PHILIPS

IntelliSpace Portal

Security

Are you protecting your advanced visualization platform from patient data breaches?

Like every industry that relies on increasingly connected computer networks, healthcare is faced with a growing number of security breaches.

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 Portal addresses these security concerns by focusing on three key areas:

- Establishing security processes during product development
- Enabling a secure software development lifecycle
- Providing governance of a comprehensive risk management strategy

These security areas are the foundation for the **confidentiality, integrity, and availability** of patient data in your healthcare enterprise.

Delivering a **secure hosting environment**

IntelliSpace Portal software was developed using a secure software development lifecycle process. During product development, we reviewed every requirement using our internal security risk assessment template, to uncover any potential security vulnerabilities. Identified risks are ranked by severity and the likelihood of occurrence, and requirements are updated to mitigate vulnerability.

Security risk assessments

Product security risk assessment and privacy impact assessment, based on NIST 800-53 R4.

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

Automated code analysis in each development cycle.

Automated tools such as HP Web Inspect and Nessus to uncover any findings.

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

"The HIMSS cybersecurity survey revealed that most healthcare organizations, **69%**, are still using some form of outdated technology in their networks.[1]"

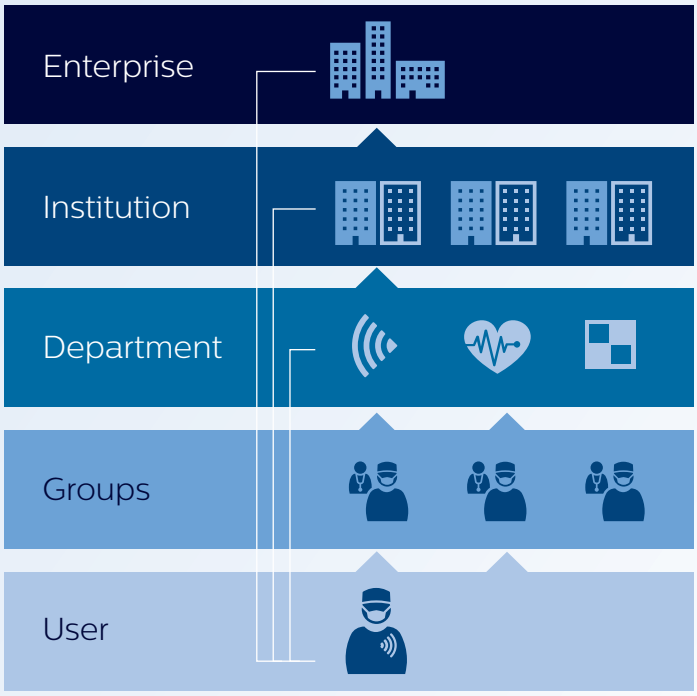
IntelliSpace Portal is designed to **protect your patient data**

IntelliSpace Portal 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 and DICOM.

Patient and role-based access controls to protect sensitive patient data from unauthorized access

- IntelliSpace Portal supports hospitals in their GDPR compliance by preventing unauthorized access to patient data.
- Provides a data segregation mechanism for patient and role-based access controls:
  - **Role-based privacy** – what a user may or may not do with study data.
  - **Patient-based privacy** – whether or not a user may access a particular patient's study data.



"It is estimated that **22%** of security breaches since 2009 were due to unauthorized access.[2]"

A partner **you can rely on**

Products and product-related services – such as Remote Service Infrastructure – are vital assets that are essential to Philips' business and its customers. **The Philips Product & Services Security Policy Framework** contains a set of defined policies, standards, guidelines, procedures and processes that ensures security by design and operational excellence. Each Philips product or service integrates the appropriate controls applicable to the intended use and management of the product or service.

Philips has a Product & Services Security Office that regularly monitors the security measures that have been implemented as well as the implementation of new security requirements. Compliance with Philips Product & Services Security Policies is accomplished through annual training, periodic reviews of local and organization policies, procedures, and audits.

"Cybersecurity attacks that **infiltrate a network by exploiting remote access** on connected devices and systems is the top health technology hazard.[3]"

References

1. HIMSS 2019 Cybersecurity Survey
2. McCann E. HIPAA Data Breaches Climb 138 Percent. Healthcare IT News. February 6, 2014
3. ECRI Institute 2019 Top Health Technology Hazards: Executive Brief