PHILIPS

IntelliSpace

PACS

Security

Confidentiality, integrity, availability

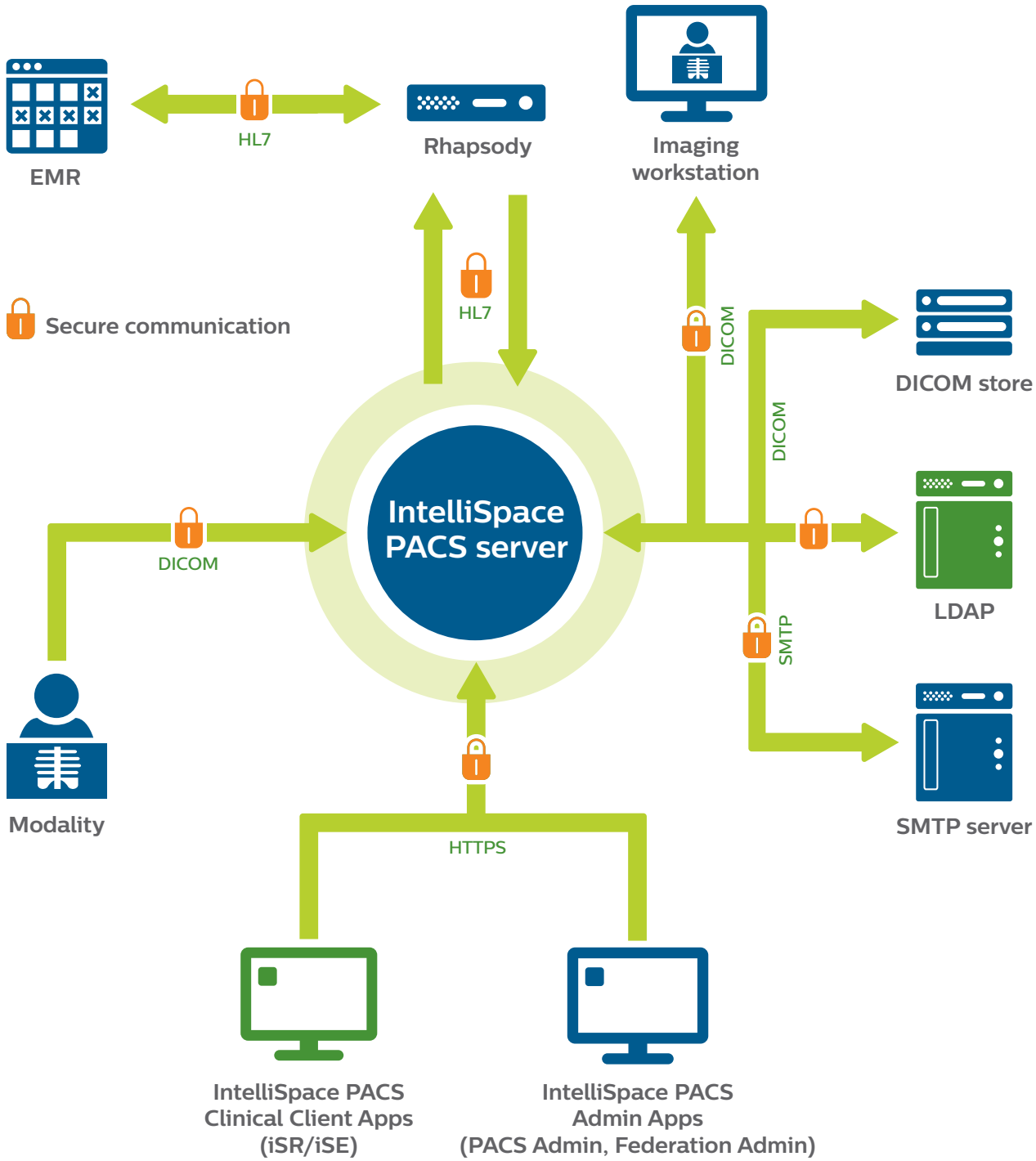
IntelliSpace PACS security

Malicious or inadvertent security breaches compromise patient confidentiality and expose healthcare enterprises to financial and legal risks. Enacting system security measures helps to mitigate these vulnerabilities and facilitate the availability of information to support clinical decisions and delivery of patient care.

IntelliSpace PACS addresses these security concerns by meeting the United States Department of Defense (DoD) Risk Management Framework (RMF) in three key areas: **secure hosting environment, secure software development lifecycle (SSDL), and secure application software.** These three security areas are the foundation for the confidentiality, integrity, and availability of patient data in your healthcare enterprise.

Managed, secure hosting environment **delivers peace of mind**

IntelliSpace PACS frees you from many system security maintenance tasks, while providing peace of mind that you are using the latest technology. Our Windows Server 2012 and SQL 2012 database platform* offers features that comply with the National Institute of Standards and Technology (NIST) security standards. Additionally, the IntelliSpace PACS software application hosted on Windows server operating system is secured in accordance with the Security Technical Implementation Guides (STIGs) released by the US Department of Defense, Defense Information Systems Agency (DISA). By complying with both NIST and DISA standards, we deliver a system with deep security.



Secure Software Development Lifecycle (SSDL) addresses security compliance

IntelliSpace PACS software was developed using the Secure Software Development Lifecycle (SSDL) process. During development, we review every requirement using our internal security risk assessment template to uncover potential security vulnerabilities. Identified risks are ranked by severity and the likelihood of occurrence, and requirements are updated to mitigate vulnerability.

Security risk assessments

PSRA + PIA
Product security risk assessment and privacy impact assessment, based on NIST 800-53 R4

Threat modeling and design review
Review of current advanced persistent threats (APTs) and their possible impact, and design modification or controls to mitigate threats

Secure code analysis
Automated code analysis in each development cycle

Application security testing
Automated tools such as HP Web Inspect and Nessus to uncover any findings

Vulnerability and penetration testing
Philips Security Center of Excellence performs penetration testing on the system and mitigates any findings

Features that promote a secure hosting environment

- A web server that is configured in secure communication mode, has the latest security updates, and uses selective ports, protocols, and services
- Antivirus software and third-party applications, such as JAVA and SQL
- Application whitelisting to allow only authorized applications to run and to prevent unauthorized changes
- A network firewall that separates the internal network from the Internet, and only allows use of required communication ports
- Transport Layer Security (TLS) 1.2 data encryption in transit
- Federal Information Processing Standards (FIPS) 140-2 encryption algorithm
- Support of IPv6 network protocol on the hosting environment
- Certificate-based authentication
- Support of Personal Identify Verification (PIV)/ Common Access Card (CAC)

* IntelliSpace PACS 4.4.550 application software supports both Windows Server 2008 and Windows Server 2012 hosting environments. The secure hosting environment is based on the Windows Server 2012 and SQL 2012 database platform.

Secure application software enhances security at the application level

IntelliSpace PACS provides application level security, including authentication, session management, user-defined password management, access control at user and role levels, auditing, and data integrity checks.

Secure client-to-server and server-to-server connections protect patient information during transmission. Patient data is encrypted before it is transmitted over the network using compatible cryptographic protocol between the endpoints. The server communicates in secure mode for all protocols supported by the system, including web service, HL7, SMTP, and DICOM.

In addition, session management features allow you to configure session rules to enhance availability as well as data security. You can limit the number of concurrent sessions in use by a single user, as well as the number of concurrent sessions per application, and the number of sessions at the system level. You can also determine which applications can join a session, and set a time limit after which idle sessions are automatically terminated.

Additional features that support application level security

Password management, which delivers configurable options for locking accounts and password security, and the option to use Personal Identify Verification (PIV)/Common Access Cards (CAC) – rather than user name and password – to access accounts

Detailed audit trails allow you to track how individuals, modalities, services, and systems access the PACS

Support of IPv6 network protocol at the software application level

Input validation to ensure data is correct and in the appropriate format

User access control that provide the ability to limit what data users can see and what they can do

Note: The customer is responsible for procuring and administering renewals of security certificates.
We accept TLS and SSL 3.0 and higher.

www.philips.com

Printed in The Netherlands.
4522 991 21101 * AUG 2016