Creating an Environment of Trust for Patients and Consumers

By Cassi Birnbaum, MS, RHIA, CPHQ, FAHIMA

From the year 2009 through 2014, nearly 42 million people had their protected health information (PHI) compromised, according to data from the Department of Health and Human Services' Office for Civil Rights (OCR). Each passing year brings into sharper focus the challenges associated with covered entities' and business associates' inability to consistently safeguard PHI. This year has proven to be no exception.

On February 4, health insurer Anthem announced that hackers had accessed a database containing the personal information of about 80 million of its customers, former customers, and employees in California and other states.

Before February, the largest previously known data breach attributable to a cyberattack occurred last year, when Community Health Systems announced that an external group of hackers stole the non-medical data of 4.5 million patients, according to *Modern Healthcare*.

Investigators believe the hackers who broke into Anthem's network did so by stealing the company administrators' login credentials, according to a report from *The Hill*. The hackers got the credentials of five Anthem technology workers and then used targeted phishing campaigns to lure network administrators into revealing login information or clicking a link that granted hackers access to their computers, according to the report. Such an approach rendered any would-be encryption moot, according to a security expert at Tripwire.

What keeps me up at night are the risks that are often completely unanticipated due to a breach of policy: social media temptations, pictures taken of patients and posted on social media or shared with colleagues not directly involved with the patient's care team, nosy staff accessing records of co-workers and neighbors without a business need to know, rogue employees who use their access to steal health records or leak a VIP patient's information to the press.

As HIM professionals, we spend our careers safeguarding PHI and delicately balancing access privileges to ensure four basic "rights": the **right** data is directed to the **right** provider for the right reason using the **right** safeguards.

I do not foresee any end to breaches, but AHIMA's privacy practice guidance and gold standard resources will assist you in identifying gaps, mitigating your risks, and ensuring a solid foundation in privacy and security.

Creating an environment that enables an organization's staff to see privacy as their most important role is critical. OCR has announced even more annual HIPAA compliance audits, so now is the time to get ready. There are creative and innovative ways to energize your workforce and use techniques to get them engaged. Don't forget about your growing remote workforce and the need to develop a consistent, seamless approach to safe computer use outside of a healthcare facility.

Remember that the biggest threats are typically internal. Focusing on securing remote access for end users, especially as care is extended outside of an integrated delivery system to the home and alternative settings, is a good place to start.

Now is the time to realize the vision of increased consumer confidence in our ability to safeguard their most private information, and to truly engage patients in sharing and exchanging their information when and where it is needed.

Cassi Birnbaum (cassi.birnbaum@ahima.org) is senior vice president of HIM and consulting at Peak Health Solutions.

Article citation:
Birnbaum, Cassi L. "Creating an Environment of Trust for Patients and Consumers" *Journal of*

AHIMA 86, no.4 (April 2015): 8.