Privacy—It's Up to Us

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

"Medical Record Breach at Stanford Hospital: 20,000 Exposed," "Texas Data Breach Affects Medical Records of 4.9 Million Patients," "Hospital Records Breach Involves 93,500 Patients"-these were just some of the headlines we saw in 2011 when privacy breaches and data security incidents involving patient records came to light.

These headlines catch our eye because of their broad scope. And their effect is chilling because they go to the heart of what we as HIM professionals do-keep private, personal information safe and secure.

And we know what these headlines mean. Another breach notification letter sent to thousands of people. Another consumer wondering if his or her data are in the wrong hands. Another moment where trust in the healthcare system is damaged and needs to be rebuilt.

In its report on the top data breaches of 2011, the Privacy Rights Clearinghouse hit the nail on the head with this assessment: "Unfortunately, it is virtually impossible for individuals to protect themselves from a data breach. It is up to organizations that collect data on consumers to take the steps to ensure the privacy and security of the data they collect and maintain."[1]

Adapt, Learn, and Teach

In many ways, the public takes privacy for granted. Think about all the personal transactions and data going into our personal smartphones. We love the portability and the convenience, until something breaks or is lost or stolen. In the healthcare setting, the stakes are even higher: privacy breaches can damage lives.

As HIM professionals, we are the people patients trust to protect their information. As technology continues to change, we need to adapt to the new environment and learn new skills so that we can continue to keep that trust. And we need to be the standard bearers for privacy in our workplaces, to lead and educate others to do the same.

From ROI to Texting

This issue of the Journal showcases some of the critical privacy and security issues of the moment. In our cover story, "The New Privacy Officer," staff writer Chris Dimick takes a look at how the role of privacy officer has changed since it was first created-and how it continues to evolve.

Release of information continues to present new challenges as information increasingly becomes digital. Jan McDavid and Rita Bowen offer tips on how to improve workflow and mitigate risk in "Everyday Risk."

In "HIPAA Compliance for Clinician Texting," Adam Greene offers ways to mitigate risks in physician-to-physician texting. And Barry Herrin gives us an overview of how the European privacy directive affects physicians in the US in "Long Distance Records." Finally, don't miss the updated "Mobile Device Security" practice brief.

Keeping our organizations out of the headlines-and ensuring that patient information is private and secure-is a responsibility all HIM professionals must live up to daily. It's up to us.

Note

1. Privacy Rights Clearinghouse. "Data Breaches: A Year in Review." December 16, 2011. https://privacyrights.org/data-breach-year-review-2011.

Article citation:
Gordon, Lynne Thomas. "Privacy—It's Up to Us" *Journal of AHIMA* 83, no.4 (April 2012): 19.