Automation for Privacy and Security Compliance

Save to myBoK

By Kelly McLendon, RHIA, CHPS

There has been a lack of enforcement of the privacy and security rules ever since HIPAA's inception. As such the adoption of comprehensive HIPAA compliance programs has lagged behind EHR development and implementation.

This in turn has caused little funding to be budgeted by providers, large and small, to formally detect, monitor, document, and report on the details of privacy and security incidents and investigations. Processes controlling these tasks have, typically, been manual and relegated to spreadsheets and shared-drive libraries.

The picture is becoming strikingly different now that ARRA-HITECH has placed enforcement center stage, mandating comprehensive auditing and establishing substantial penalties for noncompliance with HIPAA regulations. The most noticeable difference between the current state and past years is the introduction and expansion of automated compliance programs involving third parties and computer-based applications.

Why Automate Privacy and Security Compliance?

Compliance automation is a direct result of the complex changes to HIPAA, which have grown beyond the basic stage where cobbled together processes and manual tools suffice. Accounting of disclosures is one area where HIPAA continues to evolve.

The current accounting of disclosures notice of proposed rulemaking proposes the requirement of an access report to patients who request one.

Although it has not yet been finalized, this requirement will change the current structure for managing and processing accounting of disclosures.

Breach determination and reporting, HIPAA violation mitigation and sanction tracking, meaningful use-driven security risk analysis, and response to Office for Civil Rights (OCR) requests for information and audits all demand more reporting of a unified data set of HIPAA information.

Labor costs for compliance programs are increasing, as are the penalties for noncompliance, with both monetary levies and reputational hits to healthcare organizations from breaches of PHI access, use, or disclosure.

This trending toward privacy and security compliance automation is now becoming feasible for the mainstream marketplace, especially as new rules are issued and health information exchanges become commonplace. Providers are taking a proactive stance toward increased audit log monitoring.

In addition, patient demands for increased privacy and security protections and requests related to their HIPAA rights are placing increased pressure on compliance programs, which automation can relieve.

Areas of Privacy and Security Automation

There are several focal points for the new generation of privacy and security automation. Vendors are beginning to offer products to help privacy and compliance staff manage a wide scope of privacy functions. These products include rules-based audit log monitoring and privacy information management systems, which document HIPAA investigation, breach determination, and the workflows associated with patient requests for any of their rights under HIPAA. These trends will continue, and the number of product offerings will increase as budgets and user needs expand.

Descriptions of the different types of HIPAA privacy and security compliance automation follow below, including areas of regulation fostering their development and acquisition for use.

Audit Log Monitoring

The most common privacy and security automation to date has been in the area of audit log monitoring. These systems gather information through interfaces or "connectors" from disparate audit logs contained within all types of healthcare applications, from EHRs to financial systems.

They take the audit logs and combine database information about the users, commonly called identity management, with programmable rules to detect and alert when certain conditions are found. For example, if a user logs on twice simultaneously from different locations or a workforce member looks up his or her own medical records the system triggers an alert, which then must be investigated. The deeper these systems are used to delve into user activities, the more alerts are triggered and the larger the burden to investigate and report.

These systems are very promising to not only detect HIPAA access, use, and disclosure violations and breaches, but also to meet the anticipated new access reporting regulations under the accounting of disclosures proposed rule. The proposed access reports, which are already being requested by patients, are burdensome to create and have a potential liability for huge productivity impacts on compliance staff.

Privacy Information Management

The investigation, breach determination, documentation, and reporting activities surrounding detected events (or incidents) and privacy complaints from patients and workforce members are complex and require more data to report. Privacy information management systems organize and structure the data collection required for all types of privacy compliance and produce comprehensive reports about the data in several different formats, some of which can mimic OCR reporting requirements.

Investigation and documentation of possible HIPAA violations and breaches can be labor intensive and contain many steps. Customizable workflows and dashboards can sometimes be delivered within these types of systems.

Privacy information management systems can also consolidate the massive libraries of rules, policies, procedures, forms, letters, and other supporting materials into concise libraries that offer appropriate access for compliance staff and workforce members. Version controls are crucial because all of these materials tend to change as regulations evolve.

Security Information and Event Management

A security information and event management system is a type of detection and monitoring system that is more comprehensive than audit log tracking. Firewalls, malware, and many other kinds of threats are detected and alerts generated, again many of which must be investigated and documented to determine whether breaches have occurred that must be reported under the HITECH modifications to HIPAA.

Although it sounds similar to privacy information management there are somewhat different requirements for tracking security events (or incidents), many of which can be found in National Institute of Standards and Technology guidelines. The key is documenting security events in a manner that also addresses privacy breaches, when appropriate.

There have been generic security information management systems in the past, but they lack the coherence and attributes required for privacy compliance, but this is also changing. This is an important technology that will eventually find widespread adoption in healthcare.

Privacy and Security Risk Analysis

The meaningful use program requires participants perform and attest to a security risk analysis. OCR's HIPAA audits announced in June 2011 do not mandate privacy risk analysis, but the implications are clear. If a site wants to prepare for these audits, it must perform its own privacy risk analysis in advance of any audits.

Privacy and security are two separate and distinct, yet intertwined areas of focus and compliance. To date the healthcare industry is still unclear on the exact mix of what privacy and security requirements the OCR audits will focus on. Therefore, it is important that organizations address both the privacy and security rule requirements.

Tools automating these risk analysis processes, from macro-driven spreadsheets to Web-based, workflow-driven applications are becoming available.

As with many other HIM areas that become automated, the initial offerings from vendors into the marketplace may be slow to build and refine. But the drivers of automation are clearly present, which ensures an increasing trend toward more sophistication and reliance upon computer-based applications to manage both privacy and security compliance within healthcare.

HIM professionals should watch for privacy and security applications to evolve as the regulations do, expanding to meet the increasingly complex regulatory and electronic environment.

References

Anderson, Howard. "HIPAA Audits Move Forward." *Healthcare Info Security*, January 6, 2012. www.healthcareinfosecurity.com/articles.php?art_id=4379&opg=1.

National Institute of Standards and Technology. "Risk Management Guide for Information Technology Systems." Special Publication 800-30. July 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

National Institute of Standards and Technology. "Computer Security Incident Handling." Special Publication 800-61. March 2008. http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

Kelly McLendon (kmclendon@complianceprosolutions.com) is a managing director of CompliancePro Solutions.

Article citation:
McLendon, Kelly. "Automation for Privacy and Security Compliance" *Journal of AHIMA* 83, no.3 (March 2012): 38-39.