COSMOS
Navigate the Compliance Universe

Compliance Today - December 2018
Enterprise-wide PHI disclosure management: Closing the compliance gaps

by Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB

Rita Bowen (rbowen@mrocorp.com) is Vice President, Privacy, Compliance and HIM Policy at MRO Corporation in Norristown, PA.

Privacy and security within a healthcare enterprise are top of mind in an era of regulatory reform and breach. With risks including financial penalties, lawsuits, and reputational damage, healthcare organizations are seeking ways to mitigate risk by implementing new technology and Health Insurance Portability and Accountability Act (HIPAA)-compliant policies and procedures to ensure proper disclosure of protected health information (PHI). Many are embracing the benefits of enterprise-wide PHI disclosure management to close the compliance gaps.

Increased focus on small healthcare breaches

Although the primary focus has been on large cyberattacks, small breaches affecting fewer than 500 patients at a time are actually more frequent. These breaches are often the result of improper disclosure of PHI during the release of information (ROI) process. Since the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009, the Health and Human Services (HHS) Office for Civil Rights (OCR) has received a total of 347,090 reports on breaches of patient data as of March 31, 2018, according to reporting by Health Information Privacy/Security Alert. Roughly 344,823 of those breaches affected fewer than 500 patients each.[1]

With increased frequency and impact on patient privacy, small breaches are getting more attention from the OCR. In 2016, OCR increased investigations of small breaches to identify the root causes, improve efforts to measure HIPAA compliance, and address compliance gaps across the industry. Small breaches can be just as costly as large ones in terms of penalties and reputational damage.

Trends leading to the rising tide of small breaches include a greater demand for PHI among third-party requesters and patients, expanding points of PHI disclosure across health systems, and quality assurance gaps in the ROI process. The risks involved with multiple disclosure points and the lack of standardized processes make PHI disclosure difficult to govern and track, making breaches more likely. An enterprise-wide approach to PHI disclosure management is the recommended solution to the challenges faced by healthcare organizations.

PHI disclosure across the enterprise

Although HIM departments still hold primary responsibility for handling PHI disclosures, other areas, including Radiology, business offices, and physician practices, increasingly receive requests to release patient information. The issues around this trend pose risks that can lead to privacy breaches. Here's why:

- ROI is not a core responsibility of non-HIM staff — and it is not a top priority.
- Other departments lack sufficient knowledge of rules and regulations governing the compliant release of patient information.

- Specialized training and multi-tiered quality assurance are required to properly disclose PHI.

To assess potential risks, the next logical step is to conduct an enterprise-wide audit of all disclosure points. For example, a recent audit of a large health system's PHI disclosure compliance revealed 40 different disclosure points — 39 other than HIM. That is a lot to handle for HIM and compliance leaders concerned about mitigating risk.

Risk due to multiple disclosure points

In Radiology, business offices, and physician practices, the core competence is not centered on proper disclosure of PHI. For example, business office personnel release millions of medical records annually to commercial health plans and government payers to expedite payment of claims, appeal denials, or fulfill auditor requests. This is not their area of expertise — they should be focused on reimbursement. Their core competence is to maintain cash flow for the business office, working with payers to collect bills. ROI is not a primary objective. HIPAA risks are a concern when ancillary departments or practices release PHI versus having HIM professionals manage that task. In each department or practice, it is critical that staff know when an authorization is required and how to handle compliant PHI disclosure.

Here are common PHI requests received by the three areas:

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 offices – 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 – In an attempt to fulfill their responsibilities, office managers sometimes give information without proper authorizations in situations such as when:

- Patient requests a copy of their chart following an office visit
- Family requests a copy of chart
- Other providers request information

Other disclosure points do occur, such as in the Emergency department, but the greatest liability — and where quality assurance methods help the most — is in physician practices. Overall, their record-keeping methods are less accurate than those of larger organizations.

The two most common concerns in physician practices are comingled records and misfiled documents. Comingled records occur when patient information is placed in another patient's chart or electronic file (i.e., mixed patient records within a single chart). Misfiled documents are another frequent issue in physician practice settings. Practice staff need specific training to prevent comingled records, avoid misfiles, ensure access to the

right records, and release of the right information to the right requester.

Due to inadequate staffing and training to support HIM practices, centralizing ROI would result in significant benefits, including meeting regulatory compliance and managing the increased ROI request volume. HIM and other disclosing parties can then focus on their core competencies to help the healthcare organization avoid breach and deliver higher quality care.