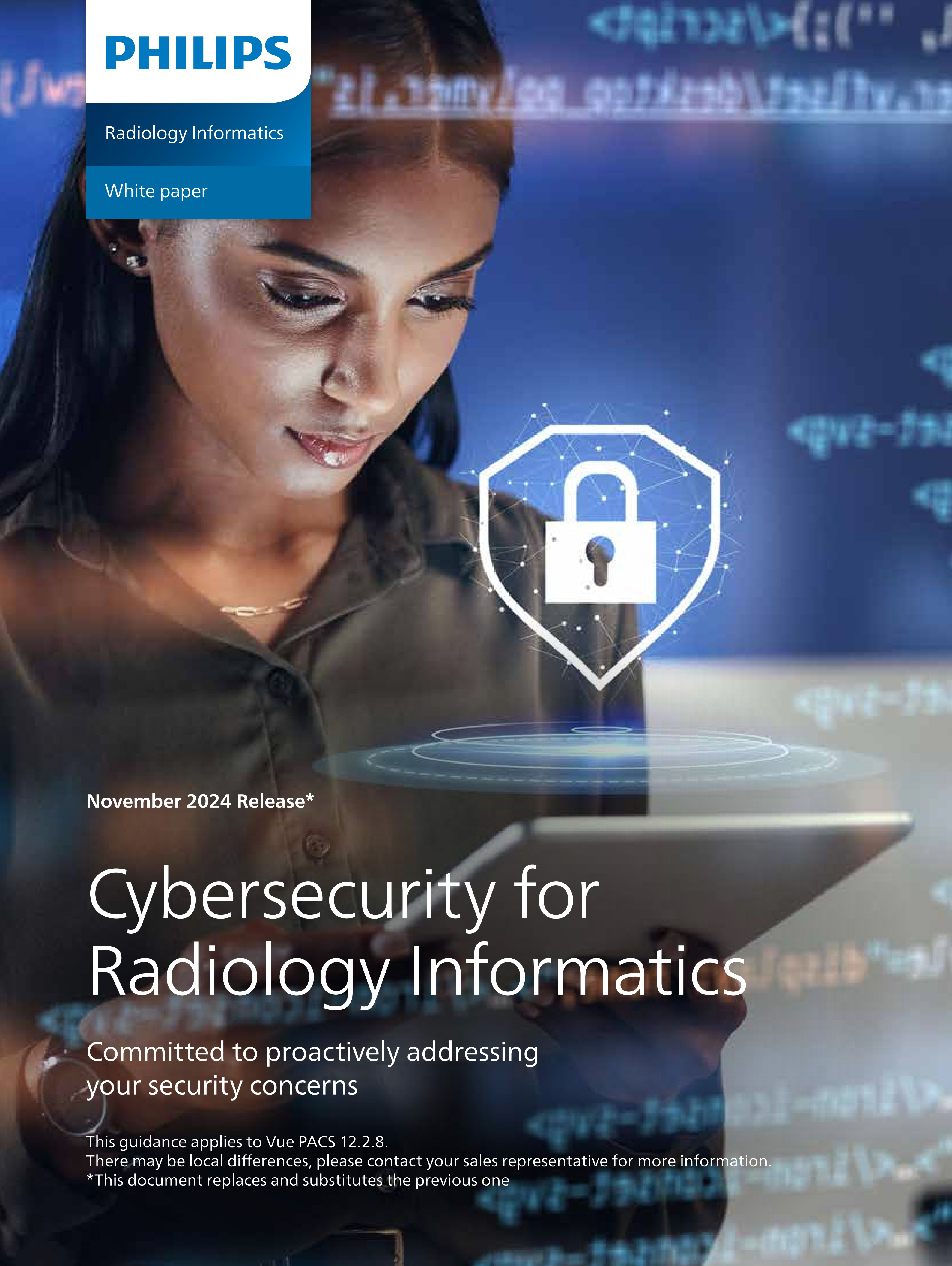


PHILIPS

Radiology Informatics

White paper

November 2024 Release*

Cybersecurity for Radiology Informatics

Committed to proactively addressing your security concerns

This guidance applies to Vue PACS 12.2.8.
There may be local differences, please contact your sales representative for more information.
*This document replaces and substitutes the previous one

Table of contents

Executive summary

The convergence of healthcare and technology has revolutionized the medical field, offering advanced solutions to improve patient care and reduce costs. However, this progress has also heightened the vulnerability of medical solutions to cyber threats. As interconnected systems provide new opportunities for hackers to exploit vulnerabilities, protecting patient data and the integrity of healthcare systems has become a critical concern.

This whitepaper delves into Philips' comprehensive approach to cybersecurity, emphasizing how it is adopted in Radiology Informatics and highlighting the need for ongoing vigilance in the face of evolving threats. It outlines our commitment to meeting the stringent requirements of medical devices' regulations, which mandates a layered defense strategy in the design of medical solutions.

A comprehensive approach to security requires consideration of three different domains: people, processes, and technology. Philips implements control across these three domains covering the whole spectrum of identify, protect, detect, respond, and recover to protect confidentiality, integrity, and availability. Moreover, Philips takes a leading role in collaborating with regulatory agencies, industry partners, and healthcare providers to close security loopholes and implement safeguards, playing a pivotal role in creating global standards as part of cybersecurity task forces, including the International Cybersecurity Guidance initiative by the International Medical Device Regulation Forum (IMDRF).

In the intricate ecosystem of cybersecurity within healthcare organizations, the responsibility for protecting systems from cyberattacks is a shared endeavor between the manufacturer and the customer. By integrating robust security measures into their products, such as encryption protocols, access controls, and regular software updates, manufacturers aim to fortify their systems against potential vulnerabilities and mitigate the risk of cyberattacks. However, customers also bear responsibility for safeguarding the systems they deploy within their organizations. This entails implementing proper security configurations, regularly updating software patches, and conducting thorough risk assessments to identify and mitigate potential vulnerabilities within their network infrastructure.

Effective cybersecurity in healthcare requires collaboration and shared accountability between manufacturers and customers to protect the integrity, confidentiality, and availability of critical patient data and healthcare services. This whitepaper serves as a guide for radiology healthcare professionals navigating the complex landscape of cybersecurity, offering insights into Philips Vue PACS robust security measures and our unwavering dedication to protecting patient data and ensuring the integrity of healthcare radiology systems.

How to apply industry standards to protect patient information

Product security

Patient-related health information is one of the most important assets you need to protect. In fact, many governments and industry organizations demand this confidentiality by statute. We must take strict security measures to guard it.

Philips Product Security provides a full lifecycle of product and services security support. This lifecycle begins with assertive acceptance of NIST, ISO, DICOM, IHE and DIACAP (now RMF) as valuable sources of security standards. Additionally, we carefully review international laws ranging from HIPAA to the General Data Protection Regulation (EU) 2016/679 to identify product requirements and implement the latest guidance.

Philips' 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 help mitigate cyber threats effectively.

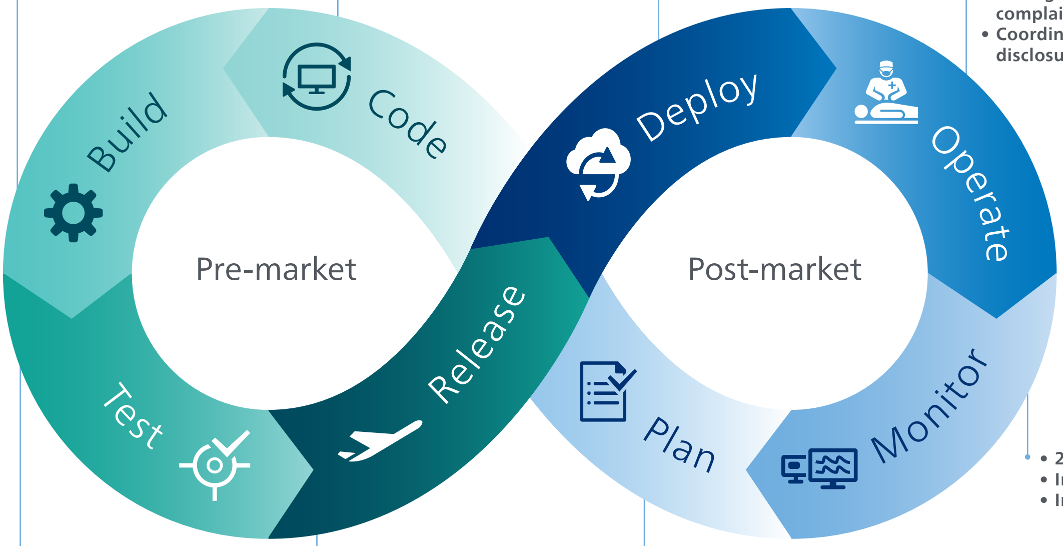
Furthermore, our Secure Development Lifecycle (SDLC) ensures that security is ingrained in every phase of the product lifecycle. Through rigorous processes such as Product Security Risk Assessment (PSRA), Data Protection Impact Assessment (DPIA), and continuous product security training, we prioritize security from architecture and design to post-market support.

- OS hardening and patching
- Secure systems engineering
- Security documentation

- Secure coding standards
- Secure code reviews
- Static code analysis
- Open-source review

- Supply chain security
- Timely delivery of security updates
- Secure installation

- Security patch analysis
- Secure operation guidelines
- Vulnerability advisories
- Threat analysis
- Manage customer complaints
- Coordinated vulnerability disclosure



- 24X7 monitoring
- Intrusion analysis
- Incident response

- Security requirements testing
- Threat mitigation testing
- Vulnerability testing
- Penetration testing

- Product defense in depth
- Secure hardening guidelines
- Security guidelines
  - Instructions for use
  - Installation manuals
  - MDS2
  - White papers

- Specific security requirements
- Threat modelling
- Secure by design principles
- Security design review
- Risk assessments

By embedding a culture of “Secure by Design” within our organization, we strive to deliver resilient solutions that meet the evolving security needs of our customers. Philips remains committed to collaborating closely with healthcare providers and IT organizations to address current challenges and develop innovative, security-centric solutions for the future.

In line with industry-standard best practices, the cybersecurity measures we implement in radiology informatics include:

- Physical security
- Operational security
- Procedural security
- Risk management
- Security policies
- Contingency planning

The practical implementation of technical security elements varies by site and may employ several technologies, configurations and software solutions. As with any computer-based system, protection can include firewalls, network segmentation and other security devices between the medical system and your network. Perimeter and network defenses are essential elements in a comprehensive medical device security strategy.

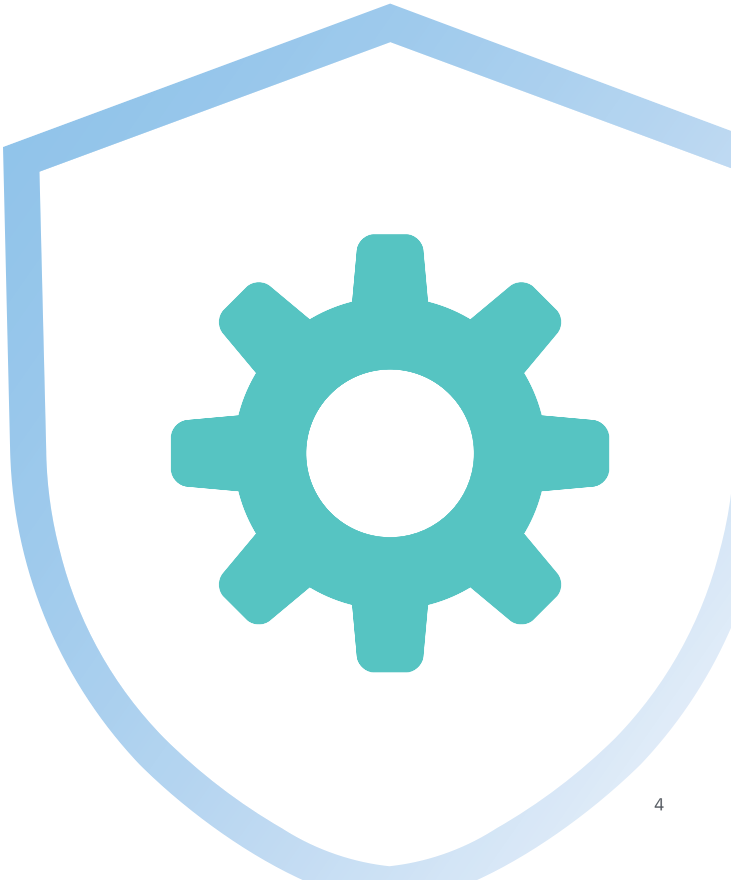
At each phase of the secure development lifecycle, we address leveraging this methodology, requirements and controls, including:

- Product Security Risk Assessment (PSRA): Identify and implement key security controls in our applications. Prevent application security defects and vulnerabilities
- Threat Modelling: Identify requirements, pinpoint potential vulnerabilities, quantify threat and vulnerability criticality, and prioritize remediation methods
- Privacy Impact Assessment processes: Aligning with privacy regulations and enhancing overall data protection measures
- Static code analysis: We use BlackDuck and SonarQube, for open-source components and code quality
- Third-party Software Bill of Materials (SBOM) analysis: Provides transparency into software composition, enabling effective vulnerability management, enhancing supply chain security, supporting incident response and forensics, and improving risk management practices
- Ethical penetration testing with automated and manual testing
- Continuous product security training across the Philips organization

Moreover, we also implement additional security measures to help satisfy the current regulatory demands and industry best practices, such as:

- Adherence to product security and privacy standards aligned with the FDA-recommended ISO/IEC-80001 and serving as the foundation for the 80001-2-2 standard
- Development of customer-facing information such as the industry-standard Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- Adherence to FDA guidelines on Premarket Management of Cybersecurity in Medical Devices and FDA Post-market Management of Cybersecurity in Medical Devices

The Philips cybersecurity team revises privacy and security policies annually at a minimum and adjusts them to meet the ever-changing security landscape. We also utilize industry-standard protocols and formats for the storage, transmission and protection of images and other data with high focus on security and privacy. Many security tools and configuration parameters are available to help our users meet their local regulatory requirements. Philips has been and will continue to be committed to addressing regional and country-specific requirements as needed.



Third-party management

Supplier management

Philips Vue PACS has implemented supplier security lifecycle as part of the broader supplier management process.

The organization relies on **Supplier Quality** and **Supplier Security** functions working together to help ensure that supplier security and quality requirements are met.

- **Supplier Quality:** This quality function is tasked to manage all suppliers to meet quality requirements and the monitoring process. Once suppliers are qualified, they are entered into the **Approved Supplier List** (ASL) .
- **Supplier Security:** This function manages those suppliers classified during procurement process, where additional security controls must be met due to its interactions with information security.

During all phases of the supplier management process a due diligence is performed by a continuous engagement of Philips teams to collect and evaluate security information from suppliers, define a proper security service level agreement and define roles and responsibilities of the supplier in handling security incidents.

Governance of SBOM (Software Bill of Material)

Effective SBOM management is crucial in cybersecurity, serving as a foundational tool for understanding and mitigating software-related risks. By providing detailed insights into the components and dependencies within a system or application, SBOM enables organizations to promptly address vulnerabilities, track patching status, and respond swiftly to emerging threats. This proactive approach enhances resilience against cyberattacks, minimizes the likelihood of exploitation through known vulnerabilities, and bolsters overall security posture.

Philips has a specific SBOM governance program that comprises the generation of an SBOM on all the products, the integration of the SBOM tooling and processes into the software development/build process, and the creation of a Security Risk Summary for each product.

The Philips Product Security SBOM process is integrated into the system development lifecycle for each product developed by Philips.

How to protect data from malicious accesses

Malware, antivirus and OS patching

Malware and antivirus

In the increasingly interconnected landscape of healthcare technology, updating operating systems is crucial to protect against cyberattacks. It ensures that vulnerabilities are patched, reducing the risk of exploitation by malicious actors seeking to compromise system integrity and patient data.

In case of a malware attack, having installed antivirus software is crucial for protecting your device. Installing antivirus software and keeping your OS updated is the first step to protect your data.

Antivirus
Malware – short for malicious software – encompasses a wide range of harmful programs designed to disrupt, damage or gain unauthorized access to your computer or data. These threats include viruses, worms, trojans, spyware, ransomware and more.

Our physical and network security solutions for radiology informatics support antivirus tools, and provide formal guidelines for virus scanning our software.

The updating and operational management of the antivirus solution and its virus definition file(s) is the responsibility of the customer, who is free to select any antivirus software it wish to run on the medical device.

Philips formally qualifies the image management system with CylancePROTECT® and TrendMicro*, which focus on providing malware protection from our servers using whitelisting technology.

Whitelisting identifies all trusted software allowed to execute on the equipment. The protection software prohibits the execution of untrusted software, effectively blocking malware before damage is done. Rather than relying on frequent updates required by the reactive antivirus software to remain up-to-date, it offers proactive protection against a wide spectrum of malware and malware alterations by only allowing known executables.

Patching process

The patching process* within the Philips Security Operations Center (SOC) follows best practices tailored to the unique demands of healthcare IT environments. In the first stage, our team performs an in-depth assessment to evaluate the criticality of systems, considering factors like patient data sensitivity and regulatory compliance requirements.

The assessment informs our patch management policy, which outlines procedures for regular updates, emergency patching and rollback protocols. Using automated tools specifically designed for healthcare environments, we prioritize risk mitigation to help ensure integration with our systems and compatibility with regulatory standards.

To help reduce the risk of compatibility issues and support swift deployment, our patching process emphasizes collaboration among Philips and other vendors to obtain pre-validated patches tailored to our software. Before deployment, patches undergo rigorous testing in a dedicated environment that mirrors our production setup, which supports thorough evaluation of their impact on system stability and patient data integrity. Automated deployment tools streamline the patching process, scheduling updates during off-peak hours to minimize disruption to clinical workflows, while maintaining high availability through failover mechanisms.

Real-time monitoring and reporting enables continuous oversight of patch application and identification of any issues that may arise. To verify patch effectiveness and promptly address any remaining security gaps, we regularly perform vulnerability scanning. Our team remains vigilant, continually refining our patch management practices through training, incident response exercises and adherence to evolving industry standards.

By adhering to these best practices, the Philips SOC supports that our Vue PACS software remain secure, compliant and highly available, while safeguarding patient data and supporting uninterrupted clinical operations.

*Availability restricted to some geographical areas

Hardening and data security

Hardening

Vue PACS design enables security system hardening best practices such as CIS benchmark 3.1.

The system is designed for hardening access control and uses least-privilege principle by default. The client application uses session timeouts to lock out users not actively working in the system. Windows Server Host Firewall is enabled and configured by default to block any network traffic except the ports utilized by the application.

Encryption

Vue PACS provides encryption through several different methods to enhance information protection and security.

Data at rest

The encryption at rest is supported by self-encrypted drives (SED) for encryption of data and images which must be supplied by the customer or purchased through Philips. This is not a standard approach in the commercial space but has been implemented for the Department of Defense (DoD) under the risk management framework (RMF) hardening requirements.

Data in transit

To ensure encryption in transit of communications, we use encryption protocols to communicate between endpoints and servers. The site will need to supply SSL/TLS certificates for those services that require encrypted communications.
The following primary services/protocols offer encryption as part of their communication processes:

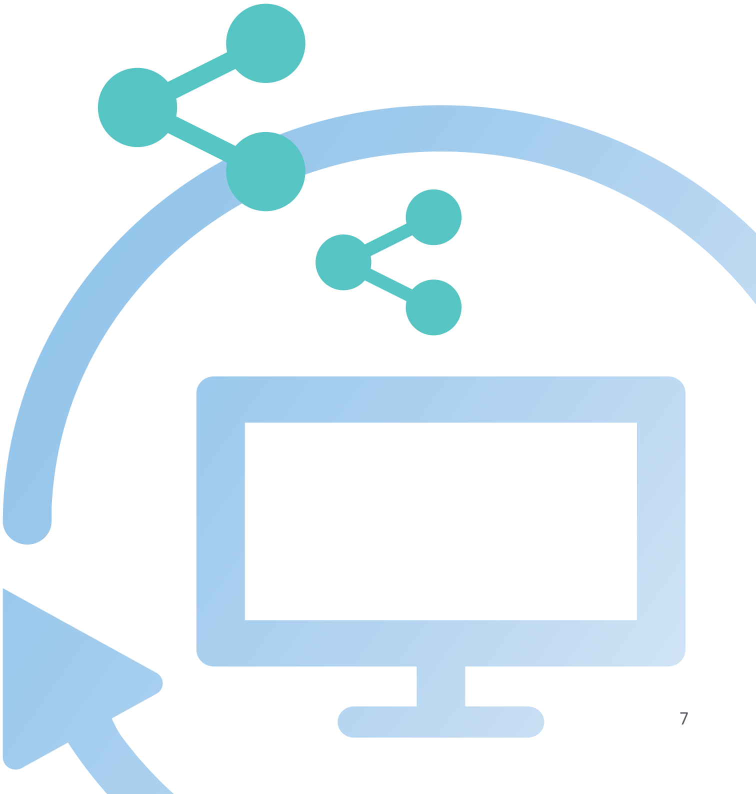
- CONN (proprietary protocol) for internal services
- DICOM to communicate with devices that support the DICOM standard and HE ATNA profile, which enables secure transmission of ePHI between configured DICOM devices
- HTTPS for web services

Vue PACS supports de-identifying data for allowing saving images, while removing any identifying marks of the patient, such as patient name and patient ID.

Data integrity

When a new stored study is important to guarantee the integrity of the data, Philips PACS uses several mechanisms to overcome missing information or non-standard fields coming from the modalities. This supports the correct identification of the patient and the consistency of the archives. These include:

1. **DICOM Parsing -** Allows changing the DICOM data before it is written to the database and storage. Can be useful to overcome non-standard behaviors
2. **Patient Matching -** Provides that studies are associated with the correct patient and order
3. **RIS Synchronization -** Provides the patient details are the same in the RIS and in the PACS
4. **DICOM validation -** The archive validates that the tags of the study meet the DICOM standard
5. **Validation table -** If a tag is found as non-valid or if the patient is invalid a report of the rejection is inserted to a specific table in the database
6. **Archive Compare -** The archive compare is a utility used to compare the current contents of two archives. The utility compares the meta-data of the two archives for a given range of study date
7. **Data integrity constraints associated with the oracle database**



Application-level security

User and password management

The system provides an extensive mechanism to manage user authentication and authorization and supports local or federated authentication using SSO through the user management administration tool.

Access control is comprised of permissions, profiles and features, and data access control. To prevent unauthorized access to restricted information or unavailable features for that user, permissions and profiles are checked at the login and at any access to a system resource.

To support sites with various authentication needs, the system provides different authentication mechanisms such as:

- Local user authentication using local user's repository
- External Lightweight Directory Access Protocol (LDAP) user's repository
- Security Assertion Markup Language (SAML)
- OpenID Connect
- Smart card

The system uses a Role-Based Access Control (RBAC) mechanism to limit the users and provide versatility in the different entity layers:

- Each user is assigned to only one role
- Each role defines the user or group privileges, and it is configurable and set by the administrator
- Roles can be assigned to groups defined by the customer and created locally on the system or mapped to an existing LDAP group owned by the customer

Permissions can be granted to the entire system, specific group or specific user. In addition to functionality permissions, the system can also limit user access to specific data, including data originated from a specific site, department or modality.

Privacy and data protection

Philips places a high value on privacy and data protection. For all propositions that involve the processing of personal data, including HealthSuite Imaging*, we have implemented data protection by design and by default principles.
Our commitment to safeguarding privacy is evidenced by the incorporation of appropriate controls in the early stages of product development, as well as throughout its lifecycle.

Our approach to privacy and data protection is based on the following principles:

- **Security:** We are committed to ensure the security of the personal data entrusted to us. We operate under global security policies that guide our activities to protect against vulnerabilities and manage any incidents
- **Compliance:** We handle all personal data with integrity in compliance with all applicable privacy regulations of the countries in which we operate
- **Beneficial:** We aim to create innovative solutions that benefit our customers, patients and society as a whole. We use your personal data in line with your reasonable expectations

For more information about how Philips approaches privacy and data protection – and how we comply with relevant data protection laws – please see the following resources:

- **Privacy at Philips**
  www.philips.com/a-w/privacy.html
- **How Philips complies with the GDPR**
  www.philips.com/a-w/privacy/gdpr.html

We take our responsibility to handle personal data seriously and constantly strive to improve our practices with the aim to exceed our customers' expectations in terms of data protection and security.

* The use of cloud services can be subject to local laws and regulations.
HealthSuite Imaging may not be available in all regions. Please consult your local Philips representative for more details

How to arrange secure connection for support

Philips secure remote service access

With increasing privacy concerns and strict government regulations to protect electronic patient and health information against unauthorized access, healthcare organizations need reliable solutions to protect their local networks and on-premises healthcare devices and data against any possibility of unauthorized access.

For optimum security and control, a remote service solution must:

- Provide a single point of entry into your site from a single point of access at Philips
- Prevent all other remote access methods to eliminate the risk of social engineering attacks and ensure only authorized Philips service technicians have access to your network and devices
- Safeguard patient data in compliance with governmental guidelines and regulations.
- Provide a timely audit trail of all service operations

To that end, Philips continuously researches best practices and tests technologies and architectures for providing secure remote service – while considering guidelines and regulations including HIPAA (USA), PIPEDA (Canada), EC 95/46 (EU), GDPR and its country-specific implementations (EU), HPB 517 (Japan) and many others. Philips is fully committed to providing superior customer service and support by leveraging the latest standards-based technologies built to the highest network-centric secure standards.

Philips Secure Remote Service Access (SRSA) provides secure access over the internet via a fully encrypted, point-to-point Virtual Private Network (VPN). It employs the least-privilege access principle to ensure essential and authorized-only access to medical devices and reports all activity for audit purposes.

SRSA access is only permitted for Philips employees appropriately trained to support your medical applications and devices. Access is contingent upon review by the SRSA security team with management approval.

We centrally manage all Philips assets with several proactive measures to with the aim to eliminate any risk of malware injection, cross-contamination between networks and exposure of protected patient data.

Four levels of security

Philips takes the issues involved in accessing healthcare sites over the internet very seriously. To ensure that every connection is made with the highest integrity and tightest security, SRSA provides four levels of security:

Level 1

Two-factor authentication to Philips VPN

Level 2

Two-factor authentication to SRSA

All user actions are documented in the SRSA service logs, including unsuccessful connection attempts. These logs can be cross-checked against your own logs for verification.

Level 3

Role-based access and least-privilege principle

Philips service technicians can support only customers they're authorized to support, accessing only the resources required for legitimate, essential purposes.

Level 4

Authentication on the device

The user must also authenticate to each specific medical device's operating system and/or application software to service the device and all information traversing the internet between Philips and your site is encrypted using either the IPSec or SSL protocol.

How to arrange redundancy for your data

Business continuity and disaster recovery

Business continuity and disaster recovery are essential for safeguarding healthcare organizations against cyberattacks by enabling swift response and recovery in the event of a security breach. These measures help safeguard the uninterrupted delivery of critical healthcare services and the protection of sensitive patient data, bolster resilience and minimize the impact of cyber threats on patient care and organizational integrity. Their effectiveness hinges on the support of proper technology infrastructure – including robust backup systems, secure data storage, and reliable communication channels – to support operations and data protection in the face of cyberattacks.

The discussions on disaster recovery and business continuity configurations are collaboratively undertaken between the customer and the supplier to ensure robust protection of sensitive healthcare data, considering carefully the infrastructures and the processes already at customer site to support security and operational continuity.

Philips PACS solutions are designed to provide different levels of redundancy in every project in accordance with the requirements expressed by the customer.

Busines continuity and disaster recovery

The Oracle database is backed up using a "hot backup" strategy performed while the system is online. The default plan is full and incremental backup with different and configurable cadence, and always two backups are maintained.

To achieve further redundancy, it is recommended to copy the database backup daily to an external media, which is part of the standard operation policies documented in the Philips Image Management Administration Guide.

An internal table inside the database maintains backup history statuses. Backup jobs are monitored as part of the system check and will alert on failure of or if no valid backup is available for the database in the last 24 hours.

In the case of total loss and full database recovery, standard procedures include many recovery scenarios and levels that support rebuilding the database.

.

In addition, we provide standard configurations for business continuity provided via a fully replicated infrastructure, which can operate your full production load at any time. In the event of primary system failure, load balancers can route traffic to the secondary system.

In addition to the redundancy of the infrastructure, the primary and secondary systems are synchronized using an application-based service Philips developed and maintains. It ensures images are replicated in both systems' storage pools and that metadata is synchronized for both database instances.

Disaster recovery is generally achieved by geographically separating the two instances of the solution described above. In the event of a disaster at one of the data centers, the second instance is used to rebuild the impacted data center when the infrastructure is available. Restoration typically includes configuration files, databases, image storage and virtual machines where appropriate.

Philips HealthSuite Imaging Data Protection

This Philips data protection offering is a cloud-based service that secures medical imaging data and PACS file systems, leveraging Amazon Web Services (AWS) technology. AWS's advanced security features include encryption in transit and at rest, and compliance with over 50 global standards. This robust protection minimizes the risk of ransomware attacks, supporting that your critical medical imaging data remains secure and accessible, allowing healthcare organizations to maintain uninterrupted patient care.

The Philips data protection offering supports regulatory compliance, high durability, and quick data recovery in case of disasters without disrupting the onsite medical imaging workflow and PACS configuration. The service eliminates the need for on-site backups, reduces management burdens, and offers cost-effective scalability, enabling healthcare organizations to focus on patient care without compromising data integrity.

How to monitor and respond to threats and security incidents

A threat has been identified. Now what?

Logs and audit trails

Logs and audit trails play a pivotal role in threat detection and security incident response by providing a detailed chronicle of system activities and events.

When organizations handle Protected Health Information (PHI), regulations require them to log all activities. Each logged event can include warnings and failures, operation performed, user who performed it, location from which it occurred (including the client's IP) and the information affected (including the study instance unique identifier).

An audit is an event log that collects important actions and events in the system for the purposes of tracking and investigating past actions in the system. It's a write/read only table, which means we can only write to it and read the information afterwards. It won't be updated or deleted.

Log and audit trails are crucial in cybersecurity because they provide a detailed record of system activities, allowing for the detection of security incidents, investigation of suspicious events, compliance with regulatory requirements, and analysis of historical data to improve security posture and response strategies.

We provide detailed audit trail logs that are IHE ATNA-compliant, which apply to logging on, reading and modifying clinical information.

Audit trail logs are either stored locally (in an encrypted form) on the system or can be transferred to a central Syslog server. Local audit logs can be viewed using the Audit Log Viewer.

Hospital administrators can access Audit Log Viewer to monitor logged events and identify unusual system activity or suspicious user behavior. They can then filter records according to their needs and export if necessary. We can work with the customer or third parties to set up the best workflow to make your audit available according to the organization need.

Responding to cybersecurity threats

Within our threat response framework, safeguarding the security of vital assets such as the Vue PACS and Image Management Software is our top priority at the 24/7 Philips Security Operations Center (SOC).* We employ a comprehensive approach tailored to swiftly and effectively address cybersecurity challenges. Our multifaceted strategy integrates proactive measures such as continuous monitoring and threat detection – leveraging state-of-the-art technologies .

In the event of an incident, our SOC is prepared to respond with agility and precision. Rapid triage and containment procedures swiftly isolate affected systems to mitigate harm and prevent the spread of the threat. We perform meticulous investigation into the incident's specifics. Our analysts delve deep into forensic evidence, log data and network traffic to grasp the attacker's tactics, techniques and objectives. This granular analysis informs our response strategies and enhances our threat detection capabilities, enabling us to anticipate and thwart future threats more effectively.

Collaboration and transparent communication is central to our approach. We maintain open channels of dialogue with internal stakeholders, external partners and regulatory bodies to keep all relevant parties informed throughout the incident response process. This collaborative ethos extends to our remediation efforts; we work tirelessly to restore affected systems to a secure state. From patching vulnerabilities and deploying security updates, to resetting compromised credentials and restoring data from backups, our focus remains steadfast on safeguarding critical assets and maintaining operational continuity.

Post-incident analysis serves as a cornerstone of our approach, providing invaluable insights into areas for improvement. We conduct thorough assessments to identify gaps in security controls, weaknesses in incident response procedures and opportunities for enhancement. We bolster our commitment to continuous improvement with ongoing investment in training and skill development to ensure that our analysts remain at the forefront of cybersecurity best practices.

The 24/7 Philips SOC is dedicated to delivering a robust, agile response to cybersecurity threats. We're committed to safeguarding the integrity and availability of critical assets such as the Vue PACS and Image Management Software while fortifying operational resilience in the face of an ever-evolving threat landscape.

* Check SOC services availability for yor market with your local representative

How to reach us
Please visit www.philips.com/
radiology-informatics