Health Information Compliance Alert

Case Study: How To Handle Employee 'Snooping' HIPAA Breaches

Follow these tips to protect yourself when terminating peeping employees.

You know what curiosity did to the proverbial cat, and the consequences are just as dire when you have curious employees meddling in your patients' records. If an employee is accessing patient information for personal or otherwise non-business purposes, this is a HIPAA violation (and technically a breach). Here's what you can learn from this recent breach case.

Prying out of Curiosity is Not Okay

Background: San Francisco-based **California Pacific Medical Center** (CPMC), an affiliate of **Sutter Health**, recently notified 844 of its patients after a self-audit of its electronic health record (EHR) system revealed inappropriate "snooping" by an employee, according to a Jan. 23 CPMC announcement.

The initial audit revealed that a pharmacist employee accessed 14 patients' records, but an expanded investigation identified 844 patients whose records the pharmacist may have accessed without an apparent business or treatment purpose, CPMC said. From October 2013 to October 2014, the employee accessed information like patient demographics, Social Security numbers (last four digits only), clinical information and diagnoses, and prescription information.

CPMC fired the employee and notified the 844 affected patients. "CPMC has no evidence of a malicious intent or any unauthorized sharing of patient information by the employee," the provider stated. "CPMC believes that the employee accessed the information out of curiosity."

Cultivate a 'No-Spying' Culture

Employee "snooping" is nothing new to the world of HIPAA data breaches but it's a big problem, especially because employers are suffering the consequences for employees' bad behavior. "There have been a number of cases where the employers were held accountable," such as the cases of **Walgreens** and the **University of California Medical Center**, according to a recent blog posting by **Mary Beth Gettins** of **Gettins' Law LLC.**

So what can you do to prevent, or at least mitigate the impact of, employee snooping? Gettins offered the following tips:

- **Expressly and unequivocally state** in office policies and procedures that access to patient records for personal and non-business reasons is strictly prohibited.
- **Take a strong stance and disciplinary action** against employees for accessing records for personal or non-business reasons.
- **Use software or applications** that track and/or monitor patient record access.
- **Fire any employee** who is snooping.

Cover Yourself When Terminating Employment

Caveat: But if you fire an employee for prying, this could cause liability on the employee front, Gettins warned. Make sure you have the following in place before firing a nosy employee:

- Evidence of the snooping;
- Policies and procedures regarding wrongfully accessing health information;
- A confidentiality and non-disclosure agreement signed by the employee;
- Documentation showing the employee received training regarding wrongful use, access and disclosure of health information; and

- A clear history showing that you have consistently responded to violations of HIPAA and state healthcare privacy laws.

Lesson learned: Have the above items in place before firing the employee, so you can minimize your risks of claims for unemployment compensation, wrongful termination, and discrimination, Gettins advised. And beware that if you fail to take action in the event of improper access to health information by an employee, you're violating HIPAA and other health care laws and you could damage your reputation and expose your organization to claims for liabilities and damages.