Health Information Compliance Alert

Case Study: Compliance Fails Equal Major CMPs

Tip: Don't ignore your risk analysis recommendations.

If you fail to fix your HIPAA issues, you may find the feds knocking on your front door. A recent case illustrates that repeat offenders will have to answer the call and pay the price.

Background: Miami-based **Jackson Health System** (JHS) discovered that ignoring HIPAA violations comes at a cost. The "nonprofit academic medical system" hit the triple crown of HIPAA noncompliance with failures linked to the Privacy, Security, and Breach Notification Rules, suggests an **HHS Office for Civil Rights** (OCR) release. JHS' troubles started in 2013 with an investigation that uncovered the lost paper records of 756 patients and snowballed with more violations in the years following. The end result: a $2.15 million civil monetary penalty (CMP) imposed by OCR.

In addition to JHS' 2013 issue, the organization - which consists of 12,000-plus employees across a spectrum of hospitals, urgent care centers, offices, nursing homes, and clinics and serves more than 650,000 patients every year - also suffered these HIPAA infractions:

- In the thick of the first internal audit, JHS found that its Health Information Management Department had also misplaced three more boxes of patients' records in 2012, bumping its original lost protected health information (PHI) numbers to 1,436, the OCR says. The caveat, however, is that JHS didn't report the violation until 2016.
- After a famous NFL player's PHI was exposed in a media incident, OCR got involved in 2015, indicates the Notice of Proposed Determination on the case.
- Two hospital staffers checked out the patient's EMR for nonmedical purposes, JHS discovered after the media exposure.
- Finally, JHS sent OCR a breach report in 2016 due to an inside threat; an employee was caught selling PHI and had accessed more than 24,000 patients' records.

"OCR's investigation revealed a HIPAA compliance program that had been in disarray for a number of years," acknowledges **Roger Severino,** OCR director, in a release. "This hospital system's compliance program failed to detect and stop an employee who stole and sold thousands of patient records; lost patient files without notifying OCR as required by law; and failed to properly secure PHI that was leaked to the media."

Why Is the JHS Case Important?

There were numerous instances when JHS dropped the ball on HIPAA compliance, but the overarching factor in the case relates to its failure to properly address risks. According to the Notice of Proposed Determination, third parties conducted risk analyses of JHS in 2014, 2015, 2016, and 2017 - and the covered entity (CE) passed on those details to OCR. Plus, the CE audited itself in 2009, 2012, and 2013 and submitted those risk assessments to OCR, too.

"From July 22, 2013 through Jan. 27, 2016, JHS failed to implement policies and procedures to prevent, detect, contain, and correct security violations as required by 45 C.F.R. § 164.308(a)(l)," the notice says. "Specifically, JHS failed to conduct an accurate and thorough risk analysis, implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, and implement procedures to regularly review records of information system activity."

CMP Amount Doesn't Necessarily Translate to Violation Severity

Over and over, OCR determined that JHS did not follow through and manage its HIPAA risks, exposing individuals' PHI at

every turn. In reality, the penalties could have been a lot worse.

However, JHS waived its rights to a hearing before an Administrative Law Judge (ALJ) as well as a petition for a judicial review. This seems to have impacted the CMP amount; moreover, the Tier 2 penalty aligns with OCR's decision making in other cases this year.

Reminder: Medical Informatics Engineering, Inc. received a $100,000 settlement for the unauthorized access of 3.5 million patients' PHI in May while **Elite Dental Associates** agreed to pay $10,000 for a social media violation last month.

But experts caution CEs to remain vigilant as the smaller than usual settlements and/or penalties may have more to do with a CE's willingness to work with OCR than the actual severity of the violations.

"I do find the Tier 2 penalty surprising," says attorney and shareholder, **Danielle L. Dietrich,** with **Tucker Arensburg** in Pittsburgh. "When you compare it to other recently announced penalties and settlements, it does seem that JHS got a good deal - considering the circumstances."

"I am also surprised that OCR considered this to be a Tier 2 violation given the pervasive neglect of HIPAA obligations, particularly after OCR previously investigated JHS," agrees attorney **Lauren M. Ramos,** with **McGuire Woods LLP** in Richmond, Virginia. "OCR may have considered that JHS did not fight the allegations and cooperated with OCR."

Ramos continues, "Enforcement actions in the last few years indicate that OCR does not want to be overly punitive and will take into account mitigating factors when possible. However, the enforcement actions that have been publicized in recent years have been settlements, rather than imposition of civil monetary penalties under the statutory penalties."

In fact, two cases finalized last week reiterate that JHS' situation was unusual. "There was a $1.6 million Tier 2 civil money penalty against **Texas Health and Human Services Commission** just announced on November 7, 2019. In that case, due to a server migration, 6,617 patients had their information available on the internet," relates Dietrich. "It appears that THHSC reported pretty promptly - less than 60 days."

She adds, "Also, there was just a $3 million settlement announced on November 5, 2019 with the **University of Rochester Medical Center** regarding the loss of a flash drive and the theft of an unencrypted laptop involving far less patient data than in the JHS scenario."

These breaches are relatively small potatoes compared to JHS' laundry list of issues, yet the organizations received harsher treatment from OCR.

And that's why Dietrich advises CEs to remain on top of compliance. "Take every single breach seriously, even if it seems very small," she cautions.

End game: There's no denying that OCR enforcement this year has been significantly scaled back after 2018's record-setting year. But with three big cases heading into the final stretch of 2019, there's no telling what's around the bend.

Note: See the JHS case specifics at www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jackson/index.html.