Canon

imageRUNNER
ADVANCE DX

imagePRESS Lite

Security Solutions For Medical Offices

Medical practice managers across the healthcare ecosystem are tasked with a wide array of challenges, from recruiting and retaining staff and overseeing operational excellence to negotiating with payers and supporting their regulatory compliance efforts. While many practices have dedicated IT or security professionals, they may be contract workers or spread thin across a variety of locations. Understanding security vulnerabilities and taking steps to mitigate risk is everyone's responsibility. Here are three ways that Canon products and solutions can help support security efforts for your medical practice.

Devices That Can Support the Implementation of the NIST Cybersecurity Framework

The NIST CSF (Cybersecurity Framework) can help organizations determine how to manage cybersecurity risk by providing a common language and systematic methodology that can complement existing risk management processes. This framework allows healthcare organizations to scale their activities based on what's economically or organizationally viable for their security environments and cybersecurity maturity. The HIPAA Safe Harbor Act grants the Department of Health and Human Services (HHS) the right to reduce fines if a healthcare organization can demonstrate implementation of a recognized security framework 12 months prior to a data breach or other security-related HIPAA violation. **Adopting technology that can align with NIST CSF guideline efforts could potentially help demonstrate your organization's implementation efforts.**

imageRUNNER ADVANCE DX and imagePRESS Lite devices support features and functionality that can be implemented in support of NIST Cybersecurity methodology. Find out how recommended settings for standard and optional features can help you align with the NIST Cybersecurity Framework here.

Administrators who are unsure about which settings to implement can choose from six options by referencing the *Recommended Security Settings for Usage Environment* on imageRUNNER ADVANCE DX and imagePRESS Lite devices. There is also a web-based Security Settings Navigator Tool that can help recommend printer security settings based on your needs. These settings can be applied by authorized users within the device settings screen.

Information Management Platforms That Can Support a Zero Trust Strategy

Rooted in "never trust, always verify, assume a breach," Zero Trust security requires users to continuously authenticate and validate at every stage of a digital transaction. Zero Trust security can be applied to software applications, endpoints such as MFPs, laptops, and other Internet of Things (iOT) devices as well as network infrastructure. Zero Trust processes are often incorporated in effective cybersecurity models such as the NIST CSF.

uniFLOW Online—a public, cloud-based print and scan solution hosted in Microsoft Azure—can support your Zero Trust efforts. It allows healthcare organizations of all sizes to implement device authentication, identity access management, device security features, and remote monitoring and reporting tools that can help track user behavior and identify device anomalies. This allows administrators to control what information is printed, scanned, stored, or shared.

Additionally, uniFLOW Online enables authentication at compatible Canon and non-Canon devices for the release of print jobs to help limit sensitive information from being exposed in output trays. Learn more about how uniFLOW Online can help support your Zero Trust here.

Mail-to-Cloud Software That Limits Data Sprawl

Email can expose sensitive Personal Health Information (PHI) and Personally Identifiable Information (PII) both inside and outside your healthcare organization. Having the ability to control who has access to email attachments and ensuring that emails are not sitting in multiple inboxes where they can be accessed through social engineering attempts, such as phishing, is an ongoing challenge. If unchecked, data sprawl can pose a risk when sharing information with business associates.

Canon offers mxHERO mail-to-cloud capabilities that automatically replace email attachments with a link to an access-restricted and indexed cloud storage account such as Google Drive, OneDrive, Therefore™, Box, etc. Users can enable automatic expiration of the link access and prevent file downloads, by automatically incorporating password protection and file restrictions through supported cloud storage systems without any effort on the sender's part. Because the attachment lives in your organization's cloud repository, attachments containing sensitive information can't be accessed via email in-boxes. Learn more about mxHERO here.

Contact your Canon Authorized Dealer to learn more about security features on Canon products.

Canon

usa.canon.com/healthcare

Scan QR code for more
information about Canon's
Advanced Solutions for Healthcare.

PREMIER®
Contracted Supplier

The authors of this content are not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the products and suggestions discussed herein. Canon U.S.A., Inc. does not make any warranties concerning the accuracy or completeness of the opinions, data, and other information contained in this content and, as such, assumes no liability for any errors, omissions, or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data, or other information.

Canon, imageRUNNER, imagePRESS, and imagePRESS Lite are registered trademarks or trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. uniFLOW is a registered trademark of NT-ware Systemprogrammierung GmbH. Therefore™ is a registered trademark of Therefore™ Corporation. All other referenced product names and marks are trademarks of their respective owners. All features presented in this brochure may not apply to all Series and/or products and may be optional; please check with your Canon Authorized Dealer for details. Neither Canon Inc. nor Canon U.S.A., Inc. represents or warrants any third-party product, service, or feature referenced hereunder.Specifications and availability subject to change without notice. Not responsible for typographical errors.