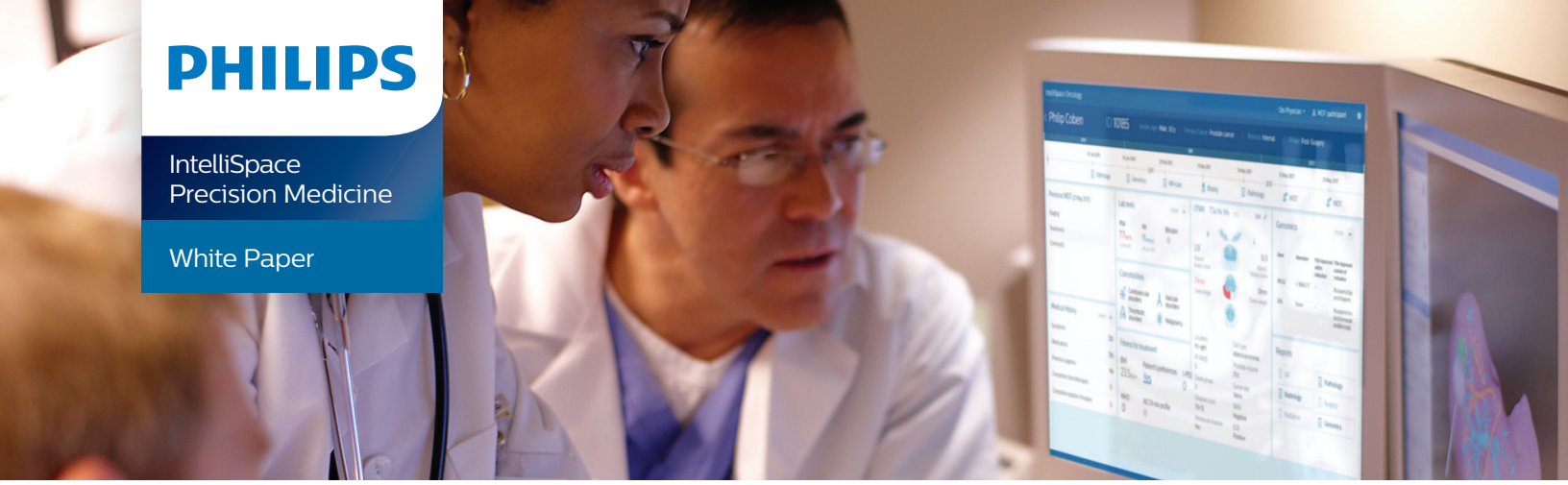
PHILIPS

IntelliSpace Precision Medicine

White Paper



Overview of Philips IntelliSpace Precision Medicine Security

IntelliSpace Precision Medicine is a secure cloud-based software solution that enables patient-centered precision care. It is a SaaS (Software as a Service) application built on Philips HealthSuite cloud platform with workflows for pathologists, oncologists, and researchers. It protects patient data, streamlines collaboration, provides a comprehensive molecular picture, and delivers actionable reports for a better path towards precision care.

IntelliSpace Precision Medicine is built on Philips HealthSuite cloud platform, which has achieved ISO/IEC 27001:2013 and ISO/IEC 27018:2014 certifications for the Information Security Management System. Also, IntelliSpace Precision Medicine has undergone a formal risk assessment and implemented technical safeguards in accordance with the HIPAA security rule. It obtained an official third-party HIPAA audit by the VERIS Group LLC. Personal Health Information (PHI) contained within the IntelliSpace Precision Medicine system is secured at rest and transit using ISO27001 encryption and cryptography best practices.

IntelliSpace Precision Medicine security enforcement is made via multi-level security policies and implementations.

1. Security policy for product design and development

Products and services need appropriate security features and controls to ensure that our customers and Philips can comply with regional legislation, recommended security best practices and internal policies. The health system product security risk management framework developed by Philips is consistent with other business risk management processes. The security policy for product design and development defines standards, procedures, templates, financial sponsorship, and business risk acceptance, and governs the roles and responsibilities of employees to maintain confidentiality, integrity, and availability of data. The security policy requires businesses to conduct security risk assessments for every release of the product to ensure that data and functionality are as secure as possible.

2. Implementation of the security policy

The security policy is implemented via a comprehensive communication and operation management framework. This framework establishes the rules to protect the confidentiality, integrity, and availability of the system. It provides control measures to support the separation of duties, such as an external user (e.g., the test ordering physician) and internal user (e.g., pathologist or oncologist) roles. It also controls the separation of the development environment and the production environment. Any change to software components has to be authorized and tested in the development environment before migrating to the production environment.

IntelliSpace Precision Medicine security at-a-glance:

ISO27001, ISO27018 certified. HIPAA attestation from Coalfire Systems, Inc.
Encrypt data at rest with AES-256 and transit with SSL/TLS keys/certificates
Super lightweight browser frontend, no information stored locally
Secure authentication and authorization mechanisms to ensure data privacy
Acquire, manage, and archive data through a secure cloud-hosted repository

Product Security Risk Assessments and Privacy by Design Assessments are performed at the feature-level throughout the design and implementation phases. These risk assessments identify additional security and privacy requirements and operational controls to be implemented. Further due diligence efforts and assessments are executed to evaluate Philips suppliers' organizational and technical capabilities and suitability.

Both static code analysis and dynamic code analysis are performed using various utilities and deployed as part of the regular build process throughout the software development cycle. Philips Security Center of Excellence team conducts a series of penetration tests before the software release. Additional penetration testing is periodically performed by independent third parties and as part of ongoing compliance and risk management efforts. In the event of a security incident, the Product Security Incident Response Team will implement the procedures put in place to minimize the impact of the incident.

The system uses strong cryptography and security protocols to protect confidential and personal information. Data is encrypted whenever it is transmitted (in transit) using SSL/TLS and is encrypted when stored (at rest). Multiple cryptographic functions are supported for compatibility purposes. By default, AES-256 (or better) is specified for symmetric encryption, Diffie-Hellman 2048-bit (or better) for asymmetric encryption, and SHA-256 (or better) for digital signatures and hashes.

3. Identity management and access control policy for IntelliSpace Precision Medicine users

The access control policy ensures authorization and authentication to access the right information. Authorized service activity is logged and auditable across the platform ecosystem. Centralized identity management and shared control processes enable identity integration across applications. Supported standards include OAuth2 for authentication/authorization and "OpenID Connect" to allow cross-platform federated access to third-party systems.

Before granting access, the system displays privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance. All access privileges to individuals are assigned using "role-based access control" approach. User IDs and passwords for new end-users are distributed via the secure mail. All passwords are protected by strong cryptography.

The password management policy follows common good practices. Passwords expire after a limited amount of time, and the user is required to set a new password. The system enforces a limited count of consecutive invalid login attempts by a user and automatically locks the account for increased durations or until released by an administrator.

4. Backup and recovery

IntelliSpace Precision Medicine is responsible for defining the backup and archiving requirements of electronic data files according to the customer business needs, as well as the consideration of regulatory, compliance, and legal obligations. All data elements are encrypted at the disk storage level. They are stored only at the cloud encrypted storage and databases. The backup of the system is performed on a pre-defined schedule and retained for the mutually agreed period. The backup and recovery processes ensure that data elements can be saved and restored within the allotted time.