HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Fourteen
Number One
January 2012
Published Monthly

Meet

Our 10,000th member: Vernita Haynes, Compliance & Privacy Analyst, University of Virginia Health System

PAGE 17

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ—SEE PAGE 65

Feature Focus:

2012 OIG Work Plan: Part 1, Priorities by provider and supplier type

PAGE 48

Keeping criminals out of the health care system

PAGE 61

Effective practices for HIPAA and HITECH compliance measurements

By Rebecca Herold and Mahmood Sher-Jan

Editor's note: Rebecca Herold is CEO and Principal with Rebecca Herold & Associates, LLC. She may be contacted by telephone in Des Moines, Iowa at 515/996-2199 or at rebeccaherold@rebeccaherold.com.

Mahmood Sher-Jan is Vice President of Product Management with ID Experts. He may be contacted by telephone in Portland, Oregon at 971/242-4706 or at mahmood.sher-jan@idexpertscorp.com.

It is often said that if you can't measure something, you can't improve it. The same can be said about how an organization manages its information security and privacy program compliance activities. The goal isn't just measuring compliance with federal and states' regulations, but equally important is protecting the organization's reputation and its customers.

For example, health care data breaches are now common occurances within hospitals, practices, and their business associates (BAs). Stolen laptops, missing USB drives, or unintentional human error can put an organization—and patients' protected health information (PHI)—at risk. When a breach happens, organizations are often surprised and challenged by the time, people, and expertise needed to assess privacy risks; respond to a privacy or security incident; and meet an ever-changing, complex regulatory environment.

On the fifteenth anniversary of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations, the Office for Civil Rights (OCR) has finally identified its audit goals. Like a teenager with growing pains, HIPAA compliance and enforcement has been erratic and OCR has recently announced its audit plans, putting incident detection and response at the top of the list.[1]

Given all of these challenges, how do you know if you are in compliance with all of the requirements? How do you measure your level of compliance? Metrics can help you address these challenges. However, the metrics must be understandable and as simple as possible, without losing their meaning.

Using metrics to support compliance

Metrics support compliance in many ways. With regard to HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH), there are several requirements that inherently involve metrics. Here are some examples:

- Risk assessments use metrics to determine risk levels and priorities.
- A gap analysis creates numbers, just as a matter of identifying the gaps. And once identified, you must then update your metrics as the gaps are eliminated and as new gaps occur as a result of changes in business, operations, and technology.
- Hospitals do audits of patient records to ensure they are accurate, to identify inappropriate access and changes, determine disclosures, and so on. They have a lot of metrics involved with these activities, including determining the percentage of records to audit, how often to audit, and determining what percentage of errors in the records will be considered as acceptable. All of these numbers need to be documented and maintained to demonstrate compliance with various HIPAA and HITECH requirements, in addition to ensuring that the audits are performed consistently.

- HIPAA requires training and awareness, so you need to maintain metrics related to those activities.
- HITECH widened compliance requirements for the HIPAA Security Rule, in addition to the new breach response requirements, for all BAs. The Department of Health and Human Services (HHS) has published statements indicating that it expects covered entities (CEs) to take reasonable steps to ensure that their BAs are actually meeting and staying in compliance. Metrics can help you manage BA compliance monitoring more effectively and efficiently.
- HITECH also established many different breach identification and response requirements. CEs and BAs alike can use metrics to support and manage these requirements more effectively and efficiently.

Compliance challenges

Implementing an effective information security and privacy program that also meets all applicable compliance requirements can be daunting for most organizations. The following are some of the current compliance challenges facing health care organizations:

- The complexity of knowing all of the compliance requirements.
- Risk assessments can help identify risks, but if you don't do a comprehensive or effective risk assessment, you may overlook significant risks, such as in cloud services, social media use, or mobile computing.
- After identifying all existing risks, you need to prioritize their mitigation. Most organizations choose to focus on doing the quick hits, so then the more severe and complex risks do not get addressed.
- Ensuring consistent compliance at both headquarters and branch/remote locations.
- Business associates' compliance with all of their requirements.
- Knowing exactly where all of your patients' information, especially PHI, is located. How can you protect it if you don't know where it is? And if you don't know where your PHI is located, then how will you know if it has been breached?
- Knowing when a breach occurs. Many organizations have learned of a breach from their patients or news reports.

Knowing the requirements and creating associated metrics

To demonstrate how to meet these challenges, let's look at a specific area of compliance where establishing and maintaining ongoing metrics is of critical importance for demonstrating compliance: breach response. We have identified five distinct phases of a best practice data breach incident response lifecycle. Each of these phases is supported by OCR requirements for risk assessment, notification, and regulatory investigations. Metrics, when tied to each distinct phase, provide privacy and compliance officers with a measureable and defendable plan of action and ability to strive for the best outcome.

Phase 1 – Incident detection and investigation

Requirement: Organizations must have a defined process, procedure, and tools to document and report a suspected incident internally, so the core incident response team can initiate the incident response plan.

Recommended metrics:

- Speed of detection (date of incident vs. date of discovery)
- Speed of incident response team assembly and internal communication protocol
- Speed of containment and service restoration, and
- Cost of investigation as percentage of total cost and/or per record cost
- Source of the incident—internal or business associate

These metrics help identify any gaps in your incident response plan, including incident reporting and training your incident response team, and/or forensics investigation resources. Additionally, the metrics provide criteria that can be incorporated into your business associate agreements.

Continued on page 32

Effective practices for HIPAA and HITECH compliance measurements

...continued from page 31

Phase 2 – Incident risk assessment

Requirement: The HIPAA Breach Notification Interim Final Rule's administrative provision (45 CFR 164.414), places the burden of proof on covered entities and business associates to conduct and document an incident-specific risk assessment and demonstrate whether the incident did or did not qualify as a breach. OCR investigators also request evidence of this risk assessment.

Recommended metrics:

- Incident types (laptop, e-mail, application, malware, etc.)
- Speed of risk assessment (investigation to notification decision)
- Quality and consistency of risk assessment and documentation
- Number of total reported incidents
- Number of data breaches
- Number of resources required per incident assessment
- Number of incidents assessed per resource

These metrics help identify where your organization is most vulnerable to incidents as well as any gaps in the tools and resources needed for regulatory analysis and compliance. These metrics, which can be found in an incident assessment dashboard, also help you improve the effectiveness and efficiency of the process to ensure timely notification of individuals and regulatory agencies to avoid fines and to protect your organization's reputation and patients.

Phase 3 – Legal notifications to patients, regulators, and media

Requirement: When the risk assessment process triggers notification, both HITECH and states' breach notification requirements must be quickly incorporated into clear and compliant notification letters to the affected individuals and patients. The number of compromised records, geographic location, and profile of individuals

affected greatly influence the complexity and outcome of this phase.

Recommended metrics:
- Level of clarity of the notification letters
- Regulatory agency acceptance vs. change requests
- Speed of notification (days from decision to notification)
- Number of notification channels used (letters, e-mail, website, media)

These metrics help you identify the scope of regulatory expertise and resources (internal and/or external) necessary to ensure compliance within the timelines allowed by federal and states' rules and to reduce the risk of fines.

Phase 4 – Call center (protection and recovery services)
Requirement: Once patients are notified, the most important thing you can do to influence their perception of your organization and create a positive outcome is to offer real help by handling their inquiries by using live and knowledgeable staff who know about data breach response and the specifics of the incident. Understaffing or using impersonal, canned phone trees may appear to reduce costs, but can cause immeasurable damage to your reputation, impact patient retention, and possibly result in fines.

Recommended metrics:
- Number of callers as percentage of all notified patients
- Length of time per caller
- Percentage of calls resolved on the first call without escalation
- Number of callers enrolling into protection services offered, if any
- Number of complaints to regulatory agencies
- Number of complaints to management/executives

These metrics help you identify whether you have trained internal resources and a scalable infrastructure to handle the volume, or whether you should look at alternative vendor solutions. The metrics also tell if you have offered real and useful help to the affected patients, which go beyond typical credit monitoring offers.

Phase 5 – Regulatory investigation by OCR and state agencies
Requirement: When a data breach incident is reported to HHS/OCR and state agencies, typically the agencies will follow up with an investigation. The scope of this investigation varies depending on the nature of the incident, the impact of the incident, and the organization's response to the incident.

Recommended metrics:
- Number and scope of OCR investigations
- Number and scope of state agency investigations
- Costs (time and resources) of responding to the request for documentation
- Number and amount of any regulator fines imposed
- Correction action plan imposed

Although regulatory investigation is inevitable when you have a reportable breach incident, you can control the complexity and reduce the implications, such as avoiding the imposition of a regulatory corrective action plan or fines, if you can establish a burden of proof and show investigators your privacy and security best practices.

Creating a culture of compliance—What to do now

Awareness of compliance requirements and a plan to implement a metrics-based program is only the beginning. As the information security, privacy, or compliance officer, you know too well that a culture of compliance means that the privacy and security of patients' PHI is an integral part of patient care. Often, much to your chagrin, incidents that compromise PHI happen—sometimes unintentionally or maybe intentionally—and you are responsible for cleaning up the mess. Regardless of the cause, you must restore trust in the institution. In a hospital or clinic setting,

Continued on page 34

 ...continued from page 33

there are many potential sources of PHI breaches and each incident is often very unique. As a privacy officer, you can access resources such as the Privacy Rights Clearinghouse[2] or the Department of Health and Human Services website[3] to monitor the dominant types of electronic and non-electronic breaches. And as an additional, more valuable action, you can use a compliance program lifecycle management approach to collect metrics for optimizing the management and execution of your information security and privacy compliance activities.

Regardless of your approach, the following process changes will shift your organization from compliance-aware to proactive and compliance-centric.

Ongoing monitoring

Organizations are realizing the need for ongoing monitoring, both internally and externally. For example, business associate compliance poses great risks by entrusting a third party with data and processing. Growing numbers of breaches are occurring as a result of poor BA security. And, it is increasingly becoming important to find effective ways to monitor your own organization's compliance.

Ongoing monitoring can be accomplished through real-time compliance meters. A compliance meter can keep track of the different components of a compliance program, and the associated levels of compliance for each, on an ongoing basis so that those responsible for managing the program can see how they're doing at any point in time. This also allows business partners, such as covered entities who want to monitor their BAs, to be able to see and confirm that they are performing due diligence activities to keep information protected.

Significant benefits result for doing ongoing monitoring by using real-time compliance meters:

- You can check in to see what your organization, business associate, or remote facility is doing at any point in time with regard to compliance activities.
- Ongoing monitoring capabilities do not take any personnel away from doing their job responsibilities.
- Ongoing monitoring allows you to quickly and easily check your compliance progress with your tasks, as well as the progress of your business units and business associates.

Compliance audits

Unlimited types of audits can be performed to ensure your organization, BAs and others are following established policies as well as contractual and other legal requirements. Doing audits provides evidence of your due diligence to ensure you and your BAs are appropriately safeguarding information.

First, establish the scope of what you are auditing, and then choose a method for doing the audit. This will drive the metric to show compliance, non-compliance, and risk levels; for example:

- Compare the number of patients seen against the number of signed Notice of Privacy Practice acknowledgements. These numbers should be the same to be in full compliance with HIPAA requirements.
- Compare the workforce training records against sign-in sheets or logs of online training modules, such as those provided within Learning Management Systems.
- Compare the number of patient requests to see their corresponding PHI against how many were fulfilled within appropriate timeframes.

Audits have many benefits, but there are also drawbacks:

- Audits provide only a view of how an organization looks at a specific point in time. As soon as the audit is complete and normal business activities cause changes within the organization, the audit will no longer be valid to represent current practices.
- Audits are limited in scope. There may be significant risks that exist that fall outside of the audit scope.

- Audits are largely subjective. Generally, the less experience and understanding of HIPAA, security, and privacy the auditor has, combined with how your organization works with the auditor, the less accurate your audit will be.
- Audits are time consuming. Compliance audits typically require six to ten weeks, and even longer in some cases.
- Audits are labor intensive. This often causes a problem with those who are being interviewed and providing information to the auditors, such as OCR.

Third-party assurances

A wide variety of third-party assurances are available through many assorted security and privacy vendors. These include Information Security Management Systems certifications for ISO/IEC 27001/27002, and seals that indicate that recent audits and risk assessments have been performed.

All of these third-party certifications, seals, reports, and assessments can provide very good metrics and demonstrate due diligence. Use these to report:

- how often your site is scanned for malware;
- how well your privacy policy meets compliance with a wide range of standards and principles;
- how many of the HIPAA/HITECH requirements the organization is in compliance with, and areas where work still needs to be done;
- results of penetration tests and vulnerability scans, which show the number of security and privacy problems found; and
- your progress with specific security and privacy activities.

However, there are some drawbacks in using third-party assurances:

- They are typically very limited in scope. Assurance of one small part of an information security and privacy program does not mean appropriate activities are going on elsewhere.
- They are similar to audits in that they show a point in time; however, they are typically performed with more frequency than audits.
- Because of the automation involved with most of these, the human factors and physical security factors are not considered, and these are areas where significant threats and vulnerabilities exist.

Attestations

Attestations are statements from the CEO, or other executive of the company, indicating that he/she personally attests to the security and privacy practices of the organization. Good attestations list the general safeguards in place, and also state that the business leaders not only support having safeguards, but that they also actively ensure their personnel follow the policies and procedures. If business leaders are willing to attest to their responsibility on paper, they are more likely to ensure effective and compliant security and privacy programs are in place.

Attestations can document an organization's commitment to implementing an effective security and privacy program. Each month, you can ask your business associates different questions that cover different information security and privacy categories. From this, a metric can be created for the questions the BAs completed correctly. The results of the answers to the questions, along with how they completed the rest of the sections within the attestation, are then represented within compliance meters similar to the real-time compliance meters.

Ongoing research

Organizations should be tracking a wide variety of activities and data items to help ensure security and privacy efforts are effective and to also help identify problems areas before they turn into full-blown incidents. For example, organizations can track the number of complaints received from patients and customers, according to compliance categories, and then view the corresponding statistics for resolutions.

Continued on page 36

 ...continued from page 35

Key data stats for managing BAs

Several ongoing activities can be measured with metrics when overseeing BAs. For example:

- How often do you hold meetings with each of them?
- How many meetings do they actually show up for?
- How many BA webinars have you organized?
- How many of those BAs you invited actually attended?
- How many phone calls have you made to your BAs regarding incidents and breaches?
- How many times have they called your organization?
- What were the calls about? Call statistics can reveal how responsive your business partners are, as well as provide a history of problems, or how much service they provide.

You can also ask your organization and BAs for several types of key statistics that can be monitored as well. For instance:

- How often do they provide training to their personnel?
- What percentage of their personnel participates?
- How often do they provide awareness communications or activities?
- How many business changes do they experience each week? Each month? Within specific, security-impacting, categories?
- What kind of security incident stats do they maintain and monitor?

Protecting an organization's reputation and meeting HIPAA and HITECH requirements are top of mind for health care organizations. Metrics and data measurement should move to the top of your priority list. Creating systems and processes takes time; however, once in place, metrics will enable your organization to be a best practice leader in protecting patient privacy and your organization's reputation.

1. Dom Nicastro: "OCR Identifies HIPAA Audit Goals." Available at http://www.healthleadersmedia.com/page-1/PHY-269729/OCR-Identifies-HIPAA-Audit-Goals)
2. Available at http://www.privacyrights.org/data-breach/new
3. Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

People on the Move

Catherine Howell appointed to the Bernalillo County Ethics Board

Catherine Howell has been appointed to the Bernalillo County Ethics Board, New Mexico. Catherine previously served as Program Chair for the North Texas Healthcare Compliance Association, has been a member of HCCA's Southwest Regional Conference Planning Committee since 2006, and is currently a consultant in Albuquerque, NM.

Wetzel named Compliance Officer at The Reading Hospital and Medical Center

Recently Kathleen S. Wetzel, Shillington, PA, was named Senior Director of Compliance and Legal Services/Chief Compliance Officer at The Reading Hospital and Medical Center in Reading, PA.

Received a promotion? Have a new hire in your department? If you have received a promotion, award, or degree; accepted a new position; or added a new staff member to your compliance department, please let us know. It's a great way to let the Compliance community know where you have moved on to, or who has joined the Compliance team. Send your job change information to: service@hcca-info.org.