PHILIPS

Remote Services

Protect your vital healthcare assets and information

Philips Remote Services

FAQs 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 you make the most of your clinical solutions. Our innovative set of proactive services aim to continuously support your systems remotely without interrupting your daily routine. They allow us to provide high system uptime and deliver innovative new services to your healthcare facility. Philips Remote Services are delivered via an advanced, business to business virtual private network (VPN) or through a secure socket layer (SSL) outbound connection that establishes a secure connection between your clinical solutions and our Remote Service Data Center.

2. What connection method(s) are used to provide remote support?
To meet the needs of different IT infrastructures, Philips Remote Services connects via a VPN using internet protocol security (IPSec) and/or via a direct outbound SSL connection (depending on the clinical solution). For both VPN and SSL connections, customer data transmitted over the internet is encrypted.

Your facility can choose which type of connection it prefers to use, but we usually recommend an SSL connection. It offers the advantages of enhanced speed and quality of your connection and provides you with more control over the connection. To make an informed decision, please see more details about the different options further in this document.

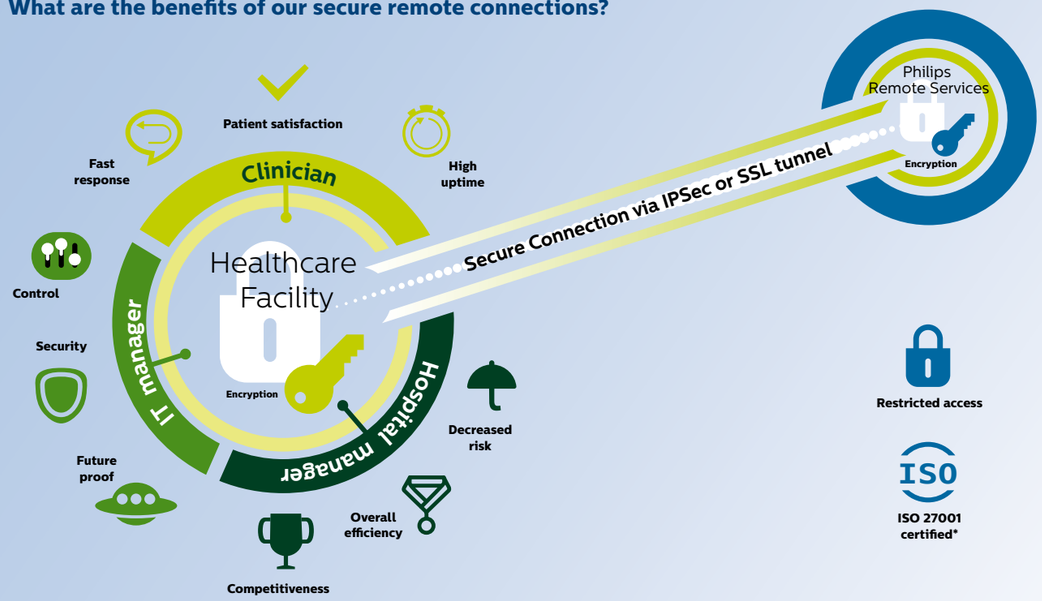
3. What is the difference between a Philips Remote Services VPN and SSL-based connection and what does that mean for my facility?
For the Philips VPN connection, your facility must have an IPSec compatible VPN router, and the remotely supported medical devices must be configured with static IP addresses. An SSL-based connection uses your facility's existing network to set up a secure connection over the internet and supports remote access to medical devices deployed with dynamic IP addresses via DHCP.* The IPSec VPN tunnel provides site-to-site encryption. Data transmitted within the healthcare facility's network may not be encrypted depending on the remote tool used. SSL-based connectivity provides encryption between the two end points, e.g. the medical device and Philips Remote Services Data Center.

4. How often does the medical device connect with the Philips Remote Services server and how much bandwidth does the SSL-based connection use?
If and how frequently device status information is sent to Philips depends on the specific product and remote service options that are enabled. As an example, for proactive services it is typically about every 5 minutes, but can range from every 30 seconds to every 15 minutes. The size of the typical device status data packet is just a few bytes. However the application traffic volume varies based on the modality (Computed Tomography, Magnetic Resonance, conventional and interventional X-ray*, Ultrasound, Nuclear Medicine, and Patient Monitoring Solutions) and specific usage (status update, downloading anti-virus files, uploading daily log files, etc.).

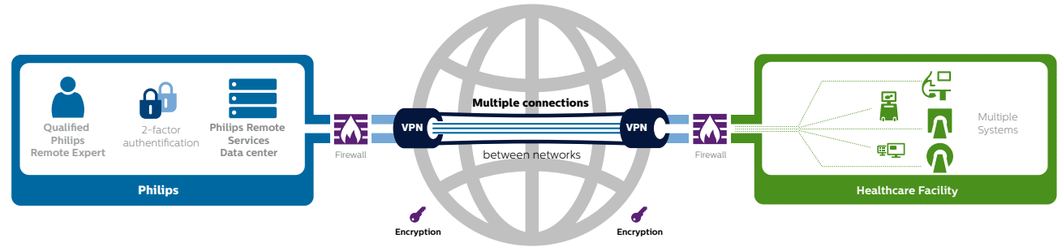
If my facility already has a Philips Remote Services connection via VPN, can I use SSL-based connectivity?
Yes, you can still use SSL-based connectivity. Devices that support SSL-based connectivity do not interfere in any way with devices that operate over the Philips Remote Services VPN. SSL-based devices can connect and operate directly over the internet using your existing network or also be routed over the Philips Remote Services VPN.

Does Philips support use of my non-Philips Healthcare Facility (HCF) 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 hospital VPN clients for remote support. Philips Remote Services uses a secure environment that provides advanced security and management features. See Security measures.

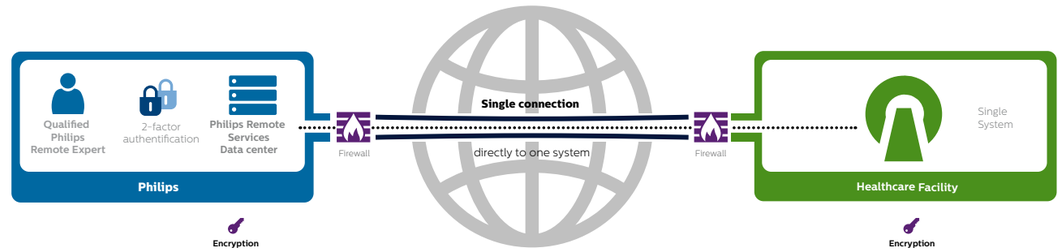
What are the benefits of our secure remote connections?



Philips solutions for secure connection



IPSec VPN tunnel
A VPN tunnel can be used to establish a secure connection between your Healthcare Facility and Philips Remote Service Data Center. The 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 Service Data Center.



Outbound SSL connection
This solution establishes a fully encrypted tunnel between the two end points. The advantage of an outbound SSL 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. There are no additional router configurations required.

Security measures

5. What security standards does Philips Remote Services adhere to?
Philips Healthcare is committed to proactively addressing the security and privacy concerns of your healthcare facility. Our Remote Services are based on a comprehensive security infrastructure as well as stringent procedures and controls to safeguard system security and data privacy. Philips operates under its Binding Corporate Rules to facilitate that privacy is addressed with the same high standard across the organization.

You can find the details of our privacy policies on the Philips internet site under Investor Relation / General Business Principles. The Philips Remote Services operating environment implements security controls that meet the internationally recognized ISO 27001 information security management systems standard and is audited annually by an independent third party.

6. What control do I have over my systems and information?
To meet your facility's fundamental needs we offer a portfolio of remote capabilities and access controls that give you the flexibility to manage and monitor Philips remote access to your solution. You can decide to allow your devices to be proactively monitored 24/7 – depending on product capabilities and/or local regulations. Automatic downloading can enable technical log files for system analysis and uploading of security patches.

To save time, you can choose to allow a remote service engineer to fix an issue that you reported or use a remote access application for remote service, clinical support, and training purposes. You can also enable certain features on a per session basis if preferred.

To provide security at all times, safeguards are implemented in our solutions to limit remote user access to specific device functions when performing remote diagnostics. Your healthcare facility can monitor all remote services activities. If you would like to find out more about how you can monitor our remote services activities, please see below.

7. 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 can be traced to the individual Philips Service user. Audit logs are stored for one year within Philips. Product specific application or configuration changes executed remotely are not logged within the Philips Remote System, but are logged in the product's service registry/ audit logs. Customers can access the detailed audit logs of Philips Remote Services activities at any time via the Philips Remote Services Audit website. For remote service activities carried out via Philips SSL connection, Philips can provide logs to your healthcare facility upon request.

* The full list of abbreviations is provided at the end of this document.

8. How does Philips safeguard my Protected Health Information (PHI) / sensitive data?

Only Philips experts with a “need to know” authorization, using two-factor authentication are 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 by designing Philips Healthcare products that limit collection of personal data and sensitive data (ePHI) in system log files, and/ or automated scrubbing of personal information when retrieving log file data via the Remote Services Network.

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

The type of information reviewed depends upon the device. In general, it includes reports on the device’s status and health using critical parameters such as helium level, temperature, CPU & memory utilization, etc. The device can send log files to Philips periodically, or immediately, upon detection of a fault. In the event that your device requires servicing, the system software on the device may allow service applications for example Remote Desktop to enable Philips remote access. Remote console applications allow a specialist to gain a live view of your screen, and remotely access the system when requested by you.

10. Where can I get more information?

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

List of abbreviations

CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
HCF	Healthcare Facility
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO 27001	Information Security Management systems standard
IT	Information Technology
(e)PHI	(Electronic) Protected Health Information
RSN	Remote services network
SSL	Secure Sockets Layer
VPN	Virtual Private Network
X-Ray	Electromagnetic radiation

Proactive support

To help you gain even higher uptime and control over your clinical solutions, we are innovating new services to optimize the performance, utilization and availability of your Philips clinical solutions. To deliver these advanced services, we continually monitor key parameters, alert you about potential issues, and capture trended performance data to proactively maintain the health of your solution.

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

4522 991 07511 * NOV 2014

www.philips.com