REGULATORY CHANGES DEMAND AN ENTERPRISE-WIDE APPROACH TO DISCLOSURE MANAGEMENT OF PHI


By Don Hardwick,
Director of Client Relations and Compliance at MRO Corporation
REGULATORY CHANGES DEMAND AN ENTERPRISE-WIDE APPROACH TO DISCLOSURE MANAGEMENT OF PHI


Healthcare organizations in the United States operate in a rapidly evolving environment that includes integrating new technology into their facilities and workflows, fulfilling more requests for access to protected health information (PHI) and addressing a growing need for stronger compliance safeguards as new federal and state regulations are introduced to the healthcare industry. As a result of these tighter regulations, health information management (HIM) professionals have been called to examine the methods by which they deliver, track, manage access to, and disclose PHI.

This white paper outlines the challenges healthcare organizations face as a result of regulatory changes and increased access to health information, and explains how deploying an enterprise-wide disclosure management solution can standardize disclosure processes, minimize liability and financial risks and drive system-wide compliance for healthcare organizations.

Tightening Federal Policy

To understand the challenges healthcare organizations face, we must first understand the changes to the privacy rule that spells out how health systems and covered entities use and disclose PHI.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 introduced rigorous privacy and security regulations, stricter penalties for breach, the meaningful use incentive program and discussion about maintaining better documentation for accounting of disclosures - all of which affect how healthcare organizations securely, properly and efficiently handle PHI.

The following year, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) published a proposed rule mandated under the HITECH Act to further strengthen the security and privacy provisions under the Health Insurance Portability and Accountability Act (HIPAA). The rule calls for more stringent access, disclosure and tracking rules, and steeper penalties for non-compliance with HIPAA.

While the HITECH Act provides for penalties at all levels of culpability, it particularly emphasizes enforcement of cases due to “willful neglect”–or the conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. HITECH requires HHS to formally investigate any complaint of a violation if willful neglect is indicated, and if a violation is deemed a result of willful neglect, HHS is required to impose a penalty. Moreover, HHS implemented the “HIPAA Privacy and Security Audits” to assess covered entities’ compliance with the privacy, security and breach notification rules. With stricter regulations and steep potential penalties on the line, hospital leaders have had to focus more time and attention on achieving compliance than ever before.

Policy enforcement across an enterprise is challenging because HIM, risk management, billing, compliance and other departments accessing PHI within the hospital and disclosing PHI outside the hospital may work independently of each other. More communication between departments is vital in identifying disclosure points which may be susceptible to PHI leaks and enforcing policies across an enterprise.
More Disclosure Points, More Challenges

Meaningful Use and EHRs
The Medicare and Medicaid Electronic Health Record (EHR) Incentive Program established by HITECH promotes the use of EHRs to improve quality of patient care through the secure use and sharing of health information, but for providers, transparency comes at a price. Some of the core objectives outlined in stage 1 of the meaningful use program require healthcare organizations to produce patient information electronically upon request and offer electronic discharge instructions to patients. Proposed stage 2 rules mandate that healthcare providers allow more patient online access to electronic records, whether downloaded, transmitted, or viewed online or via patient portals.

While the proposed changes continue to strengthen the right of individuals to access their health information electronically, they also create more challenges for the healthcare providers, especially in the areas of security and privacy, requiring healthcare organizations to re-evaluate how they interact with their patients in disclosing PHI.

Accounting of Disclosures
Similarly, the proposed accounting of disclosures (AOD) rules that further promote patient privacy and the secure exchange of PHI have led hospital and IT leaders to examine how disclosures are handled both from within and outside a healthcare organization. If implemented, AOD rules may require that healthcare organizations provide patients with details concerning not only which individuals within an organization accessed their records but also any disclosures to unauthorized requesters from the outside. It also will stipulate that those instances are properly documented for the purpose of the disclosure. Additionally, tracking the access to records and disclosures made for purposes of treatment, payment and operations (TPO) will be demanded of healthcare organizations. Previously, it was not necessary to track and report such instances of PHI access or disclosure. These rules will add to the prudence of managing disclosures across a healthcare enterprise to ensure that all access and disclosures are compliant and properly tracked and reported.

Escalating Payer Audits
As the number of audits for fraud and overpayment continues to escalate, healthcare providers are being asked to release more and more records to third parties. Buoyed by the success of Medicare recovery audit contractors (RACs) recouping more than $1 billion in improper payments in recent years, Medicare audits have become a permanent process nationwide. And now, other payer organizations have jumped on the bandwagon and initiated their own audits to ferret out possible fraud or overpayment. To add fuel to the fire, the upcoming transition to ICD-10 coding may bring about even more scrutiny of medical documentation. With an 800 percent increase in the number of available codes, there is a potential for more coding disputes and a wealth of additional audits. The already-increasing volumes of audits are forcing healthcare organizations to establish defense mechanisms in order to properly manage audit requests, track audit limits and ensure proper billing according to each payer’s contract.

The Electronic Trend
Across the healthcare industry, there is a general migration from paper to electronic documentation and systems. More frequently, requesters of PHI are asking for the movement of transactions to an online platform, such as portals or other direct connections. Third-party requesters want to request, check status, pay for and receive electronic copies of PHI through the Internet, as opposed to using the historical standard of fax, paper, CD and other portable electronic devices. Portal access to medical documentation is not being demanded solely by third-party requesters, but by patients as well. Although the electronic exchange of PHI should improve the quality of patient care, the transition from paper to automation
will create more disclosure points while also requiring the healthcare organization to control access and manage consents accordingly.

Additionally, provider-to-provider communication is moving online, creating new challenges for managing disclosures. For example, the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology are using a gateway to the Nationwide Health Information Network (NHIN) through electronic submission of medical documentation (esMD) to provide a more efficient way to deliver medical records to payer audit contractors. Similarly, the federal government’s Direct Project, which is pushing to establish a means for healthcare providers to exchange information via direct email messages, will reduce the volume of paper that enters and exits their facilities.

With tighter regulations, new technology, increased access to records, and more disclosure points, managing the flow and disclosures of PHI across the enterprise will be progressively challenging for hospitals and healthcare systems.

**The Enterprise-Wide Solution**

An enterprise-wide approach to disclosure management is the optimal solution to the imminent challenges that healthcare professionals face as the industry experiences fundamental changes in the way PHI is accessed, exchanged, tracked and reported.

This approach offers hospitals and healthcare systems the ability to utilize software and services that can be deployed as a common tracking platform across the healthcare enterprise including HIM, radiology, outpatient, the business office and numerous other departments. By implementing a centralized system for handling the access and disclosure of PHI, healthcare facilities obtain the interdepartmental communication, policy enforcement, level of oversight, quality assurance and transparency that they need to comply with the increasingly complex, technologically-driven, regulatory and legislative environment.

The centralized platform opens the doors to communication needed to enforce policies across all departments. By processing all disclosures through one system, all hospital departments that disclose PHI receive the benefits of secure technology, comprehensive workflow and quality assurance checks on all disclosures sent through the system.

When all disclosures are managed centrally, enterprise-wide policy enforcement is possible. By standardizing processes throughout an organization and applying best practices under HIM’s expertise across the system, healthcare organizations can ensure a steady enforcement of enterprise disclosure policies, a manageable workflow and a consistent experience for patients and requesters.

This approach allows healthcare organizations to have complete confidence in their compliance. Not only does this approach protect a patient’s privacy, it also protects the institution against breach, financial risk, lawsuits and reputational damage. Embedded compliance tools and breach assessment capabilities help an organization properly manage its disclosure of PHI and determine if a breach has occurred so it can respond quickly and effectively when necessary.

Healthcare organizations are also able to leverage EHR capabilities through integration with disclosure management systems to improve reporting quality and turnaround time. Providers can coordinate workflow and capture all process documentation in one location and benefit from centralized database tracking and reporting for all departments. The disclosure management system synchronizes with master patient indexes for easier data capture and restriction monitoring.
These systems automatically capture disclosures (i.e., print routines), provide advanced reporting functionality and allow a range of disclosure options that include paper, thumb drives, film, CDs, patient portals and esMD delivery. In the future, even more advanced disclosure services such as direct email messaging will be available.

As the exchange of health information continues to move online, utilizing a sophisticated disclosure management system designed by the industry’s technology leaders will be vital to the success of a healthcare organization – not only within HIM, but throughout the enterprise.

**KEY BENEFITS OF ENTERPRISE-WIDE DISCLOSURE MANAGEMENT**

- Increased communication between departments
- Policy consistency across the enterprise
- High level of oversight
- Quality assurance and compliance across the enterprise
- Centralized database tracking and access to PHI
- Centralized audit management
- Centralized workflow management
- Faster turnaround times