New Technology Creates New Privacy, Security Challenges

Save to myBoK

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

Looking for some help around the house? Proponents of what has become known as the "Internet of Things" have been developing products that will do just that. For instance, the winners of the 2014 Internet of Things Awards represent a tempting array of Internet-connected products that can help with household tasks.[1] One product tracks conditions in the garden and tells you when it's time to water. Others allow you to change your home thermostat, mow your lawn, or monitor home security via apps on your phone. Networked devices that monitor, collect, and analyze data are appearing in transportation, retail, and healthcare as well. At the same time, the rise of the Internet of Things has led to questions by privacy and security advocates. How can we be sure the data that is collected is handled properly?

The Federal Trade Commission recently released a staff report urging companies developing Internet of Things devices to adopt best practices to address consumer privacy and security risks.[2] Many of the recommendations will seem familiar to those of us who know HIPAA, such as training employees about the importance of security, ensuring that outside service providers can maintain reasonable security, and considering measures to keep unauthorized users from accessing a consumer's device, data, or personal information stored on a network.

We in HIM may know the best practices, but that doesn't mean we have "solved" privacy and security. We have plenty of existing challenges, as this month's articles illustrate. In our cover story, "Cracking Encryption," Mary Butler looks at why encryption is still not widely used to combat costly breaches. Many providers are slow to invest in this technology, and the article looks at barriers and myths that may be hindering adoption.

As healthcare organizations consolidate, the process of managing protected health information (PHI) has become increasingly complex. Collette Zeiour, RHIA, and Mariela Twiggs, MS, RHIA, CHP, FAHIMA, explain how they created a more streamlined, consistent release of information process across the board in "Instituting an Enterprise-wide PHI Disclosure Management Strategy."

As electronic health records (EHRs) advance, HIM professionals with the right background and skills can fill more occupational roles than ever before. But it can be hard for us to understand all the options, especially when considering obtaining additional education. Lisa Eramo talks to some HIM professionals about various ways to climb the career ladder in "Learn More to Earn More." Another issue arises in trying to connect all of the disparate health IT systems and gadgets in order to foster meaningful, interoperable use of health information. In "Clearing the HIPAA Cobwebs," Chris Dimick speaks with the new ONC Chief Privacy Officer Lucia Savage on how she plans to balance privacy and security issues while fostering EHR data exchange.

As technology evolves, new challenges—like those presented by the Internet of Things—will continue to develop. We'll need to keep our skills in top form to continue to meet them.

Notes

1. Postscapes.com. "Fourth Annual Internet of Things Awards." http://postscapes.com/internet-of-things-award/2014/index.
2. Federal Trade Commission. "Internet of Things: Privacy and Security in a Connected World." January 2015. www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Article citation:
Gordon, Lynne Thomas. "New Technology Creates New Privacy, Security Challenges" *Journal of*

AHIMA 86, no.4 (April 2015): 17.