Privacy and Security: The Perennial Dialogue

By Lynne Thomas Gordon, MBA, RHIA, FACHE, CAE, FAHIMA, chief executive officer

For years, pundits have been pointing to the popularity of social media and reality TV, bemoaning the "end of privacy."

But for HIM professionals, after a decade that started with the implementation of the HIPAA rules and culminated in the rules' augmented HITECH counterparts last year, it feels more like the "decade of privacy."

More than 10 years ago, privacy and security came into the spotlight in healthcare. And they're not going away any time soon. Now the national dialogue is starting to catch up.

The E-mail You Don't Want to Get

While I was writing this article, I received a message from a small online social networking site: "During a security review, we found that [online service] suffered a data breach. While no financial information was taken, lost or changed, the hackers did take e-mail addresses and encrypted password hashes for some accounts…" The message suggests I change my password and describes the website's tightened security measures.

As the world becomes more connected through technology, people have taken their privacy and security for granted. But that's starting to change. Social media accounts and other websites routinely get hacked. High-profile breaches of credit card information at Target and other retail stores have made consumers newly wary of information security issues. A recent article published by the American Bar Association notes that even car makers are taking steps to reduce vulnerabilities to malware and cyberattacks.[1] The issues of privacy and security are indeed becoming part of the national dialogue.

In healthcare, providers have been working to implement the provisions of the HITECH-HIPAA Omnibus Privacy Rule. Through it all, HIM professionals are reminded that we must always balance the issues of enabling patient access while protecting patient privacy.

A Status Check

This month's features give us a look at the present and future of privacy and security. In "Top HITECH-HIPAA Compliance Obstacles Emerge," Mary Butler examines how HIPAA-covered entities are faring with their compliance efforts and what the biggest changes to the HIPAA guidelines have wrought.

Medical identity theft has become a high-profile issue in recent years, and preventing it requires collaboration by both providers and consumers. In "Combating the Privacy Crime That Can Kill," AHIMA Director of HIM Practice Excellence Harry Rhodes and Joanne McNabb, director of privacy education and policy in the California attorney general's office, share best practices on preventing medical identity theft.

In 2013, Johnathan Coleman wrote in the *Journal of AHIMA* about the Data Segmentation for Privacy Initiative (DS4P), which applies special handling instructions to parts of an electronic record. In "Protecting High-Stakes PHI," Coleman describes recent progress in the development of technical standards that support interoperability and introduces additional use cases being explored by DS4P.

I hope you will find these articles thought-provoking reading. Now I have to go change my password.

Note

1. Balough, Cheryl Dancey and Richard C. Balough. “Cyberterrorism on Wheels: Are Today’s Cars Vulnerable to Attack?” *Business Law Today*. November 2013. http://www.americanbar.org/publications/blt/2013/11/02_balough.html.

Article citation:
Gordon, Lynne Thomas. "Privacy and Security: The Perennial Dialogue" *Journal of AHIMA* 85, no.4 (April 2014): 19.