Curiosity Can Often Kill the Cat in Healthcare

Save to myBoK

By Traci Waugh, RHIA, CHPS, CHC

“Being inquisitive about other people’s affairs may get you in trouble.”

“Momma always said to mind your business.”

“Curiosity killed the cat.”

There are plenty of well-known, well-worn sayings that warn us about the dangers that come with unchecked curiosity. And yet, curiosity can be a difficult impulse to curb—even when it comes to healthcare employees with the means to access sensitive information without proper authorization.

In addition to the various external threats to privacy in healthcare, privacy officers also need to keep an eye out for the potential threat of “curious cats,” and have a plan to mitigate and prevent their actions. This can be an issue in rural and small town healthcare settings in particular—where employees are more likely to know the patients being treated. Improper access of fellow hospital employees’ information is also a danger, regardless of the setting.

While breaches involving ransomware, malware, and other cybersecurity issues continue to monopolize the news, rural privacy officers are often more concerned with snoopy employees. These might be curious staff members who feel that knowing why a patient presents to the hospital can help them provide assistance to the patient or their family, or might simply be people being nosy.

Justifications for a breach that have likely been heard before include “I was concerned with the co-workers well-being” or “I didn’t want to bother the family so I just checked the computer really quick.” It is so easy—the temptation is only a few clicks away.

Although privacy officers provide training to employees to help combat this issue and facilitate resisting the temptation, is it enough? What if the employee doesn’t think before clicking? What is the proper response from a privacy officer? Consider the following scenario.

Example Scenario: The Incident

Janet, a manager of utilization review at Hospital A, has been an employee for 20 years and has a stellar performance record. Occasionally, Janet is called to assist with patients in the emergency room. On Tuesday at 11 a.m., Janet hears that Molly, a nurse at Hospital A, was in a car accident and is being seen in their emergency room. Janet heard that the police were in the emergency room, too. Janet is worried about Molly because rumor has it that Molly may have a drinking problem and has been going through a divorce. Janet wanted to check if Molly needed any assistance so she quickly logs in to check Molly’s status in the emergency room. Janet discovers Molly has only minor injuries but her blood alcohol level is high. Janet was not asked to go to the emergency department for a consult nor did she go see Molly in the emergency room. Molly is discharged.

Two days later, Molly is concerned that her privacy has been breached and requests a privacy audit on her health record. The audit reveals that Janet accessed Molly’s medical record and reviewed lab results. The privacy officer interviews Janet. Janet explains that she accessed Molly’s chart in case she was going to need to assist in the emergency room.

What steps should Hospital A’s privacy officer take in response to this incident?

Example Scenario: The Investigation

First, the privacy officer should refer to the definition of "breach." A breach is the acquisition, access, use, or disclosure of protected health information (PHI) in a way that compromised the security or privacy of the PHI.[1]

Next, it's time to review the incident. Does it meet any of the breach exceptions outlined in the HIPAA Breach Notification Rule 45 CFR §§ 164.400-414?[2] Questions to ask include:

- Was Janet's access an unintentional acquisition, access, or use of protected health information by a workforce member or made in good faith and within the scope of authority?
- Was Janet's access an inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity?
- Does Hospital A have a good faith belief that Janet would not have been able to retain the information?

In the above scenario, Janet's actions do in fact constitute a breach. Her access compromised the privacy of Molly's PHI. In addition, the access was intentional; this was in no way an inadvertent disclosure, and the information accessed was retained. Therefore, since the incident is considered a breach, the privacy officer must develop a recommendation.

After the Breach: How to Respond

While the process outlined above seems like relatively straightforward decision-making, working in rural healthcare settings brings forth unique challenges. The routine apology and offering of credit protection may not be satisfactory or appropriate, especially in a scenario like the one described above. Unfortunately, there may be no sufficient resolution in the patient's eyes, but the facility must focus on prevention and mitigation.

Is terminating Janet after 20 years of loyal employment in a difficult-to-recruit position the best solution? Employee morale may suffer if a 20-year loyal employee is terminated for being "curious." There also might be backlash from the local community at the sudden termination of an employee that might be well known and respected in the community. However, lack of corrective action may cause distrust among employees and the community that the privacy of their health records is not protected at Hospital A. There could also be community backlash at the news that someone's healthcare privacy was violated without repercussions. Organization reputation is a concern, as well as the related decrease in patient volume and associated revenue that could occur.

No facility wants to experience a breach. The impact of such an occurrence—as well as the resolution—will be widespread, from the employee and patient to staff and community members. While termination of employment is one option, there are other options to consider as well. The privacy officer should work with human resources or another leader who can ensure corrective action is executed in a consistent manner based on the violation. After the appropriate corrective action has been determined, it can be administered by the employee's manager. Even in the smallest of facilities, the privacy officer should not be acting alone.

The repercussions of Janet's access would be determined by organizational policy. In this scenario, because Janet's inappropriate access of PHI was intentional, HIM professionals might expect her employment to be terminated. But in rural facilities, this would not necessarily be the case. The organization would also take into consideration prior disciplinary action and the impact to patient care and safety if a position were to be left vacant—potentially for months when recuritment is difficult.

When it comes to healthcare privacy and PHI, "curious cats" should be warned—no matter how well-intentioned, curiosity is not an acceptable justification for a privacy breach.

Notes

1. 3Lions Publishing, Inc. "HIPAA § 164.402 Definitions." HIPAA Survival Guide. www.hipaasurvivalguide.com/hipaa-regulations/164-402.php.
2. Department of Health and Human Services Office for Civil Rights. "Breach Notification Rule." HHS.gov. July 26, 2013. www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Traci Waugh (twaugh@krmc.org) is director of outreach services and compliance at Kalispell Regional Healthcare, based in northwest Montana.

Article citation:
Waugh, Traci. "Curiosity Can Often Kill the Cat in Healthcare" *Journal of AHIMA* 89, no.1 (January 2018): 38-39.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.