RICOH
imagine. change.

Safeguard Your Infrastructure

Five steps to strengthen the “weak link” in your healthcare infrastructure

August 2016

Physical Theft & Loss Outpace Hacking in Healthcare Breaches

Though hacking is on the rise, most data breaches are due to lost or stolen health records.

With each of these losses fetching an average of $363 on the black market — compared to $154 from non-healthcare entities[1] — today's healthcare organizations face greater security risks than other industries. In fact, a shocking 89 percent of healthcare organizations have experienced data breaches over the past two years.[2]

High-profile attacks have escalated cyber security to a hot button issue. Examples of widely publicized hacks include one involving 11 million customers, while another breach resulted in 78.8 million leaked customer records. Some healthcare organizations have even been "held hostage" by cyber criminals.[3]

Large-scale data hacks and ransomware incidents may make splashy headlines, but hacking actually trails behind physical loss, human error and misuse as the most common causes of breach.[4] Electronic records are not the only targets of protected health information (PHI) theft. Many stolen records involve paper documents.[5]

The majority of breaches are small[6] (under 500 records) and not even reported to the US Department of Health and Human Services. Though the media often does not cover these small breaches, they still cause significant financial consequences for the healthcare organization.

With an industry-wide focus on protecting digital information, it can be easy to forget about security gaps in physical infrastructure, like printers, copiers and fax machines. However, as the print landscape evolves, what were previously single function devices are now taking on greater risks than just abandoned print trays. Local single function printers are being replaced by networked multifunction peripherals (MFPs) that have the capabilities to capture, transform and manage data.

Five steps to strengthen the "weak link" in your infrastructure:

1. Identify gaps in your print infrastructure security.
2. Centralize and harmonize your print device fleet.
3. Improve workflows to reduce misuse and mishandling.
4. Take control in a device and content sharing environment.
5. Monitor and audit for ongoing security and compliance.

Even so, many enterprises neglect to secure MFPs, with research finding just 22 percent have implemented secure printing. It's a surprisingly low number given the fact that a majority of organizations with MFPs (63 percent) admit they have experienced one or more print-related data breaches.[7]

Despite these challenges, there are steps that healthcare leaders can take to turn these hurdles into opportunities to help protect their organization.

[1] https://securityintelligence.com/cost-of-a-data-breach-2015/

[2] http://www.infosecurity-magazine.com/news/healthcare-data-breaches-cost-62/

[3] http://www.modernhealthcare.com/article/20160217/NEWS/160219920

[4] http://www.verizonenterprise.com/resources/reports/rp_2015-protected-health-information-data-breach-report_en_xg.pdf

[5] https://www.databreaches.net/raleigh-clinic-says-x-rays-were-stolen-may-have-included-patient-information/

[6] http://www.infosecurity-magazine.com/news/healthcare-data-breaches-cost-62/

[7] http://quocirca.com/content/printing-false-sense-security

Five Steps to Strengthen the "Weak Link" in your Infrastructure

In today's new world of care, connectivity and communication are key — and MFP technology has advanced to meet this need. While these connected device systems are able to improve workflows, productivity and convenience, they also pose a greater security risk than the era of local single function printers. Here are 5 steps to consider to help strengthen your MFP infrastructure security:

1 Identify gaps in your print infrastructure security.

Conduct an assessment to identify any gaps in your output security before they become a full-blown crisis situation. From unattended trays to illegally accessed printer hard drives, device fleets pose real challenges to overall security and governance. There are numerous checklist items to help support HIPAA security and privacy requirements,[8] like locking down patient wristbands and protecting printed prescriptions, which can also reduce the risk of breach.

2 Centralize and harmonize your print device fleet.

With paper output, it's hard to track what is being printed, scanned and copied (and by whom). With the right tools, you can centralize print management and harmonize backend systems for improved fleet device monitoring capabilities. Certain software can track sensitive print jobs and store that data in one central location, so you can easily trace back exactly where a document originated. Paper is one of the highest information security risks; even paper falling off the back of a truck (yes, it's happened) can cause a breach. Switching to a paperless system can also help avoid lost or misplaced documents and lower the risk of compromising PHI.

> *"By focusing on securing your print output, you can prevent both large and small-scale data breaches while meeting compliance requirements."*

3 Improve workflows to reduce misuse and mishandling.

Large volumes of data move across healthcare enterprises in various directions to multiple devices, creating many chances for information loss or mishandling. Instead of moving paper through the enterprise and then deciding what to do with it at the end, it's important to capture it in the beginning and move it more efficiently and securely through whatever processes are associated with those documents. Improved workflows can help reduce the chance of human error. Even simple mistakes like printing the wrong address on an envelope can have costly consequences, which has happened to a provider who was charged with both breach fines and patient compensation for emotional harm.[9]

[8] http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/
[9] http://m.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11668139

Five Steps to Strengthen the "Weak Link" in your Infrastructure

4 Take control in a device and content sharing environment.

Moving to a centralized MFP infrastructure means more users are sharing devices, opening up the potential for breach or compliance violation — whether accidentally or maliciously. However, you can maintain a centralized printing strategy without sacrificing security. Convenient and secure card-based methods can be ideal for printing confidential documents, even in an open and communal workspace. You can also authenticate users and encrypt data to protect sensitive information before it hits the print queue. Devices equipped with image overwriting capabilities can be used to protect the printer's hard drive against more sophisticated thieves.

5 Monitor and audit for ongoing security and compliance.

Meeting compliance requirements ranks as one of healthcare leaders' top IT security spending concerns. This should come as no surprise as compliance requirements have become increasingly complex and costly in recent years. By conducting regular internal audits, you can relieve compliance pressures, locate and correct gaps in the process before they become a problem and manage your print infrastructure with peace of mind.

> *"Improved workflows can help reduce the chance of human error. Even simple mistakes like printing the wrong address on an envelope can have costly consequences."*

While today's cyber criminals pose a real threat to healthcare security, the most common villain is often more commonplace. By focusing on securing your print output, you can prevent both large and small-scale data breaches while meeting compliance requirements.

To learn about Ricoh solutions for healthcare, visit ricoh-usa.com/healthcare

RICOH
imagine. change.

www.ricoh-usa.com/healthcare

Ricoh USA, Inc., 70 Valley Stream Parkway, Malvern, PA 19355, 1-800-63-RICOH

The content of this document, and the appearance, features and specifications of Ricoh products and services are subject to change from time to time without notice. Products are shown with optional features. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. Actual results will vary depending upon use of the products and services, and the conditions and factors affecting performance. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them.