Breach Risk in Release of Information
Don’t Leave Risk to Chance

Key trends impacting healthcare providers
INTRODUCTION

Privacy and security within a healthcare enterprise are topics often on the minds of many stakeholders. As of February 2016, the U.S. Department of Health and Human Services (HHS) reported that over 250 million patients have been impacted by breach since 2009. Approximately 1400 large breaches have been reported to the Office of Civil Rights (OCR), and during this same time over 180,000 small breaches impacting fewer than 500 patients at a time have been reported as well. While small breaches can be one-off incidents resulting from sending the wrong patient’s records to the wrong person, they can be equally detrimental to a healthcare organization.

Key trending factors related to the rising tide of small breaches include:

- Expanding points of Protected Health Information (PHI) disclosure and requests for health information
- Increasingly complex regulations for sharing health information
- Quality assurance gaps in the Release of Information (ROI) process
- Steepening penalties and financial impact to provider organizations

Don’t leave risk to chance. In this eBook, you’ll learn more about mitigating risk with a strategic, enterprise-wide approach to PHI disclosure management.
SMALL IS BIG, AND COSTLY

Although small breaches affecting less than 500 patients per incident are not usually broadcasted as widely as a large cyberattack, the financial impact is real.

- **Each breach can cost $8,000 to $300,000,** not including HIPAA violation civil penalties.
- **Penalties are rising to as much as $50,000** per breach with a maximum of $1.5 million annually for repeated occurrences.
- **As many as 10 states** now consider HIPAA to be the “relevant standard of care for state privacy violation claims brought by individuals.”

Patients may sue your organizations.
BAD NEWS TRAVELS FAST

While cyberattacks or device thefts make for sensational headlines, breaches due to employee or organizational errors are also reported in the news.

• One news outlet reported that a 2014 clerical error at St. Vincent Breast Center in Indianapolis resulted in 63,325 patients receiving a mailing containing incorrect information, including the names, addresses and appointment times of other patients.6

• In 2013, Oakland, Calif.-based West Coast Children’s Clinic notified patients of a PHI breach after it faxed just one patient’s information to an incorrect fax number.7 As the clinic explained to news outlets in a written statement and to patients in a letter, a number of PHI disclosure protocol steps were not followed, including checking the fax number and notifying the recipient that the fax was sent.

According to Deloitte’s 2014 global survey on reputational risk, a “negative reputation event,” such as a data breach, can cause a “loss of brand value” for healthcare providers.8 Word of a breach can also spread online through social media platforms, such as Facebook and Twitter, through consumer rating sites, such as Yelp, and even through Google results when someone searches for the hospital.
RISKY BUSINESS

- As large health systems acquire more hospitals and physician practices, PHI disclosure policies, procedures and technology may vary greatly between facilities—and add to risk levels.
- Another factor driving breach risk—disclosing PHI electronically, or ePHI—has emerged as more organizations recognize electronic disclosure’s efficiencies over paper.
- Electronic Medical Records (EMR) systems allow more people to access PHI from within a healthcare enterprise, including those who are not specially trained in the ROI function.

When onboarding one Pennsylvania-based health system, MRO discovered **40 points of disclosure** in the system—not including physician practices. Most of the disclosure points were managed outside of the Health Information Management (HIM) department by individuals who were not specially trained in ROI and PHI disclosure compliance.

**Talk about risky.**
Criminal attacks and lost or stolen devices were the root cause of most PHI data breaches last year, but almost as many—40 percent—were due to “unintentional employee action,” according to 2015 survey results from the Ponemon Institute.\(^9\)

Unintentional employee actions include more than using the wrong fax number or mailing address when disclosing PHI. \textbf{There are multiple points in the ROI process where a misstep can result in breach.}
• With typical ROI workflows, 20 to 30 percent of all submitted authorizations are initially found to be invalid.\textsuperscript{10}

• However, with over 100 possible combinations of errors or omission points across a wide variety of request types, as much as 10 percent are processed with errors if the only line of defense is the person onsite logging the request.

• Five percent or more of patient data in EMRs have integrity issues, including comingling of patient records.

• Well-trained ROI specialists will catch the majority of mixed records; however, with just one level of quality control, 0.7 percent will contain mixed patient data.

PHI breaches are not isolated incidents. Ninety-one percent of healthcare organizations surveyed by Ponemon reported a PHI breach in the last year, while 40 percent reported more than five. Also of concern is that 69 percent of organizations did not discover the breach until an audit; therefore, the improper disclosure may have occurred weeks or months earlier.
In the typical ROI workflow, requests for health information come into a facility and are logged by onsite ROI staff that also handle many other responsibilities. **There is no second set of eyes for Quality Assurance.**

This approach results in inefficiencies, distractions and increased errors.
DON’T LEAVE RISK TO CHANCE

At MRO, we focus on two things: service and quality. With MRO’s industry-leading Quality Assurance program, our clients can have full confidence they are HIPAA compliant. Not one, but two teams check each ROI authorization for accuracy, and then a combination of our optical character recognition (OCR) validation technology and human intervention check for comingled records. An additional quality check is done through a barcoding system to maintain shipping integrity.

This all results in a 99.99% accuracy rate.

Watch this video to see how.

MRO’s technology and people can manage PHI disclosure across multiple departments and locations to standardize policies and procedures and safeguard your organization against the risk of breach.
THE MRO DIFFERENCE

MRO, headquartered in Valley Forge, PA, was founded in 2002 on the premise that a better ROI service could be created with better workflow, improved quality assurance, and use of innovative technology.

Because of our focus on service and quality, we have been recognized by KLAS as the leader in ROI services multiple times.


10 MRO research based on client data.
Don’t leave risk to chance. Cover your assets with MRO.

Want to learn even more?
Read our white paper on mitigating breach risk.