Codify
BY AAPC

Health Information Compliance Alert

Case Study: 5 Breaches Net $3.5 Million in Fines for Large Health Organization

Risk management must be pervasive or violations will ensue, OCR advises.

The old saying "the bigger they are, the harder they fall" epitomizes many of the large-scale HIPAA violations impacting healthcare today, with penalties for the breaches costing providers millions. One organization's recent failure to properly define, control, and reduce the loss of its patients' electronic protected health information (ePHI) spotlights the importance of risk assessment, analysis, and management no matter the practice size.

Lowdown: With locations spanning the United States, provider and supplier for patients suffering from chronic kidney failure, Fresenius Medical Care North America (FMCNA), reported HIPAA breaches at five of its branches in January of 2013. The events occurred "between February 23, 2012 and July 18, 2012," and exposed the ePHI of these "five separate FMCNA-owned covered entities," indicated an HHS Office for Civil Rights (OCR) release on Feb. 1, 2018. The potential violations ran the gamut from HIPAA Privacy rule charges to failure to register and integrate measures that are required under the Security rule.

"The number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprise-wide risk analysis for a covered entity," said OCR Director **Roger Severino** in the OCR release. "Covered entities must take a thorough look at their internal policies and procedures to ensure they are protecting their patients' health information in accordance with the law."

Result: The five breaches, which happened at FMCNA facilities in Florida, Alabama, Arizona, Georgia, and Illinois, cost the group $3.5 million in penalties paid to OCR. In addition, the feds required Fresenius to institute a "comprehensive corrective action plan, in order to settle potential violations of HIPAA," the release noted.

Don't Ignore the Security Requirements

In the FMCNA case, the organization failed to implement the necessary safeguards at its numerous facilities under the HIPAA Security rule. Unfortunately, this negligence to properly assess risk across the board led, also, to the impermissible disclosure of patients' ePHI, which violated the HIPAA Privacy rule. Most of the problems identified in these five breaches could have been solved with better compliance protocols upfront.

Important: Controlling practice processes to protect patients and secure your data is essential - and it's mandated by the federal government. The HIPAA "Security Rule requires organizations to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations," states Section 45 C.F.R. § 164.308(a)(1) of the HIPAA Security rule. "Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard."

"Planning is the key," advises attorney **John E. Morrone**, a partner at Frier Levitt Attorneys at Law in New York. "Practices need to have appropriate policies and procedures in place and follow those procedures." He adds, "All too often we are retained by clients to help with a payor audit or a HIPAA breach investigation, and the entity has never implemented any type of comprehensive plan."

Beef Up Your Practice Risk Management with These Basics

You can stave off crippling fines by performing a thorough HIPAA risk analysis in order to comply with the Security rule, if you haven't already. "The first step in the risk analysis is to look at the 'big picture' to identify potential risk points," explains **Jim Sheldon-Dean**, Principal and Director of Compliance Services for Lewis Creek Systems, LLC, in Charlotte,

Vermont.

Start by identifying what systems are holding onto electronic health information that contains PHI, including electronic health records and business files, Sheldon-Dean advises. "Look at how those systems move information within the entity, as well as to business associates outside the entity or to other entities for other purposes."

After identifying the risk points, do a more detailed risk assessment of your individual systems. You identify their specific risk points, as well as significance - and the likelihood that a problem will occur - and then address it, Sheldon-Dean instructs.

There are several ways to do the risk analysis assessment, he adds, but the simplest approach is to use a methodology defined by the National Institute of Standards and Technology (NIST) special publication on risk analysis. NIST also offers step-by-step instruction with its HIPAA Security rule toolkit on how to set up and maintain electronic and technical standards.

You can find NIST's guidance at: https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final#.

Endnote: Part of any strong risk management program includes staff training on HIPAA. Employees need to know not only the basic requirements to run a compliant practice, but also the cost of a violation to a provider's reputation and bottom line. Oftentimes, training is not a priority and that's when problems arise. Morrone cautions, "It seems that compliance with laws, regulations and documentation standards are left to chance, as little direction has been provided to the workforce in how to properly perform."

Resource: To read the OCR release on the FMCNA breaches, visit www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.