7 DOCUMENT MANAGEMENT RISKS TO AVOID

The digitization of Personal Health Information (PHI) presents an enormous opportunity for healthcare organizations to mine data that can significantly improve disease detection as well as the management of individual and population health. In fact, according to a survey by the American Society of Health-System Pharmacists, 99% of hospitals are now reaping the benefits of using electronic health record systems (EHRs)1. But these rewards come with many risks.

Increasingly, single-physician offices, multi-provider groups, large hospital networks and accountable care organizations are being targeted by hackers and cybercriminals who are able to sell valuable EHR records for significant amounts on the Dark Web. The steady rise of attacks combined with the use of legacy technology systems, internet-connected devices and lack of resources and expertise to address emerging threats means healthcare leaders must be more aware of potential risks than ever before.

One often overlooked device that sits in every healthcare office is the printer.

PHI exposure due to unsecured document management practices at the printer can lead to HIPAA and HITECH violations, hefty fines, increased regulatory scrutiny and loss of patient trust, organizational reputation and revenues. Here are seven ways your document management process may be putting your organization at risk.

39% of organizations have low confidence in their ability to secure printers.[2]

Canon

CANON SOLUTIONS AMERICA

RISK 1

THE PRINTER IS UNSECURED

Healthcare providers all along the continuum of care place their printers in high-traffic areas. While this is convenient for employees scanning, printing and collecting documents, it can also pose a security threat as data stored on the printer's internal drive can be compromised. Physical ports for USB drives and other data storage devices make it simple for anyone to make an unauthorized copy of a data file kept in a device's memory. In addition, if unencrypted devices or disks are stolen, anyone can access information stored in the printer's memory. All MFPs should be hardened to eliminate unauthorized use of the machine.

RISK 2

THE PRINTER IS COMPROMISED

While IT is zealous in protecting workstations and laptops from outside intrusions, printers are often overlooked. However, today's printers have the same exposure to external hackers as every other endpoint on your network. Unauthorized open ports, default passwords, outdated firmware, and missed security patches can all provide a hacker entry to the printer—and by extension the rest of your network. Even at the end of life, the printer's hard drive may contain sensitive PHI that can be retrieved if the drive isn't securely erased and destroyed.

90% of enterprises have suffered at least one data breach through unsecured printing.[4]

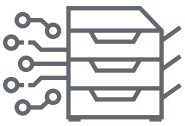
[1] American Journal of Health-System Pharmacy July 2017
[2] The Insecurity of Network Connected Printers, Ponemon Institute, September 2015
[3] Ibid.

RISK 3

DOCUMENTS ARE LEFT EXPOSED AFTER PRINTING

It happens to everyone: you send a document to the printer, but then get distracted or forget to pick it up. Documents left for hours or even days on a printer tray could be accidentally or intentionally collected by an unauthorized recipient. In a payer workplace, a significant portion of printed documents contain some type of sensitive personal or financial data that, if read by the wrong person, puts the organization in immediate violation of HIPAA.

47% of companies have experienced an inadvertent data leak from unclaimed print jobs at the output tray.[4]



RISK 4

EMPLOYEES ARE SENDING PHI TO THE WRONG PRINTER

Integrated delivery networks (IDNs) can have hundreds of printers within a single or multiple buildings, all connected to the same network. As patients move throughout a healthcare facility seeking treatment from a variety of medical practitioners, their clinical and personal. information travels with them. It can be easy for clinical and non-clinical staff to overlook the destination to which PHI was sent. A nurse practitioner, doctor or physician assistant can inadvertently send a print job to the wrong printer or distribute an electronic health record (EHR) to an unauthorized email address or network folder. Once a document or data file containing PHI is sent to the wrong place, it can be difficult to figure out where it went or who saw the PHI.

15% of all reported HIPAA breaches are due to errors when printing.[5]

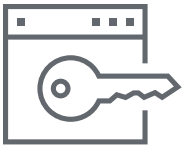
RISK 5
FAXES LEAVE PHI EXPOSED

Despite the move to electronic medical records, a significant amount of PHI is still transferred via fax. In fact, as much as 10% of healthcare print volume is due to faxes. However, unless the document is going to a secured fax inbox, PHI coming in via fax is often automatically printed out and left in a tray or delivered to a general open inbox. Additionally, faxes can be sent to the wrong machine or number. The many risk factors associated with fax use have captured the attention of federal health officials who have called for the elimination of fax machines from physician offices by 2020.

RISK 6
UNAUTHORIZED SCANNING, COPYING, AND PRINTING OF PHI

Both clinical and non-clinical staff do not need access to all of the information in medical records to do their jobs. Few employees need access to all of that information, or even a sliver of it, to do their jobs. However, without Enterprise Digital Rights Management (EDRM), any employee can scan, print, or copy massive files containing sensitive PHI, while IT teams cannot prevent file access, sharing, or distribution.

[6] Quocirca, *Print security: An imperative in the IoT era,* January 2017
[7] HIPAA Journal, "Another HIPAA Breach Courtesy of a Printing Error," Dec. 8, 2015
[2] Becker's Hospital Review, "Three steps to achieving document efficiency in healthcare," April 25, 2017



RISK 7

INABILITY TO TRACK VIOLATIONS

If your organization doesn't require personal logins for scanning, printing, and copying documents, it is impossible to know how, when or by whom a document was accessed. Without this ability to follow an audit trail through the entire document management process, healthcare leaders will struggle to investigate a breach, prove compliance to a regulator, track down the perpetrator or unauthorized recipient, or even detect the breach in the first place. In addition, a lack of regular auditing prevents an IT team from being able to conduct a sophisticated analysis that may identify patterns exposing outside data breaches or internal fraud.

1 IN 5 consumers who are the victim of a health insurance data breach changed their insurance company afterward[8]

[8] Accenture, *Are You One Breach Away From Losing A Healthcare Consumer?,* 2018

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

Canon
CANON SOLUTIONS AMERICA