RITA BOWEN / KARI P. SPRADLIN

Enterprise-wide PHI Disclosure Management: What Risk Managers Need to Know

Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB, is Vice President of Privacy, Compliance, and HIM Policy at MRO. In her role as Vice President, Bowen serves as the company's Privacy and Compliance Officer (PCO), overseeing the company's compliance with HIPAA and chairing the organization's Data Protection Steering Committee. She has more than 40 years of experience in Health Information Management.

Kari P. Spradlin is the HIM Manager at Carilion Clinic (*www.carilionclinic.org*). Spradlin oversees HIM operations, in addition to oversight of the Administrative Applications team. Spradlin has worked for Carilion Clinic for more than 20 years in a variety of HIM roles, including Health Record Analyst and HIM Supervisor. She became HIM Manager in 2018. She is a member of the American Health Information Management Association (AHIMA) and the Virginia Health Information Management Association (VHIMA).

Understanding the Risks Associated with Various Types of PHI Mishandling

Managing demands for secure disclosure of protected health information (PHI) has become more complex as each department within a health care organization potentially represents a point of disclosure. Multiple disclosure points place organizations at risk for privacy breach, financial penalties, lawsuits, and reputational harm. To mitigate risk and ensure policy enforcement, many organizations are recognizing the value of enterprise-wide PHI disclosure management.

Multiple Disclosure Points Pose Privacy and Security Risks

Though health information management (HIM) holds primary responsibility for handling compliant PHI disclosures, other areas including radiology, the business office, and physician practices increasingly receive release of information (ROI) requests. The problem is twofold: high risk and high volume. Potential issues related to mishandling of PHI by staff who are not specifically trained to release patient information can result in privacy and security risks for the following reasons:

- PHI disclosure is a core responsibility for HIM staff. For other areas, release of information is not a priority requiring specific expertise and education. Other departments and practices must manage their own responsibilities, which makes return on investment (ROI) a lesser priority.
- Non-HIM departments lack extensive knowledge of rules, regulations, and laws that govern the compliant release of PHI.
- High volumes of patient records may be requested within a short timeline for response, increasing the risk of human error.

- Proper disclosure of PHI requires specialized training and multi-tiered quality assurance.

In radiology, the business office, and physician practices, the core competence is not centered on compliant disclosure of PHI. Unfortunately, business office personnel release numerous medical records to commercial health plans and government payers to expedite payment of claims, appeal denials, or fulfill auditor requests. Health Insurance Portability and Accountability Act (HIPAA) risks are a critical concern when ancillary departments or physician practices release patient information.

Common PHI requests received by radiology, the business office, and physician practices:

Radiology–Reports, digitized images, and films are requested by:
- Other providers for continuing care
- Attorneys to support injury claims
- Patients for specialists and referrals

Business office–High volumes of PHI are sent by billers and collectors, including:
- Unsolicited releases during initial claims submission and claims processing to expedite payment
- Disclosures for government and commercial payer audits and reviews
- Attorney requests for itemized bills

Physician practices–To fulfill their duties, office managers may give information without proper authorizations, including responses to the following:
- Patient requests a copy of their chart following an office visit
- Family requests a copy of chart
- Other providers request information

To assess potential risks, privacy and security officers should recommend that their organizations conduct an enterprise-wide audit of all disclosure points. In our experience, a single audit of a large health system's PHI disclosure compliance identified 39 disclosure points other than HIM. As part of the organization's privacy compliance assessment, an audit of all disclosure points should be performed and updated annually. Based on audit findings, best practice is for ROI experts to provide training on procedures designed to meet specific PHI disclosure management needs of each department.

Risks and Implications of Mishandling PHI

Given the complexities of the current health care regulatory environment, it is critical that risk managers understand the risks and consequences of mishandling PHI. In the pursuit of centralized ROI, Carilion Clinic, a not-for-profit health care organization based in Roanoke, Virginia, identified four areas of risk and steps to avoid mishandling of PHI.

Releasing PHI to an Unauthorized Individual or Entity

Staff must ensure they are accepting proper authorization from the patient or an appropriate patient representative. The privacy rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access, as indicated by 45 CFR 164.514(h).[1] When releasing to a patient representative, validate representation by obtaining appropriate supporting documentation, such as advance directives, living wills, general or medical power of attorney (POA), or legal guardianship.

Accepting an Authorization That Is Not HIPAA Compliant

Organizations should have a HIPAA-compliant release of information authorization

form that has been vetted by their HIM, legal, compliance, and privacy departments. Any requestor using a form other than your organization's release of information authorization form should route that request to HIM to ensure HIPAA compliance.

Releasing More Than the Minimum Necessary

Education is critical to ensuring that staff release or disclose only the information that is necessary—no more, no less—to satisfy the request. In addition, PHI access should be restricted to staff who require access to perform their job.

Failure to Respond to a Request in a Timely Manner

Staff must understand the requirement to provide records or a response within 30 calendar days of a request. Failure to do so is a HIPAA violation. For patient or patient-directed requests, failure to provide records within 30 days can be considered an intentional denial on the part of the organization.

On December 2, 2019, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services announced its second enforcement action and settlement under its HIPAA Right of Access Initiative.[2] For the health care organization at fault, failure to provide timely access to records requested by a third party resulted in corrective actions and a fine of $85,000.

It is important to note that delays can occur when information is provided from the patient's medical record rather than from the designated record set (DSR) that contains the specific information requested. The DSR is defined by the facility and is more inclusive than the medical record.

Any of these examples of mishandling PHI can place individual employees and the organization at risk of a HIPAA violation and financial liability. Such risks point to the importance and value of centralized ROI to ensure accurate and complete disclosure of PHI. Strategies to manage risks include the following:

- Restrict the number of individuals and areas outside of HIM that can release records.
  - If areas outside of HIM must release, limit to releasing directly to the patient for simple requests or to other providers for continuation of care.
  - Ensure all other requests are handled through HIM.
- Create ROI document templates for each request type—such as continuation of care, insurance, and legal—allowing the release of certain documents for specific requests.
- Restrict certain security points based on user role, allowing user access to specific departments and records necessary to perform their job.
- Conduct ongoing training for all individuals who are granted the ability to release information.
- Establish a strong collaborative partnership with your legal, compliance, and privacy departments.

And above all, take measures to establish centralized ROI processes.

Characteristics of Successful PHI Disclosure Management Programs

According to the American Health Information Management Association (AHIMA), successful PHI disclosure management programs share the following three characteristics.[3]

1. ***Successful 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, allowing for standardization and optimization. Staff can be decentralized provided their accountability is to one single entity.

2. ***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.

3. ***A successful program includes monitoring and measurement.***

Technology that embeds these capabilities can simplify efforts and 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 and 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.

Best practice is to maintain standards, governance, and accountability at the enterprise level, guided by HIM expertise, experience, and leadership. Non-HIM staff are rarely trained in PHI disclosure management, which can lead to increased risk of breach. Centralized disclosure through HIM is recommended to protect against breach and related risks. HIM departments should maintain oversight of PHI disclosure management across the enterprise. An enterprise-wide approach promotes privacy, compliance, and accountability based on uniform policies and procedures required for compliant PHI disclosure management.

Endnotes

1. U.S. Department of Health and Human Services. Individuals' Right under HIPAA to Access their Health Information. Available at *www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html*.
2. U.S. Department of Health and Human Services. OCR Settles Second Case in HIPAA Right of Access Initiative. Available at *www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html*.
3. Hardwick, Don; Twiggs, Mariela; Braden, James H. "Optimizing PHI Disclosure Management in the Age of Compliance" *Journal of AHIMA* 86, no.2 (February 2015): 32–37. Available at *library.ahima.org/doc?oid=107557*.

Reprinted from Journal of Health Care Compliance, Volume 23, Number 2, March–April 2021, pages 29–32, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.