Opportunity Behind the Headlines

Save to myBoK

By Wylecia Wiggs Harris, PhD, CAE, chief executive officer

Writing my first column in the *Journal of AHIMA*, I feel like I'm on solid ground. That's because the topic for this issue, privacy and security, is a universal concern. It's important to everyone—and it's a vital issue for AHIMA and the HIM profession.

Cybersecurity, in particular, is on everyone's mind. In the first two months of 2018 alone, we've seen healthcare industry headlines like these:

- "Survey Says Healthcare Leads All Sectors (in Ransomware Infections)"
- "Health Apps Frequently Neglect Privacy of Users, Study Finds"
- "How Healthcare Organizations Can Reduce Cyber Extortion Risk"

Such breaches and hacks hit close to home. In retrospect, the backstories of high-profile breaches are familiar, if not banal. A stolen laptop from a car, a ransomware attack, a hacker gaining access to the network and accessing a folder containing Medicaid billing data, hackers gaining access to data via a phishing email.[1]

These breaches cost organizations money and time. They may endanger patient safety if systems go offline and information can't be accessed where and when it is needed. They also cost patient trust, as victims must grapple with the potential of identity theft.

With so much bad news, it's tempting to avoid reading the headlines altogether. But the good news is that the HIM profession is well placed to combat many of the privacy and security threats we face. Through our 90-year history, we've built a reputation as defenders and protectors of health information. More recently, we have navigated a host of regulatory requirements through the various iterations of HIPAA and ARRA. We have pioneered the evolving role of privacy officer, which is now starting to encompass protecting employee information and intellectual property. Now, as we have led privacy efforts, we are starting to lead enterprise-wide information governance initiatives to secure confidential data of all types. Our deep understanding of the circulation of health information throughout our organizational ecosystems gives us the expertise to uncover work flow problems and to develop and lead processes to mitigate risk. We are also well positioned to advocate for information sharing and collaboration across organizations to support education and understanding to reduce potential breaches in the future.

The articles in this month's issue give us an idea of ways we can take meaningful action in an era of privacy and security threats. Proactively monitoring audit logs to address potential threats or unauthorized access is one approach explored by Chris Apgar in "Timber! Lax Audit Log Monitoring Can Bring Down a Healthcare Organization." And in "Keep Your Seawall Secure," Don Hardwick discusses how HIM professionals can balance the role of protecting patient privacy with the need to share information throughout an enterprise.

The tumult around privacy and security creates a great opportunity for health information management. HIM professionals are ready to step up, and now is the time; I'm so glad to be part of it.

Note

1. "The Biggest Healthcare Data Breaches of 2018 (So Far)." *Healthcare IT News*. January 15, 2018. www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.

Driving the Power of Knowledge