PHILIPS

Enterprise Imaging

Product Roundup

IntelliSpace Enterprise Imaging Solution* cybersecurity enhancements

Our security and privacy protection measures focus on providing confidentiality, integrity and availability of critical data. Read on to learn about IntelliSpace Enterprise Imaging Solution's latest cybersecurity enhancements.

Feature spotlight
Strong data encryption secures personal health information >

You asked, we listened
Hardened infrastructure minimizes vulnerabilities >

Observations from the field
The costs of security breaches and tools to prevent them >

Small changes, big impact
Patching reports expanded to assist in compliance >

Beyond the technology
Focus on privacy protection >

Quick look
What's new and improved >

* IntelliSpace Enterprise Imaging Solution includes these products: IntelliSpace Radiology and IntelliSpace Universal Data Manager. Please contact your Philips representative for version compatibility.

Strong data encryption secures personal health information

Encryption prevents unauthorized disclosure of personal health information (PHI) by converting data into an encoded form that can only be decoded by authorized users with a cipher key. In a recent study, extensive use of encryption was found to reduce the cost of a data breach by 13.59 USD per record, making it the second most effective method of decreasing data breach costs.[1]

We use powerful data encryption technologies to secure data, both at rest and in motion. Transport Layer Security (TLS) 1.2 delivers data in transit, providing data privacy and integrity between communicating imaging components. This is accomplished by the use of strong encryption and hashing standards: Advanced Encryption Standard and MD5/SHA-1. Because TLS was designed to prevent eavesdropping, tampering and message forgery, it is a standard encryption technology used to secure DICOM and other types of data. Data In Transit Encryption is also used to secure back-up operations by establishing a virtual private network (VPN) connection between the Philips Data Center and a VPN router at customer sites.

Strong encryption also protects data at rest as part of IntelliSpace PACS SW release versions 4.543.x and higher. Additionally, the optional Archive Encryption Service is a one-time service that extends data protection by encrypting existing studies in the archive using strong encryption based on the Advanced Encryption Standard with a 256-bit key length.

Ask your Philips representative to learn more about encryption options.

[1] 2019 Cost of a Data Breach Study: Global Overview. Ponemon Institute LLC, July 2019, p. 38.

Hardened infrastructure minimizes vulnerabilities

Unsecure devices offer many security vulnerabilities that can be exploited by a bad actor and result in a breach. To minimize risk, healthcare providers look to vendors to incorporate hardened components in their solution. Hardening is identifying and closing security vulnerabilities in components at the operating system level, and is very effective in reducing the risk that a system will be exploited.

To protect against vulnerabilities in your infrastructure, we follow the United States Department of Defense Security Technical Implementation Guides (STIGs), which are configuration standards for Department of Defense devices. Information Assurance (IA) and IA-enabled devices. STIGs describe how to minimize attacks and prevent system access, list identified system level vulnerabilities and their severity, and discuss maintenance procedures that can decrease vulnerabilities. We also enact robust measures to help mitigate potential vulnerabilities and facilitate the availability of clinically relevant information where needed. These measures meet our cybersecurity guidelines, which are aligned with NIST 800-53 Rev4, ISO 14971, EU GDPR, MDR Cybersecurity for Medical Devices and HIPAA Security and Privacy Rules.

The costs of security breaches and the tools to prevent them

A security breach can be very costly in both time and money. In addition to the cost of identifying the type and extent of the breach and determining what data was compromised, there are also costs involved in securing and updating the network and recovering data. Less obvious costs include HIPAA and other fines, possible litigation costs, and the cost of rebuilding your reputation. One study listed healthcare as the industry with the highest data breach cost per record, at 429 USD.[2] To reduce the risk of a data breach, we implement cybersecurity technologies that protect the confidentiality, integrity and availability of sensitive data. Confidentiality supports only authorized users viewing data. Integrity verifies that only users with the proper permissions can modify data, and that all modifications are verified and tracked for audit purposes. Availability enables data to be available when needed and delivered securely and in a non-disruptive manner.

[2] 2019 Cost of a Data Breach Study: Global Overview. Ponemon Institute LLC, July 2019, p. 27.

Patching reports expanded to assist in compliance

Healthcare providers are facing increasing requests for compliance reporting and verification that their devices and systems are up-to-date and patched to current levels to minimize the threat of exploits. Our detailed patching reports aid in documenting compliance with government and industry regulations by providing a consistent method to track patching activity. Delivered monthly, the reports identify the type of patches applied, the components being patched, and the dates of application.

The reports have now been expanded to address more systems, including LINUX and VMWare. In addition to providing useful documentation during audits, the reports also provide peace of mind that your IntelliSpace Enterprise Imaging Solution is equipped with up-to-date security patching.

Focus on privacy protection

Healthcare providers and patients are applauding privacy protection that ensures that patients are in control of their personal health information (PHI), such as the General Data Protection Regulation (GDPR) implemented in May 2018.

The GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union. However, compliance with GDPR is more than a legal issue. It is based on a fundamental understanding that there are people behind healthcare data, and that they deserve protection from the harm that comes from data breaches, including the financial loss and stress of identity theft.

Our focus on privacy begins with the patient. It is based on the principles of confidentiality, integrity and availability to safeguard PHI while supporting effective healthcare delivery. Building on the success of our Security by Design guidelines, we are supporting efforts to safeguard privacy through Privacy by Design. Privacy by Design embeds privacy and data protection controls throughout the entire data lifecycle.

What's new

- Philips Enterprise Imaging participated in the creation of the NIST/NCCoE Cybersecurity Practice Guide, SP 1800-24, Securing Picture Archiving and Communication System: https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs
- Privacy by Design Guidelines – baseline requirements to ensure data privacy safeguards are instilled in our products
- Multi-factor authentication – additional security safeguards beyond user name and password designed to prevent unauthorized people from accessing the system

What's improved

- Data Loss Prevention (DLP) – monitors users to prevent the transmission of sensitive or critical information outside the corporate network
- Security Information and Event Management (SIEM) – Philips Data Center monitoring
- Security Operations Center (SOC) – staffed by security professionals who respond to security incidents
- Secure Software Development Lifecycle (SSDLC) – baseline requirement for security during software development
- Static/dynamic code analysis – multi-level testing of code
- Vulnerability assessment – checks security vulnerabilities and resolutions
- Anti-virus coverage and compliance – additional managed nodes and adherence to guidelines
- Security hardening and updates
- Unique user ID and authentication

philips.com

Printed in the Netherlands.
4522 991 56901 * FEB 2020