Privacy Compliance: Maintaining the Gains

Save to myBoK

by Nancy Vogt, RHIT, CHP

Most HIM professionals would probably agree that the state of information privacy has dramatically improved as a result of all the HIPAA efforts over the past few years. Executive leadership has tuned in, and even boards of directors have addressed information privacy. Awareness is at an all-time high—not only within healthcare organizations, but also among staff and throughout the communities we serve.

However, it is quite possible that the biggest hurdle is still ahead. How do we maintain the gains? How do we continue to improve privacy practices and staff awareness when there are so many other competing priorities—patient safety, quality, revenue cycle, service management, employee engagement? This article explains how we can keep information privacy and security a top priority within our organizations.

Promoting Awareness and Compliance

There are two key methods for promoting continued awareness and improved compliance. The first is ensuring that all staff receive necessary training and ongoing education; the second is monitoring the effectiveness of training and other components of the privacy program through ongoing audits.

Training and auditing are two of the seven elements of an effective compliance program required by the Office of Inspector General. From a practical standpoint, an organization cannot expect its work force to comply with regulations if effective training has not been delivered. The most difficult challenge is to make sure the training effectively prepares employees to comply with privacy and security policies. A second hurdle is to make sure employees complete the available training.

Privacy is an inherent part of so much that we do, and it affects many types of staff and disciplines. How can an organization audit such a broad scope of compliance? With the need to control the cost of healthcare, hiring an army of auditors is not a realistic solution, regardless of the organization's size.

As we have discovered in other aspects of healthcare delivery, the effective use of technology may be part of the solution. Technology (especially Web-based technology) affords new opportunities for auditing and monitoring without the cost of traditional auditing methods.

Training Compliance: A Case Study

Take for example the case of an integrated delivery system with 25,000 employees, 700 of whom are physicians. The chief privacy officer was charged with monitoring compliance as well as with training and other privacy policy requirements.

Mandatory privacy and security training was deployed across the organization via a Web-based program. The chief privacy and security officers, information services developers, and organizational development experts all contributed to the internal development efforts. Eight modules were developed to incorporate the varied needs of different categories of employees. The Web-based courses were made available to all employees via an intranet-based learning management system.

When an employee completes a training module and takes the test, the completion is electronically recorded on the employee's online transcripts in the learning management system. Online transcripts are available to the employee and the employee's manager. In addition, management staff has access rights to run online exception reports to identify staff by facility and department who have not yet completed the training.

To further promote ongoing compliance with training, site-based privacy officers generate online queries for the entities for which they are responsible. They then follow up with managers who have staff who continue to appear on the untrained list. The chief privacy officer monitors overall compliance and creates a quarterly report showing compliance by entity. This information is used to identify entities or departments who have exceptional compliance rates, and these privacy officers share their best practices with other entities.

A compliance Web site is currently being tested that will allow electronic audits to be assigned and distributed to department managers, privacy officers, or other designated individuals. Electronic audits will replace the current paper-based audits, which are inefficient to administer and whose results are often difficult to collate.

Components of the System

The first systemwide electronic audit will be the confidential information security checklist. This audit will be distributed via e-mail to all individuals with a title of manager or director. The distribution list is electronically created using a file from a human resources Web-based application. The e-mail message includes the purpose of the audit, simple instructions, and a link that will take the individual directly to the checklist on the secured employee portal of the intranet.

After logging in with unique log-ins and passwords, managers and directors will see their home facility and department defaulted and can then proceed to enter data into the checklist. This online checklist walks the auditor through a list of eight criteria. Since not all managers and directors have responsibilities that relate to patient information, the checklist was crafted in a way that applies to all types of confidential information, including payroll and employee files. The auditor (the manager or director or his or her designee) responds “yes,” “no,” or “not applicable” and is allowed to enter comments. Upon completion, the auditor is provided the opportunity to complete a checklist for an additional department, since many directors or managers are responsible for more than one department.

Upon completion of the checklist, data are stored in a database. An administrative Web site has been developed that can only be accessed by the organization’s privacy officers. When the privacy officers enter the organization codes for their areas of responsibility, they will be presented with the results of the responses to the eight safeguards criterion. A drill-down menu is available to view the results by individual department and to review comments. In addition, the privacy officers are presented with a list of departments that have not completed the audit.

The compliance Web site has been developed to allow for additional planned audits to be delivered in a similar fashion. An employee questionnaire has also been drafted to monitor the effectiveness of certain components of the mandatory training. For example, the questionnaire tests employees’ understanding of how to direct a patient complaint about privacy when unable to resolve it on their own. A random sample of employees will receive this audit via e-mail, and by clicking on the link, they will be automatically directed to the online form. Other planned audits include an authorization audit that will be sent to the managers of all health information departments. This will provide a convenient, electronic method to enter audit data regarding authorizations received from external parties. Results will be stored and collated electronically, allowing for quick and easy identification of trends. Problem areas will be addressed by additional education.

While these audits are just a few examples of the possibilities, it is clear that using electronic technology opens new doors for auditing compliance in a secure and economical manner. In addition, ongoing monitoring keeps awareness high. Managers and staff directly participate in the auditing process, which reminds them of the importance of privacy and security. Audits also demonstrate the organization’s ongoing commitment to complying with state and federal regulations.

Nancy Vogt *(nancy.vogt@aurora.org) is the manager of privacy compliance and chief privacy officer at Aurora Health Care in Milwaukee, WI.*

Article citation:
Vogt, Nancy. "Privacy Compliance: Maintaining the Gains." *Journal of AHIMA* 76, no.9 (October 2005): 90-91,96.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.