Curiosity Killed the Career

Save to myBoK

By Nancy Davis, MS, RHIA, CHPS

While serving as a system privacy officer for a Wisconsin-based healthcare system, the author of this article met regularly with the organization's president to review privacy and security compliance. This time was spent reviewing breaches that members of the workforce were directly responsible for, as well as the consequences for Health Insurance Portability and Accountability Act (HIPAA) sanctions that resulted from their actions. At one point, the president thoughtfully commented that "curiosity not only kills the cat, it can also kill the career."

This profound summation reflected the professional and personal impact of a workforce member's decision to ignore internal policies as well as state and federal privacy and security regulations. This reflection quickly inspired a new series of HIPAA awareness training and tools, which were rolled out with the eye-catching title "Curiosity Killed the Career." Subsequent modifications to HIPAA affirmed the need for ongoing training.

Privacy Laws and Potential Fines

The HIPAA Privacy Rule became effective in 2003, and was followed by the HIPAA Security Rule in 2005. The HIPAA Privacy and Security Rules dramatically changed the way healthcare organizations create, manage, safeguard, retain, and destroy confidential protected health information (PHI). They required healthcare organizations to have processes in place to apply appropriate sanctions to workforce members who fail to comply with HIPAA and internal policies.

As the HIPAA Privacy Rule evolved, greater emphasis was directed toward unauthorized access, use, and disclosure of patients' PHI—or breaches, as they are commonly known. Further revisions occurred in 2009 with the Health Information Technology for Economic and Clinical Health (HITECH) Act and the 2013 HIPAA Final Omnibus Rule. Together, these rules expanded direct accountabilities to the level of the individual workforce member. As a result, no longer did the healthcare organization have to bear sole responsibility for the acts of a rogue workforce member.

The Department of Justice assigns criminal penalties for individuals who knowingly or maliciously misuse patient PHI. The penalties are structured as follows:

- Covered entities/individuals that "knowingly" obtain or disclose PHI can face a fine of up to $50,000, as well as imprisonment up to one year.
- Covered entities/individuals who commit offenses under false pretenses face penalties of up to a $100,000 fine, with up to five years in prison.
- Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm can face fines of $250,000 and imprisonment up to 10 years.[1]

Personal Risk Key Part of HIPAA

Regardless of established administrative, physical, and technical safeguards, a healthcare organization cannot always control the actions of the rogue workforce member. Until HIPAA directed compliance responsibilities to the individual level, the healthcare organization was often left standing alone as the responsible party for a HIPAA breach. Once it became clear that an individual workforce member could suffer personal consequences as a result of their failure to safeguard PHI, it raised the stakes considerably.

In 2009, Huping Zhou of Los Angeles, CA was sentenced to four months in prison and a $2,000 fine after pleading guilty to unauthorized access of confidential medical records.[2] In 2018, Jeffrey Luke of Collierville, TN, pleaded guilty to downloading the PHI of 300 patients on his computer and was sentenced to 30 days in jail, three years of supervised release, and ordered to pay $14,941 in restitution.[3] From 2009 through the present, the healthcare industry has seen continued criminal penalties

assigned to healthcare workers who have violated HIPAA. It is highly unlikely that any of these individuals will ever work in healthcare again.

Privacy and security officers are wise to leverage these fines, penalties, and criminal cases when creating training, education, and awareness tools for workforce members on the need to safeguard the privacy and security of PHI. It is critical that workforce members are aware that failure to adhere to privacy and security policies puts them at great personal risk for sanctions. At the organizational level, HIPAA sanctions can include:

- Counseling
- Retraining
- Corrective action
- Suspension
- Termination
- Loss of unemployment benefits

On a broader scale, HIPAA breaches can also include reporting breach activity to the following organizations, which may levy greater sanctions:

- Local, state, and federal law enforcement agencies
- Office for Civil Rights
- State attorney general

HIPAA breaches can also be reported to the workforce member's professional licensing or certification board and ethics committees. Reports to licensing boards become public records and are often the basis for future employment background checks. Professional organizations such as AHIMA certifies its members and has in place a code of ethics setting forth ethical obligations of practice. Members who fail to adhere to the code may be subject to review by the organization's ethics committee and could lose AHIMA certification as a result of the violation. Many leadership positions in health information management (HIM) require AHIMA certification. To lose this would greatly jeopardize employment in the field. Clearly, there is much at risk for licensed or certified workforce members.

Finally, workforce members can be sued by their victims in private lawsuits. Invasion of privacy is a willful tort that constitutes a legal injury, and damages for mental suffering are recoverable without the necessity of showing actual physical injury.

In addition to formal internal and external HIPAA sanctions, the workforce member may lose their personal reputation in the community. Relationships with family members and friends can be severed by HIPAA breaches when the actions of the workforce member are disclosed to the victims of their behavior. In healthcare organizations where an electronic health record (EHR) system may be shared, termination for inappropriate EHR access, use, or disclosure at one organization may very well close the door to employment at other participating organizations. In working with a system such as this, it is not unusual for an individual who has been terminated from one organization to find that they are not eligible to work at another organization using the same EHR system because they are on the "no-access" list.

While every effort should be made to promote the safeguarding of patient privacy and security on a positive note, there should also be consideration of the personal and professional risks associated with failure to do so. Workforce members need to be aware that "curiosity can kill the career" and they have much at stake in order to preserve their personal and professional well-being.

Notes

1. US Department of Health and Human Services. 45 CFR SS 164.530(e)(1). HIPAA Privacy Rule Administrative Requirements. www.govinfo.gov/content/pkg/CFR-2012-title45-vol1/pdf/CFR-2012-title45-vol1-sec164-530.pdf.
2. Dimick, Chris. "Californian Sentenced to Prison for HIPAA Violations." *Journal of AHIMA*. April 29, 2010. http://journal.ahima.org/2010/04/29/californian-sentenced-to-prison-for-hipaa-violation/.
3. "Jail Terms for HIPAA Violations by Employees." HIPAA Journal. March 22, 2018. www.hipaajournal.com/jail-terms-for-hipaa-violations-by-employees/.

Nancy Davis (Nancy.Davis@dcmedical.org) is the director of compliance and safety at Door County Medical Center, based in Sturgeon Bay, WI.

Article citation:
Davis, Nancy. "Curiosity Killed the Career." *Journal of AHIMA* 90, no. 6 (June 2019): 26-27.
