CANON SOLUTIONS AMERICA

CANON SEE IMPOSSIBLE

DOCUMENT MANAGEMENT: BEST PRACTICES FOR HEALTHCARE ORGANIZATIONS

Overview

On a daily basis, healthcare organizations receive and process thousands of documents containing valuable personal health information (PHI), personally identifiable information (PII) and medical intellectual property. Health leaders know that it is their moral, legal, and ethical responsibility to protect this data and uphold the trust that patients put in their hands. A well constructed cybersecurity policy should safeguard delivery of care, patient data, and administrative operations across the healthcare ecosystem.

Greater government oversight and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the EU's General Data Protection Regulation (GDPR) impose increasingly complex information governance (IG) requirements that are difficult to achieve in a document-intensive environment. What's more, healthcare organizations are increasingly susceptible to accidental and malicious user-related breaches as well as external cybersecurity breaches.

In a recent KPMG survey, **55%** of organizations revealed that they have experienced email phishing techniques with malicious links or attachments.[1]

Unauthorized disclosure of protected health information (PHI) is an all-too-common violation of the HIPAA Privacy Rule and can trigger significant financial penalties. Clinical data in transit such as physician notes, prescriptions, imaging results, or insurance and payment information is vulnerable at multiple points—both inside and outside of an organization's protected network. Whether documents are being shared among multiple providers, accessed via patient portals, or printed and left on a printer tray, healthcare organizations must ensure both digital and hard-copy versions are protected throughout the continuum of care.

Secure the Network

Chief Information Security Officers (CISOs) at hospitals and healthcare systems know that network perimeter security is the foundation of any data security effort—and that the healthcare industry is an especially appealing target for cyberattacks:

- Healthcare data breach costs
- Stealing healthcare information is highly lucrative
- Top concerns for healthcare organizations

In a Ponemon Institute survey, the average cost of a data breach in healthcare is $6.45M.[2] Cybersecurity consultants can help healthcare organizations evaluate their ability to mitigate a data breach. Steps include:

- Vulnerability assessment
- Penetration testing
- Education and training

Secure Your Devices

Networked printers, multifunction devices (MFDs), and other office equipment can be low-hanging fruit for cybercriminals attempting to breach a company's perimeter. In fact, the average cost per record in healthcare is $429.[2] The average size of a U.S. data breach in health care included 26,523 records.[2]

Ways to harden devices include:

- Protocol security (SSL/TLS and HTTPS)
- Hardware security (HDD data encryption, etc.)
- Device-level data security (IPSec support, etc.)
- Authentication
- Administrator control

Secure the Print Workflow

Paper-based information is an often-overlooked vulnerability in any organization, and it's especially important for hospitals and health systems handling PHI and personally identifiable information (PII). There are numerous points along the continuum of care that can expose sensitive information. By limiting access to both digital and physical documents only to those who are authorized, sensitive data can be locked down from scan to print.

Print infrastructure rates 2nd with a score of **66%** of the top 5 IT risks that may lead to security breaches.[3]

Solutions include:

- Access control via authentication and authorization
- Pull printing to prevent exposure of sensitive documents in the printer tray
- Secure watermarking to prevent unauthorized copying
- Keyword intercept to further limit output and distribution

Secure Your Documents

Sensitive PII and PHI data often resides in documents such as intake forms, demographic data, clinical records, insurance and personal identification cards, and clinical records. A robust document management system (DMS) is an excellent foundation for securing documents at rest, but DMS is only the beginning. Documents must also be secured outside the DMS, particularly as information flows into and out of the system.

For healthcare providers, the move towards interoperability poses special challenges. Sharing sensitive clinical data among a patient's healthcare providers is an essential part of providing comprehensive care but this information can be invaluable to hackers. Exposure can mean heavy fines, expensive litigation, and a loss of faith in your organization's ability to maintain privacy and confidentiality. Vulnerability points include:

- Scanning
- Digitization
- Approval Routing

These documents must be available to those who need them yet also protected from unauthorized manipulation. Best-in-class optical character recognition (OCR) software can intelligently capture and extract data from documents, and pass this data along to an information management system. From there, documents can securely flow to the appropriate systems or personnel, expediting decision making and saving time and expense on data entry.

Secure Your Information

Mobile devices such as laptops, smartphones, and tablets play an increasingly vital role in the healthcare industry. However, the portability of many of those devices means they can easily be misplaced, lost, or stolen.

Frequent use of mobile devices by patients and providers means that sensitive data often lives on beyond the organization's security perimeter. That fact does not relieve hospitals, physician offices, and integrated delivery networks of their regulatory responsibilities. In fact, failure to use encryption or an equivalent measure to safeguard PHI on portable devices is a common HIPAA violation.

A powerful solution to the mobile dilemma is enterprise digital rights management (EDRM). EDRM gives your organization the ability to encrypt, track, and help control how content is accessed or shared, and it allows

of breaches were malicious attacks.[2]

document owners to grant or revoke access anytime and anywhere. Because EDRM protection is embedded within the document itself, it allows authorized users—and authorized users only—to access documents safely wherever they exist.

EDRM can help your organization comply with privacy regulations such as HIPAA and GDPR with audit trail and chain of custody across all applications, devices, and platforms. Such auditing capabilities are critical since failure to perform an organization-wide risk analysis is arguably the most common HIPAA violation, and one that frequently results in financial settlements with the U.S. Department of Health and Human Services Office for Civil Rights.[4] Any end-to-end security solution must facilitate monitoring and compliance auditing with detailed reporting capabilities.

Make Security Maintenance Easy

Securing your organization's sensitive data and protected documents can be overwhelmingly complex—but it doesn't have to be. Rather than patching together incompatible solutions one on top of the other, choose an end-to-end solution that incorporates hardware and software that work seamlessly together.

Advantages include:

- A single vendor, hardware-software solution means consistency across devices
- Universal login manager for access control
- Shared firmware across the fleet
- Hardware-software interoperability
- Similar user interfaces can mean a reduced learning curve and fewer change management challenges

1 *KMPG: Cloud Threat Report 2018*

2 *2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.*

3 *Quocirca - 2019 Global Print Security Landscape*

4 *HIPAA Journal, "The Most Common HIPAA Violations You Should Be Aware Of," Oct. 2019*

To learn more about how Canon Solutions America can help you protect your sensitive and valuable PII and PHI from entry to exit and beyond, visit ***csa.canon.com/security.***

Canon
CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM

01/19-1053-4028