Regulatory Changes Demand an Enterprise-Wide Approach to Disclosure Management of PHI

Health Care Organizations Standardize Disclosure Processes, Minimize Liability and Financial Risk, and Drive System-Wide Compliance

Don Hardwick

Don Hardwick is vice president of client relations and compliance for MRO Corporation, based in King of Prussia, Penn. He works closely with MRO clients to develop comprehensive strategies for managing the efficient, secure, and compliant disclosure of PHI. For more information, visit www.mrocorp.com or contact him directly at dhardwick@mrocorp.com.

Health care 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 health care industry. As a result of these tighter regulations, health information management (HIM), compliance, and risk management professionals have been called to examine the methods by which they deliver, track, manage access to, and disclose PHI.

There is a universal need for understanding the challenges health care organizations face as a result of regulatory changes and increased access to health information and how deploying an enterprise-wide disclosure management solution can standardize disclosure processes, minimize liability and financial risks, and drive system-wide compliance.

Tightening Federal Policy

To recognize the challenges health care organizations face, we must first understand the changes to the privacy rule that spell 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 (AOD) — all of which affect how health care organizations securely, properly, and efficiently handle PHI.

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 the U.S. Department of Health and Human Services (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 Health Insurance Portability and Accountability Act (HIPAA) privacy and security audits to assess covered entities' compliance with the privacy, security, and breach notification rules.

Final Omnibus Rule

In January 2013, HHS published its final omnibus rule. The final rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law. The omnibus rule includes the following changes:

- It expands many of the requirements placed on providers, plans, and other entities that process health insurance claims to their business associates that receive PHI, such as contractors and subcontractors.
- It increases penalties for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation in a given year.
- It replaces the original and subjective "risk of harm" with quantifiable risk assessments that clarify when breaches of unsecured health information must be reported.
- It provides stronger privacy protections for genetic information.

Risk Assessment

The HITECH Act defined a "breach" as the unauthorized acquisition, access, use, or disclosure of PHI that compromised the security or privacy of that information in such a way that it posed a significant risk of financial, reputational, or other harm to the affected individual. To determine whether an impermissible use or disclosure of PHI constituted a breach under the interim final rule, facilities were required to perform a risk assessment to determine if there was a significant risk of harm to the individual as a result of the impermissible use or disclosure.

While many of the new regulations outlined in the final rule were anticipated, changes to breach notifications were not. The omnibus rule has now removed the harm standard and modified the risk assessment to focus on more objective standards to determine whether the privacy or the security of the PHI has been compromised. An impermissible use or disclosure of PHI is presumed to be a breach unless the organization or its business associate demonstrates that there is a low probability that the PHI has been compromised or unless one of the other exceptions applies.

Covered entities and business associates now have the burden of proof to demonstrate that all breach notifications were provided or that an impermissible use or disclosure did not constitute a breach and to maintain documentation sufficient to meet this burden of proof. Breach notification is not required under the final rule if the covered entity or business associate demonstrates, through a risk assessment, that there is a low probability that the PHI has been compromised.

The risk assessment must consider each of the following factors: the nature and the extent of the PHI involved (such as whether the disclosure involved sensitive information); the unauthorized person who used the PHI or to whom the disclosure was made (an employee of a covered entity has an obligation to protect the privacy

and security of the PHI); whether the PHI was actually acquired or viewed (or if only the opportunity existed for the information to be acquired or viewed); and the extent to which the risk to the PHI has been mitigated (satisfactory assurances that the information will be destroyed, returned, or will not be further used or disclosed).

Health care organizations have until September 23, 2013 to comply with the final rule. Nevertheless, keeping pace with this and other changing privacy and security regulations will be a major challenge for hospitals and their HIM, compliance, and risk management departments.

The Financial Impact of Breach

Health care organizations will need to develop a singular focus on prevention to avoid the widespread and potentially devastating consequences of breach. The American National Standards Institute (ANSI) published a business case for enhanced PHI security in 2012 titled "The Financial Impact of Breached Protected Health Information," which identified the following repercussions when there is a PHI breach:

- reputational, including loss of patients, staff, and partners;
- financial, including costs of remediation, communication, deductible and/or

Case Study: A Close Call — Tracking Disclosure for Treatment, Payment, and Operations

In late 2012, a man that was treated at his local acute care hospital awoke to find his medical records scattered across his front yard. He promptly called the hospital, demanding an explanation from the organization's risk manager.

Fortunately, the hospital's release-of-information vendor tracks all record requests to HIM within their disclosure system — including those for treatment, payment, and health care operations (TPO). It was quickly discovered that the man's health information had been formally requested by a physician's office that routinely requests copies of medical records from the involved hospital.

The hospital was able to investigate why the records were requested from that doctor's office and learned that the individual who requested the information had inappropriately made the request for personal use; it was the patient's disgruntled girlfriend who wanted access to specific information from his medical records. Part of her regular responsibilities at the physician's office included requesting medical records from the involved hospital. Because the investigation uncovered that the disclosure was made *properly* from one covered entity to another, the hospital in question was not held liable.

This incident provides a case for an enterprise-wide approach to disclosure management that includes maintaining a comprehensive accounting of disclosures (AOD) across all departments. Because the angry girlfriend had made the request to HIM, the request was tracked; however, HIM handles only a microcosm of requests for PHI.

The request could have been made to a number of other disclosure points within the hospital that do not track requests made for TPO, as it is not yet a requirement of health care providers. If that had been the case, all fingers would have pointed strictly to the hospital and not the doctor's office — leaving the hospital possibly liable and responsible for damages to the patient.

With an enterprise-wide approach to disclosure management and AOD, health care organizations can centrally manage and track the access to and disclosure of PHI throughout the enterprise. This is vital in helping to protect against breach, financial risk, lawsuits, and reputational damage.

increased insurance coverage, and business distraction;
- legal/regulatory, including Office for Civil Rights (OCR) fines and penalties, state fines and penalties, and costs associated with lawsuits;
- operational; and
- clinical.

Health care organizations that responded to surveys to collect data for the report indicated a wide range of costs associated with each incident of improper disclosure, varying from $8,000 to $300,000. Even at the low end of the spectrum, each time PHI is improperly disclosed there is a financial impact to the organization.

Accounting of Disclosures

In addition to the final omnibus rule, health care compliance professionals will need to prepare for expected changes to the AOD rules. Among the proposed changes to AOD requirements are the following:
- changing the time period to maintain AODs from six years to three;
- removing the exception under current HIPAA provisions for disclosures for the purpose of treatment, payment, or health care operations (TPO);
- requiring covered entities to provide individuals with a readable (not merely raw data) "access report" that indicates who accessed the PHI in addition to associated details, such as date, time, type of access, description of the data accessed and, of particular importance, the specific person(s) who accessed it.

Since a traditional access report does not specify for what purpose an individual reviewed the record or what he or she did as an outcome — print, send, or manipulate the information that was disclosed — it is of limited benefit to the health care organization. Moreover, many electronic health records (EHRs) lack AOD functionality since it was not required for certification.

The proposed AOD rule adds to the prudence of managing disclosures across a health care enterprise to ensure that *all* access and disclosures are compliant and properly tracked and reported. Given the magnitude of these changes, many health care organizations are already seeking solutions to keep ahead of the security curve.

A Balancing Act: Stricter Regs and More Exchange

Despite tightened regulations to secure PHI and steeper penalties for breach, federal legislation is simultaneously pushing for patients, providers, and payers to have greater and easier access to medical records through electronic health information exchange (HIE), creating a need for HIM, compliance, and risk management professionals to balance the two contradictory demands.

Escalating Payer Audits

As the number of audits for fraud and overpayment continues to escalate, health care 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 surge of additional audits. The already-increasing volumes of audits are forcing health care 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 Age of Electronic Exchange

Across the health care industry, there is a general migration from paper to electronic documentation and systems. 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 health care organization to control access and manage consents accordingly.

Meaningful Use

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 health care organizations to produce patient information electronically upon request and offer electronic discharge instructions to patients.

Stage 2 rules now mandate that health care providers allow patients to view, download, and transmit their medical information online, typically via patient portals. Stage 2 also requires providers to send summary of care documentation for follow-up providers through secure, directed exchange-based email messaging. Beginning in 2015, providers who are not meaningful users will be assessed a financial penalty in the form of a downward Medicare payment adjustment.

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

Health Information Exchange

Stages 1 and 2 of the meaningful use program have set the stage for electronic exchange of PHI between providers, patients, and payers, which consequently creates new challenges for managing disclosures. Electronic exchange is currently taking place across the health care industry through a number of methods.

The Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) are using a gateway to the Nationwide Health Information Network (NwHIN) 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 health care providers to exchange information via direct email messages, will one day eliminate the need for faxes between providers and reduce the volume of paper that enters and exits their facilities. Additionally, the emergence of HIEs, public and private alike, are creating more disclosure points and requiring health care organizations to control access and manage authorizations accordingly.

Portals are also quickly becoming an important means for exchanging information. 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.

More Disclosure Points, More Challenges

This year, the challenges for hospitals and health systems in managing PHI disclosure across the enterprise while utilizing new technology and complying with regulations will start to grow beyond the capabilities and bandwidth of most organizations.

From the constant stream of new privacy and security regulations and AODs to compliance with meaningful use requirements to the rapid deployment of HIEs, the rate of change in how medical information is

disseminated is reaching epic proportions. These changes will affect core release-of-information processes and require an investment in education and training of various hospital and physician practice staff, inside and outside of HIM, to keep pace and ensure breach prevention and risk mitigation.

It is also important for staff outside of HIM to receive training, as the digitization of medical documentation has made it easier to access and disclose PHI from multiple points throughout a health care organization. We have graduated from the days of solely housing paper copies of patient records in the medical records department. Today, HIM, risk management, billing, lab, radiology, outpatient physical therapy and occupational therapy, hospital-owned clinics and physician practices, and other departments are accessing and/or disclosing PHI through various electronic methods.

In fact, there are as many as 40 disclosure points within an organization where PHI can be disclosed. But because accessing and disclosing health information is not one of the primary responsibilities of the personnel at all of these points, they may not be following the latest guidelines for proper disclosure of PHI. These uncontrolled points of disclosure are where health care organizations are most at risk of improper disclosure and breach.

As a result of added points of disclosure, policy enforcement across an enterprise has become increasingly challenging. More communication between departments and enforcing policies across an enterprise is vital in identifying disclosure points which may be susceptible to PHI leaks.

Additionally, with the movement of hospitals to acquire physician practices come more points of disclosure — and the responsibility and liability on behalf of the acquiring facility to control how those individual office records are disclosed and under what conditions. Organizations will need to manage and maintain an array of policies on devices, technology controls, education, and pre- and post-breach reporting procedures to ensure staff is keeping up with security management and all requirements for proper disclosure and following the same requirements and guidelines of the hospital.

Health care organizations will be hard pressed to develop and implement in-house training and quality improvement programs that keep patient information safe, given the continual roll out of new regulations and guidelines. Additionally, a major area of concern will be the lack of HIPAA compliance training — specific to the disclosure of PHI — outside of HIM. These uncontrolled points of disclosure are where health care organizations are really at risk of improper disclosure and breach; however, it would be an extremely daunting task to train personnel at all points of disclosure.

This makes communicating the concept of enterprise-wide disclosure management to various departments within health care organizations imperative. A collaborative effort between HIM, compliance, and risk management professionals to create centralized disclosure policies and procedures will help prevent improper disclosure and ensure that best practices are in place.

Bridging Gaps with an Enterprise-Wide Solution

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

This approach offers hospitals and health care systems the ability to utilize software and services that can be deployed as a common tracking platform across the health care 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, health care 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.

A Centralized Approach

Previously, the majority of a hospital's disclosures required to have proper accounting were made within the HIM department through requests for medical records or PHI. This department is equipped with years of competence, tools, training, and professional support to manage this effectively.

Today, with the expected AOD requirements, almost every department within the hospital or health system is responsible for disclosures that are in need of proper tracking. As dictated by HITECH, many of these requests must be recorded and accounted for so that a patient can see an audit of which individuals and entities have accessed his or her medical record, and for what reasons. Yet it is highly likely that departments that are focused more directly on patient care would be less capably trained in HIPAA regulations and, therefore, inadequately equipped to handle disclosures according to the most recent stipulations.

A 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, health care organizations can ensure a steady enforcement of enterprise disclosure policies, a manageable workflow, and a consistent experience for patients and requesters.

This approach allows health care organizations to have more confidence in their compliance. Not only does it help protect a patient's privacy, it also assists in protecting the institution against breach, financial risk, lawsuits, and reputational damage. Embedded compliance tools and breach assessment capabilities can 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.

Health care 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 may synchronize with master patient indexes for easier data capture and restriction monitoring.

These systems can be built to automatically capture disclosures (*e.g.*, print routines), provide advanced reporting functionality, and allow a range of disclosure options that include paper; thumb drives; film; CDs; portals for patients, providers, and requesters; esMD delivery and today's more advanced disclosure services such as direct email messaging.

Last Words

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 health care organization.

For hospitals and health care systems, achieving successful disclosure management is all about understanding all the components of the processes involved while realizing that without effective centralized oversight, it is easy to lose step with stringent ARRA and HIPAA disclosure compliance regulations that now affect the organization far beyond the HIM department. It is to the benefit of the en-

tire institution that all resources are considered in building a disclosure management system that will protect both the hospital and its patients.

Reprinted from Journal of Health Care Compliance, Volume 15, Number 4, July-August 2013,
pages 19-26, with permission from CCH and Aspen Publishers, Wolters Kluwer businesses.
For permission to reprint, e-mail permissions@cch.com.