PHILIPS

IntelliSpace

PACS

Sicherheit

Vertraulichkeit, Integrität, Verfügbarkeit

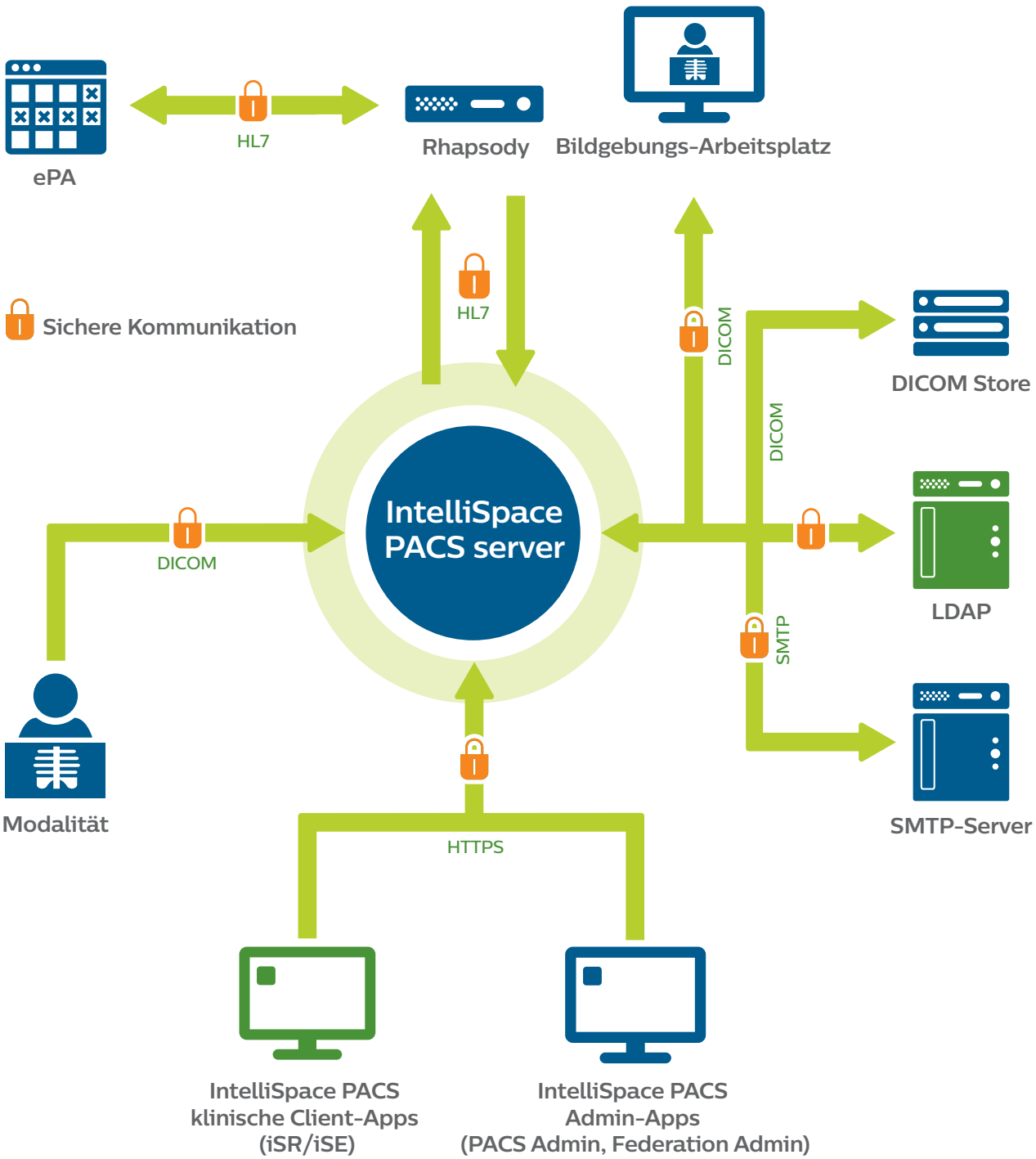
IntelliSpace PACS Sicherheit

Böswillige oder unbeabsichtigte Sicherheitsverletzungen gefährden die Vertraulichkeit von Patientendaten und setzen Gesundheitseinrichtungen finanziellen und rechtlichen Risiken aus. Systemsicherheitsmaßnahmen können Sicherheitslücken entgegenwirken und die zuverlässige Bereitstellung von Informationen ermöglichen, die für die klinische Entscheidungsfindung und eine adäquate Patientenversorgung notwendig sind.

Daher entspricht IntelliSpace PACS in drei Kernpunkten dem Risk Management Framework (RMF) des US-Verteidigungsministeriums: **sichere Host-Umgebung, sicherer Softwareentwicklungs-Lebenszyklus (SSDL; Secure Software Development Lifecycle) und sichere Applikationssoftware.** Diese drei Schwerpunkte bilden die Grundlage für die Vertraulichkeit, Integrität und Verfügbarkeit von Patientendaten in Ihrer Gesundheitseinrichtung.

Eine kontrollierte, sichere Host-Umgebung **für hervorragenden Schutz**

IntelliSpace PACS erspart Ihnen zahlreiche die Sicherheit betreffenden Wartungsaufgaben und gibt Ihnen gleichzeitig die beruhigende Sicherheit, dass Ihre Technologie stets auf dem neuesten Stand ist. Unsere Windows Server 2012 und SQL 2012 Datenbankplattform* bietet Leistungsmerkmale, die den Sicherheitsstandards des National Institute of Standards and Technology (NIST) entsprechen. Zusätzlich ist die auf dem Windows Server Betriebssystem gehostete IntelliSpace PACS Software gemäß den Security Technical Implementation Guides (STIGs) gesichert, die von der Defense Information Systems Agency (DISA) des US-Verteidigungsministeriums herausgegeben werden.
Dank seiner Konformität mit den NIST- und DISA-Standards bietet unser System umfassende Sicherheit.



Secure Software Development Lifecycle (SSDL) zur Einhaltung der Sicherheitsrichtlinien

Die IntelliSpace PACS Software wurde nach dem SSDL-Prozess (Secure Software Development Lifecycle) entwickelt. Basierend auf unserem internen Template zur Beurteilung von Sicherheitsrisiken prüfen wir während der Entwicklung sämtliche Anforderungen, um mögliche Sicherheitslücken zu erkennen. Identifizierte Risiken werden nach Schweregrad und Wahrscheinlichkeit ihres Auftretens klassifiziert und die Anforderungen entsprechend aktualisiert, um möglichen Schwachstellen weitestgehend vorzubeugen.

Beurteilung von Sicherheitsrisiken

PSRA + PIA

Beurteilung der Produktsicherheitsrisiken und Auswirkungen auf den Datenschutz basierend auf NIST 800-53 R4

Bedrohungsanalyse und Designprüfung

Prüfung der aktuellen Advanced Persistent Threats (APT) und ihrer möglichen Folgen und Designänderung bzw. Implementierung von Kontrollmaßnahmen zur Abwehr von Bedrohungen

Code-Sicherheitsanalyse

Automatische Code-Analyse in jedem Entwicklungszyklus

Applikations-Sicherheitstests

Automatische Tools wie HP Web Inspect und Nessus zur Erkennung möglicher Schwachstellen

Prüfung auf Sicherheitslücken und Penetrationstests

Das Philips Security Center of Excellence nimmt Penetrationstests für das System vor und ergreift bei erkannten Schwachstellen entsprechende Abhilfemaßnahmen.

Merkmale einer sicheren Host-Umgebung

- Ein im sicheren Kommunikationsmodus konfigurierter Web-Server verfügt über die aktuellsten Sicherheitsupdates und verwendet selektive Ports, Protokolle und Dienste.
- Virenschutzsoftware und Anwendungen von Drittanbietern wie JAVA und SQL
- Applikations-Whitelisting gestattet die Ausführung nur von autorisierten Applikationen und verhindert unbefugte Änderungen.
- Eine Netzwerk-Firewall trennt das interne Netzwerk vom Internet und lässt nur die Nutzung der erforderlichen Kommunikationsschnittstellen zu.
- Transport Layer Security (TLS) 1.2 Datenverschlüsselung bei Übertragung
- Verschlüsselungsalgorithmus nach Federal Information Processing Standards (FIPS) 140-2
- Unterstützung des IPv6-Netzwerkprotokolls in der Host-Umgebung
- Zertifikatbasierte Authentifizierung
- Unterstützung von PIV-Karte (Personal Identity Verification) und CAC (Common Access Card)

* Die IntelliSpace PACS 4.4.550 Applikationssoftware unterstützt Windows Server 2008 und Windows Server 2012 Host-Umgebungen. Die sichere Host-Umgebung basiert auf der Windows Server 2012 und SQL 2012 Datenbankplattform.

Sichere Applikationssoftware verstärkt die Sicherheit auf Applikationsebene

IntelliSpace PACS bietet Sicherheitsfunktionen auf Applikationsebene, z.B. Authentifizierung, Sitzungsmanagement, Verwaltung von anwenderdefinierten Kennwörtern, Zugriffskontrolle auf Benutzer- und Rollenebene, Auditing und Prüfungen der Datenintegrität.

Sichere Client-Server- sowie Server-Server-Verbindungen schützen die Patientendaten während der Übertragung. Die Patientendaten werden vor der Übertragung über das Netzwerk mit einem kompatiblen kryptografischen Protokoll zwischen den Endpunkten verschlüsselt. Der Server kommuniziert bei allen vom System unterstützten Protokollen, wie Webdiensten, HL7, SMTP und DICOM, in einem gesicherten Modus.

Außerdem ermöglichen Funktionen zum Sitzungsmanagement das Konfigurieren von Sitzungsregeln für höhere Datenverfügbarkeit und verbesserte Datensicherheit. Sie haben die Möglichkeit, die Anzahl zeitgleicher Sitzungen eines Anwenders, pro Applikation oder auf Systemebene zu begrenzen. Zudem können Sie bestimmen, welche Applikationen in einer Sitzung geöffnet werden können und ein Zeitlimit festlegen, nach dessen Ablauf Sitzungen ohne Anwenderaktionen automatisch beendet werden.

Zusätzliche Leistungsmerkmale für die Sicherheit auf Applikationsebene

Kennwortverwaltung mit konfigurierbaren Optionen zum Sperren von Konten und Einstellen der Kennwortsicherheit sowie der Option, den Zugriff auf Konten über PIV-Karten (Personal Identify Verification) bzw. CAC (Common Access Cards) anstelle von Benutzername und Kennwort zu ermöglichen

Detaillierte Prozessprotokolle (Audit Trails) gestatten das Zurückverfolgen von Zugriffen auf das PACS durch Einzelpersonen, Modalitäten, Dienste und Systeme.

Unterstützung des IPv6-Netzwerkprotokolls auf Software-Ebene

Validierung von Eingabewerten zur Sicherstellung, dass Daten korrekt sind und das richtige Format haben

Benutzerzugriffskontrolle mit der Möglichkeit, zu begrenzen, welche Daten ein Benutzer anzeigen und welche Aktionen er durchführen kann

Hinweis: Für die Beschaffung und Verwaltung von Sicherheitszertifikaterneuerungen ist der Kunde verantwortlich.
Von unserem System werden die Protokolle TLS und SSL 3.0 und höher unterstützt.

www.philips.de/healthcare

Gedruckt in den Niederlanden.
4522 991 21103 * SEP 2020