RICOH
imagine. change.

Safeguard Your Hospital

Six Proactive Best Practices to Improve Healthcare Data Security

April 2015

A Piece of Paper Can’t Cause that Much Harm. Or Can It?

Imagine a piece of paper arriving at ABC Hospital’s 5th floor nursing station from a lab. A nurse takes it to a multi-function printer (MFP) to scan it electronically into the patient’s health information management record (HIM), but fails to properly secure the original paper document, leaving it in the tray. Minutes later, another employee arrives to use the MFP and sees the paper, noticing that it includes the patient’s Social Security number. He takes the paper into his colleague’s office, and getting sidetracked, accidentally leaves it on the desk. The next morning, he goes back to retrieve the paper, but unfortunately it’s nowhere to be found.

The hospital has just experienced what might be considered a “minimal” data breach that could wreak havoc for not only the patient but also the hospital and the device vendor, potentially for years to come.

Recent news reports have focused on the growing number of data breaches within companies that are household names — like Sony, Target, JPMorgan Chase, U.S. Postal Service, Blue Cross and Blue Shield of Tennessee, Community Health Systems (CHS) and a large-scale attack on Anthem, the country’s second largest health insurer. As the amount of data increases, small organizations are bearing just as much risk as large healthcare organizations.

Anthem’s data breach alone impacted as many as 80 million customers, with data thieves gaining access to names, birth dates, Social Security numbers, ID numbers, home and email addresses and employment information including income data.[3] Before the Anthem breach, experts predicted the cost of healthcare breaches could be as extensive as $5.6 billion annually.[4] Now, reports indicate the Anthem breach alone may cost from $8 to $16 billion.[5]

Healthcare is Not Immune

Data security presents challenges in every industry, but especially in healthcare.

- 42.5 percent of data breaches were in healthcare in 2014 – more than any other industry segment and continuing a three-year trend.[1]
- Over 50 breaches of protected health information (PHI) affecting 500 or more individuals occurred from July 2014 through January 2015[2], including hacking, theft, unauthorized disclosure, improper disposal and loss.

Interconnected data systems (such as EHRs) and mobile information products (such as wearable technology), coupled with greater Wi-Fi access and increasing cloud storage, make healthcare especially vulnerable to data breaches. Third-party vendor access to PHI only increases healthcare’s susceptibility. In fact, a majority of healthcare organizations are only somewhat confident (32 percent) or not confident (40 percent) in the privacy and security of patient data shared on health information exchanges (HIEs).[6] Cyber criminals could be seeing healthcare’s aging computer systems and lax data security plans and features as easy targets for hacking.

[1] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

[3] https://www.anthemfacts.com/

[4] Fourth Annual Benchmark Study on Patient Privacy & Data Security,” Ponemon Institute, March 2014

[5] http://www.bizjournals.com/stlouis/blog/health-care/2015/02/anthem-data-breach-could-cost-company-billions.html?page=all

[6] Fourth Annual Benchmark Study on Patient Privacy & Data Security,” Ponemon Institute, March 2014

Compounding Risks

Several factors make securing health information difficult: Multiple data touch points, a complex data string, consumer-generated data, efforts to capture paper data electronically and lack of resources to safeguard PHI — to name a few. In addition, data privacy and security needs compete against organizational priorities such as EHR adoption, meaningful use (MU), declining reimbursement and bundled payments, accountable care, quality ratings, patient satisfaction and more. Ironically, these priorities create more and more data.

Although technology systems may be perceived as the main security concern, people-based breaches represented 80 percent of all breaches in 2014.[7]

The rising number of data touch points in healthcare can bring even more opportunities for breaches by the end user, such as these examples:

- A stolen cell phone or laptop with patients' personal data
- Hackers targeting cloud-based data to access patient billing records
- An open file on a computer screen
- A piece of paper left in a printer
- A chart visible at the patient check-in counter
- Staff discussing a patient case on the phone in a public area

As the value of stolen PHI increases, healthcare organizations and patients are becoming more concerned about the security of their personal data. Recent reports indicate more criminal activity to obtain PHI for fraudulent purposes than credit card theft and fraud. By some estimates, an individual's medical information is worth 10 times more than his or her credit card number on the black market.[8] Bear in mind that credit cards can be quickly cancelled by banks when fraud is detected, which limits the window of opportunity for fraudulent use. On the other hand, if medical identity theft is not immediately identified by the patient or provider, criminals could have more time to use the stolen credentials without detection.

According to Reuters, last year the FBI warned healthcare organizations to improve their data security and breach preparedness plans — or else face possible penalties from federal regulators.[9] That warning, combined with the massive Anthem breach, reinforces the need for data privacy and security to be top of mind within all healthcare organizations and at all levels, from the C-suite to front-line staff.

[7] Experian 2015 Data Breach Industry Forecast

[8] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[9] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Six Best Practices for Improved Privacy and Security

HIPAA compliance requires data security as personal information moves throughout and beyond each healthcare organization.[10] Yet as more data is captured it can have more uses and be shared more freely, which in turn can increase opportunities to compromise privacy and security.

By taking a close look at your current information flow, you can close gaps where data might be getting lost or mistranslated, leading to breaches. The goal is to efficiently move information in a secured way among clinical and administrative workers regardless of whether it's paper-based or digital. When you seamlessly capture, access and share data so that it's as mobile as your people are, you'll be on your way to achieving information mobility. Ask yourself these questions about your organization's specific needs:

- Where are gaps within my information flow that could be leading to privacy issues?
- Do I have a strong and secure technology infrastructure?
- Is my organization's current technology and environment set up to support the work styles of my staff while still keeping information secure?

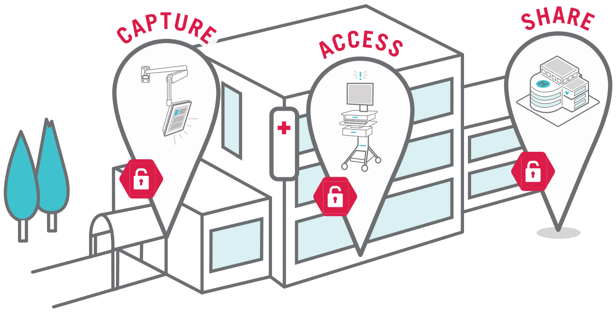
Asking these questions helps to pinpoint areas of opportunity within your current workflow where clinical and nonclinical improvements can be made to build stronger privacy and security controls. Check out these tips to help healthcare organizations improve privacy and security measures that can, in turn, reduce risk of breach:

1. Understand all data access points.

While starting at the source is important, organizations also should take a close look at vendors and clearinghouses that receive and send patient data to be sure the information is secure on both ends. For example, before partnering with a vendor or clearinghouse, ask questions to find out how they secure information that is being passed back and forth. If an organization has not looked at closing the gaps within their information management system to make sure it is secure when it leaves their hospital or within their information management system to make sure it is secure when it leaves their hospital or practice, it probably is not secure on the portal or other destination.It's also important to understand what is classified as a workstation and monitor access, keeping in mind that every workstation should be secure. For example, take a look at who is accessing MFPs as well as patient portals to help assure that information is in the right hands at all times.

IS YOUR **DATA SECURE?**

Healthcare data is more abundant than ever before, and uses for that information—from population health management, to identifying workflow inefficiencies—are endless.



INCREASED DATA MEANS INCREASED RISK

With unprecedented volumes of data may come increased risks to the privacy and security of information. So what do you have to do in order to keep your data from getting into the wrong hands no matter how you capture, access or share it?

KEY

CAPTURE

When you initially capture data, it often starts as unstructured data, such as loose paper, which can jeopardize the security of information if mishandled by staff or if devices are not designed to handle personal health information. Making sure data is **accurately digitized and stored** according to your security standards may help combat these risks.

ACCESS

Unprotected work stations, staff discussing a patient within earshot of others and other data access points can cause risks that compromise information without most organizations even noticing. Properly training your team in **HIPAA compliance** can reduce some of these issues.

SHARE

When data is shared, risks increase exponentially, as other organizations or referring networks may not have the same strict policies in place. Adhering to **HL7 exchange requirements** can help safeguard your information.

✓ **Protect your data—protect your patients, employees and your bottom line.**

[10] http://www.hhs.gov/ocr/privacy/

Six Best Practices for Improved Privacy and Security

Some technology has built-in safeguards to protect against unauthorized users accessing technologies. These can include badge scanning, thumbprint recognition or other user authentication, which can help detect breaches. For example, let's say a clinician scans a medication history form and fails to log out of the MFP. Another staff member sees the open screen when they attempt to use the device, which leaves the patient's personal information vulnerable. This may not seem like a big deal, but if that information gets into the wrong hands, you may have a crisis. By reviewing the control safeguards, your hospital can be better positioned to determine who is responsible for the breach and how to prevent future issues.

2. Install and implement security tools and support them with policies and procedures.

Certified health information systems and EHRs can provide a foundation for privacy and security adherence. However, addressing security goes beyond simply having the technology installed. For example, if a system is put in place but never fully implemented, you may be running in circles and contradicting all of the hard work you've done to secure your information. Instead, once implemented, organizations should support security tools with clear and actionable policies and procedures. After all, you don't want a failure to do so to surface during an audit.

For example, an auditor might ask someone in the HIM department for a chart to test a policy that states only clinicians are allowed to give out charts. The auditor might also observe an open computer screen at a nursing station to certify it adheres to another policy that calls for screens to time-out after 15 seconds. Making sure your technologies and staff are updated on the latest policies and procedures can help you avoid security issues.

3. Track and enforce patients' HIPAA preferences.

Whoever manages an organization's patient portal should clearly understand the importance of adhering to patient preferences for PHI and financial information. Keeping a log of responsibility based on patients' HIPAA preferences can help you not only improve patient experience, but also can help you to adhere to rules and regulations.

For instance, patient portals should be password protected regardless of whether patients have specifically requested their PHI to be restricted or if they have requested that access be granted to family members or other individuals. It is also important to balance ease-of-use by patients with security measures, such as verifying identity and authentication processes to create the highest level of security.

Risk Assessment Checklist

Consider including the following assessment check points to help get you started on the right path:

- ✓ Track anyone who uses the organization's devices and data, as part of the HIPAA-required audit trail.
- ✓ Implement decryption and encryption to control and protect how documents, images, messages and other PHI are captured, accessed and shared.
- ✓ Conduct a test run on data security by applying scenarios for both the network and cloud services and storage.
- ✓ Hire a professional to test the network and the cloud and to identify gaps.
- ✓ Address potential weaknesses and gaps to proactively help prevent adverse security events.
- ✓ Include mobile devices in your risk assessment to make sure they are used in conjunction with privacy and security requirements. (One common misconception is that private phones are secure. However, data is often not secure on the received end.)
- ✓ Document and test breach notification policies.

Taking the time to complete a risk assessment can lead to a strong data management strategy for protecting your information to save time, money and assure your patients that you take their privacy and security concerns seriously.

Six Best Practices for Improved Privacy and Security

4. Perform regular risk assessments to reveal where PHI could be at risk.

An annual risk assessment can uncover gaps within your information flow to help save your organization time and money. Assign an individual within your hospital who can assess audit readiness and be an accountable leader to manage the organization's privacy and security strategy.

Whether an assessment is done internally or with an external vendor, having a thorough understanding of the physical, technical and administrative safeguards outlined by HIPAA can help you avoid mistakes and harmful breaches.

5. Consider security and audit support in business associate (BA) contracts.

Although providers are ultimately accountable for privacy and security, the Omnibus Rule extends liability to business partners who now share the risk if and when PHI is compromised.[11] As a result, vendors understanding HIPAA requirements and enforcement processes — along with audit components — can help to meet full compliance for all data management technology, from patient record and test result scanners to cloud storage of clinical and operational data.

Taking appropriate actions to address vulnerabilities and threats that expose organizations to risk can help protect valuable information. For example, when selecting a vendor, you can help avoid risk by selecting a vendor that understands the threats and risks present within the forms that can adversely affect the provider. If you notice that a potential vendor appears to simply "check the box" on standard forms rather than demonstrating a proficient understanding of what is being signed, it may put you at added risk for a security breach.

10 Sample Questions to Answer for Improved Healthcare Data Security

1. Are there gaps within your information flow where the security of data could be jeopardized?
2. Is your staff equipped with the technology and tools they need to successfully and securely share PHI?
3. Have you secured information with encryption?
4. Is your information secured and safely managed throughout your hospital?
5. Do you know how often private information within your hospital is left unsupervised?
6. Do you use security features to capture, access and share information both internally and externally?
7. Can you prove HIPAA compliance?
8. Are all of your staff members trained on and aware of the latest compliance regulations?
9. Does your technology help to bridge the gap between paper and digital, mobile and desktop, structured and unstructured data?
10. Are you able to support the unique work styles of your employees and still keep information secured?

[11] http://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem

Leave No Touch Point Unturned

6. **Educate every end user.**
HIPAA requires training on policies and procedures related to the privacy and security of PHI. Training should cross all levels of the organization as necessary and appropriate for the function – from custodian to provider to C-suite, for example – and be documented and updated. It is helpful to include real-life audit examples, such as a staff member not asking a caller for the patient's designated HIPAA password; a nurse and physician discussing a patient's treatment in a public hallway; a document with PHI left open on a nursing station desktop; or a visible patient file at check-in.

Think back for a moment to the breach scenario at ABC Hospital. If a strong foundation of privacy and security measures had been in place to protect PHI, the breach likely would not have occurred.

New digital applications and devices mean greater accessibility to — and sharing of — PHI both internally and externally. While increased access to data and analytics can pave the way to better clinical care and population health management, it can also lead to potential increases in hacking, theft and other security compromises.

As a result, the privacy and security of health information should be top of mind for healthcare leaders. Strategies and tools to help you achieve information mobility must be in place to help you capture, access and share secured clinical and operational information at every step as it moves throughout and beyond your healthcare organization.

> *" While increased access to data and analytics can pave the way to better clinical care and population health management, it can also lead to potential increases in hacking, theft and other security compromises."*

For more information,
visit ricoh-usa.com/healthcare

RICOH
imagine. change.