HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

November 2014

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Donald A. Sinko
Chief Integrity Officer, Cleveland Clinic

Dr. Mark J. Sands
Vice Chairman for Clinical Operations & Quality, Cleveland Clinic Imaging Institute; and Chairman, Corporate Compliance Committee

Quality improvement, patient safety, and the zeal to comply:

What a CPA and a radiologist bring to Compliance leadership

an interview with Don Sinko and Mark Sands

See page 18

by Mariela Twiggs, MS, RHIA, CHP, FAHIMA

HIPAA compliance audits: Best practices for standardizing PHI disclosure processes

» HIPAA audits are resuming; the age of compliance is now.
» The risk of HIPAA breach has increased.
» Unknown PHI disclosure points can put provider organizations at risk.
» Centralizing PHI disclosure processes provides standardization across an enterprise.
» Proper documentation is vital in preparing for OCR audits.

Mariela Twiggs *(mtwiggs@mrocorp.com) is National Director of Training and Compliance for MRO Corp, in King of Prussia, PA.*

Healthcare organizations are in a constant battle against forces known and unknown that can threaten the privacy and security of an organization's patient health information (PHI). The Ponemon Institute's fourth annual Benchmark Study on Patient Privacy & Data Security[1] found that the number of organizations reporting criminal attacks on patient data has doubled since 2010, with employee negligence by far the largest reason for data breaches.

Twiggs

The risk of breach has increased, in part, due to the transition to electronic records, the rise of health information exchange (HIE), and the increased use of personal unsecured devices such as smartphones, laptops, and tablets. In this rapidly changing environment, departments outside of Health Information Management (HIM)—including Risk Management, Billing, Lab, Radiology, and hospital-owned clinics and physician practices—are accessing and/or disclosing PHI through various electronic methods. In fact, there are as many as 40 PHI disclosure points within an organization, increasing the risk of breach via improper PHI disclosure.

Adding to the mounting risk of improper disclosures are business associates (BAs) who are not yet compliant with the final HIPAA Omnibus rule. The rule, which took effect in 2013, expands the obligations of covered entities (CEs) and their BAs to protect patients' privacy and PHI. A study[2] by the Office for Civil Rights (OCR) concluded that 45% of healthcare providers and other CEs had an average of five HIPAA data breaches in a single year, with two-thirds of incidents involving a BA.

Hand in hand with the tightening of regulations are steeper penalties for data breaches. Providers that fail to comply are subject to penalties of up to $1.5 million per incident per calendar year. Criminal penalties range from $50,000 to $250,000 in fines and up to 10 years in prison. An American National Standards Institute survey[3] of hospitals found a wide range of costs associated with each incident of improper disclosure, varying from $8,000 to $300,000. In addition, due to factors such as social media and healthcare consumerism, the

damage to a hospital's reputation can have a long-lasting and far-reaching impact.

With the OCR resuming its HIPAA audit program, a good way for organizations to mitigate the potential for breaches is to eliminate gaps or weaknesses by carefully evaluating PHI disclosure management processes. Best practices for an enterprise-wide, ongoing approach to PHI disclosure management—including standardized processes, training and proper documentation—will help providers increase compliance, minimize liability, and reduce financial risk.

Standardizing processes

Federal healthcare legislation, including HIPAA, HITECH, and the HIPAA Omnibus rule, promotes patient privacy and underscores the need to manage PHI disclosures across a healthcare enterprise in order to ensure compliance. Centralizing the disclosure process into a single system overseen by a single department can eliminate many of PHI disclosure management's challenges and enables healthcare providers to use software and services that can be deployed as a common tracking platform.

By processing all PHI disclosures through one system, hospital departments that disclose PHI have the benefits of secure technology, comprehensive workflow, and quality assurance checks on the information sent through the system. It also supports the organization's efforts to standardize policies and procedures by obtaining the interdepartmental communication, policy enforcement, and level of oversight needed to comply with the increasingly complex regulatory environment.

Training

Standardization of PHI disclosure processes also allows for improved training and education. Workforce awareness about sharing and using PHI is essential. Given today's increasingly digitized environment, coupled with numerous PHI disclosure points, patient information is often accessed or disclosed by employees who may not have received full training regarding privacy and security, or may not be following the latest guidelines.

The HIPAA Privacy and Security Rules require healthcare organizations to formally educate and train the workforce to ensure ongoing accountability for the handling of PHI, as well as documentation verifying that it was provided. Although there are no set guidelines for exactly how an organization should conduct training, the American Health Information Management Association (AHIMA) recommends the following best practices:

- Provide annual training for all staff
- Include education, training, and ongoing awareness, and cover PHI in all its forms (i.e., verbal, written, electronic)
- Develop a repository of current policies and procedures
- Test staff on information to ensure that they have completed training before they are able to access PHI

Training should be based on the employee's role, access to PHI, and responsibilities that present potential compliance risk. In addition, AHIMA advises CEs to work closely with BAs to ensure that all privacy and security training has been documented.

Proper documentation

In addition to maintaining a log of all privacy and security training, healthcare providers need to have a variety of other documents in order. For example, an organization may wish to centralize documentation such as completed checklists, security risk assessments, risk management action plans, BA agreements, and HIPAA training certificates. It would be a good idea to review all of the components

of the OCR audit protocols and pull all of the policies, procedures, and other documentation that will prove compliance. The audit protocols can be downloaded from OCR's website. Because documentation is a key component of the overall plan to protect PHI, record and retain these documents for 6 years after attestation as required by HIPAA.

Healthcare providers should also track all instances of PHI disclosures. The ideal way to maintain the accounting of disclosures is for organizations to deploy a PHI disclosure platform across the enterprise. This single solution can work as a common tracking mechanism, accounting for each instance of disclosure of PHI. The date of disclosure, name of recipient and address (if known), brief description of the PHI, and purpose of the request are required data elements, but accounting of disclosures (AOD) systems also may gather many more data elements. In the future, the requirements for what is included in an accounting of disclosure system may become more complex; forward-thinking leaders in the healthcare industry are paying close attention to how they capture instances of PHI disclosure now.

Now is the time

The OCR has plans to conduct HIPAA compliance audits for hundreds of CEs and their BAs in coming months. According to data provided by CMS contractor Figliozzi and Company,[4] an estimated 80% of providers failed audits in 2012. By standardizing policies and processes, deploying the proper training and education, and documenting it all, providers can prevent significant risks associated with failing an audit.

The topic of OCR audits has gone mainstream, gleaning so much attention that the consequences of a failed audit extend beyond fines and penalties to a damaged reputation, negative media coverage, and potentially lower revenue.

In this age of compliance, providers must act now to address proper PHI disclosure. Working with a trusted and compliant BA for PHI disclosure management services will fortify the organization against possible OCR audits and absorb the risk of harm with regulatory knowledge, sophisticated systems for PHI disclosure, specialized tracking, reporting, and billing systems, along with the high-touch service capabilities.

1. Ponemon Institute LLC: "Fourth Annual Study on Patient Privacy and Data Security." March 2014. Available at http://bit.ly/1tbTZf6
2. Lindy Benton: "HHS raises the stakes for patient data breaches" *Healthcare IT News*, November 2014. Available at http://bit.ly/Zl0q8u
3. American National Standards Institute: "The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security." 2012. Available at http://webstore.ansi.org/phi
4. Cynthia E. Keen: "HIMSS: Are you ready for a meaningful use audit?" March 4, 2013. Online. Available at http://bit.ly/1mHpwZk