Canon

SECURITY SOLUTIONS AND SERVICES FOR HEALTHCARE

A multi-layered approach to help protect your sensitive data

OUR MISSION

Securing healthcare environments continues to be a challenge as hacking/IT incidents are the leading cause of data breaches followed by unauthorized access or disclosure.[1] Increasingly, healthcare IT and security professionals have come to the realization that it's not a matter of IF a data breach will occur, but WHEN. This is true for both acute and ambulatory settings.

Our mission is to offer healthcare leaders solutions and services that can support security best practices to help:

- Identify cybersecurity risks as they pertain to our products.
- Protect against vulnerabilities by developing and implementing appropriate safeguards.
- Detect the occurrence of a cybersecurity event through integration with appropriate monitoring systems.
- Respond to a data breach with actionable steps.
- Recover from a threat and restore any impaired capabilities in a timely fashion.

A MULTI-LAYERED APPROACH TO EHR SECURITY

Security is not a destination, it is an ongoing journey that requires organizations to regularly assess, address, and anticipate risks associated with their technology investments. Significant resources and know-how are required to stay ahead of malicious actors and maintain control over all aspects of the document lifecycle, especially when sensitive, proprietary, or lucrative financial data may be at stake. According to a recent report, system intrusion, basic web application attacks, and miscellaneous errors represent 68 percent of breaches in healthcare.[2]

According to a study published in the HIPAA Journal in July 2023, the majority of hacking IT/incidents involve hacking groups exploiting vulnerabilities through network servers to steal data for ransomware purposes. Canon U.S.A. approaches data security through a holistic, multi-layered approach comprising five pillars that cover how data is used both inside and outside healthcare environments.

5 PILLARS OF SECURITY

Device Security

- Authentication
- Role-based Access
- SSD Encryption
- SSD Lock
- Network & Protocol
- Whitelisting

Print Security

- Authentication
- Pull Printing
- Encryption (in transit and at rest)
- Keyword Intercept
- Auditing
- FedRAMP-Authorized MPS

Document Security

- Secure Storage
- Encryption
- Role-based Access
- Copy-lock

Information Security

- File Encryption
- Access Control
- Tracking & Auditing
- Data Loss Prevention

Cybersecurity

- Consultation
- Assessments
- Penetration Testing
- Incident Response
- Training & Awareness

1 HIPAA Journal, July 2023 Healthcare Data Breach Report
2 Verizon, 2023 Data Breach Investigations Report

DEVICE SECURITY

WHAT ABOUT PRINTERS AND MFDs?

PRINTERS AND MULTIFUNCTIONAL DEVICES ARE OFTEN OVERLOOKED.

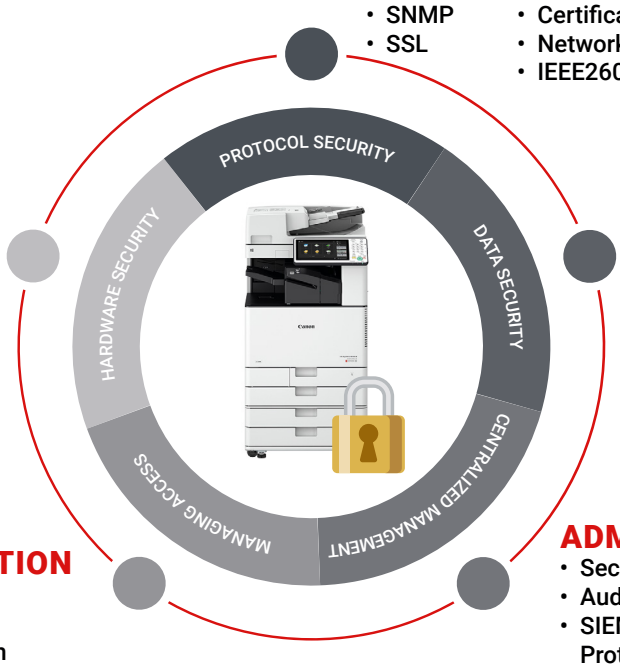
The Canon imageRUNNER ADVANCE DX and imagePRESS Lite devices all come equipped with the ability to "harden" the configuration to reduce the chances of compromising data privacy. Certain features and functionalities on these devices support the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). In addition, the Security Navigator interface on imageRUNNER ADVANCE DX multifunction printers helps users select the appropriate configuration to support organizational security policies. Our National Consulting Services (NCS) organization can assist IT personnel and administrators in healthcare settings to harden their endpoint devices. For more information about device hardening, please visit Canon U.S.A.'s Security Solutions & Services website at usa.canon.com/security and view imageRUNNER ADVANCE security white papers.

DEVICE HARDENING

- SNMP
- SSL
- Certificates
- Network & Web
- IEEE2600 Common Criteria

DATA AT REST

- Trusted Platform Module (TMP)
- SSD Data Encryption (FIPS 140-2, 256 AES)
- SSD Lock
- Start-up Verification
- Runtime Intrusion Detection
- Whitelisting



DATA IN TRANSIT

- Encrypted PDF
- SSL/TLS Encryption
- IPSec Support
- Wireless LAN/IEEE 802.1

AUTHENTICATION

- Device Based
- Card Based
- User Authorization
- AD/LDAP

ADMINISTRATOR CONTROL

- Security Policy Management
- Audit Logging
- SIEM Integration with Syslog Protocols RFC5424 & RFC5426
- Auto Certificate Update

YOU CANNOT MANAGE WHAT YOU CANNOT SEE

CYBERCRIMINALS PERSISTENTLY EXPLOIT SYSTEM VULNERABILITIES TO ACCESS CONFIDENTIAL DATA AND INTELLECTUAL PROPERTY.

Your security and IT teams need to have visibility into print infrastructure to stay aware of any perimeter and end-point security failures or anomalies that may indicate malicious activity. Deploying a security information event management (SIEM) system can aggregate security data from across your organization, help security teams detect and respond to security incidents, and create compliance and regulatory reports about security-related events. Incorporating a Printer Fleet Cybersecurity as a Service™ solution can help healthcare organizations access information about device vulnerabilities, operations, and needs, even for mixed fleets. Through this type of remote concierge service, healthcare IT personnel are relieved of the burdensome task of perpetually hardening, patching, and maintaining selected controls on printer fleets that comprise various makes, models, types, and ages.

OUTPUT AND SCAN MANAGEMENT

- Flexible authentication
- Secure printing of confidential documents
- Delegated printing
- Printing from Chrome
- Secure document scanning, including to FedRAMP-authorized cloud services such as: Teams®, OneNote®, Google Drive, Exchange®, and BOX
- Tracking of print, scan, and copy costs
- Mobile printing

SECURE AUDITING AND FLEET MANAGEMENT

- Centralized usage reporting
- Print device status and alerting
- Automated toner replenishment
- Automated meter collection tools
- Service-alert notifications
- Inventory change tracking
- Service-performance analysis
- Robust fleet analysis and reporting
- ServiceNow alerts integration
- Device security audit and alerts

PRINT SECURITY

Despite the rate of digitization, paper continues to play a significant role in healthcare settings. More than one billion printed documents continue to be produced in the U.S. each year. The next logical progression after securing printers and a multifunctional device fleet is to secure the output of those devices. Closing security gaps in your printing and imaging environment should be an essential piece of your overall security strategy. Additionally, there are key features and functionality embedded in many print management solutions that can aid you in your security journey.

UNAUTHORIZED REPRODUCTION SECURITY

As healthcare organizations upgrade their devices and move into the world of digital high-speed variable print processes, security features need to be enhanced to maintain the confidentiality of back-office files as well as personal health information (PHI). Whether your organization needs to prevent altering or duplicating sensitive information from a digital document, or photocopying a hard copy lab result, the need for privacy is paramount. As a healthcare leader, you are continually being called upon to provide solutions that protect information throughout the continuum of care.

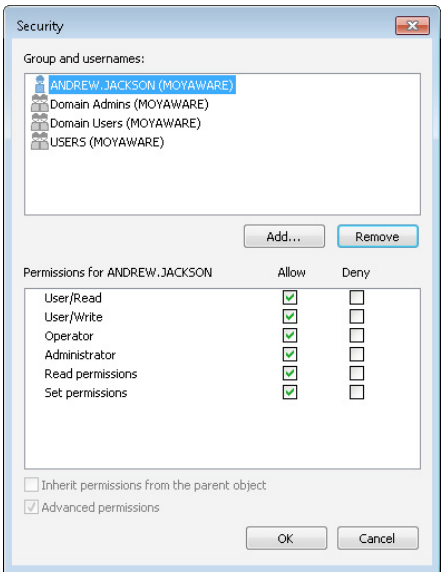
FEDRAMP-AUTHORIZED MANAGED PRINT SERVICES

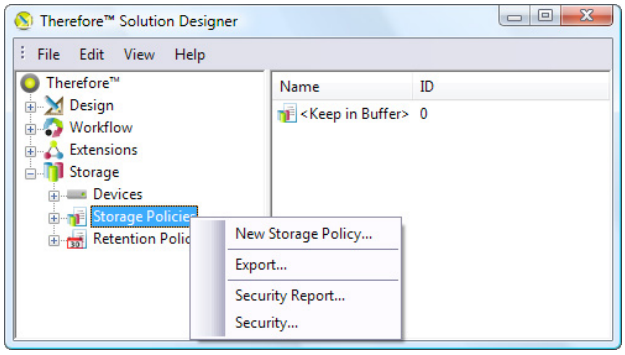
Through Canon Office Cloud, Canon U.S.A. offers a FedRAMP-authorized service platform focused on enabling secure cloud-based managed print services. FedRAMP-authorized solutions provide a standardized approach to security assessment and authorization of these services. Adopting such solutions can help save the costs, time, effort, and staff needed to vet cloud solutions independently. Canon Office Cloud can also help simplify security audit processes and ensure that systems are continuously monitored for security risks.

DOCUMENT SECURITY

Comprehensive care requires interoperability among providers, payers, and institutions. Throughout the healthcare ecosystem, structured and unstructured data needs to be thoroughly protected, meticulously managed, and easily accessible. However, the consolidation of healthcare systems, incompatibilities between technology from different vendors, and privacy and data protection rules, can place a significant burden on healthcare IT and security professionals. Canon U.S.A. provides content management solutions that can help protect sensitive information both in transit and at rest once it is transitioned into an unstructured format with features such as:

- System permissions restrict unauthorized access to document repositories.
- Fully customizable access permissions for specific content and data.
- Anti-tamper measures ensure document authenticity.
- Automatic document back-up for disaster recovery.
- Audit Trail for tracking user and document activity.
- Conformity with security standards and regular penetration testing.
- Automated Retention Policy configuration.





SAFEGUARDING THE SECURITY OF YOUR INFORMATION

Canon U.S.A. understands that managing information securely is a fundamental aspect of healthcare collaboration. You need to know that sensitive documents are only available to authorized users and are backed up securely, and that all activity can be fully traceable via an audit log.

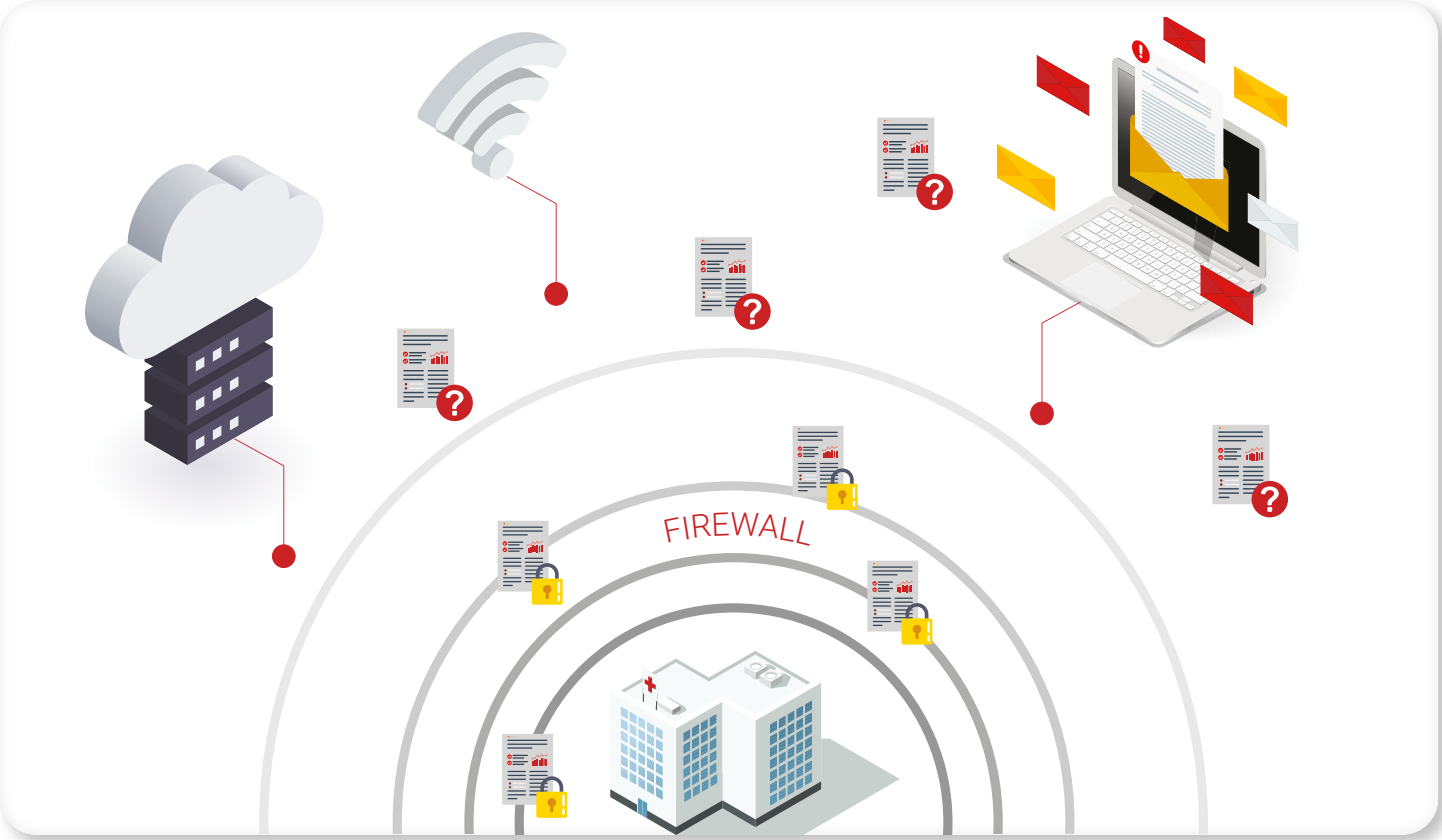
INFORMATION SECURITY

DO YOU EVER WONDER WHAT HAPPENS TO INFORMATION ONCE IT TRAVELS BEYOND YOUR WALLS?

Canon U.S.A. offers our customers a flexible enterprise digital rights management (EDRM) solution that helps users protect their data and personally identifiable information (PII) at the file level, as it travels. Most organizations focus on protecting the perimeter through firewalls and the inside with malware and virus protection solutions but can miss taking critical steps to safeguard electronic health records (EHR) when they travel outside of the original point of care for the purposes of collaborative treatment.

Now clinical document owners can manage access through cloud-based encryption keys and set parameters around:

- Access privileges
- Editing, copying, printing, or exporting rights
- Availability time frame
- Real-time granting or revoking of access
- Uneditable audit trail
- Global file tracking



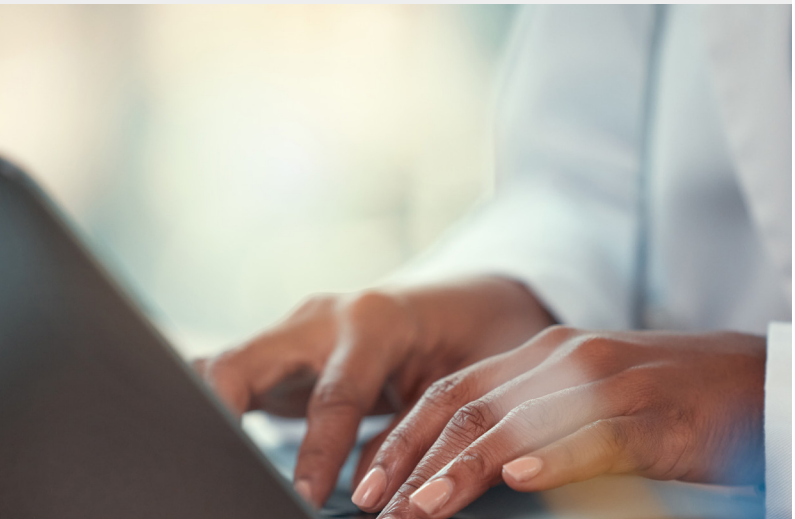
CYBERSECURITY

With the support of our preferred cybersecurity service providers, healthcare leaders can help secure patient data without feeling like they must do it alone. We work with executives in a variety of health settings to help source managed detection and response services that can assist in the development and maintenance of a successful security posture ranging from cyber-awareness training for staff to implementing security orchestration, automation, and response (SOAR) technology to guidance with supporting HIPAA compliance policies.

- Vulnerability Assessments
- Penetration Testing
- Consultation
- Training and Awareness
- Managed Detection and Response
- Application Testing

More than 5,000 healthcare data breaches of 500 or more records have been reported to the department of health and human services since 2009. These breaches have resulted in the exposure or unauthorized disclosure of almost 4 million healthcare records–this equates to more than 1.2 times the population of the United States.

HIPAA Journal July 2023 Data Breach Report



trust. Awareness training, due care, and due diligence are table stakes toward protecting valuable information and avoiding costly data breaches. Ask us how we can help you get started.

PREEMPTIVE ACTION CAN HELP PREVENT COSTLY FINES

In 2021, the U.S. government passed the HIPAA Safe Harbor Act, an amendment to the HITECH Act. The 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. As a result, adopting technology that meets NIST Cybersecurity Framework guidelines could potentially help mitigate penalties in the event of a security breach. Canon imageRUNNER ADVANCE DX and imagePRESS Lite devices have certain functionality and features that help support the NIST Cybersecurity Framework. Find out more about the NIST Cybersecurity Framework here.

PEOPLE–YOUR WEAKEST LINK OR YOUR BEST DEFENSE

LEVERAGE PHISHING SIMULATION TRAINING AS A HUMAN FIREWALL

Social engineering has been the culprit of some of the most catastrophic data breaches to date. It has never been more critical to create awareness of this threat vector and to educate your personnel to not fall prey to phishing and pre-texting as email has become weaponized and the medium of choice for malicious cybercriminals.

Deploying a phishing simulation platform in your organization can provide a flexible and consistent way to modify, test, and measure employee behavior with electronic communications. You can convert potential risk takers into front-line defenders.

1-844-50-CANON

usa.canon.com/security

11/25-0159-9308