Everyday Risk: Protecting against Breach in Release of Information

Save to myBoK

By Jan McDavid, Esq., and Rita Bowen, MA, RHIA CHPS, SSGB

Big data breaches grab the headlines, but mounting release of information requests pose everyday risks that require constant diligence.

While many within the healthcare industry are focused on preventing large, massive data breaches (such as those involving a missing laptop or stolen hard drive), a major component of HIM practice is safeguarding patients' personal medical information one chart at a time.

The release of information (ROI) function, the responsibility of HIM professionals, facilitates treatment, payment, and healthcare operations as well as fulfills legitimate record requests from patients, auditors, lawyers, and a multitude of quality and research entities. ROI requests have grown in number, and this increase in requests brings with it increased opportunity for inadvertent privacy breaches from human error, system error, or other mishap.

Eliminating errors in the ROI process is a key HIM opportunity to protect patients and help covered entities avoid breaches, fines, penalties, and reputational harm. Doing so requires ongoing assessment and training.

Requests-and Risks-on the Rise

Requests for medical records and protected health information (PHI) are fueled by increases in the number and types of audits and auditing bodies, the movement to wellness and patient awareness, and an ever-increasing litigious society.

Beyond these drivers, there are further changes in healthcare that promote information exchange and increase the inherent risk of breach such as EHRs, health information exchanges, and accountable care organizations.

Physical law states that a body in motion tends to stay in motion. Physics applies to electronic information as well. Once PHI leaves its initial resting spot it tends to remain in motion, and the risks of human error and wrongful disclosure expand.

At the same time that this large increase in information movement occurs, the regulations around this process have become more restrictive, the costs to remedy a breach are now higher, and the fines for information leaks are more onerous. HIPAA enforcement finally has teeth.

In 2010 alone (the most recent data available), the Office for Civil Rights investigated 4,229 reports of information breach, and 64 percent of these, or 2,703 events, required corrective action.[1] One incident involving a nonprofit corporation resulted in a total cost to the organization of $288,808 in legal fees, credit-monitoring services, staff time, and more.[2]

Audits on the Way

Further, the age of "voluntary" compliance with HIPAA is ending. OCR contracted with KPMG to conduct up to 150 audits of covered entities and business associates at random. These audits started in November 2011 and will continue through this year and likely into the future. They are expected to produce corrective action plans for facilities regarding HIPAA compliance.

HITECH's meaningful use incentives under ARRA also require that organizations attest to a risk analysis and risk management program. As providers start vouching for their organizations' security they are becoming more aware of their

deficiencies and compliance risk is making it to the executive dashboard, further reinforcing the need for HIM professionals to get proactive and get involved.

HIM's Role: Policy, Training, Workflow, Action

HIM professionals must tighten ROI workflow to mitigate risk of human error and breach. Every organization is at risk for breach, but the differences between entities will be reflected in how they implement policies, procedures, and corrective actions.

Policy and Procedures

All providers have a policies and procedures manual and conduct initial HIPAA training. Risk arises when training is done only once and policy manuals remain on the shelf collecting dust.

ROI policies and processes should be adaptive. That is, the process should change to meet new regulatory requirements and technology implementations. For example, changes to the HIPAA rules regarding the accounting of health information disclosures expected this year have the potential to dramatically expand HIM and ROI responsibilities and pose operational challenges. Similarly, EHRs and health information exchanges are pushing the frequency and scope of information transfer. HIM professionals must remain aware and on top of all changes to ensure HIPAA compliance and change processes accordingly.

Training

Training is a living process requiring continual attention. If this is not the responsibility of a chief compliance, privacy, or security officer, then HIM must fill these shoes.

Training is best delivered using a multitiered approach that builds on each preceding course. Every step within the ROI process should be addressed through training, with particular focus on three areas: front desk personnel, document identification, and pre-shipment validation.

Front desk personnel should always validate the requester by the photo ID contained with the patient's medical or business record (if applicable). Document identification staff should be trained to always narrow the search for specific documents from the EHR or paper chart. Particularly, they should use as many known identification factors as possible to ensure the correct, but minimally necessary, documents are pulled. Identification factors include such things as patient's full name, date of birth, Social Security number and visit date, if possible.

Finally, just prior to submission to the requester, ROI staff should always validate that only the uniquely authorized information has been included and that the information imported into the ROI process for disclosure belongs exclusively to that patient. Many facilities scan patient information from paper forms that were completed during the patient's visit. If this is the case, then the ROI staff must implement and perform quality control measures to validate that another patient's information was not inadvertently imaged or indexed to the original patient's record.

These individual errors represent the highest volume of breached records and are within the direct purview of HIM professionals. Training staff and ensuring quality controls are woven into each piece of the ROI process and are the most important steps HIM professionals can take to mitigate risk of breach.

Workflow

There are two steps in lessening ROI's vulnerability through workflow improvement. The first step is to create a tight, streamlined ROI process to mitigate risk. The second step is to test that workflow and conduct a risk assessment. Some of the more common examples of inadvertent disclosure include:

- Wrong chart sent to a requester
- Wrong information in patient charts with the same medical record number
- Co-mingled charts: family members, junior and senior

HIM departments should re-assess their ROI processes at least once a year-more often if regulatory or technology changes warrant a new review. Once assessed, corrective actions must be taken to close any privacy or security gaps in ROI workflow. Once workflow is tightened, a thorough risk assessment can be conducted.

Action: Risk Assessment and More

Risk assessments are best if they employ a combination of internal and external assessments. External reviewers wear no blinders, and they carry a wider breadth of experience. Both privacy practice and IT security assessments should be performed. Risk assessments must include follow-up to address identified risks.

Organizations often fail to adequately implement recommendations resulting from an assessment. This may be a product of financial or staffing constraints; however, investing minimal effort is no longer acceptable. Covered entities must continually test their processes and implement additional technical safeguards, such as:

- Semi-annual tested disaster recovery plans
- Internal vulnerability scans
- Third-party audits and measures
- SOC reports (formerly SAS 70)
- Penetration testing
- PCI Data Security Standard

Organizations should also consider obtaining legal counsel's advice on regulatory requirements and perhaps pursue cyber liability insurance, which could extend coverage for damages resulting from a breach. While purchasing more insurance and legal help are typically not high on an organization's compliance list, the old adage of an ounce of prevention being worth a pound of cure holds here.

Encryption is another critical step. With mobile devices giving anytime, anywhere access to virtual HIM departments, the traditional physical access controls are no longer adequate. Even telecommuter policies and procedures must be revisited.

HIM's technology investment must include data encryption for mobile devices, as well as audit logs and log management. Under the federal breach notification law, breach of encrypted data does not require notification, thereby providing a safe harbor if data loss or theft occurs.

HIM departments should recognize that human tendency is to take shortcuts when it comes to security. Common but risk-inducing behavior includes deactivating encryption functionality due to performance issues; using weak, old, or shared passwords; writing passwords on notes stuck to the computer; and failing to log out from computer systems. These behaviors are a major concern across hospital departments and within employees' homes.

HIM professionals should work with their IT counterparts to explore new technologies and methods beyond encryption that further ensure technical security. For example, tools can shut down a computer if hacking attempts are detected. Devices can be set to erase locally stored data after a predetermined number of failed log-in attempts.

Justifying the Cost

Nothing gets the attention of the executive suite faster than a series of large unexpected expenses. Freeing up budget to invest in privacy and security measures requires preparing a business case in advance.

Governmental and media coverage of the big data breaches are going a long way toward this goal. No organization wants to be front-page news for having exposed patient information.

A Ponemon Institute study reported that healthcare costs per breached record climbed to $301 in 2010 from $294 in 2009.[3] This is a good starting point for estimating the potential cost of a breach, but there is sure to be wide variances in individual experience. Hard costs will be more easily identified and measured than softer costs such as customer loss or reputational harm.

The hard costs include:

- Potential fines (federal files can reach $1.5 million per incident)
- Patient notification costs (e.g., employee time, printing, and postage)
- Bill write-offs, if patient owed money
- Credit monitoring and identity theft monitoring for each patient for a year or more
- Legal fees
- Forensic investigation
- Time and effort of staff
- Call center support for patients affected by the breach
- Media consultants

The soft costs tend to be reflected in a decrease in market share. The problem is that it is difficult to discern whether that decrease stems from the breach. It is somewhat uncommon for patients to completely shift their care to a different hospital facility. Changing physicians is much easier. The rate of patient churn is much higher than the average customer churn in other industries, indicating willingness on the part of patients to move to different providers.

Facing ROI Reality

The one certainty about ROI is that it will change and continue to evolve as healthcare delivery, regulations, and reimbursement changes and evolves. And HIM professionals are at the center of its transition.

Staying ahead of the risk curve means implementing best practices in policies, procedures, training, and workflows. While nothing will completely eliminate risk, the way in which organizations proactively plan and improve the ROI process separates fire-fighters from fire-preventers.

Understanding the risks and continually seeking ways to prevent them will always be a best practice.

Notes

1. Office for Civil Rights. "Enforcement Results by Year." www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html.
2. Tripathi, Micky. "First-Hand Experience with a Patient Data Security Breach." December 3, 2011. www.histalkpractice.com/2011/12/03/first-hand-experience-with-a-patient-data-security-breach-12311.
3. Symantec. "2010 Annual Study: U.S. Cost of a Data Breach." March 2011. www.symantec.com.

Jan McDavid is general counsel, and Rita Bowen is privacy officer and senior vice president of HIM, at HealthPort.

Article citation:
McDavid, Jan P; Bowen, Rita K.. "Everyday Risk: Protecting against Breach in Release of Information" *Journal of AHIMA* 83, no.4 (April 2012): 26-29.