Data Mining a Breach's Silver Lining: Analyze Breach Data to Improve Release of Information Performance in HIM

By Elizabeth Delahoussaye, RHIA, CHPS

Health information management (HIM) professionals can pull meaningful information from privacy and security breach data to evaluate release of information (ROI) processes, uncover workflow risks, and implement corrective measures. While large scale breaches impacting millions of patients make big news when they occur, breaches of protected health information (PHI) can also occur within the ROI process in small increments—one patient at a time. For example, a single record sent to the wrong mailing address. Or perhaps more commonly, another patient's information included within a release. ROI mistakes occur nationwide, every day, in hospitals, clinics, and physician practices.

While singular breaches don't make headlines or get listed on the Department of Health and Human Services (HHS) Office for Civil Rights' "wall of shame," they are prevalent—and if analyzed provide opportunities for HIM professionals and privacy officers to improve processes and better protect patients. This article explores how HIM professionals can analyze their ROI breach data to identify deficiencies in the release process, reduce risk of breach, and improve overall ROI performance. What is your breach data trying to tell you?

Insightful Analysis Begins with a Holistic Approach

Using an enterprise-wide approach, health systems should take a look at their owned or affiliated practices to determine where and what types of incidents are occurring. Drill down by site area, looking at the possibility of improvement in clinics and physician practices where breaches could occur. For example, are most unauthorized disclosures occurring at clinics? Are employees releasing the wrong information? Is one region, one site, or one member of the workforce the root of the problem? Are physician practices and clinics properly reporting breaches to support accurate data analysis?

Failure to identify and address breaches at clinics and physician practices can severely affect quality of care and compliance—and cause reputational damage for the entire organization. As the number of breaches in clinics increases, including their data in breach reporting and analysis must be a top priority.

Privacy officers working alongside HIM directors can help improve ROI by learning from breaches across the enterprise. A strong partnership between privacy and HIM departments is needed to ensure an ongoing reporting and assessment system that also includes office managers in clinics and physician groups. Privacy officers must have accurate data for reporting breaches to HHS. Creating a process to get accurate data from physician practices and clinics is essential.

Ask Why at Least Five Times

Ideally, the privacy officer should meet with office managers at various sites to emphasize the importance of accurate, complete, and timely reporting. During these meetings, the privacy officer should clearly show why this matters and lay out a process. For example, the office manager could agree to notify the privacy officer via e-mail with responses to preformatted questions required for HHS reporting and tracking. It is important to convey the importance of reporting and tracking breaches. Part of the solution is making sure providers and their staff know—on the front end and the back end—the potential risk of fines and penalties.

In the wake of a breach at one facility, privacy officers and HIM worked with operations to implement a simple yet successful strategy for analyzing targeted issues and improving ROI based on lessons learned. It involves asking "why" five times, or as many times as necessary to discover root causes.[1] When a breach or potential breach occurs, drill down to find out why it happened and how to prevent incidents in the future.

Ask:

- Why did this breach happen?
- Employee sent the wrong record. Why?
- Wrong records were scanned into the electronic health record (EHR) system. Why?
- Had a backlog and hired temps to help with scanning. Why a backlog?
- Did not budget appropriately for volume. Why?
- Assumed staff could manage workflow of a new unit. Why was this assumed?

This simple and straightforward inquiry points to two root issues. Prior to opening a new unit, the facility failed to budget for additional staff to manage the workflow—thus the backlog. Then, temporary staff were not properly trained to scan records and to understand the importance of accuracy. HIM and privacy officers can help resolve such issues and prevent recurrence by taking measures to boost preparation and planning. These include:

- Conduct training specific to the cause—clearly identify and address core issues.
- Practice the "why" routine with potential problem areas.
- Collaborate with the information governance (IG) team to provide staff education on IG principles—particularly regarding proper levels of protection and availability.[2]
- Discuss future goals, including every hospital, practice, and clinic in planning for additional services, units, or physicians.
- Evaluate volume and workflow to ensure preparation with properly trained staff in place.

There's no good argument against the old adage that "an ounce of prevention is worth a pound of cure." It still holds true when applied consistently in any discipline.

Cost of Breach Provides Incentive for Prevention

While some internal incidents are the result of intentional misuse of information, privacy and security breach within healthcare organizations is more often due to human error. The employees responsible may lose their jobs—in fact, many have. But firing staff may not be the best strategy. The benefits of lessons learned are often found by engaging employees, especially those who made mistakes, in the process of recovery, assessment, and prevention.

Realizing the cost of each breach is critical to conveying the importance of information integrity. Employees often don't understand the economic impact of unauthorized disclosure. When you show an office manager and their employees the cost of an error and the principles that are compromised, they can exercise caution with new awareness of transparency, privacy, and accountability.

From a provider perspective, it's important to consider the actual cost of each breach—the cost of investigation by privacy, compliance, and HIM departments, and the cost of terminating versus educating an employee who was involved in the breach. Hiring and training a new employee can cost an estimated $4,000 or more.[3] Instead of firing, engage employees in a root cause analysis—the "ask why" process to find answers and proceed with retraining and education.

Data Analysis Strengthens Employee Engagement, Performance

In a recent case, a series of unauthorized disclosures occurred at a particular site in one region. An audit to evaluate workflow and ask "why" revealed that employees were not using the appropriate checklist to validate patient authorization to release information. The solution was to provide the right checklist along with training. The result: there have been no unauthorized disclosures since the process was instituted in February 2016. Employees feel valued and empowered to release the right information to the right person at the right time.

The goal is to analyze and improve processes and performance. Using breach data as a guide, here are five strategies to consider:

- Conduct deeper audits—use the "ask why" technique
- Provide education, training, ongoing assessment—and continually monitor progress
- Look for common themes as the root causes of unauthorized disclosures

- Partner with employees to improve quality of work
- Use a team approach to achieve better outcomes from lessons learned

Once employees are engaged, improvement in overall performance and compliance should follow. If employees don't know what they're doing wrong, they have no opportunity to fix the problem. And through education and awareness, others can avoid making the same mistake. Success depends on communication and collaboration. Without broader analysis, people are caught in an endless cycle of isolated incidents that are likely to recur and never be resolved.

Faced with the threat of unauthorized disclosures and ever-increasing audits, providers should focus less on when and who, and more on why and what has been done to correct the issues.

Lean Six Sigma Improves ROI, Quality Assurance Processes

According to the American Hospital Association's first quarter 2016 RAC*Trac* report, an average of 6,330 medical records were requested per hospital from RAC auditors nationwide (all four regions) during the first quarter of 2016.[4] Given the vast volume of requests for information, human error is a huge factor in medical record mistakes.

As an integral part of creating strategies to redefine and improve ROI processes, Lean Six Sigma is now being used at an ROI outsourcing company to reduce unauthorized disclosures and improve quality assurance processes. "We are combining Lean Management and Six Sigma to reduce the occurrence of unauthorized disclosures to auditors and other requestors," says Shawky Haddad, vice president CI/CX, at CIOX Health, which receives and fulfills 50 million ROI requests per year. "The company first looks at all factors related to disclosures, and then optimizes internal quality assurance processes."

Hospitals, clinics, and physician practices can benefit from analyzing Lean Six Sigma data to minimize errors, support decision making, and increase patient engagement. And Lean Six Sigma practices are aligned with conducting analysis and education before making a quick decision to terminate an employee involved in a breach.

"The best way for hospitals to avoid mistakes in the ROI process is to follow what the data reveals—by staff member, type of information request, requestor/auditor, and delivery method," Haddad says. "Lean Six Sigma is about more than reducing labor costs and staff—it's about improving processes to mitigate the risk of future errors and support patient satisfaction through more consistent, standardized outcomes."

Data-Driven Analysis Brings Benefits Beyond ROI

Healthcare organizations at all levels are realizing benefits through increased efforts to assess workflow, redefine processes, evaluate technology, bolster education, and monitor progress. Strong data-driven analysis ultimately results in improved consumer trust. Increased privacy and security compliance supports an organization's reputation through efforts to improve patient safety and clinical outcomes.

As healthcare makes the transition to a value-based model, the timing is right to advance data analysis that will strengthen both employee and patient engagement, support management decision making, and enhance staff performance and compliance.

Tracking Unauthorized Disclosures

By monitoring unauthorized disclosures using specific data elements, HIM directors are better equipped to improve ROI procedures. Targeted education can be conducted and workflow improvements made based on a thorough analysis of breach data.

Sample Incident Tracking Report

ID#	DISCLOSURE NAME	DISCOVERY DATE	LOCATION	STATUS	ASSESSMENT	DISCLOSURE TYPE	ROI STAFF	OCCURANCE DATE BEGIN	OCCURANCE DATE END	PATIENT NAME
108	Respiratory Test	9/28/2016	Hospital A	Active Violation	Privacy	A	Jane	11/28/2015		William Adams
112	IP Abstract	8/26/2016	Hospital B	Active	Breach	A	Michael	9/10/2016	9/27/2016	Sue Smith
120	Progress notes	7/14/2016	Clinic A	Active	Breach	B	Yvette	9/23/2016		Jane Wilson
156	ED Records	7/4/2016	Hospital A	Active	Breach	C	Anthony	9/25/2016		Paul Johnson
174	IP Chart	9/24/2016	Hospital A	Active	Breach	F	Jane	5/14/2016		Jane Jones

SAMPLE DISCLOSURE TYPES:

A: Mismailed documents
B: Misdirected fax
C: Wrong records sent
D: Improper disposal of PHI
E: HIPAA privacy
F: Wrong dates of service

Information provided by CIOX Health

Notes

[1] Mind Tools Editorial Team. "5 Whys: Getting to the Root of a Problem Quickly." Mind Tools. www.mindtools.com/pages/article/newTMC_5W.htm.

[2] AHIMA. "Information Governance Principles for Healthcare (IGPHC)." 2014. http://research.zarca.com/survey.aspx?k=RQsURPPsUUYsPsPsP&lang=0&data=.

[3] Welz, Erika. "Hiring Your First Employee." *Entrepreneur*. www.entrepreneur.com/article/83774.

[4] American Hospital Association. "Exploring the Impact of the RAC Program on Hospitals Nationwide." RACTrac. June 3, 2016. www.aha.org/content/16/16q1ractracresults.pdf.

Elizabeth A. Delahoussaye (elizabeth.delahoussaye@cioxhealth.com) is the privacy officer/senior vice president of compliance for CIOX Health, where she is responsible for the oversight of the organization's compliance, training, and education.

Article citation:
Delahoussaye, Elizabeth A. "Data Mining a Breach's Silver Lining: Analyze Breach Data to Improve Release of Information Performance in HIM" *Journal of AHIMA* 87, no.10 (October 2016): 33-37.