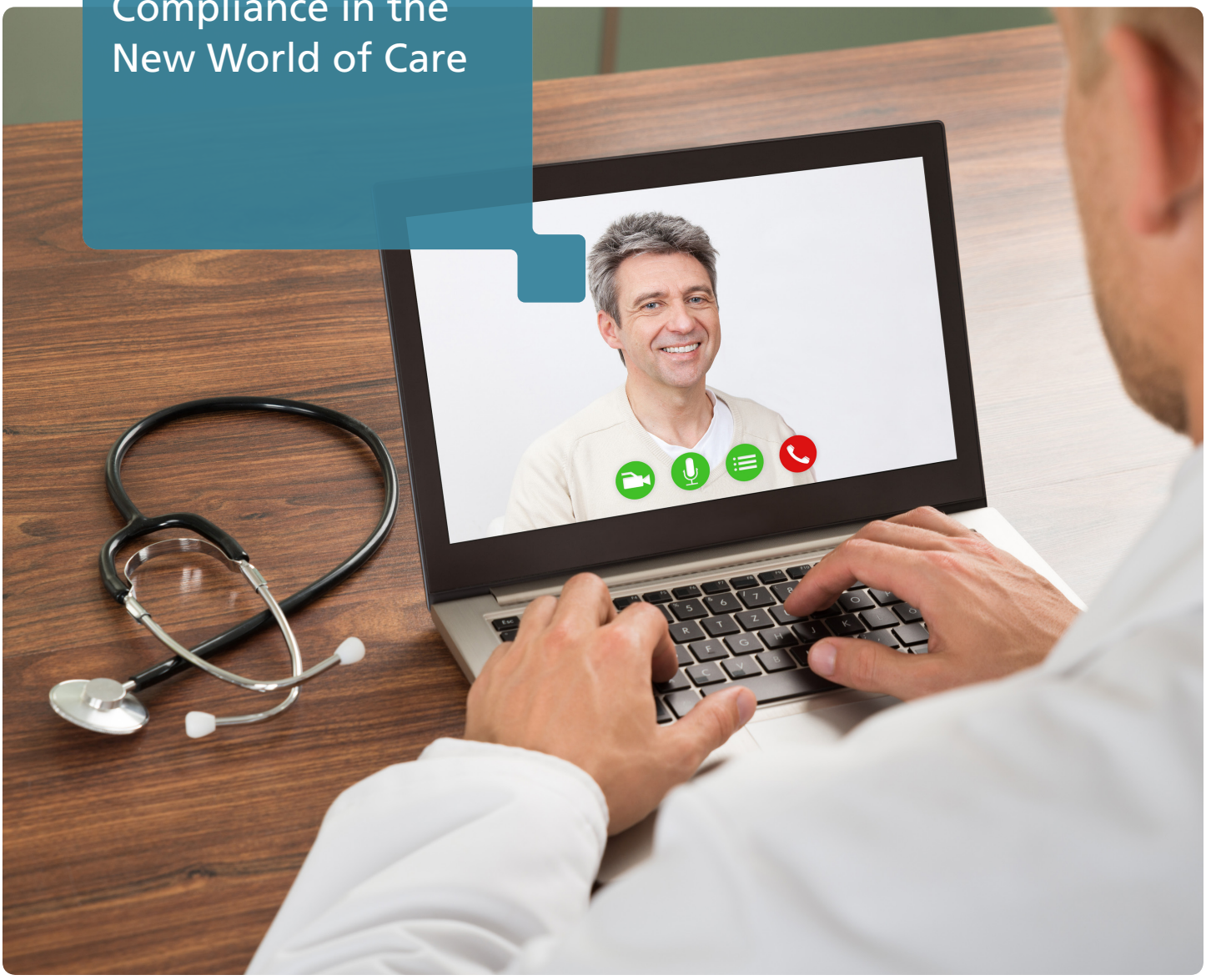
RICOH
imagine. change.

5 Strategies to Navigate Healthcare Security and Compliance in the New World of Care



January 2017

Think about all of the information that travels throughout the care continuum each day. Now consider how that information exchange will change in the new world of care as interoperability comes to life and the way healthcare leaders communicate with patients evolves. These transitions are not only accompanied by new security and compliance challenges, but they are also filled with the possibility for greater connectivity and more efficient care. Healthcare leaders are often concerned, even intimidated by new security and compliance challenges, yet there are benefits to greater connectivity and more efficient care including improved patient outcomes and more secure data.

DID YOU KNOW?

60% | **60% of patients at breached healthcare organizations will think about moving to a different provider and 30% actually do.[1]**

Consider a proactive risk assessment to reduce breaches and maintain customers.

[1] https://blog.returnpath.com/10-scary-healthcare-security-stats-2/

For the first time, healthcare leaders now have information and insights available that can help them ease into this transition and identify areas of opportunity. For example, analytics and measuring tools can help highlight where data is getting lost, areas of inefficiencies and areas of high security risk. During a time when security breaches are common in healthcare, this information can help healthcare leaders make more informed decisions that have the potential to guide smart improvements.

Healthcare is beginning to see the positive impacts of this kind of proactive approach to understanding and securing data. In the first 10 months of 2016, healthcare breaches were up only slightly from the previous year with 258 data breaches impacting 500 or more people versus 232 breaches in the same period in 2015.[1] While healthcare leaders are finding new ways to approach security and compliance within their organizations, the potential for data breaches can be found in daily processes.

Ordinary daily processes may be ripe for small changes that bring big improvements to data security. For instance, consider how often a caregiver may print a document, only to go to a printer and find the printed content is missing. In an effort to deliver appropriate and timely care, the staff member reprints the information and collects it from the printer, with little or no idea where the first paper copy went.

This common scenario of a provider or nurse doing his or her job to the best of their ability sheds light on the myriad of healthcare data security challenges, such as pool printing left in a multi-function printer (MFP) tray. Situations like this point to new opportunities to develop strategies that safely and securely connect data, while also adapting to new security and compliance regulations.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Healthcare is changing, requiring agility

The new world of care is filled with rapid changes, from care delivery to data exchange between providers and patients through a variety of electronic devices, digital platforms and mobile applications. Healthcare organizations are working with much more volume and types of data than ever before, while also trying to meet the demand for connected communication among providers and patients.

DID YOU KNOW?

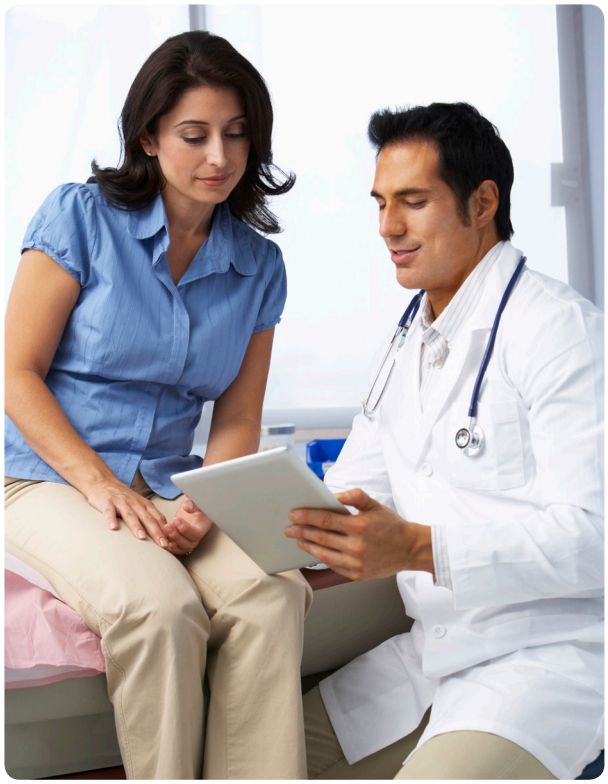
$6B | **Cyber attacks cost the U.S. healthcare system $6 billion every year.**[1]

Reduce costs by reporting and analyzing data to detect risk.

[1]https://blog.returnpath.com/10-scary-healthcare-security-stats-2/

Regardless of the type of data, there is always a need for layers of security across the care continuum as data is captured, stored, accessed or exchanged. Those layers can bring challenges and potential risks like ransomware and black market sales of valuable health information. At the same time, the comprehensive data also presents opportunities such as utilizing all data available from disparate sources from across the healthcare organization for complete visibility into the comprehensive medical record, which in turn can improve patient care.

Healthcare providers that prioritize data security while continuously making decisions about devices to capture, manage and transform content electronically will likely benefit by preemptively addressing the possibility of a breach. One example is digitally transforming content on the front end rather than moving paper through the enterprise and then deciding how to manage it only on the back end. Capturing data at the beginning and moving it more efficiently and securely through the necessary processes associated with those documents can help the organization improve both information flow and compliance.



5 strategies to navigate the new world of care

On one hand, healthcare organizations are being asked to share data across the enterprise; yet, on the other hand, they are expected to keep data secure and meet compliance rules and regulations. This requires healthcare leaders to not only look toward new technology, but also consider how systems, devices and processes are carefully planned, interconnected and implemented to achieve maximum data protection.

Healthcare organizations should consider these 5 strategies to help navigate this new and evolving world of healthcare data security and compliance while meeting the consumer's demand for connected health.

1. Identify your goals.

It's important to determine security goals that support the organization's overarching objectives. For example, the high-level goal may be to institute an interoperable data exchange while the supporting security objective is to develop and implement a system that securely captures structured and unstructured data across the enterprise.

Once potential goals are identified, it's critical to gain internal buy-in across the enterprise before looking at customized approaches in specific departments. This can help organizations achieve exactly what they need to enhance data protection.

When the goals are agreed upon, involve security and compliance teams at the onset to avoid re-scoping the project that supports the goal. For instance, at the beginning stages, educate decision makers about challenges presented by situations like pool printing, unlocked stations, lack of access tracking and lost paper documents.

DID YOU KNOW?

100M | **More than 100 million healthcare records were compromised in 2015.[1]**

Protect valuable data and improve compliance through closing information gaps.

[1]http://www.bostonglobe.com/business/2016/08/07/hackers-turn-health-care-where-records-fetch-bigger-bucks/OSi8imOSGPstwV6DyYhoJ/story.html?s_campaign=tw&utm_content=buffer8b32d&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

2. Understand the current state.

After identifying your goals, an information risk assessment is the next step in the progression toward securing data initially, while also helping to protect information through the entire data life cycle. The information risk assessment consists of delineating not only how information is being captured, stored and shared, but also what documents are currently being generated and what permissions are enabled to help identify the key strengths in converting paper to electronic documents.

Consider how information is captured securely and remains protected when it is at rest, in the conversion state or while in use. Include parameters on how documents should be handed off to a secure location and what that transition point looks like. By assessing your organization's landscape, you will be more informed on areas of opportunity in improving your data security strategy.

5 strategies to navigate the new world of care

3. Build a print strategy and follow it.

Rather than simply knowing what was printed where and when, develop a more in-depth view of how you want to scan and move a document from point A to point B. Analyze what application is processing the job, how technology is leveraged and where there are opportunities to utilize one secure server to save time and money.

Look for opportunities to efficiently and securely distribute data by enabling applications to talk to each other. Leverage technology to intercept a traditional print job and electronically distribute it to another application.

For instance, plain paper prescription prints or test results can be electronically generated instead of printed, such as an EKG report that can be captured from the print stream and digitally sent to another department. Instead of the paper report sitting on a device until someone picks it up, it can be delivered securely to where it needs to be with an HL7 message or via a secure FTP site.

4. Install and implement.

Even with cutting-edge technology, a security breach can occur if staff is unable to use the system consistently and effectively. Help mitigate this challenge by developing a post-installation plan that drives adoption by every stakeholder.

Keep in mind that users who have a voice in how the solution is built are more prone to use it, which can help resolve security issues and potential liability situations down the road. Customizing implementation for each department based on their specific needs and where they've seen breaches occur in the past – or have the potential to take place in the future – can help achieve this goal.

Despite the growing attention toward data security, compliance and advances in technology, inconsistent use is often the most challenging hurdle for any organization that has implemented a digital content management solution. To help overcome this challenge, develop policies and training as part of the implementation program to promote consistent messaging about what people are supposed to do with data and how to use enhancement tools to capture, transform and manage data. Instituting a system of checks and balances to monitor the system also can help support consistent use.

DID YOU KNOW?

33% The loss or theft of unencrypted portable devices have made up over a third of all large healthcare breach incidents to date.[1]

Protect your healthcare systems through encryption.

[1] http://www.healthcareitnews.com/news/5-ways-avoid-health-data-breaches

5 strategies to navigate the new world of care

5. Review the full data life cycle.

Consider what needs to happen beyond capturing data, such as the following:

- How the information can be leveraged,
- Policies and principles around data access and use; and
- Data retention and security standards, whether in use, in motion or at rest.

Proactively address the challenges of data capture, storage, access and management at every point in the cycle. For instance, look for opportunities to do a pre-authorization of who is allowed to use what data. Define how the data locks down if an unauthorized person attempts to access it. One scenario of a proactive measure to protect security and maintain compliance is an alert or an automatic shut down if an unauthorized person tries to access information.

Review and include access from multiple sources such as mobile devices, desktop computers, printers or views in a shared folder when assessing digital rights management across the enterprise.

This might include a data security override for optional items like a locked print tray. Implement consistent "device hardening" at workstations with a required user name and password for secure access by all providers while preventing the ability for anyone to have walk-up capabilities to fax, scan or remove a print job from the device.

Plan ahead for future success

By focusing on how data is managed and protected, healthcare leaders could play a large role in how their organization adapts to the new world of care. Healthcare leaders have more tools and ideas available to their disposal than ever before, but simply implementing these solutions alone will likely not be enough.

Those who can see the big picture and help others within their organization navigate security and compliance changes through long-term strategic planning and intuitive solutions will likely experience lower costs, increased efficiency and reduced risk. While this may require healthcare leaders to invest more time up front, it is certain to pay for itself in the new world of care.

RICOH
imagine. change.

www.ricoh-usa.com/healthcare