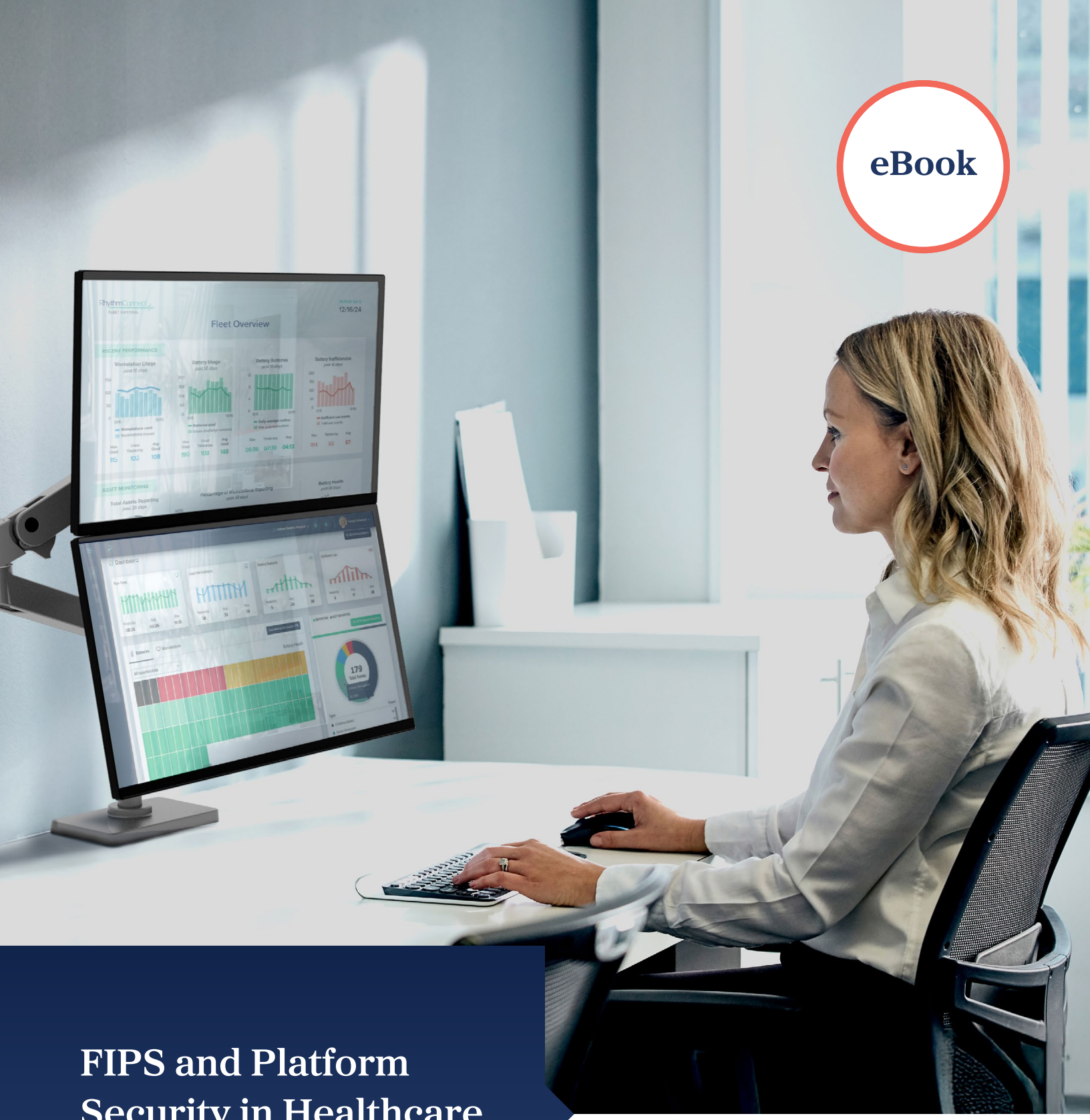


eBook

FIPS and Platform Security in Healthcare Information

ergotron

Table of Contents

FIPS validation and how it protects sensitive healthcare information

In a proprietary study, Ergotron found that the second fundamental challenge in managing fleets of connected devices–behind connectivity across complex facilities–is protecting those networks from cybersecurity threats.

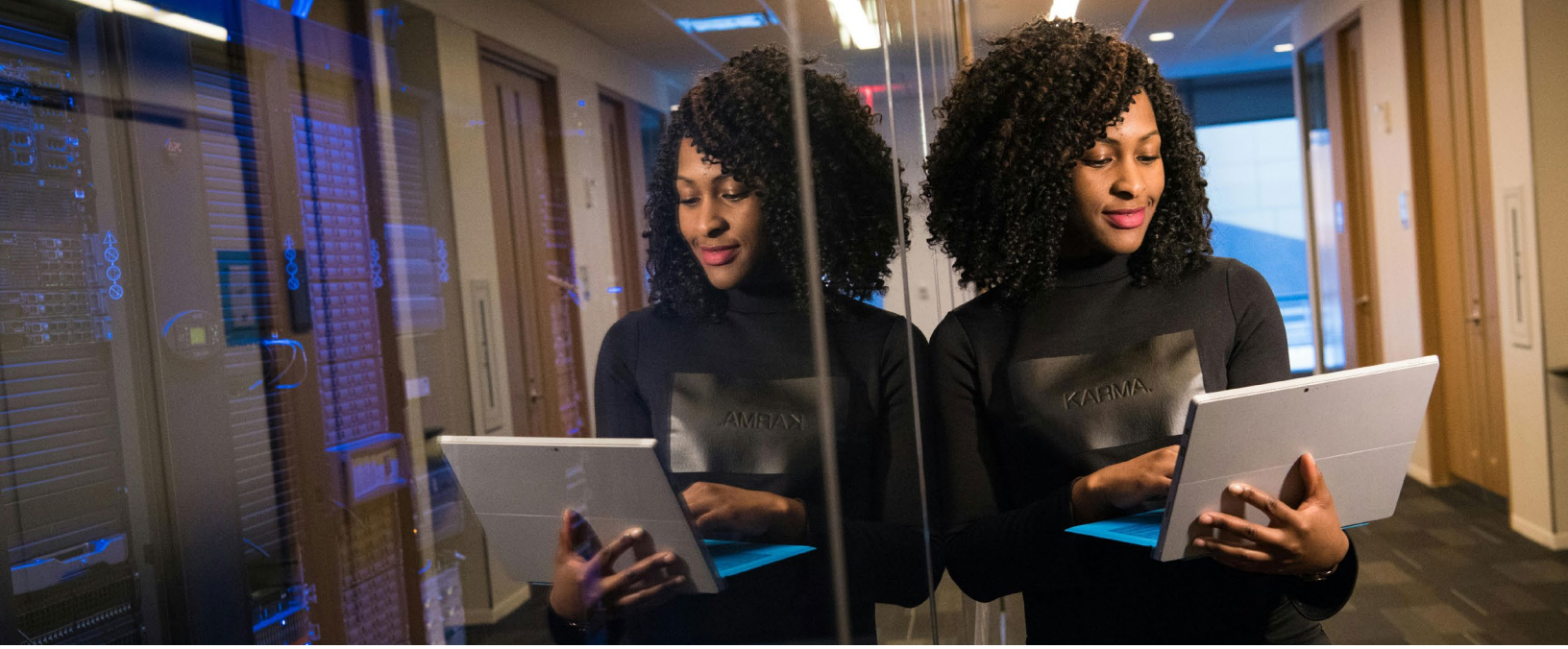
Modern healthcare organizations process huge volumes of personal and medical information every day–from patient histories and laboratory test results to medication management and insurance claims. But that data isn't just useful for care: it also makes your facility a high-value target for cyberattacks.

Imagine if vital electronic systems suddenly went offline, medical records became unreadable, and care teams couldn't access information needed at the right time. These aren't far-fetched scenarios: hackers are increasingly targeting healthcare facilities, not only stealing information and causing disruption, but also putting lives at risk.

That's why keeping the data within your organization safe and secure should be a top priority. The strongest marker of trusted encryption is validation under the Federal Information Processing Standards, or FIPS. When software meets this standard, it means a trusted third party has verified that their encryption works as claimed. Choosing FIPS 140-3 validated solutions helps your organization reduce the risk of damaging cyber incidents and gives you real proof that you're protecting patient information in line with laws and industry expectations.

The top 9 cybersecurity threats in healthcare:

1. Remote work security assurance
2. Endpoint device management
3. Human factors in cybersecurity
4. Lack of security awareness
5. Inadequate board-level risk assessment communication
6. Inadequate business continuity plans
7. Lack of coordinated incident response
8. Limited budget and need to deliver healthcare without disruption
9. Vulnerable MCPS (medical cyber-physical systems)



Understanding FIPS

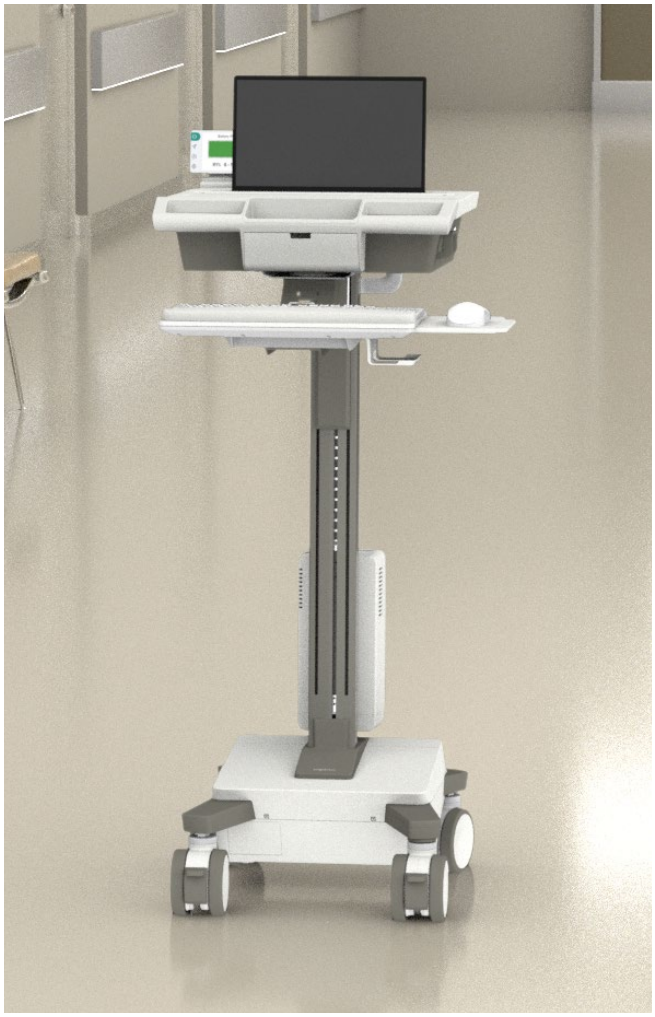
FIPS is the highest benchmark for ensuring security through software and hardware encryption requirements. The U.S. federal government sets the bar for this standard, which protects sensitive but unclassified information using cryptography, but its relevance and value extend to every sector that uses connected devices to process sensitive and personal information. Simply put, FIPS matters everywhere platform security matters. As with federal information, healthcare, financial services, critical infrastructure, and SLED all require the strongest protection measures for encryption to ensure security of sensitive data and personal information in mobile and networked technologies.

Why FIPS validation matters:

1. Mandated for any product sold to U.S. federal agencies using encryption
2. Required for Department of Veterans Affairs (VA), Department of Defense (DoD), federal health systems, and the General Services Administration (GSA)
3. Heavily relied upon in State, Local, and Education government contracting, critical infrastructure, and healthcare organizations
4. Recognized globally, including in Canada, Australia, New Zealand, the United Kingdom, Brazil, and Japan

From the same proprietary study, it was found that forty-three to forty-six percent of IT decision makers say the primary challenge in managing connected assets is ensuring compliance with security and regulatory standards.

FIPS validation is governed by the certifying body NIST (National Institute of Standards and Technology) in the U.S. and by CSE in Canada. Only FIPS validated products are tested, certified, and listed on NIST's website. FIPS 140-3 is the current standard and includes all requirements from the prior 140-2 standard, plus more stringent controls. Working with the most current FIPS validated products provides assurance that you're working with products that have passed the highest standard for federal software encryption requirements.



Compliance is not validation.

Healthcare providers know the importance of specificity. Being exact. That's also true when it comes to terminology suppliers use around FIPS. Some vendors blur the line between FIPS compliant and FIPS validated. While compliance merely suggests adherence to guidelines, validation proves it. Accepting anything less than FIPS validation is an invitation for data security risk and vulnerability.

A product is FIPS validated in the U.S. only when it has been tested, verified, and issued a certificate by NIST. A FIPS validated module is public, searchable, and auditable. Before adopting connected solutions, best practices for IT teams should include confirming validation status directly on NIST's website under their validation program. It's an easy step that separates marketing language from measurable security posture.

FIVE BENEFITS OF FIPS VALIDATION FOR HEALTHCARE IT

There are many benefits to relying on FIPS 140-3 validated cryptographic modules, including:

1

Encryption Integrity

FIPS validated cryptographic modules have been rigorously tested for tamper resistance, key management, and secure cryptographic operations, ensuring protection for every data exchange in a network. For a healthcare facility, this means patient records, connected medical devices, and internal communications are protected with independently verified encryption—not assumptions or unbacked vendor claims.

2

Risk Mitigation

When encryption is weak, mis-configured or unvalidated, attackers have easier paths into your data or systems. The healthcare sector is especially vulnerable to breaches and ransomware, but by using FIPS validated modules, you reduce the chance of a weak spot in your encryption layers being the cause of a violation.

3

Patient Trust and Confidence

Patients trust healthcare providers not only with their care but also with highly personal data. If a cybersecurity breach occurs, that trust is shattered, reputations are damaged, and recovery becomes more difficult. Using certified encryption shows patients that data protection isn't assumed—it's proven. For patients, it means their sensitive health information is handled securely and with care, which can improve confidence in your facility and, in turn, support retention, referrals, and overall satisfaction.

4

Assurance for Leadership

For CIOs, CTOs, and boards, the continuous worry about "what if" something goes wrong can be exhausting. Having FIPS validated encryption means one less major risk area to fret over. Because the modules are tested, documented, and part of a government recognized program, you can feel more confident that you are meeting key technical standards with auditable evidence.

5

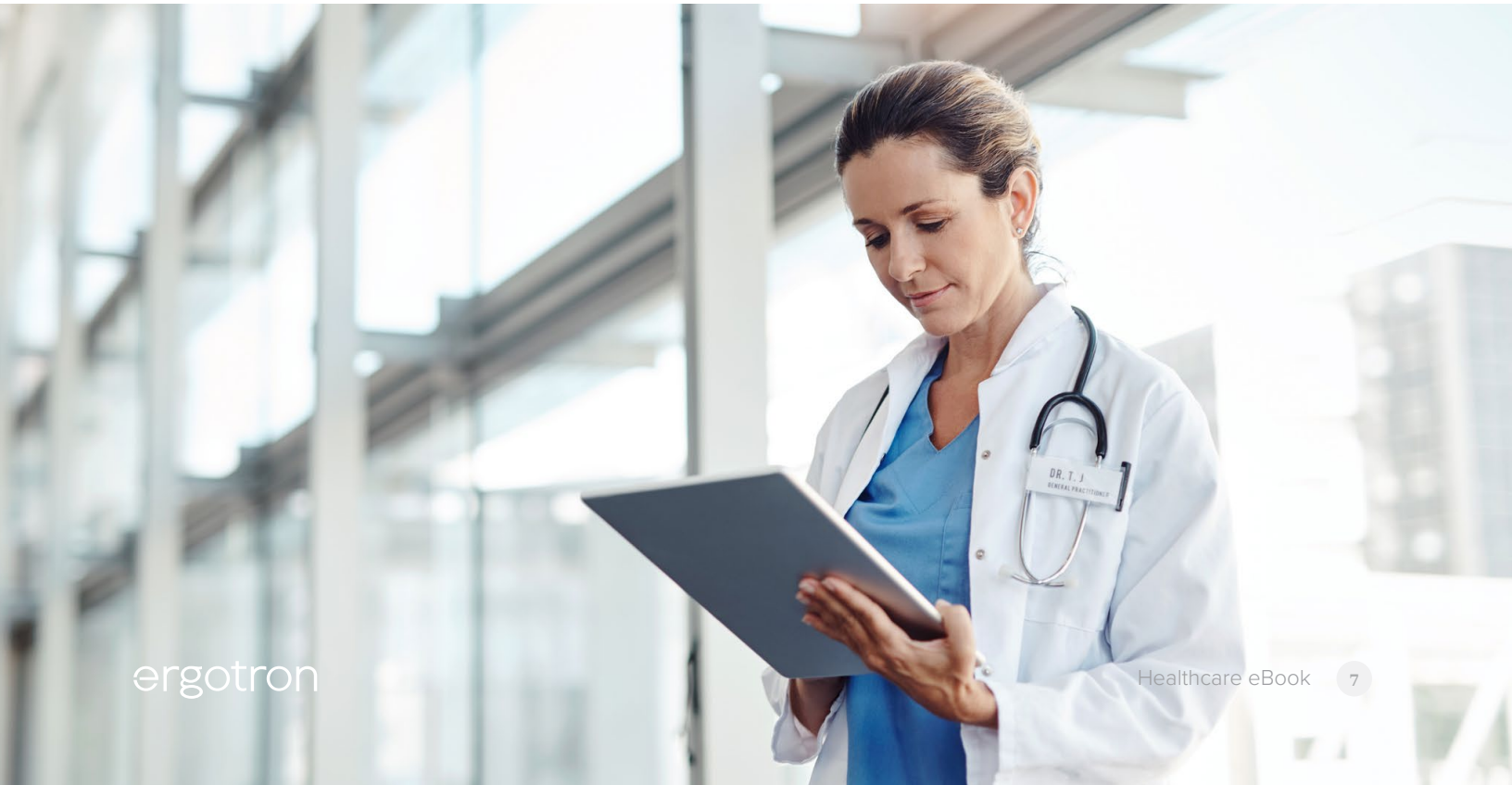
Regulatory Compliance

Healthcare organizations must meet a host of regulatory requirements (i.e., Health Insurance Portability and Accountability Act (HIPAA) in the U.S.). While HIPAA doesn't explicitly say "must use FIPS 140-3", guidance makes clear that encryption should use validated cryptographic mechanisms and that modules should be properly tested. Adopting FIPS validated tools streamlines documentation for HIPAA, HITECH, and NIST Cyber Security Framework (CSF) audits—reducing cost, risk, and remediation burden.

In a two-phase study of IT decision makers, it is almost unanimous: when asked about a primary challenge in managing connected assets, 0-1% of responders admit ‘we do not face any challenges.’ **Challenges are universal!**

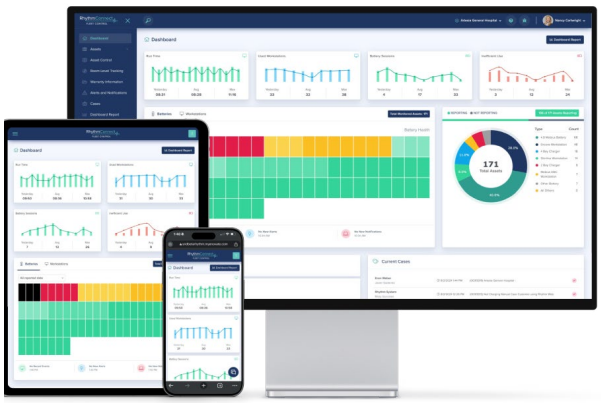
Bad actors behind modern cyber-attacks don’t just steal patient records–they can corrupt clinical data, shut down systems, and delay or even endanger patient treatment, producing measurable harm beyond fines and cleanup costs. Healthcare remains one of the most targeted sectors, with massive incident volumes in recent years that have disrupted operations and exposed millions of patient records.

Protecting patient information isn’t just a technical concern, it’s part of delivering safe and reliable healthcare. That’s why FIPS validation should be on your procurement checklist. By choosing tools and systems that meet FIPS standards, your organization takes a clear and confident step toward ensuring your facility is prepared, keeping data secure, preventing operational disruptions, building trust with patients and staff, and remaining focused on what matters most: delivering quality care.



ERGOTRON PRODUCT SPOTLIGHT

With FIPS 140-3 validation, Ergotron hardware and software features end-to-end secure architecture.



RhythmConnect
Fleet Management Software

Mosaic
LCD Cart

Mosaic
Laptop Cart

Ergotron's FIPS 140-3 validation is Level 1 for software. RhythmConnect fleet management software and RhythmConnect-ready assets that fall under Ergotron's FIPS validation include the Mosaic, Envoy, and Encore mobile workstations.

Ergotron's RhythmConnect software and RhythmConnect-compatible products include a FIPS-validated cryptographic module called the Ergotron Cryptographic Module. This module provides the cryptographic services needed to meet the strict industry requirements for FIPS 140-3, a security benchmark certification mandated by the U.S. federal government for products protecting sensitive but unclassified information using cryptography.

LEARN MORE

Click here for more information about Ergotron's platform security and FIPS validation.

FREQUENTLY ASKED QUESTIONS:

What is FIPS 140-3?

The U.S. and Canadian government standard that verifies proper implementation of cryptographic security.

What does it mean that Ergotron is FIPS 140-3 validated?

Ergotron's cryptographic module has been independently tested and officially certified by NIST and CSE (Certificate #5026).

How does FIPS validation benefit customers?

It reduces security risk, strengthens compliance, and supports a safer IT environment.

How do I check if a product is FIPS validated?

A FIPS validated module is public, searchable, and auditable. A product is FIPS validated in the U.S. only when it has been tested, verified, and issued a certificate by NIST. Confirm validation status directly on NIST's website under their validation program: *https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search*

Why is FIPS important for VA and federal healthcare?

It's required for cryptographic products used within federal systems.

Is FIPS the same as HIPAA compliance?

Healthcare organizations must meet a host of regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. While HIPAA doesn't explicitly say "must use FIPS 140-3", HIPAA guidance makes clear that encryption should use validated cryptographic mechanisms and that modules should be properly tested.

How long does Ergotron's FIPS validation last?

Active through July, 2029 with ongoing maintenance.

GLOSSARY OF TERMS

A

Auditable: When something can be reviewed, checked, and verified through clear records or evidence. In a security or compliance context, it indicates that actions, controls, or systems leave a trace that allows regulators or internal teams to confirm that required standards are being met

B

Breach: A security incident where sensitive, confidential, or personal information is stolen, accessed, or disclosed without authorization

C

Cryptographic Mechanisms: Methods and techniques that use mathematical algorithms to protect information and communications, ensuring services like confidentiality, integrity, authentication, and non-repudiation

Cryptographic Modules: A set of hardware, software, and/or firmware that securely implements security functions like encryption, digital signing, and key generation

CSE: Communications Security Establishment Canada (CSE) is the national cryptologic agency, providing the Government of Canada with information technology security

Cyber Incident: Any event that compromises the confidentiality, integrity, or availability of digital information or systems Cyberattack

D

Data Security: Methods and protections used to keep information safe from unauthorized access, misuse, loss, or theft, ensuring that sensitive data remains private, accurate, and available only to the right people

E

Encryption: The process of converting information or data into a code, especially to prevent unauthorized access

F

FIPS Validation: A process where a cryptographic module (hardware or software) is tested by an independent, accredited, third-party laboratory to ensure it meets the security requirements of a Federal Information Processing Standard (FIPS)

G

H

Healthcare IT: The technology systems and software used by healthcare organizations to manage patient information, support clinical care, and run operations, such as electronic health records, connected medical devices, and secure networks

HITECH: Health Information Technology for Economic and Clinical Health

I

Incident Response: A process an organization follows to detect, contain, and recover from a security incident, such as a cyberattack or data breach, in order to minimize damage and restore normal operations quickly

J

K

L

Level 1 Validation: Most basic level of FIPS security certification, where cryptographic software or hardware has been tested and verified to meet required encryption standards, without requiring physical tamper-resistance features

M

Module: Software or hardware component that performs encryption and decryption, protecting sensitive data by securely handling cryptographic functions such as key generation, encryption, and authentication

N

NIST: The National Institute of Standards and Technology is a non-regulatory agency within the U.S. Department of Commerce that promotes U.S. innovation and industrial competitiveness through measurement science, standards, and technology

O

Outside Threats: Security risks that come from outside an organization, such as hackers, cybercriminals, or other unauthorized parties attempting to access, disrupt, or steal data and systems

P

Q

R

Ransomware: Software used to extort money from an individual or organization by encrypting or otherwise blocking access to applications or files on a computer system until a sum of money is paid

S

Security Incident: Any event that jeopardizes the confidentiality, integrity, or availability of an information system or the data it holds

"Sensitive but Unclassified Information": Sensitive but unclassified (SBU) information in healthcare includes protected health information (PHI), personally identifiable information (PII), and other data that is not classified for national security but requires protection to prevent harm

SLED: State, Local, and Education government entities, including state agencies, city and county governments, and public schools and universities.

T

Third-Party Verification: A trusted, independent organization checks and confirms that a product, system, or claim meets specific standards, rather than relying on the vendor's own assurances

U

V

Validation: Proving that something meets a defined standard through independent testing and official confirmation, not just claiming that it does

W

Weak Encryption: Form of data protection that is easily broken or bypassed, making information more vulnerable to hackers or unauthorized access

X

Y

Z

RESEARCH RESOURCES

(2021, April 20) Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. National Library of Medicine. ***https://pmc.ncbi.nlm.nih.gov/articles/PMC8059789/***

(2020, May 13) Healthcare Data Breaches: Insights and Implications. National Library of Medicine. ***https://pmc.ncbi.nlm.nih.gov/articles/PMC7349636/***

