



Philips CT cybersecurity

Enhancing hospital security and patient data integrity

Overview

Philips recognizes the greater growing cybersecurity risks in an increasingly connected world, and works closely with providers, IT organizations, and customers to provide flexible solutions supported by security by design for its CT systems. This includes a multi-layered defense-in-depth approach for system protection.

Contents

- Background
- Designed with security in mind
- Defense-in-depth strategy
 - Physical protection
 - Firewall
 - Operating system hardening
 - Malware protection
 - Access controls
 - Patient data encryption
- System security features
- Password policy
- Protecting privacy
- Technology Maximizer
- Commitment to continuous cybersecurity development
- Additional resources

Background

All of us are facing the same challenge: How to protect your medical equipment from patient data breaches and ensure the medical equipment does not create a vulnerability in a customer environment? Like every industry that relies on increasingly connected computer networks, the healthcare industry is faced with a growing number of security breaches.

Whether these breaches are caused by hackers, malware or instances of unauthorized access, they present a threat to patient safety and data security. In addition, the cost of healthcare breaches can exceed several millions of dollars, and that cost can be compounded by civil suits and other legal actions, as well as by the damage caused to an institution's reputation. The average breach cost for healthcare is projected to be \$9.77 M in 2024, topping the chart for costliest industry for data breaches.²

According to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), 725 healthcare data breaches were reported in 2023, which equates to approximately 133,068,542 individuals who had their protected health information exposed or stolen.¹ This is more than twice the number of breaches reported in 2017 and more than triple the number of patient records exposed in 2022.¹

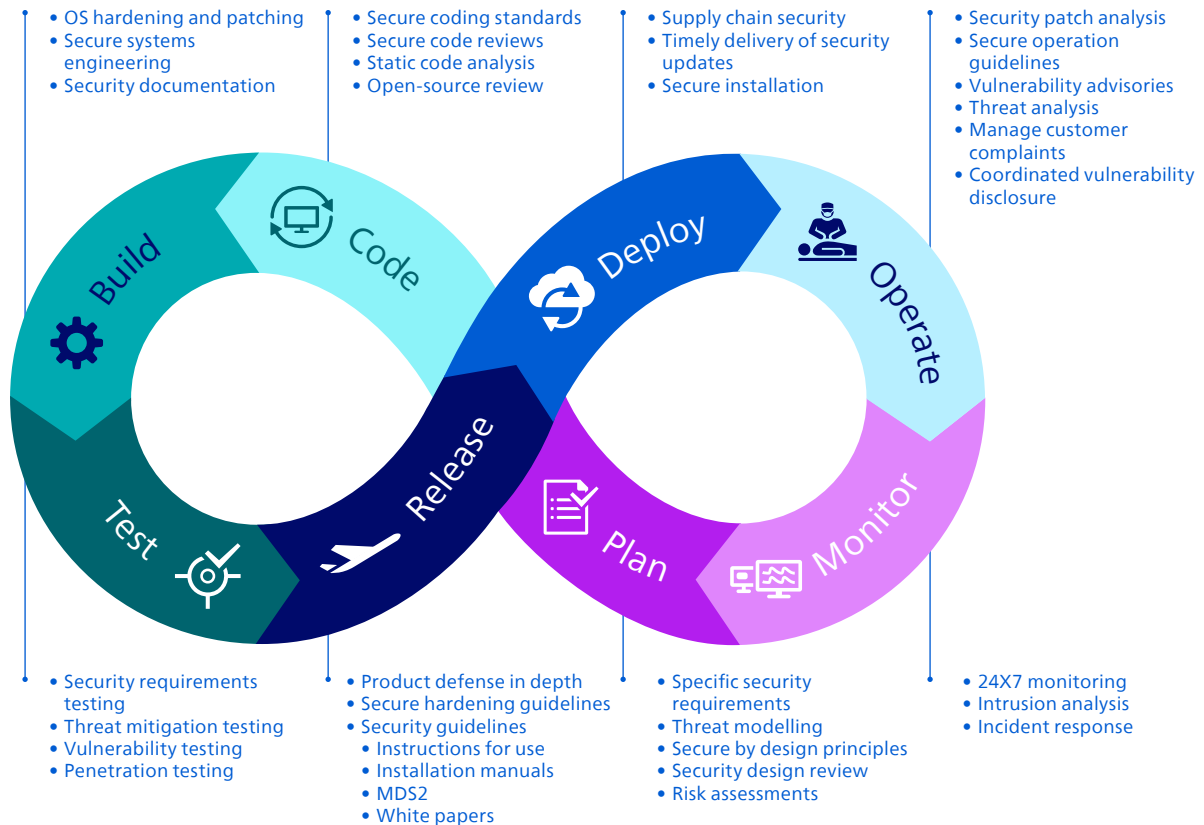
\$9.77 M

average cost of a 2024
healthcare data breach²



Philips CT is designed with security in mind

Secure by Design



Patient-related health information is one of the most important assets to be protected. In fact, many governments and industry organizations demand this confidentiality by statute. Philips takes strict security measures to help institutions guard the safety and security of patient-related data through a full lifecycle of product and services security support.

The Philips software development lifecycle (SDLC) ingrains security in every phase of the product lifecycle. Through rigorous processes such as product security risk assessment (PSRA), data protection impact assessment (DPIA) and continuous product security training, we prioritize security from architecture and design to post-market support.³

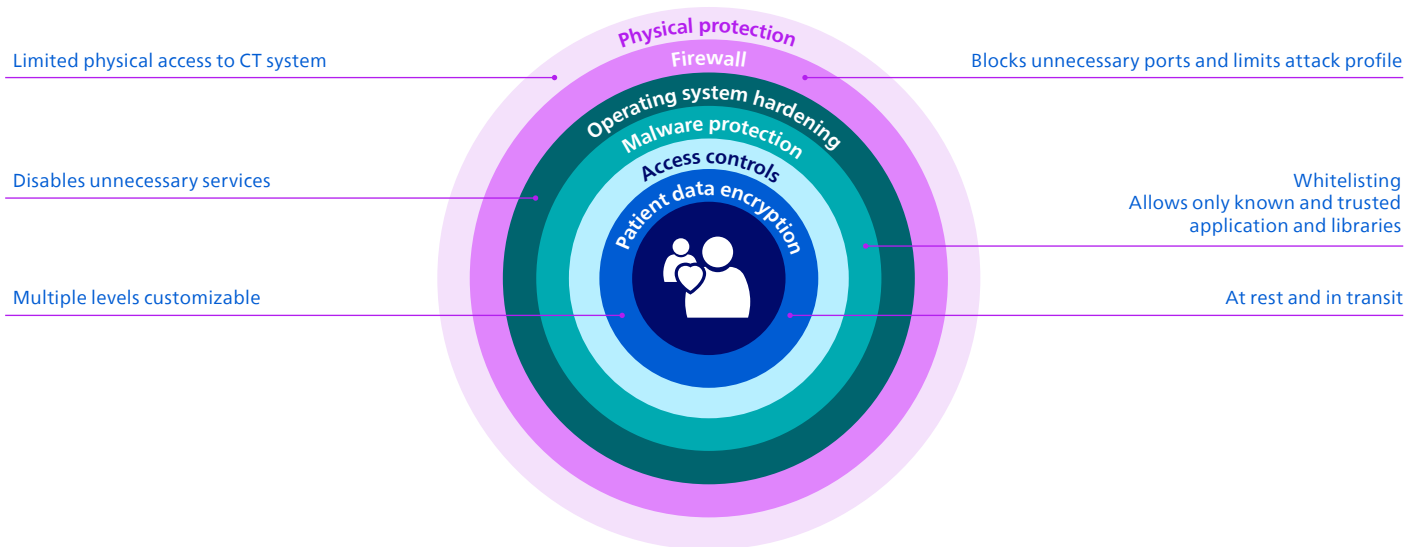
Security aligned with recognized standards such as:

- | | |
|-----------|----------------|
| IEC 80001 | ISO 27001 |
| ISO 27034 | ISO 27002 |
| ISO 27018 | NIST SP 800-53 |

In addition to regulatory requirements such as FDA pre/post-market cybersecurity guidance, National Medical Products Administration (NMPA) and General Data Protection Regulation (GDPR), the Philips CT security framework product development is based on IEC 80001 series, which has several standards that contribute to product security requirements, including IEC TR 80001-2-2, IEC/ISO 27001, IEC/ISO 27034 and NIST SP800-53. We carefully follow international laws ranging from the US Health Insurance Portability and Accountability Act (HIPAA) to the GDPR.

Defense-in-depth strategy

The Philips CT product security framework employs a defense-in-depth strategy, incorporating multiple layers of security controls spanning application, computing, data and network security. These controls, aligned with global security standards, are meticulously integrated into our medical solutions to significantly reduce cyber threats.

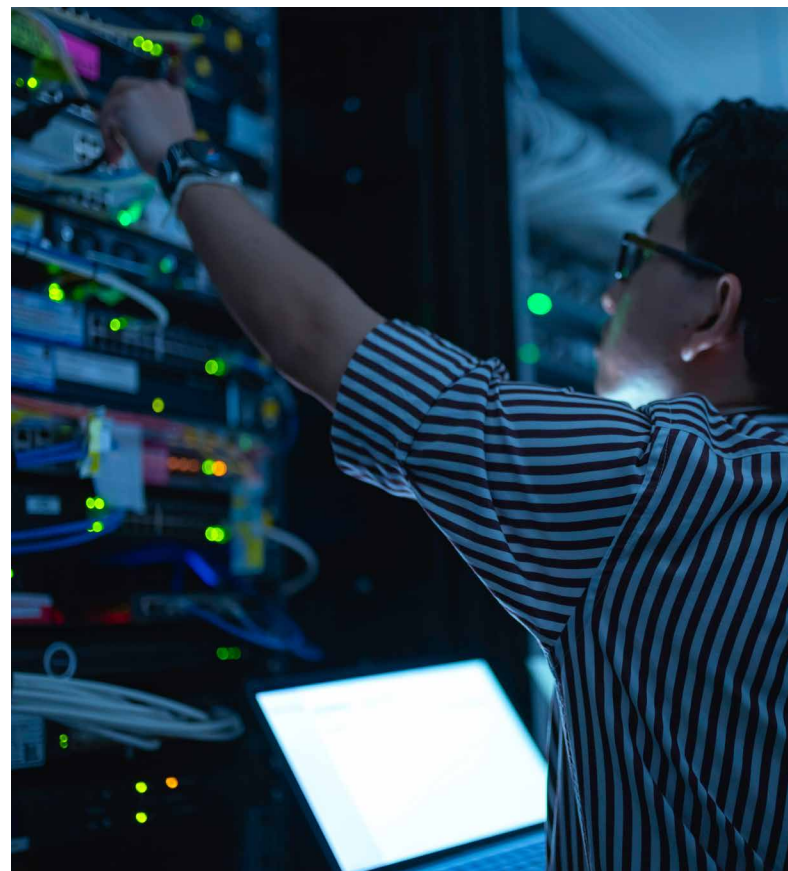


Philips applies the principle of defense-in-depth security for its Philips CT products using the Microsoft Windows operating system for the Philips iPatient-S Software platform, implementing a security strategy comprised of six layers of protection.

Each of these layers plays an important role in helping you defend against hackers, defend against malware and prevent unauthorized access.

1. Physical protection

Attacks are greatly limited by software and hardware measures, and this layer ensures that human behavior, hospital processes and logistics make the systems watertight from a security point of view. Customers are instructed to apply physical security controls for CT systems in the instructions for use (IFU) or technical reference guides (TRG).



2. Firewall

Strict firewall polices limit traffic to and from the CT system by blocking all unnecessary ports, preventing communication with unauthorized computers, limiting the attack profile that malicious hackers may try to exploit. A pre-configured firewall allows only authorized network traffic to CT systems for clinical and service usage, while blocking unauthorized network traffic through ports and protocols.

3. Operating system hardening

Similar in principle to firewalls, operating system (OS) hardening involves identifying all unnecessary services and functions that are included within the operating system and disabling those not required by the CT system. OS hardening reduces the attack surface by eliminating those services that may become vulnerable over time. This set of security controls implemented in the system includes disabling unnecessary services, unused features and applying security controls following Security Technical Implementation Guides (STIGs).

OS security patches will be available in 2025 for all Windows 10-based systems. Philips CT plans to release OS security patches based on a monthly security vulnerability assessment. For Spectral CT 7500 5.2 and CT 5300 OS patches may be installed remotely.

4. Malware protection

The traditional method of malware protection, anti-virus (AV) software, requires frequent updates to keep pace with new viruses and malware being released every day. Hospitals risk being attacked before AV software has addressed new malware. To mitigate this risk, Philips has implemented the feature of application-control policies, with white-listed rules which will allow only trusted and signed executable files, scripts and dynamic link libraries files. Philips CT systems use application whitelisting to allow only authorized software to execute while blocking unauthorized software. This mechanism supports connected and isolated systems because it does not require signature updates, replacing traditional AV software that requires frequent updates and maintenance.



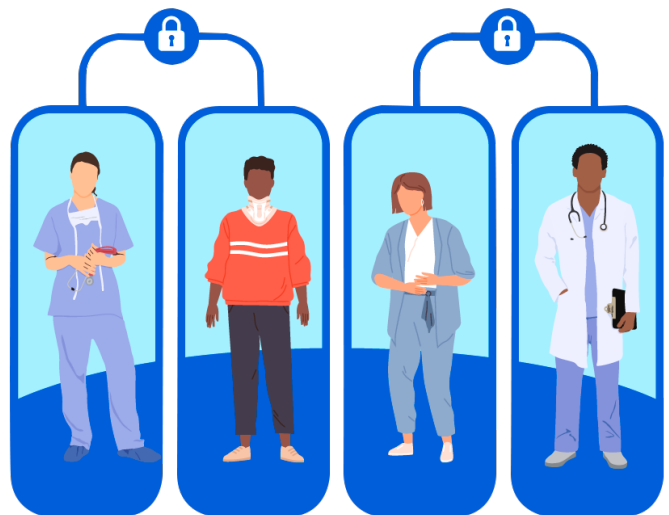
5. Access controls

An estimated 22% of security breaches are due to human error.² To help control access to Philips CT system data, privileged access has been implemented using predefined roles to restrict clinical and administrative access. Password complexity rules can be adapted to comply with the hospital password policy. Role-based access control manages different levels of permissions for system authentication and authorization. A multi-factor authentication mechanism is required for administrators. A configurable password policy is maintained, and lightweight directory access protocol (LDAP) authentication is supported in Spectral CT 7500 version 5.2 and CT 5300.



6. Patient data encryption

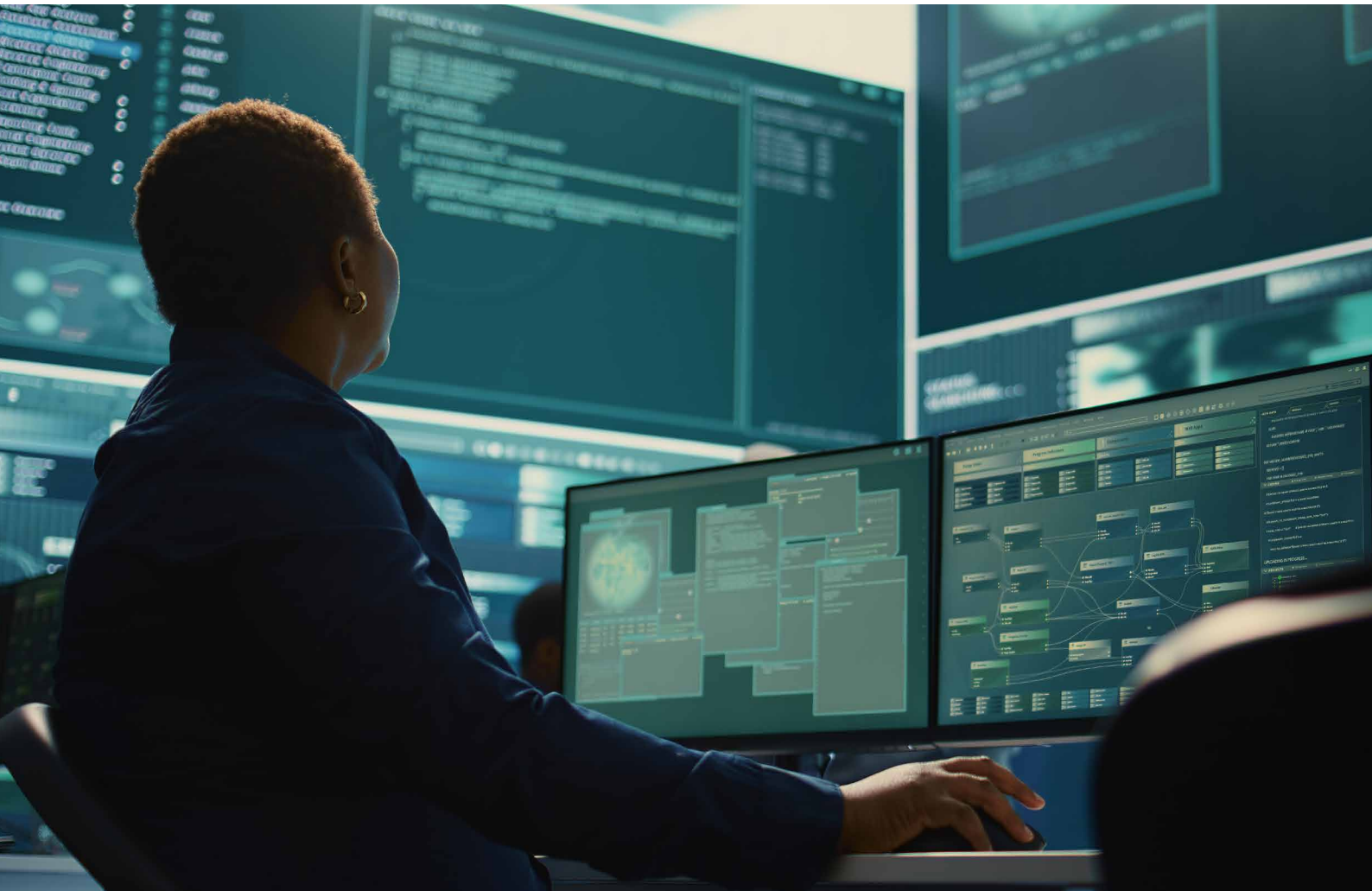
All patient data stored on Philips CT hard drives can be encrypted based on hospital and regulatory requirements. Patient data that is exported to removable media can be de-identified prior to export. Data at rest encryption is supported in all Philips CT systems with full disk encryption using Windows BitLocker. Spectral CT 7500 version 5.2 and CT 5300 also support data in transit encryption using DICOM over transport layer security (TLS) and removable media encryption using BitLocker To Go.

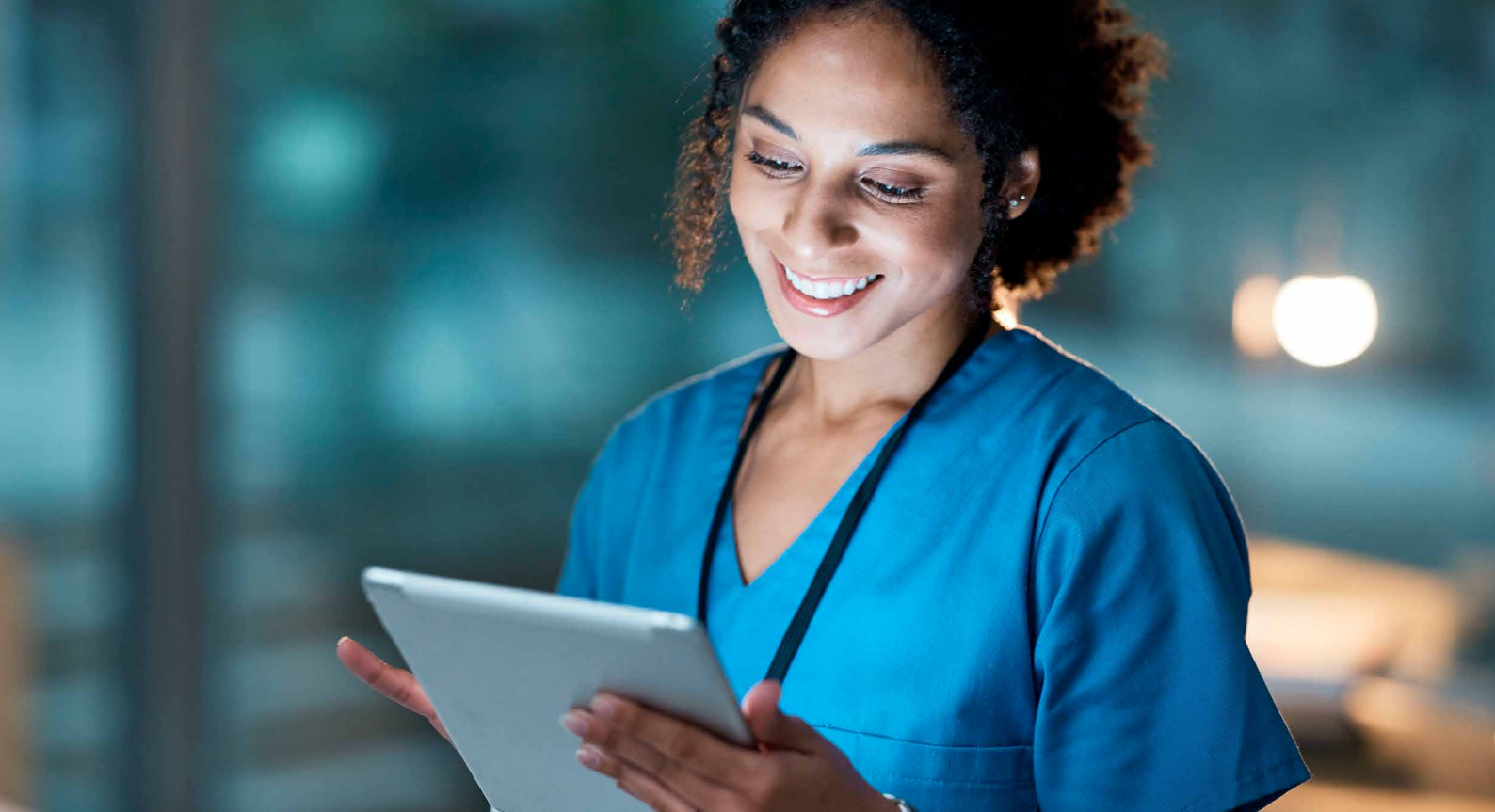


System security

Security feature summary	All Philips CT systems with Windows 10 OS and iPatient-5 software	Philips CT 5300	Philips Spectral CT 7500 5.0	Philips Spectral CT 7500 5.2
Secure login and authentication				
No hardcoded passwords	●	●	●	●
Strong passwords by default	●	●	●	●
Emergency login available with a password	●	●	●	●
Password complexity rules configured by local administrator	●	●	●	●
Screen blanking can be password protected		●		
Central user management				
Active directory domain joins and LDAP authentication				●
LDAP authentication without domain join		●		
Role-based Access control				
Role-based Access control	●	●	●	●
Least privilege access	●	●	●	●
OS Security Patching				
OS patches remotely distributed		●		●
OS Patches available through services or can be installed by local administration users or service users	●			
Data encryption				
Data at rest encryption	●	●	●	●
Data in transit encryption using DICOM over TLS 1.2		●		●
Removeable media encryption		●		●
OS hardening				
Group policy hardening based on DoD STIGs for Windows 10	●	●	●	●

Firewall				
Preconfigured firewall allows only authorized network traffic	●	●	●	●
Firewall dashboard tools allow the Philips Service User to manage firewall exceptions	●	●	●	●
Allows view of deviations from factory settings	●	●	●	●
3rd-party software vulnerability				
Enhanced mitigation of 3rd-party software vulnerabilities by migrating to supported versions of software	●	●	●	●
Basic input/output system (BIOS)				
Password- protected BIOS	●	●	●	●
Disable boot from external devices	●	●	●	●
Physical security				
Locked cabinet	●	●	●	●





Password policy

The system shall support user passwords of a configurable length, with a default minimum of eight characters and up to at least 14 characters and contains at least three of following four types of characters:

- Uppercase characters
- Lowercase characters
- Numeric characters
- Special characters

The system shall allow the local administrator to configure the number of login attempts for "Clinical user account", "Local administrator user account" and "O-level service user account" in the following range:

3 >= to <= 10 attempts: with default value of 5 login attempts, after which the system shall lock the account.

The system shall allow local administrator to configure password validity duration for "Clinical user account", "Local administrator user account" and "O-level service user account" in the following range:

30 >= to <= 180 days: with default value of 180 days.

The system shall allow local administrator to configure password character length for "Clinical user account", "Local administrator user account" and "O-level service user account" in the following range:

8 >= to <= 14 Chars: with default value of 8 characters.




Protecting privacy

With Philips focus on health technology, data privacy and security have become strategically vital, as health data is among the most sensitive types of personal data. Our strategic ambition to make the world healthier and more sustainable through innovation relies heavily on the use of this data, and public trust is paramount. Our commitment to privacy goes beyond regulatory compliance, and we embed privacy and data protection controls throughout the lifecycle of all data.

Privacy and data protection are an integral part of our general business principles whereby we submit ourselves to several commitments such as:

- The implementation of binding corporate rules (BCRs) that provide a baseline for privacy protection within Philips worldwide and allow international data transfer between Philips group companies.
- Implementation of a privacy program and governance structure which embeds privacy and data protection in the company.
- Limiting collection of data, and where appropriate, obtaining consent from individuals.
- Notifying individuals as to how collected data will be used and allowing them to exercise their rights.
- Taking appropriate steps to maintain the accuracy and relevance of the data.
- Protecting personal data using appropriate security safeguards

[For more information regarding Philips privacy policy, please visit Philips global privacy page | Philips](#)



“What we have right now... is still a very fragile healthcare ecosystem, is how I would describe it. And we need to move to a better place where devices are patchable, that they’re updateable, that they can stand an exploit, an attack or breach and still function safely and properly, and that the hospital itself and manufacturers and, again, the sector at large is resilient to be able to withstand that and deliver continuity of care.”⁴

Susanne Schwartz, MD, acting director,
Office of Strategic Partnerships and
Technology Innovation, FDA Center for
Devices and Radiological Health.

Technology Maximizer

Keeping Philips CT systems up-to-date and secure can be very challenging. However, as every clinician and hospital leader know, upgrades are vital to the performance and operational value of systems.

Technology Maximizer helps you stay clinically advanced to drive better patient outcomes and staff experience. It also allows you to predict your budget while keeping systems up to date, enhancing workflows, improving image quality and enhancing cybersecurity.

Technology Maximizer is available across selected CT systems.

 <h3>Stay clinically advanced</h3> <p>Stay clinical advanced & competitive Access system upgrades and innovations on release, instead of buying new systems hardware or software packages each time.</p> <p>Keep systems up-to-date Improve your technology – all while enhancing workflows and keeping systems up-to-date.</p>	 <h3>Cyber-Security</h3> <p>Non-obsolescence Protect your operating system software and PC hardware from becoming obsolete.</p> <p>Stay protected Keep system release versions and security controls up-to-date and to reduce cybersecurity vulnerabilities and risks.</p>	 <h3>Patient & staff experience</h3> <p>Improved staff satisfaction Empower employees by working more efficiently with latest technology, resulting in less pressure and more confidence.</p> <p>Fleet standardization Standardize and manage fleet at latest technology release level, enabling staff to work with consistent workflows and functionality.</p>	 <h3>Cost predictability</h3> <p>Upgrades at predictable budget Plan a predictable budget for upgradability throughout the system lifecycle.</p> <p>Flexible payment with Capex or Opex Choose your way of investment – pay as capital expense or pay over system lifecycle with planned operational expense.</p>
--	---	---	--

Eligible CT systems⁵



Incisive CT



CT5300



Spectral CT7500

Stay up to date, clinically advanced and secure with Technology Maximizer

Enjoy peace of mind

86% of customers agreed Technology Maximizer helped their hospital stay competitive, cyber secure and addressed staff satisfaction.⁶

Save up to

50% on the cost of upgrades⁷



Our commitment to continuous cybersecurity development

In line with the need to constantly increase the security of our products, Philips continues to examine and re-engineer existing products to best meet the requirements of our security-minded customers. We are deeply engaged in creating the products of tomorrow based on fundamental security principles.

We will continue to work closely with providers, IT organizations, and customers to provide flexible solutions to today's problems even as we create new products that offer security by design.

Additional resources

- Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (fda.gov)
- Postmarket Management of Cybersecurity in Medical Devices | FDA
- Principles and Practices for Medical Device Cybersecurity (imdrf.org)
- 2024 Data Breach Investigations Report | Verizon
- 2024-dbir-healthcare-snapshot.pdf (verizon.com)
- <https://www.philips.com.au/c-dam/corporate/security/master/mh01/452299161571-philips-prs-security-brochure-may-2021.pdf>

Let's review your CT system security. Talk with your Philips representative today.

[Find out more about Philips product security](#)

1. <https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/>
2. <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>
3. <https://www.usa.philips.com/healthcare/about/customer-support/product-security>
4. <https://www.careersinfosecurity.com/medical-device-security-fdas-view-a-12748>
5. Subject to market availability.
6. GemSeek research commissioned by Philips, N=151 (USA).
7. During the term of the agreement, for CT systems in scope, Philips Technology Maximizer delivers major upgrades. Purchasing these upgrades individually could cost up to twice the cost of the Technology Maximizer agreement.

