Health Information Compliance Alert

Case Study: Wrongful Disclosure May Net Patient Coordinator Jail Time

Tip: Ensure security at affiliate offices, too.

Under HIPAA, covered entities (CEs) are responsible for ensuring that their patients' protected health information (PHI) is safe and secure. But sometimes staff don't know the rules and seek access to information out of curiosity or even malice. A recent case highlights why poking into medical records is a bad idea.

Background: Last month, **Linda Sue Kalina** pled guilty to the wrongful disclosure of two patients' PHI, indicates a **Department of Justice** (DOJ) release. Between March 2016 and June 2017, Kalina worked as the University of Pittsburgh Medical Center (UPMC) patient information coordinator. During that time period, she also worked at its Mars, Pennsylvania-affiliate, Tri Rivers Musculoskeletal Centers (TRMC), where she improperly accessed 111 UPMC patients' PHI.

It gets worse. "On August 11, 2017, Kalina unlawfully disclosed personal gynecological health information related to two such patients, with the intent to cause those individuals embarrassment and mental distress," the DOJ stresses. These two particular patients had previously worked with Kalina at a different company.

According to the federal report, the seriousness of the crime dictates the sentencing. The total sentence may include up to 10 years in prison and/or a fine of $250,000. Kalina's sentencing date is June 25, 2019.

Include Real-World Cases and a Sanction Policy in Your Training

Remember, there is a "workforce training and management" section under the administrative safeguards of the HIPAA Security Rule. "A covered entity must provide for appropriate authorization and supervision of workforce members who work with ePHI," the **HHS Office for Civil Rights** (OCR) reminds.

The Rule also charges CEs with providing security training for staff on HIPAA policies and procedures as well as enforcing compliance protocols with sanctions for workers who violate the regulations

"Covered entities [CEs] may want to consider including Kalina's or similar cases in its workforce training to highlight the serious consequences for those who access a patient's medical record without authorization," advises Cincinnati-based attorney **Paulette Thomas** with national law firm **Baker Hostetler** in its Health Law Update blog.

When putting together your training materials, you may want to include the specifics of employee punishments for ignoring HIPAA, Thomas suggests. She mentions the following things may occur as part of a workforce sanction:

Possible suspension or dismissal from job.

- Noncompliance reported to state, professional, and medical licensing institutions.
- Notification of PHI disclosure to individuals involved.

Important: Though federal punishments may not deter employees who seek to hurt patients, "the DOJ or state agencies may bring a criminal action against the workforce member which can result in a prison sentence and payment of a fine," cautions Thomas.

Read the DOJ release at www.justice.gov/usao-wdpa/pr/former-patient-coordinator-pleads-guilty-wrongfully-disclosing-health-information-cause.

Codify
BY AAPC