PHILIPS

Remote Services

Protect your vital healthcare assets and information

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

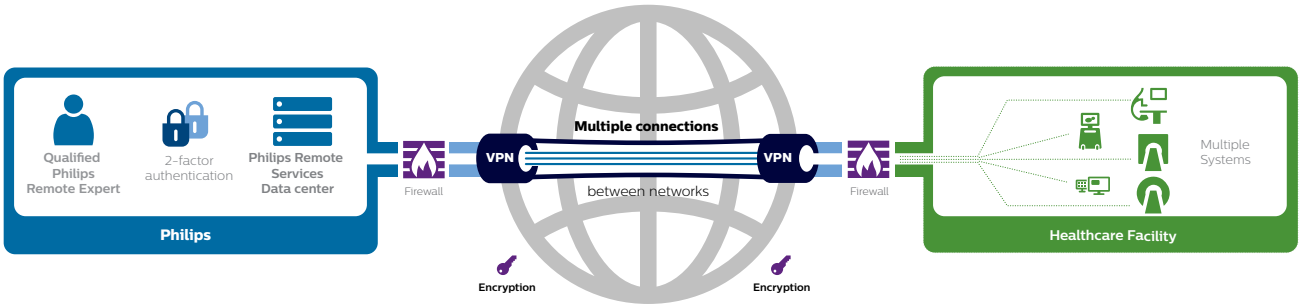
Services and Connection Methods

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.

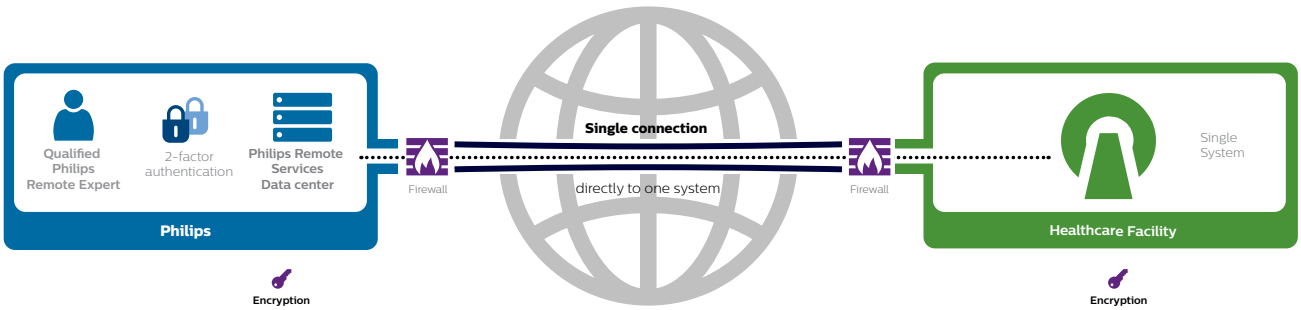
2. Are secure connection protocol(s) used to provide remote support?
To address the requirements of different customer IT infrastructure, clinical solutions connect to the Philips Remote Services either through a VPN tunnel using the Wireguard protocol or Internet Protocol security (IPsec) or through 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.

3(a). 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.

3(b). Does Philips support use of the customer's VPN 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. Philips Remote Services uses an ISO/IEC 27001 certified environment that provides advanced security and management features – see "Security Measures" for more details.

3(c). 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 an VPN tunnel. It uses encryption protocols that are supported by the FIPS 140-2 standard or better.

4. 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.

5. 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 Philips 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. The service applications available to the remote service engineers is 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 support service applications 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. At all times, remote service engineers will choose the service application commensurate with the level of troubleshooting that is necessary.

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

6. 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.

6(a). 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, Philips remote service engineers will establish a remote session to the device to address the issue.

7. 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

8. Describe how Philips is organized in terms of its approach to information security and governance
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 design-for-security 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 Global 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 / Cybersecurity Position Paper can be accessed at www.philips.com/security.

9. 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. Philips operates under its Binding Corporate Rules to ensure that privacy is addressed with the same high standard across the organization. You can find the details of our privacy policies at www.philips.com/privacy.

10. 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, including Personal Health Information (PHI). These measures are implemented in all of 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, remediated and validated in a pre-production environment and then deployed 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).

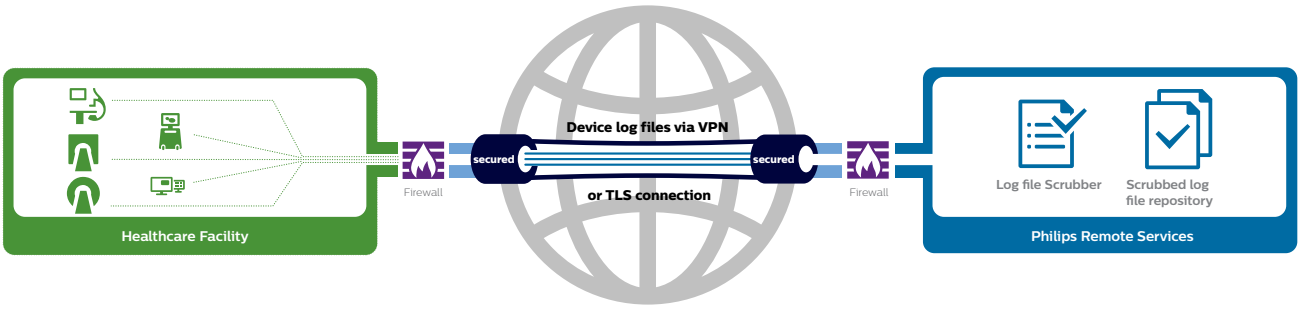
11. How can I monitor who is accessing my system through Philips Remote Services?
Remote support activities carried out via Philips Remote Services are logged and are traced to the individual Philips remote service engineer. Audit logs are stored for one year within Philips. Product specific application 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.

Philips Remote Services does not support video recording of remote sessions initiated by the Philips remote service engineer to the customer's clinical solution. This approach avoids unnecessary processing of Protected Health Information stored on the customer's clinical solution. Philips Privacy Rules enforce restrictions on the processing of customer data, to reduce privacy risks. The Philips Remote Services audit logs, in conjunction with the device logs, provide a detailed "record" of the remote service activities.

12. How does Philips safeguard Protected Health Information (PHI) and sensitive data?
Personal/sensitive data is not retrieved from clinical solutions in customer sites and is not transferred to the Philips Remote Services servers for storage. The processing of personal or sensitive data is not the intent for the provision of service. Incidental personal data (stored locally on the device) may be accessed by the Philips remote service engineer for problem resolution only.
All interactive sessions to a customer's clinical solution begin with a mandatory, formal customer service request.

Only Philips experts with a "need to know" authorization using a verified Philips Enterprise laptop and two-factor authentication is allowed access to your medical device. Philips takes several steps to decrease the risk of collection and unauthorized disclosure of personal data that may be transferred to Philips via the Remote Services. For example, all Philips products are designed to limit the collection of personal data and sensitive data (PHI) in device log files; automated scrubbing of personal information is done on the log file data retrieved via the Philips Remote Services Network (see diagram below).

Philips Service Engineers undergo annual training on the Philips General Business Principles, Data Privacy, and Information Security topics.



13. 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 is only allowed through a verified Philips Enterprise issued laptop and 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.

14. How do Philips 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. Philips remote service engineers use their verified Philips Enterprise issued laptop and 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 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.

15. What security controls are enforced on the PC/laptop used by Philips remote service engineers, to establish a remote support connection to my system(s)?
Philips remote service engineers use a verified Philips Enterprise issued laptop to connect to the Philips Remote Services Network. Philips Enterprise laptops have centrally managed security controls, which include endpoint protection software, host-based intrusion prevention system, full-disk encryption, timely security patching, and advanced threat protection.

16. Can a Philips 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 through a verified Philips Enterprise issued laptop and requires two-factor authentication.

17. Can malware from a remote service engineer's PC/laptop infect my system(s) and disrupt my healthcare facility network?
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 is only possible from Philips Enterprise issued laptops (with verified security controls, as outlined above) and requires two-factor authentication.

18. 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. Periodic DR testing scenarios are defined for the Philips Remote Services. The Philips Remote Services is an ISO/IEC 27001 certified environment, which undergoes an annual ISO audit by a 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.

19. 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 is an ISO/IEC 27001 certified environment, which undergoes an annual ISO audit by a 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.

20. 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 is an ISO/IEC 27001 certified environment, which undergoes an annual ISO audit by a third-party auditor. Philips Remote Services currently uses third-party Subprocessors to provide infrastructure services and to help provide customer support and email notifications. Before engaging any third-party Subprocessor, Philips Remote Services performs due diligence to evaluate their privacy, security & confidentiality practices and executes data processing agreements with substantially similar requirements, including EU Model Contract Clauses, where required for compliance with GDPR. 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.

21. Is the Philips Remote Services infrastructure GDPR compliant?
The Philips Remote Services infrastructure is designed to meet the requirements for a GDPR compliant organization, such as but not limited to – Privacy by Design principles are adhered to where applicable, extensive security controls are established to safeguard the protection of personal data, Data Protection Impact Assessments (DPIAs) are executed on a regular basis. Furthermore, Philips has appointed a data protection officer (DPO) and in some European countries, a local data protection officer.

22. Are independent third-party audits of Philips Remote Services facilitated to review security/privacy practices?
Customer-driven independent third-party audits of the Philips Remote Services are 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.

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

24. 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.

25. 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.

List of abbreviations
CE – Conformité Européene (European Conformity)
CPU – Central Processing Unit
DHCP – Dynamic Host Configuration Protocol
DPIA – Data Protection Impact Assessment
DPO – Data Protection Officer
DR – Disaster Recovery
EU – European Union
GDPR – General Data Protection Regulation (EU 2016/679)
HCF – Healthcare Facility
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
MFA – Multi-factor authentication
PC – Personal Computer
PHI – Protected Health Information
PRS – Philips Remote Services
SOC – System and Organization Controls for Service Organizations
TLS – Transport Layer Security
UL – Underwriters Laboratories
VPN – Virtual Private Network
X-Ray – Electromagnetic radiation

4522 991 61571 * MAY 2021

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