Shifting from Reactive to Proactive HIPAA Audits

By Danika Brinda, PhD, RHIA, CHPS, HCISPP

Stories about workforce members inappropriately accessing health information continue to plague the Department of Health and Human Services' Data Breach Portal—which lists US provider data breaches that affect more than 500 individuals. Recently two data breaches reported on the portal showed evidence that the breaches were caused by workforce members inappropriately accessing patient records without a business need.

In October 2015, approximately 2,000 patient records were accessed in a South Carolina hospital by a workforce member who sent screen shots of patient records to a former employee. And in early 2015, a data breach was uncovered that occurred over a five year span where a workforce member inappropriately accessed about 5,000 patients' records in a California hospital. While technology solutions are important for maintaining the security and privacy of protected health information (PHI), a complete security program must also focus on managing the risk presented by the human factor.

Many healthcare organizations have realized that when creating a solid HIPAA compliance program aimed at protecting PHI, workforce members must be seen as a concern for risk. In the Fifth Annual Benchmark Study on Privacy and Security conducted by the Ponemon Institute, employee negligence was ranked the top concern for security threats for both covered entities and business associates.[1]

Under the 1996 Health Insurance Portability and Accountability Act (HIPAA) Security Rule, two specific regulations discuss covered entity and business associate employee activities within electronic systems that contain protected health information:

- Information System Activity Review—This required implementation specifically states that covered entities and business associates must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." (CFR 164.308(a)(a)(ii)(c)).
- Audit Controls—This required standard mandates that covered entities and business associates need to "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." (CFR 164.312(1)(b)).

The HIPAA Security Rule doesn't define how these processes must happen, who should be the focus of the audit, or how frequently they should be conducted—this is left up to the covered entity or business associate to decide based on specific organizational needs. Most organizations will conduct reactive HIPAA audits due to a reported concern or potential healthcare data breach. However, organizations struggle to implement a HIPAA audit program that is based on both proactive and reactive HIPAA audits.

Proactive HIPAA audits are conducted based on different scenarios to evaluate access and catch unauthorized access prior to a privacy or security concern arising. When organizations only conduct HIPAA audits based on complaints or concerns regarding privacy or security issues, the risk of not uncovering improper activity within electronic systems can occur, which can lead to data breaches.

Deciding Who to Audit

It is impossible to audit every user's activity in every system that contains PHI within an organization. Organizations are challenged with a lack of resources, time constraints, technology constraints, and other various factors. Organizations should determine different events that exist within the normal course of business that increase the risk for members inappropriately accessing patient information. Some common scenarios that warrant proactive record access monitoring are:

- **Local and national well-known figures (VIP figures):** A very common group of people to monitor are local and national VIPs who receive patient care within an organization. This could be a sports star, a local news anchor, or a

hospital board member—anyone that an organization's staff may have special interest in beyond the typical patient. Other processes may be set up to protect these patients, such as alternative names and removal from the patient directory (in hospitals). However, the word usually still gets out within organizations about VIPs receiving care and can cause potential "snooping" by workforce members.

- **High profile news stories:** When local news stories mention the location of victims at local healthcare organizations, the "snoop" factor also plays a role in the potential for staff to inappropriately look at medical records to see what happened to the patient as a result of the incident. It is important to monitor who accesses patients' medical records in these cases to prevent unauthorized access and potential unauthorized disclosures of PHI to media outlets.
- **Workforce members accessing other workforce members' information:** When workforce members are looking at other workforce members' charts, it may be due to the normal course of business. However, there is a concern among coworkers when someone seeks treatment at organizations where they work. Special monitoring should be in place.
- **Demographic matches (name, address, phone number, etc.):** Same last name or same address matches can potentially mean that someone is looking into a record of a spouse, child, or other family member. Based on the organization's policy regarding access to family members' records, these cases may be evaluated to determine if the access was appropriate and warranted to support normal healthcare operations.
- **"Break the Glass" access:** Organizations that implement "break the glass" procedures—which can allow full open access to medical records due to an emergency or bypasses an additional log-in step to help protect sensitive information for specific individuals—should be a focus of audits. Due to the sensitivity of the information and the rare circumstances, it is recommended that an organization audit 100 percent of cases where workforce members "break the glass."

Best Practices for Creating a HIPAA Audit Program

Covered entities and business associates should create and establish processes for auditing information access activity within systems that store PHI. This should not only cover the process for reactive reviews based on reporting of potential privacy and security violations but also the steps and process for proactive monitoring.

Determine Which Systems that Contain PHI Produce Audit Reports

It is important that organizations understand what systems contain PHI and how activity within those systems is reported. It is common to find that not all systems that contain PHI will have audit log reporting mechanisms. Defining what systems have reporting capabilities, what those reports look like, and which systems will be evaluated as the initial step in a HIPAA activity monitoring process is important. In some cases, healthcare organizations will only audit the electronic health record (EHR), but it is important to remember that the HIPAA requirements focus on all systems that contain PHI and not just the EHR. The outcome of this step would be a clearly defined list of systems with PHI, the audit log capabilities, and the organizational plan for auditing each system.

Determine the Organization's Proactive Auditing Categories

Categories of proactive auditing that will occur should be defined by organizations. Based on the above list of common scenarios that may warrant proactive monitoring, organizations should establish a plan for what specific events will warrant the organization to conduct a proactive HIPAA audit. In some cases, organizations may choose to also determine what specific percentage of events they will audit. For example, an organization may choose to audit 100 percent of records related to high profile news stories, "break the glass," and VIP scenarios, but only audit a small portion of demographic matches and instances of workforce members accessing other workforce members' PHI. While this information may not be specifically defined in policies and procedures, a decision should be established for proactive auditing categories.

Determine How Much and How Often to Audit

HIPAA doesn't define how often or how many audits must be conducted to be compliant with the law. It is the responsibility of covered entities and business associates to determine what is best for their organizations. HIPAA audit frequency should be realistic and based on the organization's need. Proactive HIPAA audits should be done in real time as it is challenging to

evaluate activity after a long period of time has passed. The frequency and number of systems and/or workforce members to be audited should be agreed upon by the organization based on strategy and risk to the organization.

Determine How to Report Audit Findings

It is important that the findings from an audit are communicated to the appropriate individuals within the organization. Since privacy and security protections are a central focus of healthcare, a regular report to senior leadership on proactive monitoring findings should be trended and presented on a consistent basis. Additionally, it is important that trends and concerns get reported back to all leadership members so proper evaluation of processes that have been established can be evaluated when needed.

Establish Policies and Procedures for HIPAA Audits

Like many of the requirements under HIPAA, a written audit policy and procedure should be established. A clear, concise policy and procedure should be created to document the audit process within the organization. The policy should be specific enough to understand how the organization will conduct audits and how this requirement will be met for compliance.

Educate the Workforce on Audits

Organizations should be transparent with workforce members regarding the audits. The process should be clearly defined and communicated—what the intent of the audits are, what the process will be, what will occur during an investigation into questionable access, and how trending will be reported back to the workforce. Training and education can help ease audit concerns and can demonstrate the organization's commitment to protecting patient information, which may deter unauthorized accesses or disclosures.

Maintain Documentation and Proof of Audits

Documentation and proof of auditing is an important step in the success of an audit program. Organizations need to show evidence that HIPAA auditing was conducted per the defined organizational regulations. At a minimum, organizations should maintain audit logs, findings from their reviews, documentation on outcomes from the findings, and any additional information, including training activities. It is also a good practice to ensure that documentation from the audits are stored in a secure place with limited access to prevent any unauthorized access or tampering with the reports. Remember that HIPAA requires that documentation be kept and maintained for a minimum of six years. For best practices, organizations should create a clear process of documentation maintenance, define the process, and provide education for those tasked with documentation maintenance.

A proactive HIPAA audit process can help an organization prevent and deter unauthorized access and unauthorized disclosures of PHI. Additionally, it can help evaluate issues and trends that are present for accessing patient information.

Note

1. Ponemon Institute. "Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data." May 2015. http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf.

References

AHIMA. "HIPAA Security Rule Overview (Updated)." *Journal of AHIMA* 84, no. 11 (November–December 2013): expanded web version.

AHIMA. "Privacy and Security Audits of Electronic Health Information." *Journal of AHIMA* 88, no. 3 (March 2014): 54-59.

AHIMA. "Privacy and Security Training (Updated)." *Journal of AHIMA* 84, no. 10 (October 2013): expanded web version.

Minnesota E-Health Initiative and the Minnesota Department of Health, Office of Health Information Technology. "Summary of Proactive Monitoring Procedures for Secure Individual Identifiable Health Information." October 2014. www.health.state.mn.us/e-health/privacy/ps102114monitoring.pdf.

Tomes, Jonathan P. "Keeping It Private: Staying Compliant with the HIPAA Privacy and Security Rules." *Journal of AHIMA* 83, no. 3 (March 2012): 32-34. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049380.hcsp?dDocName=bok1_049380.

Danika Brinda (dbrinda@tripointhealthcaresolutions.com) is an assistant professor in the health informatics and information management department at the College of St. Scholastica, and is the owner of TriPoint Healthcare Solutions.

Article citation:
Brinda, Danika. "Shifting from Reactive to Proactive HIPAA Audits" *Journal of AHIMA* 87, no.1 (January 2016): 34-36.