news
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601

phone »(312) 233-1100
fax »(312) 233-1090
web »www.ahima.org

For more information, please contact:
Bridget Stratton
Public Relations
312-233-1097
bridget.stratton@ahima.org

Information Governance Key to Cyber Security, Data Privacy

Evolution in information flow creates new role for privacy and security officers

WASHINGTON – March 23, 2016 – An enterprise-wide information governance (IG) program is a key component to preventing security breaches and ensuring the privacy of all information within healthcare organizations, according to an American Health Information Management Association (AHIMA) presentation at the National HIPAA Summit today.

In her presentation, AHIMA's Kathy Downing, senior director, information governance, MA, RHIA, CHPS, PMP said the ever-increasing frequency of electronic communications in the workplace makes IG a business imperative for healthcare organizations. Privacy and security officers are tasked with safeguarding against data breaches and protecting not only health records, but employee information and intellectual property.

"We're seeing a flood of information flowing through healthcare organizations whether it's patient electronic health records, employee email correspondences, social media posts or even physician text messages," said Downing. "A strong and continuous IG program aimed at securing confidential data of all types, not just clinical, is key to ensuring an organization's information is secure."

As the amount of information and access to data grows, the role of privacy and security officers must also evolve to lead IG efforts, Downing said.

Once focused largely on protecting clinical information and ensuring compliance, with their knowledge and skills, privacy and security officers are poised to take on the role of chief information governance officer (CIGO). The CIGO is responsible for driving enterprise-wide management of privacy and security of information through a continuous IG program.

"We are experiencing a new era in privacy and security," said AHIMA CEO Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA. "The emerging role of chief information governance officer makes certain that an IG framework is enterprise-wide to ensure the security of all types of information as well as access to quality information when needed."

Reporting to senior leadership, the CIGO should drive new standards, processes and initiatives including procedures to protect patient and organization information from social media or mobile device breaches.

“Too often social media content or information shared on mobile devices is not managed by an organization’s IG policies,” Downing said. “Having a CIGO responsible for IG will help ensure policies are put in place so information is secure and organizations are compliant.”

To protect information shared on mobile devices, AHIMA recommends organizations develop operating standards and consider text encryptions to secure messages and protect against Health Insurance Portability and Accountability Act (HIPAA) violations. Similarly, an organization’s IG framework for social media should include a social media policy, controls and operations guidelines as well as sanctions for violations.

All of AHIMA’s resources for starting and implementing IG within an organization are available at www.IGIQ.com – the home page for everything in healthcare information governance.

###

About AHIMA
The American Health Information Management Association (AHIMA) represents more than 103,000 health information professionals in the United States and around the world. AHIMA is committed to promoting and advocating for high quality research, best practices and effective standards in health information and to actively contributing to the development and advancement of health information professionals worldwide. AHIMA’s enduring goal is quality healthcare through quality information. **www.ahima.org**