

PATIENT DATA IN JEOPARDY:

SECURING HEALTHCARE'S PRINTER ENVIRONMENTS

Help Boost Security and HIPAA Compliance Efforts From Virtually Anywhere

Protecting sensitive, “individually identifiable health information” in compliance with HIPAA is a significant challenge facing healthcare industry professionals. With uniFLOW, providers can safeguard patient health information (PHI) to support compliance without impacting the quality of care.



According to a Ponemon Institute survey*

- The average cost of a data breach in healthcare is 6.45M.
- 51% of breaches were malicious attacks - 24% were caused by human error and 25% were due to system glitches.

Limit Device Access to Authorized Personnel

With uniFLOW, you control who is authorized to access, print, copy, fax, scan, or send important healthcare documents and patient medical records from all networked MFPs. You can facilitate authorized device access with user IDs, passwords, or proximity cards. This helps you ensure that no one prints or sends sensitive patient information—whether intentionally or accidentally—without authorization. Efforts like this help you facilitate compliance with HIPAA and other regulations.

Grant Access to Print Functionality Based on Role

uniFLOW enables you to gain control over all print usage—even across a large hospital or network of specialist offices—and restrict user access from unauthorized device features.



Profiles can be set, according to user or role, that allow or restrict access to specific device features as needed.

Leverage Secure Mobile Printing

uniFLOW Secure Mobile Printing enables medical staff the option of sending print jobs in two ways: via email or the uniFLOW app.

The email option is fairly simple. Authorized staff can forward a message with an attachment to a predetermined email address. From there, they receive a job code that can be used to release the print job from the MFP.

The uniFLOW app provides users with visibility to network devices available so jobs can be sent directly to them. The server-based app also allows users to use their mobile device as a release station for an MFP that may have an intuitive interface.



For traveling medical practitioners, uniFLOW Secure Mobile Printing provides the option for guest printing. This convenient feature enables visitors (outside the network) to submit print jobs to a guest printing email address that will generate limited prints under rules that are preset by your organization.

Offer Healthcare Staff Print Options that Help Reduce Costs and Promote Sustainability Efforts

In today's regulated and highly competitive environment, providers seek ways to reduce costs and remain environmentally conscious. uniFLOW solutions help administrators assess and contain costs by influencing staff behavior, preventing wasteful practices, and providing greater control over device use across healthcare facilities.



According to a Ponemon Institute survey*

- The average cost per record in a data breach in healthcare is \$429.
- The average size of a US data breach included 26,523 records.

Track Document Activity and Allocate Expenses Back to Department Cost Centers

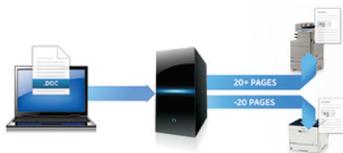
uniFLOW enables you to track costs and generate analytical reports that offer insight into who's printing and how much. You can use this data to identify inefficient behaviors and help cut costs. Now, your facility can allocate print-related expenditures to the appropriate department or cost center to help you more effectively manage your expenses.



Detailed tracking and activity reports can help you ensure that print inefficiencies are reined in and overhead expenses are accurately billed to the appropriate internal departments.

Route Print Jobs to More Cost-Effective Devices

Through uniFLOW Rules and Routing, your facility can automatically direct all print jobs over a predetermined size or complexity to output on a lower-cost-per-page device. This allows healthcare administrators to enforce cost-conscious print behaviors throughout their organizations.



Facilitate more cost-efficient network printing across your practice or hospital with uniFLOW rules-based routing.

Curb Inefficient Printing and Boost Environmental Efforts with Reports

uniFLOW lets you to gain control over print activity, even across large hospitals. When you encourage healthcare professionals to print more purposefully—by authenticating with password or ID card before retrieving printouts, for example—you help cut costs, reduce waste, and boost efficiency.



Additionally, with uniFLOW you can generate Environmental Analysis reports that summarize key usage levels between two audit periods (such as years or financial quarters). With data like this, administrators can compare usage stats such as total reams of paper used, greenhouse gases conserved per year, and the number of trees that have been saved through double-sided printing, for example.

Providers Successfully Controlling Output Costs and Implementing Intelligent Printing Strategies

To overcome multiple printing challenges, healthcare organizations are turning to uniFLOW to help facilitate security and compliance efforts, gain visibility into data analysis, track individual output activities, enable staff to print more securely, help reduce IT overhead, and improve sustainability.

Saving Lives and Eliminating Human Suffering. – Fred Hutchinson Cancer Research Center



For the Fred Hutchinson Cancer Research Center, uniFLOW provided quick authentication of walk-up users through proximity cards, secure printing capabilities, and complete accounting of usage through Canon's Printing Intelligence Report.

"We continue to be impressed by the technology, vision, and support of Canon Solutions America and we're encouraged that, over a year and half later, we have not had a single issue with the solution."

– Mark Burch, Director of Materials, Fred Hutchinson Cancer, Research Center

Endnote

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

Canon
CANON SOLUTIONS AMERICA

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

Many variables can impact the security of your devices and data. Canon Solutions America does not warrant that the use of its features will prevent malicious attacks, or prevent misuse of devices or data or other security issues. Nothing herein should be construed as legal counsel or regulatory advice concerning customers' compliance with laws related to privacy and security. Customers must have their own qualified counsel determine the feasibility of a particular solution as it relates to regulatory and statutory compliance.

Canon is a registered trademarks of Canon Inc. in the United States and may also be registered trade marks or trademarks in other countries. Nothing in this brochures should be considered as legal counsel or advice pertaining to regulatory compliance, including without limitation with respect to statutes such as HIPAA, Sarbanes Oxley or the U.S. Patriot Act. Each customer should have its own qualified counsel to determine the advisability of a particular solution as it relates to regulatory compliance. Canon is not responsible for typographical errors. All other referenced product names and marks are trademarks of their respective owners. Some items may not be available at this time; please check for availability. Specifications and availability subject to change without notice.

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

01/19-1050-4010