Exposure Leads to Big CMPs

Even state-run agencies collide with HIPAA rules now and again. That's what happened to the **Texas Health and Human Services Commission** (TX HHSC), a subsidiary of Texas HHS, after it failed to clean up an ePHI issue that allowed 6,671 individuals' names, addresses, Social Security numbers, and treatment information to be viewable on the internet, an OCR release says.

The commission assists vulnerable Medicaid beneficiaries, offering a plethora of care like mental health and substance abuse services as well as operating a variety of state-run venues, including nursing homes, childcare facilities, and supported living centers. The **Department of Aging and Disability Services** (DADS), a part of TX HHSC since 2017, is central to the HIPAA violation details.

"The breach occurred when an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials," OCR relates. The agency follow-up showed that DADS didn't conduct "an enterprise-wide analysis," nor did it implement HIPAA Security Rule requirements.

In addition, these audit failures and access problems led to the exposure of the ePHI online, suggests the release. And

that resulted in a $1.6 million civil monetary penalty (CMP) from OCR.

"No one should have to worry about their private health information being discoverable through a Google search," Severino reminds in the report.

Review TX HHSC's case at www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html.

Know What Constitutes PHI

Two of the most important elements of HIPAA relate to identifying PHI and breach notification - one organization stumbled over both. **Sentara Hospitals** agreed to pay OCR $2.175 million and enter into a CAP plus monitoring for an April 2017 breach that exposed the PHI of 577 patients, a release notes.

Sentara, which operates 12 acute care hospitals in North Carolina and Virginia, received a complaint that it had mailed a patient's PHI to another person, but that was only part of the issue. After analyzing the breach, the organization significantly miscalculated how many individuals were impacted by the incident, which resulted in the underreporting of the breach to those affected.

After a risk assessment, Sentara erroneously thought it "only needed to notify eight individuals of the breach because the other disclosures did not contain a patient diagnosis, treatment information, or other medical information," explain **Foley & Lardner LLP** attorneys **Jennifer J. Hennessy** and **Kelly A. Thompson**, in a post from the law firm's Health Care Law Today blog. "That is, Sentara determined the other disclosures created only a 'low risk of compromise' to the PHI and thus, notification was not required."

But OCR felt differently about the matter. "HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed." Severino says in the release.

He adds, "When healthcare providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."

See details of the Sentara settlement at www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html.