PHILIPS

Remote Services

Security and privacy

with HealthSuite Remote Services Enablement (HS-RSE)

The HealthSuite Remote Services Enablement (HS-RSE) solution consists primarily of Philips Remote Services (PRS), HealthSuite Remote Services Gateway (HS-RSG) and optionally HealthSuite Edge. The following sections provide details on the security and privacy controls in each of these 3 components of the HS-RSE solution.

In this document you will find information about security, privacy and data protection of these three components:

Philips Remote Services

HealthSuite Remote Services Gateway

HealthSuite Edge

Philips Remote Services

Enabling secure connection to protect your vital healthcare assets

Philips
Remote Services

Frequently Asked Questions about Connectivity and Security

To support you in delivering efficient quality care to your patients and protecting your sensitive medical information, we have put in place secure remote support solutions and facilities. Find out more about our remote connection technology and security measures in this document.

Security

Decreased risk

High uptime

Fast response

Control

Services and Connection Methods

1. What is Philips Remote Services?

Philips Remote Services offers remote technical and clinical support to help customers make the most of their clinical solutions. Our innovative set of proactive services aims to continuously support clinical solutions remotely, minimizing interruptions to patient care. Philips Remote Services helps provide the highest clinical solution uptime and delivers continuous innovative services to the customer's clinical healthcare facilities. Philips Remote Services is delivered via an advanced, business-to-business virtual private network (VPN) or through a transport layer security (TLS) outbound connection that establishes a secure connection to the customer's clinical solutions.

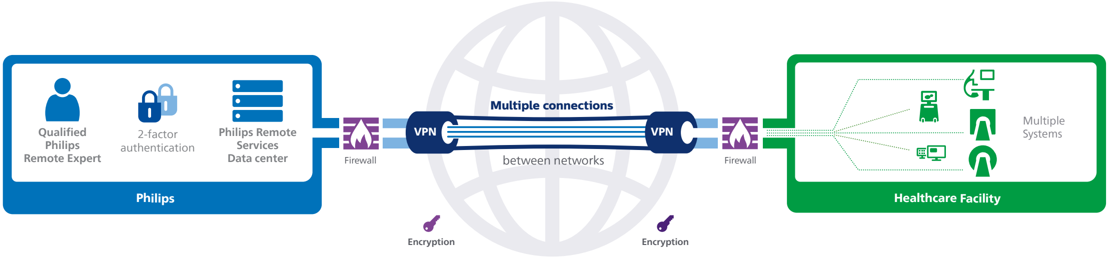
2. Are secure connection protocol(s) used to provide remote support?

To address the requirements of different customer IT infrastructure, clinical solutions connect to the Philips Remote Services either through a VPN tunnel using the Wireguard protocol or Internet Protocol security (IPsec) or through a direct outbound TLS connection. To help customers make an informed decision, Philips works with each customer, providing details and recommendations for the best-fit secure remote connectivity option.

3. What are the customer requirements between a Philips Remote Services VPN and TLS connection?

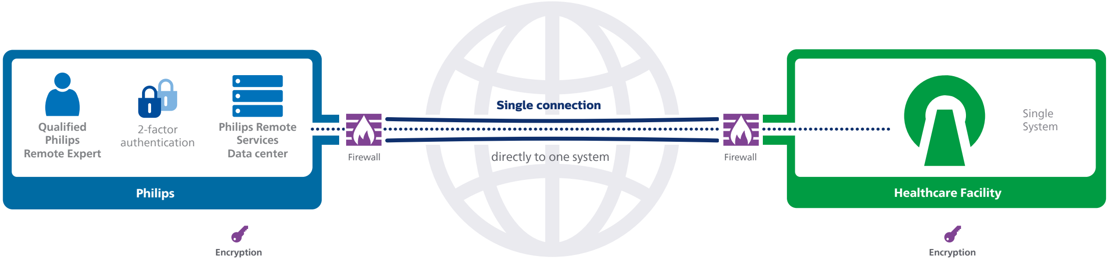
For the Wireguard VPN connection option, Philips will deploy the Philips HealthSuite Edge appliance and the remotely supported clinical solution must be configured with static IP addresses. For the IPsec VPN connection option, your facility must have an IPsec VPN compatible appliance/device, and the remotely supported clinical solution must be configured with static IP addresses. The VPN tunnel option provides site-to-site encryption, which terminates at the VPN router, and data transmitted within the healthcare facility's network may not be encrypted, depending on the remote tool used.

The TLS connection option uses your facility's existing network to set up a secure connection over the Internet. It supports remote access to clinical solutions deployed with dynamic IP addresses via DHCP. TLS-based connectivity option provides end-to-end encryption between the clinical solution and Philips Remote Services.



Wireguard/IPsec VPN tunnel

A VPN tunnel can be used to establish a secure connection between your Healthcare Facility and Philips Remote Services Data Center. The Wireguard / IPsec VPN tunnel provides site-to-site encryption. We use a VPN tunnel to establish a secure connection between your Healthcare Facility and Philips Remote Services Data Center.



Outbound TLS connection

This solution establishes a fully encrypted tunnel between the two end points. The advantage of an outbound TLS connection from the medical device to the Philips Remote Services Data Center is that the medical device only needs to be able to connect to the Internet to establish a connection. No additional router configuration is required.

4. If the customer's facility already has a Philips Remote Services connection via VPN, can they use TLS-based connectivity?

Yes, you can still use TLS-based connectivity. Devices that support TLS-based connectivity do not interfere in any way with devices that operate over VPN. TLS-based devices can connect and run directly over the Internet using your existing network or also can be routed over VPN.

5. Does Philips support use of the customer's VPN clients for remote access?

To provide you with the optimal services and a full suite of remote solutions at any given time, we do not support the use of customer VPN clients for remote support. The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management Systems standard and is audited annually by an independent third-party auditor – see the "Security Measures" section for more details.

6. Is the VPN connection to the customer site FIPS 140-2 compliant?

The connection between the Philips Remote Services Network and the customer site is persistent via a VPN tunnel. It uses encryption protocols that are supported by the FIPS 140-2 standard or better.

7. What is the Philips HealthSuite Edge appliance?

Philips HealthSuite Edge for Services is a small form factor endpoint device that delivers secure connectivity and lightweight, on-premises compute support for next-generation Philips cloud services. It establishes a secure connectivity gateway to the full Philips portfolio of remote services. Philips HealthSuite Edge for Services is designed to enable secure remote software upgrades and patching. Philips HealthSuite Edge for Services routing also uses an upgraded network infrastructure from Philips that brings increased reliability and efficiency compared to the existing routers.

8. What types of remote support services does Philips provide for my clinical solutions?

The remote support services that Philips provides, via the Philips Remote Services environment, can be categorized under either reactive services or proactive services. The differentiation is based on the trigger for the service.

For reactive services, customers raise a formal service request when they notice issues with their clinical solutions, by contacting their designated Philips customer support representative. The service request is then assigned to qualified and authorized remote service engineers, who will analyze the reported issue and determine the actions to resolve the issue – this may include initiating a remote connection to the clinical solution. At all times, remote service engineers will choose the service application commensurate with the level of troubleshooting that is necessary. The service applications available to the remote service engineers are dependent on the clinical solution configuration – some devices may be configured to allow service applications, like Remote Desktop, to enable remote service engineers to establish a remote session to the device. Other devices like MR/CT scanners support a "look-over-the-shoulder" service application that allow a specialist, upon authorization by the customer's clinical personnel, to gain a live view of the device's screen, to help with clinical problem resolution. To ensure customers remain in control of their data, Philips explicitly requires customers to acknowledge a disclaimer and grant this "look-over-the-shoulder" remote access. This allows customers to track and terminate access at any point during the live support session. In addition, during this screen-sharing mode, Philips specialists have viewing rights only. Therefore, they will remotely view only information disclosed by the customer during the live support session, but they cannot download/transfer/extract any files or data.

For proactive services, see the next question below, for more details.

9. What kind of proactive services does Philips offer?

To help customers gain even higher uptime and control over their clinical solutions, Philips continuously develops innovative services to optimize the performance, utilization and availability of Philips clinical solutions. To deliver these advanced services, we monitor key parameters, alert customers about potential issues, and capture trended performance data to proactively maintain the health of the clinical solutions.

Philips performs advanced data analysis on this performance data over a long time span and is able to draw conclusions based on that information, which enables Philips to carry out advanced remote diagnostics on your Philips clinical solution. In many cases, this allows Philips to determine when the device is developing a problem before symptoms are obvious to the user. The data volume and frequency of transfer varies by product.

10. What types of information are reviewed by Philips experts and how is it managed?

The type of information reviewed depends upon the device and the associated business policies. In general, it includes reports on the device's status and health using critical parameters such as helium level, temperature, CPU & memory utilization. The device can send log files to Philips periodically, or immediately, upon detection of a fault – depending on device configuration. In the event that your device requires servicing, remote service engineers will establish a remote session to the device to address the issue.

11. How often does the clinical solution connect with the Philips Remote Services and how much bandwidth does the TLS- based connection use?

The frequency of transmission of device status information to the Philips Remote Services depends on the specific clinical solution and remote service options that are enabled. As an example, for proactive services, it is usually every 5 minutes. However, it can range from every 30 seconds to every 15 minutes, depending on device configuration. The size of a typical device status data packet is generally a few bytes. However, the application traffic volume varies based on the type of medical device (Computed Tomography, Magnetic Resonance, conventional and interventional X-ray, Ultrasound, Nuclear Medicine, and Patient Monitoring Solutions) and specific service requirements (status update, downloading anti-virus files, uploading daily log files).

Security Measures

12. Describe how Philips is organized in terms of its approach to information security.

The Philips General Business Principles set the standard for acting with integrity at Philips. They govern all our decisions and actions throughout the world and apply equally to our group actions and to our conduct as individuals. Philips operates under a global Product Security Policy which defines a "Security Designed In" framework, based on internationally accepted standards, for all product and services creation, along with risk assessment and incident response activities for vulnerabilities identified in existing products and services. The Head of Philips Product Security oversees the governance and compliance of this policy. The Philips Product Security Policy Framework consists of policies, procedures and standards, requiring the organization to implement security best practices in our products and services. The Philips Product Security Statement can be accessed at www.philips.com/security.

13. What security standards does Philips Remote Services adhere to?

Philips is committed to proactively addressing the security and privacy concerns of the customer's healthcare facility. The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management Systems standard and is audited annually by an independent third-party auditor.

14. Describe how Philips ensures the correct and secure operation of Philips Remote Services information processing facilities.

The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management System standard, supported by policies and procedures to safeguard system security and access to protected data. These measures are implemented in our activities, including remote system log-in, troubleshooting and proactive maintenance.

Servers in the Philips Remote Services infrastructure are scanned for vulnerabilities bi-weekly. The vulnerability scan results are assessed, mitigated and/or remediated and then validated in a pre-production environment, before deployment to the production environment. Compliance of Philips Remote Services servers to defined internal security specifications is monitored via customary monitoring tools.

An annual penetration test of the Philips Remote Services environment is done by Philips Security Center of Excellence, which is an "Underwriters Laboratories (UL) product cybersecurity testing certified" group (UL Certificate Number 2962).

15. How can I check who is accessing my system through Philips Remote Services?

Remote support activities carried out via Philips Remote Services are logged and are traced to the individual remote service engineer. Product specific application or configuration changes executed remotely are logged in the product's service registry/ device logs. Philips can provide detailed audit logs of Philips remote support activities – customers can make a request to their designated Philips customer support representative for the audit logs. Additionally, Philips has developed a Customer Service Portal that allows a customer to access the remote session audit logs for their products and systems.

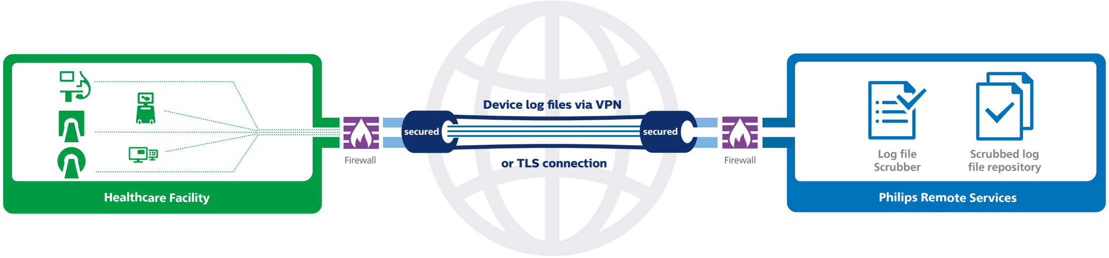
To safeguard the privacy of the relevant individuals, Philips Remote Services does not support video recording of remote sessions initiated by the remote service engineer to the customer's clinical solution. This avoids the collection of personal data data related to health, which is stored on the customer's clinical solution. The Philips Remote Services audit logs, in conjunction with the device logs, provide a detailed record of the remote service activities.

16. How does Philips safeguard personal and sensitive data?

The processing of personal data is not the intent for the provision of the Philips Remote Services. Therefore, Philips aims to avoid the collection and further processing of personal data via the Philips Remote Services. Consequently, we take steps to refrain from collecting directly identifiable data relating to patients and other individuals, for example by scrubbing log-files retrieved via the Philips Remote Service network.

All interactive sessions to a customer's clinical solution begin with a mandatory, formal customer service request. This means that only remote service engineers with a "need to know" authorization and using Philips Enterprise two-factor authentication are allowed access to your medical device.

Lastly, all Philips employees undergo annual training on the Philips General Business Principles, Privacy and data Protection, and Information Security topics.



17. Why is device data collected via Philips Remote Services and where is it stored?
Philips collects only log files from devices connected to the Philips Remote Services network. The aim of such collection is to perform troubleshooting and proactive monitoring activities. For customers in countries that are members of the European Economic Area (e.g., EU) and customers in North America, the device log-files are stored on Philips-managed servers hosted in the AWS EU-West cloud (Ireland).

18. Does Philips utilize multi-factor authentication to authenticate Philips remote service engineers when they access the Philips Remote Services Network?
Access to the Philips Remote Services Network requires two-factor authentication via a timed one-time password and Philips Enterprise Single sign-on. Philips Enterprise credentials follow a Philips IT group policy, enforcing strong passwords. When Philips employees leave the company, their Philips Enterprise credentials are promptly revoked as part of the employee off-boarding process, thereby disabling their access to the Philips Remote Services Network. A review of inactive Philips Remote Services accounts is performed annually and accounts older than a year are disabled proactively.

19. How do remote service engineers establish a remote connection to my systems?
All interactive sessions to a customer's clinical solution begin with a mandatory, formal service request from the customer, authorizing remote access, and the same is documented in the ticketing system. Authorized remote service engineers connect to the Philips Remote Services Network via two-factor authentication. After successful authentication, remote service engineers are presented with a list of sites and modalities, for which they have received access authorization from the Philips accountable Zone Lead. They then select the specific location and modality associated with the respective customer. Remote service engineers will choose the service application commensurate with the level of troubleshooting that is necessary (engineers are trained in modality-specific troubleshooting guidelines). At all times, the connection types used by the remote service engineer towards a customer device are logged in an audit log. Philips can provide detailed audit logs of Philips remote support activities – customers can make a request to their designated Philips customer support representative for the audit logs.

20. What security controls are enforced on the PC/laptop used by remote service engineers, to establish a remote support connection to my system(s)?
Remote service engineers use laptops that have security controls like endpoint protection software, host-based intrusion prevention system, full-disk encryption, timely security patching, and advanced threat protection.

21. Can a remote service engineer establish a remote connection to my system(s) from an unmanaged PC/laptop with Internet access?
Access to the Philips Remote Services Network is only possible via laptops connected to the Philips Enterprise network and require two-factor authentication.

22. Can malware from a remote service engineer's PC/laptop infect my system(s) and disrupt my healthcare facility network?
No, Philips Remote Services is designed to enable a secure and managed remote session to clinical solutions in a healthcare facility, via application virtualization (stepping stone architecture). Access to the Philips Remote Services Network always requires Philips Enterprise two-factor authentication.

23. Does Philips have a Disaster Recovery Plan for the Philips Remote Services and perform periodic testing of the plan?
Philips has defined Business Continuity / Disaster Recovery (DR) Plans for the Philips Remote Services, to coordinate and manage the response to failures/disasters and outline appropriate recovery actions. The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management Systems standard and is audited annually by an independent third-party auditor. As mitigation for disruption of remote service operations, Philips' Service teams will work directly with the customer to ensure that urgent support requests are handled and all related problems are addressed.

24. Describe how Philips Remote Services assets are identified and managed and how the information within Philips is classified, labeled and handled.
The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management Systems standard and is audited annually by an independent third-party auditor. Philips Remote Services has policies that define how assets are identified and managed. The Information Classification scheme is based on determining confidentiality, integrity and availability. Labeling assigns a classification to information and ensures that information gets the appropriate level of protection. The handling of information is in line with the Philips General Business Principles / Code of Conduct.

25. Who manages/maintains the Philips Remote Services? If you use a third-party contractor to maintain your systems, describe the vetting process by which the contractor is selected?
Philips Remote Services infrastructure and networking are maintained and managed by authorized Philips employees. The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management Systems standard and is audited annually by an independent third-party auditor. Philips Remote Services currently uses third parties to provide infrastructure services. Before engaging any third-party, Philips performs due diligence to evaluate their security & confidentiality practices. Philips Remote Services requires hosting providers to hold valid ISO/IEC 27001 certification and provide their SOC 2 Type 2 reports. This requirement provides an independent attestation that the necessary external security controls are implemented.

26. Are independent third-party audits of Philips Remote Services facilitated to review security practices?
Customer-driven independent third-party audits of the Philips Remote Services can be facilitated by contacting Philips, at productsecurity@philips.com. The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO/IEC 27001 Information Security Management System standard and is audited annually by an independent third-party auditor. The Philips Remote Services ISO/IEC 27001 certificate can be provided to customers, upon request.

27. Describe Philips' information security incident management procedures?
Refer to the Philips Product Security Statement, which can be accessed at www.philips.com/security.

28. Does Philips Remote Services have the CE marking and a Declaration of Conformity?
Following the guidance provided by the European Commission and the list of product groups that are in the scope of the CE marking, the Philips Remote Services Network does not fall into any of the defined categories and hence does not qualify for the CE Marking. The products that Philips sells in the European Union would qualify for the CE marking, and all Philips products have obtained the CE marking. Customers can check this in the respective Philips product documentation.

29. Where can I get more information?
For more general information about Philips Remote Services or to find out about the specific network characteristics of your device, please contact your regional Philips Customer Care Center.

Security controls

at the heart of the HealthSuite Remote Services Gateway

Introduction

1. What is the HealthSuite Remote Services Gateway?

HealthSuite Remote Services Gateway (HS-RSG) is software that serves as a gateway for devices in a healthcare facility to securely communicate with the HealthSuite Cloud (HS Cloud) for the purposes of service. HS-RSG facilitates remote service capabilities through Philips Remote Service (PRS) applications in HS Cloud.

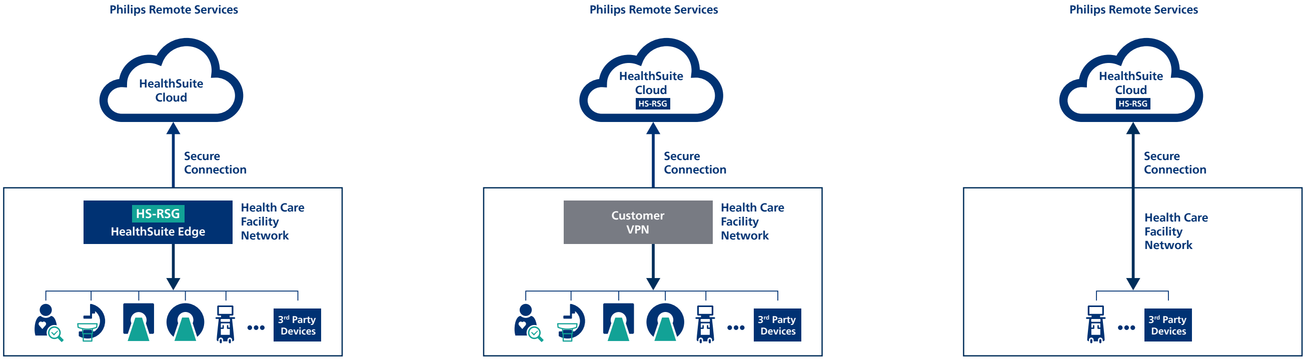
2. What are the key remote service capabilities that are enabled by the HealthSuite Remote Services Gateway?

HS-RSG can facilitate the secure remote access of registered devices in the healthcare facility by authorized Philips personnel. It also enables these devices to securely and reliably transfer service log files and service data to the HS Cloud for remote monitoring and diagnostics. HS-RSG also provides a mechanism to make software updates available to these devices for installation under user control.

3. What are the variants in connectivity available with HS-RSG?

Based on the customer infrastructure Philips can recommend the best-fit connectivity variant for HS-RSG. HS-RSG can be deployed on HealthSuite Edge on premises where feasible. HS-RSG can be accessed from the HS Cloud over a VPN or directly over the internet. These variations are illustrated in the diagram below.

Deployment scenarios for HealthSuite Remote Services Gateway



Philips on-premises VPN solution

Customer VPN solution

Solution for ambulatory devices

4. What are the requirements for the on-premise deployment of the HealthSuite Remote Services Gateway?

First an HS Edge appliance needs to be deployed on-premises and configured to work with HS Cloud. HS Edge is then provisioned to automatically download and run HS-RSG software. HS-RSG is kept up-to-date through automated patching. A device that is HS-RSE enabled can be then configured to communicate with HS-RSG on-premises.

5. What are the requirements for a device to use HS-RSG in HS Cloud?

An HS-RSE enabled device can be configured to communicate with HS-RSG in HS Cloud. Based on the site infrastructure, this communication can be over VPN or via a secure TLS connection over the internet.

Security Governance

6. What are the core security controls built into the HealthSuite Remote Services Gateway?
HealthSuite Remote Services Gateway is developed in strict compliance with the Secure Product Development Life Cycle outlined in the Philips Product Security Policy – the core activities are Product Security Risk Assessment, static code analysis, third-party SBoM analysis, ethical penetration testing and continuous product security training across the Philips organization.

HealthSuite Remote Services Gateway is deployed in a hardened environment, without any end-user application for managing it. All communication between Philips solutions in the healthcare facility, HealthSuite Remote Services Gateway and HealthSuite Cloud is based on secure connectivity protocols.

Medical device log files are not stored on the HealthSuite Remote Services Gateway at any time. Log files containing service data are securely transferred to the HealthSuite Cloud via the HealthSuite Remote Services Gateway.

7. What additional security controls have been considered in the cloud-based deployment of the HealthSuite Remote Services Gateway?
The HealthSuite Remote Services Gateway on Cloud is deployed across multiple regions to enable reliable connectivity to the HealthSuite Cloud. All communication between the healthcare facility and HealthSuite Cloud goes through either a secure VPN connection (established by the customer-managed router) or a secure TLS connection over the Internet.

Securely Connecting Care and Innovation

The Philips HealthSuite Edge and HealthSuite Platform

Our world is connected in more places and ways than ever before. This ubiquitous connectivity creates an opportunity to quickly deliver efficient, innovative, high quality services with lower cost and reduced risk to data security and privacy.

Philips HealthSuite Platform provides customers the capability to connect devices, aggregate and store data securely, analyze data, and create solutions in the cloud.

Built specifically for healthcare and life sciences organizations, HealthSuite Platform offers a diverse set of capabilities for ingesting data from multiple data sources — consumer devices, medical devices, imaging modalities, genomics, digital pathology, patient monitors, and more.

Protecting this sensitive health data is critical, and the HealthSuite Platform is extending to make it easier for you to ensure availability and protection of this information.

Introducing HealthSuite Edge.

HealthSuite Edge is a fully managed device-as-a-service and provides tools that alleviate the burdens of managing infrastructure, executing capital purchases, or maintaining operational and serviceability requirements for connectivity.

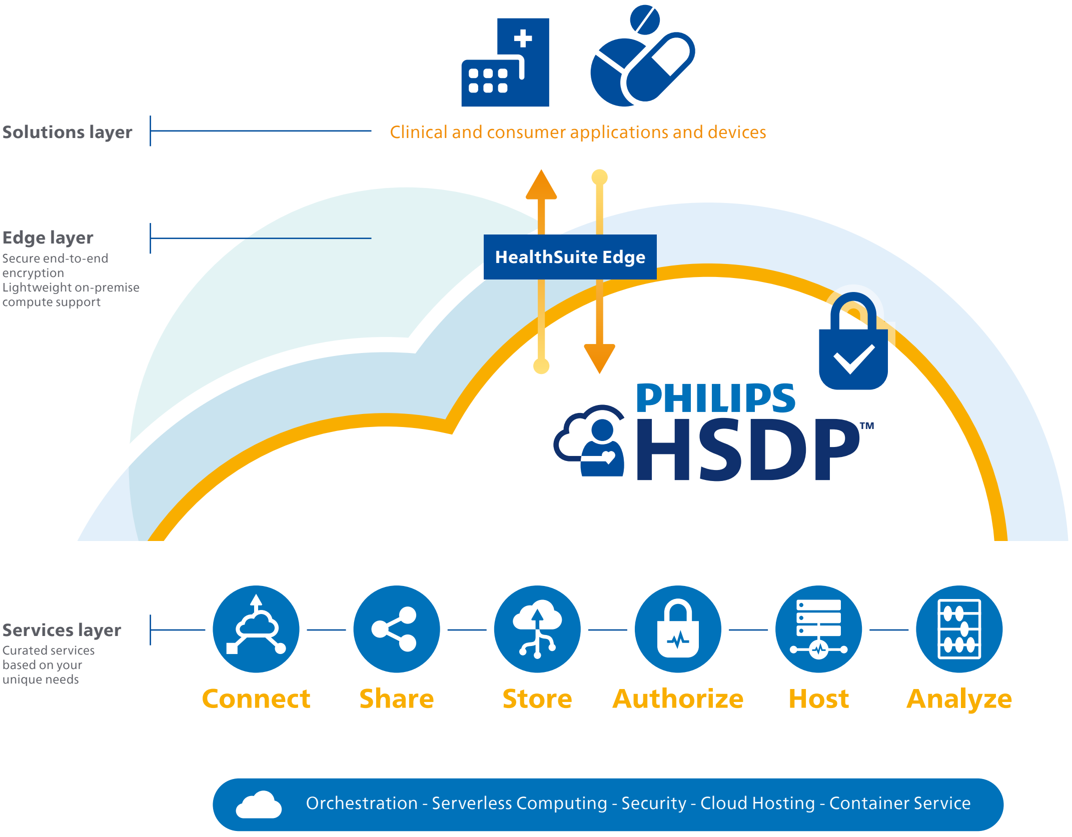
HealthSuite Edge Solution Overview

The HealthSuite Edge appliance is a small form factor endpoint device that delivers secure connectivity and lightweight, on-premises compute support for HealthSuite Platform cloud solutions.

Combined with the HealthSuite Platform, the HealthSuite Edge is designed to meet the demanding and diverse needs of healthcare and life sciences organizations across the care continuum through a secure end-to-end environment.

The device's flexible, secure gateway enables near real-time integration of medical device data at scale to keep pace with rapidly evolving care models and connected- therapy regimens.

The appliance is a sealed, fanless, solid state device designed to operate in a variety of deployments, such as a controlled data center, a healthcare office, or as part of a mobile solution. It's an easy-to-install device that requires no intervention once it is connected to the facility's network.


Solutions layer
Clinical and consumer applications and devices
Edge layer
Secure end-to-end encryption
Lightweight on-premise compute support
HealthSuite Edge
PHILIPS
HSDP™
Services layer
Curated services based on your unique needs
Connect
Share
Store
Authorize
Host
Analyze
Orchestration - Serverless Computing - Security - Cloud Hosting - Container Service

The HealthSuite Edge device is designed with a focus on security. HealthSuite Edge is:

An Enabler of More Secure Connectivity

It provides an end-to-end secure path between your onsite applications and devices, and the HealthSuite Platform cloud.

Connectivity for all applications traverses a single, secure VPN tunnel, reducing the need for multiple ports and connections through your perimeter firewall.

Designed for Secure Operations

The device has a strong default firewall configuration that can't be modified locally.

Any managed and sensitive configuration files are hashed and monitored for changes. (The device will not work if they are altered.) Also, the device UI password auto-rotates to randomized password upon provisioning.

Continuously Patched and Updated

Device software is continuously patched and updated by Philips without local user involvement.

The device-as-a-service model means facilities no longer need to pay for maintenance and always have the latest, most innovative technology.

Monitored Continuously in Real Time

The HealthSuite Platform operations center monitors system health, performance, and security in real time.

Operations center technicians proactively respond to any issues affecting operations or security.

Organizational Controls

Policies and Standards

HealthSuite Edge, combined with the HealthSuite Platform, leverages Philips security policies and standards, in conjunction with specific procedures and processes, to provide Philips employees guidance for the secure implementation and maintenance of systems and applications.

Philips HealthSuite is responsible for protecting the integrity of the platform deployed globally as well as maintaining the software-defined infrastructure, capabilities, and services of the platform to expected service-level commitments. This includes providing and securing the people, processes, and technology to effectively manage the platform and the relationships with hosting providers. Another critical responsibility is advancing the platform to maintain consistency with healthcare standards by keeping pace with technology and security-leading practices in order to assure Philips HealthSuite powers connectivity across the health continuum.

People

Philips HealthSuite security and privacy team are responsible for management and continuous improvement of each program as well as being the point of contact for privacy- and security-related activities and issues. They are required to have the appropriate subject matter expertise along with proper training including CISSP certifications and CIPP certifications to ensure consistent knowledge and capabilities.

Security and Privacy Training

All Philips personnel receive information security and privacy training consisting of security and privacy policies and procedures, privacy and data protection (including HIPAA topics), identifying and responding to security incidents, and other leading security and privacy practices. This ensures everyone is accountable and aware of their security and privacy roles and responsibilities within the organization.

Technical Controls

Encryption

Data is encrypted whenever it is transmitted (in transit) using TLS and is encrypted when stored (at rest). Strong 256 bit (or better) encryption is used.

Architecture

With a multi-layer security approach as well as centralized identity and access management built on open, cloud-based technology, the platform balances rapid, market-responsive application development with the assurance of data integrity.

Security is a key component of the HealthSuite Platform, which is embedded into all aspects of the platform development and operational lifecycle. Layering allows consistent implementation and deployment of best practices and industry-recognized standards across applications, via the platform. HealthSuite Edge, combined with the HealthSuite Platform, leverages several types of security mechanisms including password mechanisms, cryptographic keys, digital signatures, certificates, multi-factor authentication (MFA), and real-time integrity checking on key components.

Monitoring

The HealthSuite Operations Team continually evaluates security risks, and controls during the operations and maintenance of the platform to minimize risks and maximize availability. Their priority is to maintain operations, enhancing the platform's functionality and associated applications, and provide services to clients in a secure manner. Operating within leading practices including relevant ISO and ITIL (Information Technology Infrastructure Library) frameworks, the Operations Team and service representatives are trained on the relevant security and privacy obligations and secure data handling protocols to enable secure operations, effective maintenance, and comprehensive monitoring. Comprehensive monitoring of the event and audit logs serve two purposes: early identification of attacks, and potential identification of attacker actions and impacted data and quality, compliant services.

Incident Response

Philips HealthSuite Information Security Management System (ISMS) ensures a consistent, standards driven approach to security incident response. Our team of dedicated and highly experienced incident response professionals operate 24/7 to address incidents affecting HealthSuite services. The incident response team is responsible for assessment, containment, and ultimate recovery from a security incident.

Security by Design

Today's ever-changing threat landscape requires security to be managed across a system (and data) lifecycle by establishing an evolving security framework that, over time, positions these systems to be resilient and resistant to attack.

Security is integrated into the HealthSuite Edge development lifecycle, which aims to embed security controls throughout the entire data lifecycle, from the early design stage to deployment, collection, use, and ultimate data disposition and disposal. This also involves having subject matter experts to assess risk throughout the entire development lifecycle. Software review is conducted prior to production release, vulnerability scans are conducted on a regular basis, and penetration testing by third-party vendors is conducted regularly. A central repository is utilized for versioning control of all HealthSuite Edge code. Changes to code are subject to peer review and regular integration testing.

Philips has implemented an Information Security Management System (ISMS) that governs design for security in platform product and services creation, as well as risk assessment and incident response processes. It enables a "defense in depth" approach that places security controls at various levels—application security, computing security, data security, information security, network security—as well as administrative and operational safeguards. These security controls cover 20 different areas including: authorization, audit controls, emergency access, data integrity and authenticity, storage confidentiality (encryption "at rest"), and transmission confidentiality/ integrity (encryption "in transit") and they map to security frameworks and standards from around the world, including but not limited to ISO 27001/27002/27017/27018, SOC2, and HITRUST.

Disaster and Recovery

Philips leverages native cloud platform high-availability capabilities including but not limited to use of multiple availability zones. Structurally, the HealthSuite Platform is designed so each region can operate independently to avoid cascading failures.

Philips HealthSuite has developed a Service Continuity Plan (SCP) that provides guidance during situations (crises) that cannot be dealt with in the normal organization structure. A crisis management team composed of subject matter experts are trained to analyze the situation, determine course of actions, and communicate with stakeholders and internal teams.

Edge devices are considered part of the Philips HealthSuite Platform and are included in Change Management policies and procedures. Philips HealthSuite will provide notification of any material change to or discontinuation of the Edge device and in the event of discontinuation will work with customers to provide alternatives and develop a smooth transition to a new device.

As service continuity planning is not a one-time event, testing and maintenance is critical to ensure Philips HealthSuite is prepared when an actual event occurs. Philips HealthSuite performs tabletop testing on a quarterly basis. If any updates to the service continuity plan are needed as a result of the tabletop testing, then the plan is updated accordingly.

HealthSuite Edge is an important part of how HealthSuite Platform is extending to make it easier for you to protect data while ensuring it is available when needed. It provides hospitals, offices, and other healthcare settings the capability to: connect devices, collect electronic health data, aggregate and store data securely, analyze data, and create solutions in the cloud.

HealthSuite Edge also eliminates the burden of owning and managing infrastructure to enable these capabilities with an easy-to-install, device-as-a-service deployment designed specifically for privacy and security.

Philips is bringing the HealthSuite Edge to the HealthSuite Platform to relieve customers of non-core responsibilities with a compliant, easy-to-install, and secure solution so they can focus more on delivering innovative care solutions.

Ready to learn more about Edge?

The Philips HealthSuite Platform team is available to give you an introduction to HealthSuite Edge. You can contact us at HSDP-gettingstarted@philips.com

List of abbreviations

CE – Conformité Européene (European Conformity)
CISSP – Certified Information Systems Security Professional
CIPP – Certified Information Privacy Professional
CPU – Central Processing Unit
DHCP – Dynamic Host Configuration Protocol
DR – Disaster Recovery
EU – European Union
HCF – Healthcare Facility
HIPAA – Health Insurance Portability and Accountability Act
HS – HealthSuite
IEC – International Electrotechnical Commission
IP – Internet Protocol
IPsec – Internet Protocol Security
ISMS – Information Security Management System
ISO – International Organization for Standardization
ISO/IEC 27001 – Information Security Management systems standard
IT – Information Technology
ITIL – Information Technology Infrastructure Library
MFA – Multi-factor authentication
PC – Personal Computer
RSG – Remote Services Gateway
SBoM – Software Bill of Materials
SCP – Service Continuity Plan
SOC – System and Organization Controls for Service Organizations
TLS – Transport Layer Security
UI – User Interface
UL – Underwriters Laboratories
VPN – Virtual Private Network
X-Ray – Electromagnetic radiation

4522 991 82321 * OCT 2023

How to reach us
Please visit www.philips.com
healthcare@philips.com