Optimizing PHI Disclosure Management in the Age of Compliance

Save to myBoK

By Don Hardwick; Mariela Twiggs, MS, RHIA, CHP, FAHIMA; and James H. Braden, MBA, RHIA

A mere two decades ago, healthcare providers didn't face significant penalties for improperly disclosing protected health information (PHI). Since then, regulations surrounding the privacy and security of PHI have evolved to include strict requirements and corresponding steep financial penalties for non-compliance.

Since the HIPAA breach notification requirement took effect in 2009 as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, more than 31 million people have had their PHI compromised, and the Office for Civil Rights (OCR) has levied more than $25 million in fines. In addition to those fines, PHI breaches have incurred other unfavorable consequences that have had far-reaching effects on providers, including: the cost and negative impact of notifying individuals of a breach; civil monetary penalties imposed by the United States Department of Health and Human Services (HHS); civil lawsuits by patients; and damage to organization reputation through media and public opinion.

In response to the highly impactful consequences of non-compliance, providers are more focused on compliance than ever, and have charged health information management (HIM) professionals with investigating ways to improve how their organizations protect patient privacy and security.

Although compliance is top-of-mind, a variety of factors—including new regulations, widespread use of electronic health records (EHRs), organizational growth by acquisition (for instance, the addition of physician practices), and an imbalance in information governance (IG) practices—make compliance a challenging undertaking. Many HIM professionals are addressing this situation through an enterprise-wide, standardized approach to PHI disclosure management. With this approach, all disclosure points throughout a healthcare enterprise can achieve compliance by strictly adhering to state, federal, and internally developed guidelines.

This article will address the current regulatory environment, discuss trends making privacy and security compliance difficult, and provide details about how HIM professionals can lead a collaborative effort to meet compliance challenges through enterprise-wide disclosure management.

Today's Regulatory Environment: Omnibus and OCR HIPAA Audits

Healthcare leaders are more motivated than ever to ensure organizational compliance with federal privacy and security regulations. It's critical to understand how the HITECH Act's HITECH-HIPAA Omnibus Rule has changed HIPAA, and how healthcare providers are being put to the test in the OCR auditing process.

The HITECH-HIPAA Omnibus Rule

The HITECH-HIPAA Omnibus Final Rule, which went into effect in 2013, changed HIPAA in a variety of ways. It provides individuals with the right to receive electronic copies of their health information and allows them to restrict PHI disclosures to their health plans if they fully pay for treatment out-of-pocket. It outlines new breach reporting requirements, making the business associates (BAs) of covered entities (CEs) directly liable for compliance with certain HIPAA requirements. It also significantly strengthens financial penalties for breaches.

The more stringent regulations regarding patient rights and patient access have produced an advanced level of complexity for hospitals and physicians, which in turn requires a larger scale effort to meet patient needs while achieving compliance. For instance, the Omnibus Rule gives patients more rights related to receiving health information in the format they request—and in a demanding timeframe—all while safeguarding their privacy. Meeting these demands can be challenging for healthcare providers who are adjusting to new timeframes while also accommodating a broader array of requests.

On the other hand, there are very legitimate reasons for denying access to health information. Factors such as mental health, child abuse, or treatment related to a criminal assault can all influence how PHI should be handled. These many nuances can create further compliance difficulties and necessitate an optimal combination of policies, processes, and technology, along with training to safeguard against human error.

In addition to the updated patient rights, the Omnibus' new breach reporting requirements also add compliance complexity. Now, OCR presumes guilt—in cases of improper disclosure it is assumed that the provider's improper disclosure has resulted in a breach and providers must prove their patient data wasn't compromised. This reality represents a 180-degree change from the earlier regulatory environment.

This new standard of "guilty until proven innocent" makes all components of PHI disclosure management critical, but one area in particular stands out—documentation. Even if a CE properly addresses facets of PHI disclosure management such as internal audits and policy and procedure reviews, a lack of documentation can compromise compliance. As the old adage goes: "If it isn't documented, it didn't happen."

Documentation experts have traditionally resided within the HIM department, so this critical need shouldn't seem unfamiliar. The difference, however, is in meeting new demands related to patient access, the unknown terrain of health information exchanges (HIE), and the broadening scope of disclosure points. Consequently, as HIM's role grows, it must also evolve to meet a broader set of PHI disclosure management needs within the healthcare organization.

OCR Audits Entering Second, Third Phases

Despite the extra preparation time gained when OCR postponed its Phase 2 HIPAA audits, the abundance of initiatives necessary for compliance has created complexities—and a flurry of activity—for healthcare organizations. OCR's Phase 2 HIPAA audits focus on the HIPAA Security Rule and risk analysis, the HIPAA Privacy Rule and access issues, and the Breach Notification Rule. Auditors are looking for comprehensive risk analysis, documentation of follow-up risk management activities, documentation of policies and procedures and evidence of their implementation, and ongoing education and enforcement.

Although healthcare organizations are now addressing Phase 2 audits, it isn't too early to begin preparing for Phase 3 audits. The focus of Phase 3 audits will include encryption and decryption, plus facility and physical access control. Even as they're addressing Phase 2 requirements, organizations can concurrently address organization-wide encryption across all laptops, mobile devices, and e-mail systems. Current training, policy and procedure reviews, and internal audits can also incorporate physical and facility access. For instance, audits can easily include checking for PHI in waste bins and ensuring charts aren't visible at nurses' stations.

Keep in mind that OCR audits also address third-party business associates (BAs), over which healthcare organizations have little control in regard to compliance responsiveness. Therefore providers can benefit from being proactive with their BAs and requesting documentation as early as possible. BAs should be able to provide documented evidence of their own internal protocols and policies, such as:

- Security Policies
    - Information Security Risk Analysis
    - Information Security Risk Management Program
    - Information Security Audit Controls
    - System Activity Review Policy
    - Security Incident Response Policy
    - Data Backup and Storage Policy
    - Data Disposal Policy
    - Media Re-Use Policy
    - Workstation Policy

    - Electronic PHI Movement Policy
- Privacy Policies
    - PHI Uses and Disclosures
    - Patient Access
    - Accounting of Disclosures
    - Sanctions Policy
    - Breach Policies and Procedures

Healthcare Trends Bring New Compliance Challenges

The Omnibus Rule's more stringent rules and penalties coupled with the looming threat of OCR HIPAA privacy and security audits generate unprecedented compliance urgency. Compliance must be an organizational priority for both hospitals and physician practices, backed by the leadership and resources necessary to accelerate efforts.

As providers ramp up compliance programs and conduct due diligence, many of them will discover areas of risk. This risk isn't necessarily due to carelessness or ignorance; rather, it's the result of industry trends. In particular, the widespread use of EHRs, hospitals' rapid acquisition of physician practices, and the adoption of electronic health information exchange establish inherent risks that require new approaches to PHI disclosure management.

EHRs and Additional Points of Disclosure

Many hospitals have as many as 40 disclosure points. At face value, this number may seem improbably high. However, the "meaningful use" EHR Incentive Program (MU) has driven the widespread adoption of EHRs. As of December 2013, nearly 90 percent of eligible hospitals attesting to MU stage 1 had a primary vendor meeting the ONC's base EHR definition.[1] By April 2014, approximately 80 percent of all eligible hospitals received an incentive payment for demonstrating MU requirements through the use of an EHR.[2] These numbers show just how many hospitals are using EHRs, and as their use increases so too do their disclosure points.

This rapid EHR adoption has improved care coordination and patient engagement, but it most likely has achieved the opposite effect with PHI disclosure management. To prevent improperly disclosing data, many clinicians and staff using EHRs may require specific training in compliance and the proper release of PHI.

Increased Risk from Physician Practice Acquisitions

Acquisition of physician practices increases points of disclosure and risk to healthcare enterprises. A PricewaterhouseCoopers report shows that healthcare industry consolidation has increased more than 50 percent since 2009.[3] In many cases, hospitals are acquiring numerous physician practices and creating large groups under their brand names. Growing a hospital-owned physician practice group can increase an organization's footprint while enabling better care alignment. However, it can also increase PHI disclosure management risk as hospitals take on the responsibility and liability associated with properly disclosing health information. This can be particularly difficult since physician practices can vary drastically when it comes to technology, processes, standards for PHI disclosure management, and training of personnel. These variations can not only create risk, but also make it harder to prove compliance since tracking and reporting can be especially challenging.

HIE and Information Governance

The growing adoption of HIEs has caused traditional HIM information governance roles and responsibilities to shift to the information technology (IT) department at some organizations. Budget, resources, and the decision-making process around HIE and PHI disclosure management have consequently become imbalanced.

Traditionally, IT and HIM have very different views of IG, which makes it imperative that both parties' voices are heard. As HIE grows, increased collaboration between HIM and IT becomes critical. IT's knowledge of technical security aspects such as public key infrastructure, encryption, and data integrity is a necessity, while HIM has in-depth experience with privacy, compliance, breach, and risk management issues.

As providers and organizations are challenged to define optimal strategies and best practices for PHI disclosure management, they also must establish an appropriate balance in IG that will showcase each party's expertise and foster a new, deeper partnership that will ultimately be integral to their hospital's successful HIE practices.

Broadening HIM's Role to Meet Evolving PHI Disclosure Management Needs

HIM now has the opportunity to function in a more collaborative and consultative role, leveraging its core expertise with compliance and IG. By serving as the catalyst for organization-wide standardization of policies, procedures, and training, HIM can help ensure that the growing number of departments involved in PHI disclosure are doing so in a secure, compliant, and efficient manner.

While HIM and IT collaboration is important, having a single point of leadership and bottom line accountability for PHI disclosure management is also optimal. Enterprise-wide disclosure management enables quality control, standardization, and better adherence to policies. It allows for the development of the best possible processes, while also setting the stage for continuous improvement.

Overall, a centralized PHI disclosure management program can mitigate opportunities for risk, improve compliance, and better prepare an organization for audits. Below are four key steps to compliance. Ideally, HIM can conduct these steps in a centralized fashion, collaborating with IT and other departments as appropriate.

1. Policy and Procedure Review

A key component of OCR audit preparation—and ensuring proper PHI disclosure management on an ongoing basis—is a comprehensive review of policies and procedures. HIM's longstanding responsibility as the owner of PHI policies and procedures puts the department in an ideal position to offer this same expertise across the organization.

The review should include policies and procedures related to the following:

- Patient Access (very important for OCR desk audits)
- Accounting of Disclosures
- Restrictions
- Corrections/Amendments
- Breach Notification (very important for OCR desk audits)
- Notice of Privacy Practices
- Sanctions
- Business Associate Agreements
- Release of Information
- Minimum Necessary
- Designated Record Set Definition
- Legal Health Record Definition
- Confidentiality

In addition, the review should include policies related to the HIE environment such as the Data Use and Reciprocal Support Agreement (DURSA) and the sub-data set available through the DURSA, and audits of the HIE environment.

2. Internal Audits

Conducting internal audits in a variety of ways (planned, unplanned, or even "mystery" audits, when the staff doesn't know it's being audited) can promote better compliance. By going on the offensive, organizations also ensure more thorough preparation for possible OCR audits or state health department reviews. Internal audits at some facilities have revealed dangerous practices—for instance, nursing stations leaving patient information visible on a monitor, and emergency department (ED) clinicians burning CD copies of patient records for unauthorized family members. That said, consider developing an audit program that addresses various privacy and security issues. Develop a checklist and visit various areas of the hospital to review the following:

- Are printers and fax machines secured from public view?
- Are waste bins free of PHI?
- Are computer monitors equipped with privacy screens or kept away from public view?
- Can staff discussing PHI be overheard?
- Are print capabilities limited to only the necessary departments?
- If patient names are used in waiting rooms, do clinicians and staff use only the minimum necessary? (i.e., Ms. Smith)
- If sign-in sheets are used, is the minimal amount of PHI requested?
- Are doors locked and access limited to departments housing PHI?
- Is the Notice of Privacy Practices posted?

Also, conduct various tests to determine if staff is protecting PHI:

- Walk through the nursing station to see if it's possible to remove a chart or access documents.
- Ask IT to call a staff member to see if he or she will give out password information.
- Call Release of Information staff to ask how to obtain a medical record.
- Call the facility and attempt to find out verbal information about a patient.
- Call the HIM department to ask for a correction to your patient record.
- Verify the organization has revoked computer rights and badge access for recently terminated employees.

3. Tools and Technology

While departmental and enterprise-wide IT systems have advanced, their capability to support proper PHI disclosure may not be keeping up with increasingly stringent requirements. Working with IT and other appropriate departments, HIM can help ensure software is supporting the organization's enterprise-wide PHI disclosure management goals. Software enhancements such as flagging for minors' records, computing turnaround times for fulfilling requests, and adding access trails within the platform can facilitate compliance.

It's also helpful to review departmental processes and see where technology can be improved to support compliance, or where it currently creates risk by being misused. For instance, in the previous example where ED staff burned patients' records onto CDs for family members, the use of the CD burner led to improper distribution of patient records. In this case, the organization's replacement workstation didn't have a CD burner.

4. Adequate Training

A sharp increase in PHI disclosure points and a more networked and complex digitized environment are two factors that increase the importance of comprehensive, organization-wide privacy and security training. Clinicians and staff have numerous opportunities each day to disclose PHI, and if they haven't received full, up-to-date training, they can unknowingly create risk. The HIPAA privacy and security rules require healthcare organizations to formally educate the workforce to ensure ongoing accountability for the handling of PHI, as well as documentation verifying that it was provided.

While there are no set guidelines for how to conduct training, AHIMA's best practices include the following:

- Provide annual training for all staff
- Include education, training, and ongoing awareness and cover PHI in all its forms (verbal, written, electronic)
- Develop a repository of current policies and procedures
- Test staff on information to ensure that they have completed training before they are able to access PHI

Role-based training is especially important, as it enables trainees to focus on their daily responsibilities and specifically where they will encounter potential compliance risk. In addition to comprehensive employee training, it is important to work closely with BAs to ensure both thorough training and documentation is conducted.

Characteristics of Successful Disclosure Management Programs

The state of audit readiness among healthcare organizations varies widely, and there are numerous paths to achieve compliance. Successful PHI disclosure management programs do, however, share several commonalities.

Foremost, successful PHI disclosure management programs are enterprise-wide, allowing for governance of policies, procedures, and technology across the entire organization. The entity with oversight has both authority and ultimate accountability. Therefore, the structure allows for standardization and optimization with an underlying "buck stops here" atmosphere. It's important to note that staff can be decentralized as long as their accountability is to one single entity.

In addition, these enterprise-wide policies must have visible sponsorship and ongoing support by the highest levels of leadership. Clinicians and staff across all departments must understand that all training activities, along with strict adherence to policies and procedures, are a strategic priority for leadership.

Lastly, a successful program includes monitoring and measurement. Technology that embeds these capabilities can not only simplify efforts but also facilitate frequent, ongoing oversight. Leadership can easily review departments that frequently disclose PHI. They can track metrics such as the timeframe between the origin of a request until fulfillment, as well as determine who is managing turnaround times properly and who might need additional help. Ongoing measurement also provides actionable information, showing leadership where they may need to conduct additional training or internal audits.

With the myriad factors involved in ensuring proper PHI disclosure, it's critical to have a combination of the right processes, policies, and technology. Maintaining standards, governance, and accountability at the enterprise level is also critical, and HIM's expertise in these areas can help position the organization for success.

Notes

[1] Office of the National Coordinator for Health IT. "Data Analytics Update: Health IT Policy Committee Meeting," January 14, 2014. www.healthit.gov/facas/sites/faca/files/HITPC_DataAnalyticsUpdate_011414.pdf.

[1] US Department of Health and Human Services. "Doctors and hospitals' use of health IT more than doubles since 2012." HHS press release. May 22, 2013. www.hhs.gov/news/press/2013pres/05/20130522a.html.

[1] PricewaterhouseCoopers. "Medical Cost Trend: Behind the Numbers 2014." June 2013. www.pwc.com/en_us/us/health-industries/behind-the-numbers/assets/medical-cost-trend-behind-the-numbers-2014.pdf.

Don Hardwick (DHardwick@mrocorp.com) is vice president of client relations and compliance and Mariela Twiggs is national director of training and compliance for MRO. James H. Braden is senior consultant for The Advisory Board Company.

Article citation:
Don, Hardwick; Twiggs, Mariela; Braden, James H. "Optimizing PHI Disclosure Management in the Age of Compliance" *Journal of AHIMA* 86, no.2 (February 2015): 32-37.