Canon
CANON SOLUTIONS AMERICA

CANON SEE IMPOSSIBLE

HOW TO SECURE DATA WHEREVER IT LIVES

A PRIMER FOR HEALTHCARE ORGANIZATIONS

SMART CHANGE STARTS HERE.

WHERE DOES YOUR SENSITIVE DATA LIVE?

Healthcare organizations are responsible for the protected health information (PHI) and personally identifiable information (PII) and payment information for thousands of patients, as well as intellectual property related to medical research and innovation. Healthcare data exists in multiple formats at rest and in transit, and each type of data set has its own vulnerabilities, including:

- Paper enrollment forms, manual claims, and clinical decision support systems such as physicians' written notes, prescriptions, medical imaging, laboratory, pharmacy, and other data that can be lost, stolen, or subject to unauthorized viewing.
- Electronic Health Records (EHR) transmitted between healthcare providers, patient portals, and payment processors by email or other means. Electronic data transfers can be hacked, and email is especially vulnerable to social engineering tactics such as phishing.
- PHI stored on site in paper and digital formats and circulated throughout the organization during daily workflows. The use of a wide variety of internet-connected devices by clinical and non-clinical staff puts confidential data at risk every single day.

DATA IS VULNERABLE TO ACCIDENTAL OR MALICIOUS EXPOSURE AT MULTIPLE RISK POINTS

With so much sensitive data circulating in so many formats, risk of exposure is high. Data is especially vulnerable in transit, whether in digital or paper form. Risk points include:

MOBILE DEVICES

22%

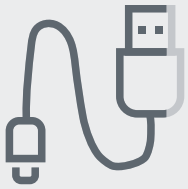
of healthcare organizations identified a major security breach from mobile devices.[1]

EMAIL

42,000

patient records from an Ohio provider were exposed as the result of an email phishing attack.[2]

PRINT INFRASTRUCTURE



#2

rates second with a score of 66% of the top five IT risks that may lead to security breaches.[3]

PRINTER OUTPUT TRAYS

47%

of companies in all industries have experienced an inadvertent data leak from unclaimed print jobs at the output tray.[4]

[1] *Verizon, Mobile Security Index 2018 Report*
[2] *Healthcare IT News, "Phishing Hack on Ohio Provider Breaches Data of 42,000 Patients for a Month," May 29, 2018*
[3] *Quocirca - 2019 global print security landscape*
[4] *Ibid.*

Healthcare data is far more valuable to malicious actors than credit card data, making hospitals and healthcare systems desirable targets for cyberattacks. At the same time, stricter government regulations are driving healthcare organizations to improve defenses against cyber threats. The Office of Civil Rights, the Food and Drug Administration, and the Department of Justice are increasing their oversight and enforcement actions related to cybersecurity and holding providers to greater levels of accountability.

$6.45M

In a Ponemon Institute survey, the average cost of a data breach in healthcare is $6.45M.[5]

45%

Healthcare accounted for 45% of all ransomware attacks in 2017.[6]

$49M

Collected in fines by HHS in 2017 for Healthcare Data Breaches.[7]

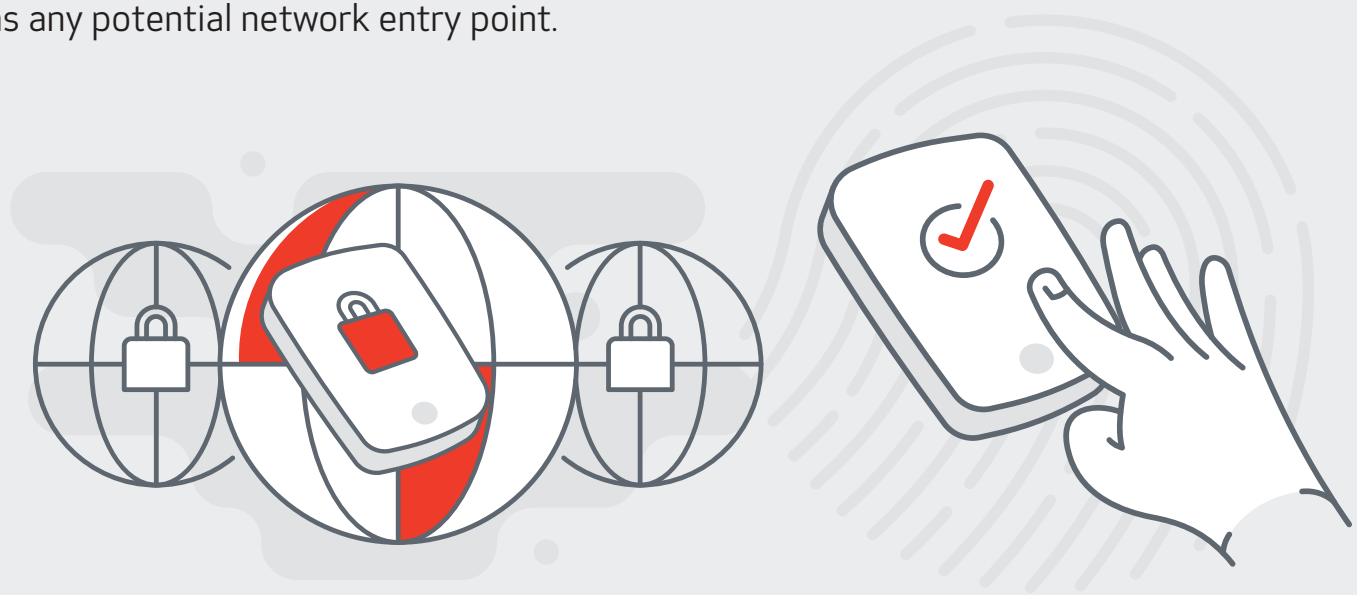
In addition to traditional network perimeter security, healthcare organizations can take steps to identify everyday vulnerabilities that help safeguard sensitive health data from malicious attacks and regulatory repercussions.

[5] *2019 Cost of a Data Breach Study by the Ponemon Institute and IBM Security.*
[6] *Healthcare Informatics: "Report: Healthcare Accounted for 45% of All Ransomware Attacks in 2017," Feb. 22, 2018.*
[7] *HIPPA Journal, "Healthcare Data Breach Statistics," March 2018*

HELP SECURE YOUR DEVICES

Printers and other networked Multifunctional Devices (MFDs) can create multiple potential vulnerabilities, from open ports to unattended output. Considering a print management solution? Make sure it includes the following features and functionality:

- Pull printing to help prevent exposure of sensitive documents in the printer tray. Users must present authentication at a device before it will execute a print, scan, copy, or fax a job.
- Keyword intercept to help prevent unauthorized scanning and copying. This optical character recognition (OCR) feature identifies designated keywords (such as "confidential" or "sensitive") that can alert administrators and even help prevent unauthorized users from printing, emailing, or faxing the document.
- Device-level data security, such as IPSec to protect data in transit, as well as data residing on the device's hard drive. Modern printers, MFPs, and other input/output devices are fully functional network nodes, and as such must be "hardened" as much as any potential network entry point.



HELP SECURE YOUR DOCUMENTS

Documents such as insurance information, enrollment forms, imaging results, machine generated/sensor data, and clinical notes often exist in paper as well as digital form, making them difficult to secure and track. Best practices require a centralized system for storing, routing, and tracking documents that is accessible across multiple locations, as well as secure from unauthorized access. To help protect documents whether at rest or in transit, digital or paper, ensure your document management solution offers the following capabilities:

- A secure method that restricts access to those who require it while efficiently routing information across functional silos and physical locations to promote interoperability.
- Automated scanning with OCR capability that recognizes document types and routes digitized forms to the appropriate recipients and folders.
- Tracking and monitoring of files that are distributed both inside and outside your organization so that every touch leaves an audit trail.

HELP SECURE YOUR DATA

These days, no hospital or health system is intrusion proof and it would be naive to believe that healthcare data can remain safely locked behind your organization's firewall. Instead, it will often exist beyond it, whether transmitted by email or downloaded onto mobile devices, medical devices and laptops. In fact, 90 percent of healthcare organizations use or plan to use mobile devices,[8] and there is increasing awareness of how networked medical devices, which include everything from insulin pumps to bedside units monitoring patient vital signs, pose significant security risk.

Healthcare organizations require new ways of safeguarding sensitive information by incorporating Enterprise Digital Rights Management (EDRM) systems that:

- Protects privacy by embedding a security solution within each document no matter where it resides, within or beyond your organization, on portable devices.
- Provides access to data only to those with proper credentials, even if it is lost or stolen.
- Allows document owners to grant or revoke user access at any time and anywhere in real time.

[8] *MobiHealthNews, "Survey: 90 Percent of Healthcare Organizations Use or Plan to Use Mobile Devices," April 11, 2018*

Canon
CANON SOLUTIONS AMERICA

To learn more about how you can secure print, visit csa.canon.com/security

Canon Solutions America, Inc. does not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment.

Canon is a registered trademark of Canon Inc. in the United States and elsewhere. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged.

© 2020 Canon Solutions America, Inc. All rights reserved.

20/20-0036-4019