Protecting systems and patient privacy

Philips Remote Services Security

Remote services deliver the benefits of faster, easier problem resolution and less system downtime during troubleshooting and clinical support engagements on medical devices. Yet providing remote access to these important systems—and the sensitive data contained therein—can raise questions about system security and patient privacy.

Philips understands that today's healthcare environment demands strong security measures. Philips Remote Services are delivered via an advanced, Virtual Private Network (VPN) that links your Philips Healthcare equipment to our global Customer Care Center. Sophisticated security features such as scrubbers and escrow servers are built-in to optimize protection for your networks, medical systems, and patient privacy.

Philips Remote Services are based on a comprehensive security infrastructure as well as stringent procedures and controls for system and data access. You'll have peace of mind knowing that the Philips global team of security experts is available 24 x 7 to monitor the Philips Remote Services environment and respond to potential security issues.

PHILIPS

Philips Remote Services Security

Advanced support and repair services

Philips Remote Services deliver a full range of support and repair services for your Philips Healthcare equipment. Remote diagnosis and repair capabilities enable Philips to connect to your system, detect the problem quickly, and usually solve problems immediately—online. If an onsite visit by a Philips field service engineer is required, remote troubleshooting allows Philips to identify defective parts in advance and accelerate the repair.

Through proactive monitoring and repair capabilities, technical experts at Philips can watch for deviations in key system performance parameters around the clock—without viewing or disrupting patient procedures. Often, Philips discovers and fixes problems *even before you have placed a service call.*

Philips Remote Services are essential to realizing maximum availability and effectiveness for your medical systems. You benefit from increased patient throughput resulting from higher equipment uptime via:

Remote Diagnosis and Repair Services

- Faster service response time
- Faster repair time
- Scheduled parts replacement
- Improved "first-time fix" repair rate

Proactive Monitoring and Repair Services

- Remote error detection and prevention
- Prevention of system downtime
- Ongoing performance and trend monitoring

Benefits for imaging and IT departments

The security design of Philips Remote Services delivers specific benefits for the medical imaging and IT departments.

For medical imaging departments:

- Reduced risk of system downtime and workflow disruption
- Protection of sensitive patient and medical data during service episodes
- Rapid response and problem resolution

For IT departments:

- Single, VPN link for remote services access
- Proactive Remote Service solution based on Secure Sockets Layer (SSL) and Private Key Infrastructure (PKI)
- Industry-standard security technologies, following NEMA remote services guidelines, for strong control of access and data transfer
- Training, authorization and authentication of Philips personnel to properly restrict activity on customer systems and access to data
- Facilitated compliance with international requirements for handling of healthcare information

Comprehensive security

Philips uses well-defined technical and organizational measures, together with the secure and reliable Philips Remote Services infrastructure, to ensure system security and patient privacy. These measures are implemented in all Philips Remote Services activities—from a remote system login to troubleshoot a user-reported problem, to a proactive maintenance task performed over the network link, to an on-site repair visit by a Philips field service engineer.

Additionally, all Philips service personnel receive extensive training in processes, procedures and policies to guard sensitive healthcare information. Only properly credentialed service personnel, with the appropriate role and relationship to the individual customer, are permitted to access your systems and data via Philips Remote Services.

You maintain control over service access to your systems by allowing service sessions to be initiated at your discretion. Philips can provide Web-based reports that show detailed information about service activity on your systems, allowing you to verify specific service events.

Standards-based security

Compliance with laws and standards governing healthcare security and privacy is critical for both healthcare organizations and medical systems manufacturers. The Philips Remote Services security solution is based on guidelines and best practices defined jointly by the NEMA/COCIR/JIRA Security and Privacy Committee. These standards emerged from a collaboration of medical imaging manufacturers in the United States, Europe and Japan, including Philips.

This standards-based approach:

- Limits the number or variety of remote connections between your site and the product manufacturer
- Limits administrative costs
- Reduces potential for security gaps
- Increases compatibility of security measures in a multi-vendor imaging environment

Data access during system service

Whenever a medical system can be accessed by someone outside of your organization, you may have concerns about which system and personal data may be seen or transferred to an external system. You want to know that personal data is accessed only when absolutely necessary, is visible only to authorized personnel, and is handled properly when no longer needed.

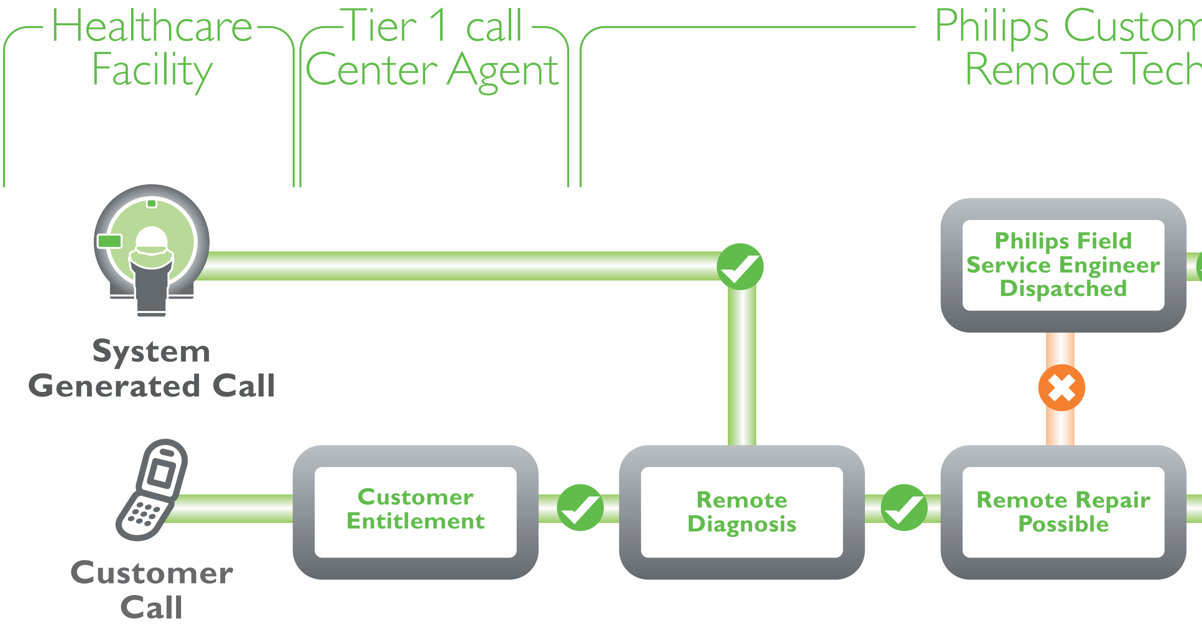
Philips Remote Services are designed to maintain strong protection for confidential healthcare information. In most cases, problems can be addressed by examining technical data from the affected system—no access to personal data is necessary.

In rare service cases, the analysis and repair tasks cannot be completed without accessing personal data. Access to personal data is limited to trained and authorized Philips technicians. For further protection of personal data, Philips implements specialized technical and organizational security measures such as:

- Files are transferred over secure VPN connections or Secure Sockets Layer (SSL)
- Transferred files are stored on an encrypted Philips server, so that when the service ticket is closed, the information collected is isolated and access restricted

When answering a user customer question regarding system operation, a Philips service engineer might make use of remote desktop management tools to view the customer's monitor display at the Philips Remote Services Center. This display appears only after you have granted access to this feature and is visible on the remote technical specialist's screen only for the duration of the service session. (See 'Screen sharing for problem identification' on page six.) However, if the service case must be escalated, the remote technical specialist may make a "screen shot" image of the customer display. This image is saved as an encrypted file and protected with the same measures that Philips applies to all healthcare information containing personal data.

For proactive system monitoring activities, only selected technical system parameters are transferred to the Philips Remote Service Center; no personal data is transferred. The system data may include logs, files, usage statistics and performance information, which help Philips analyze long-term trends in system performance and utilization.



The Philips Remote Services Network gives secure access to your medical imaging systems for Philips authorized technicians.

A security infrastructure designed for remote services

The Philips Remote Services infrastructure is based on a Virtual Private Network (VPN) tunnel with enhanced security features. This design provides a single, highly secure network link between Philips and your facility. It also helps to ensure that security threats do not interfere with patient care and reduces imaging system downtime during maintenance and repair activities.

Within the Philips Remote Services Network, the security infrastructure deters unauthorized access that could extend into the healthcare facility network. The Philips Remote Services Network can be accessed via the Philips global network and via a SSL-secured tunnel by authorized Philips computers and personnel only. Firewalls isolate the Philips Remote Services network from any other networks, including the Philips global network.

Security capabilities are also built into the Philips routers and access concentrators that manage the VPN tunnels between the Philips Remote Services data center and customer sites. Additional security measures are implemented in the network connections, and through access control lists, data transfer, data encryption methods, and a standard antivirus solution.

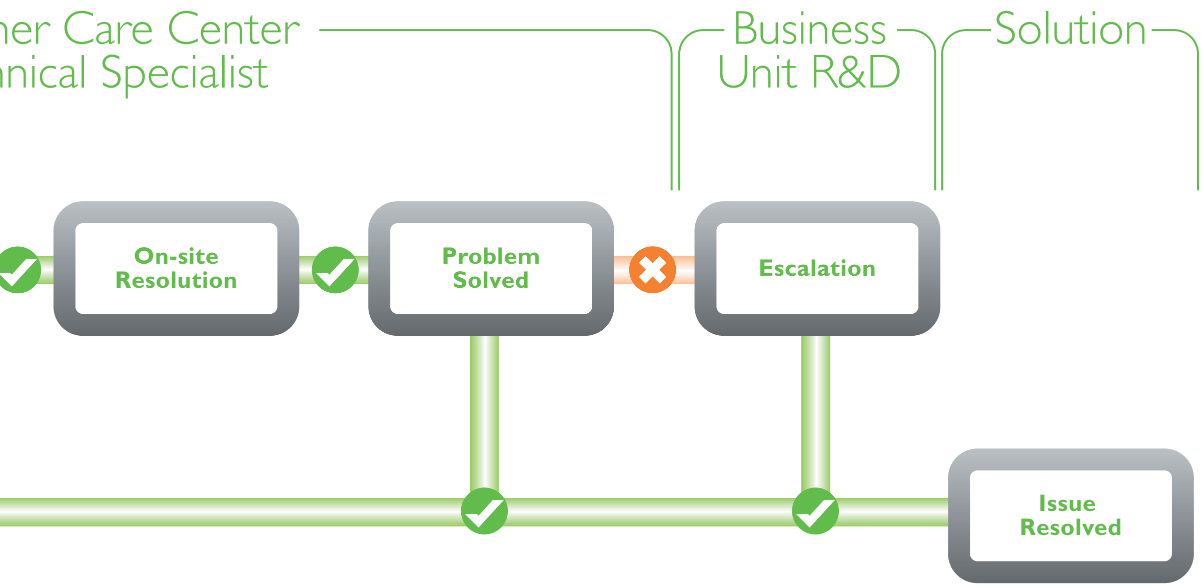
Connection-level security

The VPN tunnel between the Philips Remote Services Data Center and your site is secured through a variety of protection methods.

Secure VPN tunnel. To ensure that entry and exit points are known and fully controlled, Philips requires IPSec or Public Key Infrastructure (PKI) certificates to authenticate the VPN connections. In addition, Philips does not support analog modem connections to medical devices via the Remote Services Network because modems pose a security risk to a hospital's network and IT assets.

Secure Socket Layer (SSL). Philips also provides an SSL connection for delivering remote services as an alternative to the VPN tunnel requiring IPSec and PKI certificates to authenticate as stated above.

Port-level security. The Philips Remote Services environment uses port-level security to thwart hacker attacks targeting the Philips Remote Services Network. Traffic is limited to authorized ports and



protocols only. The VLAN architecture is implemented to isolate the various parts of the Philips Remote Services Network, so that servers on other VLANs are not accessible and thus avoid cross contamination.

Minimizing the impact of an attack. Access to customer systems by Philips Remote Services is through a Citrix-based application that runs on a Philips server farm. This access design creates a complete physical isolation of Philips computers on the Philips internal network from the healthcare facility network.

Limiting internal risk. Unfortunately, malicious security attacks can originate within a hospital or partner facility. VPN technology deployed by Philips Remote Services separates traffic and prevents hospital-to-hospital traffic bridging as well as virus proliferation into the Remote Services Network.

Limiting IP addresses. All traffic originating from Philips Remote Services is sourced from a small number of IP addresses that are controlled by Philips and are not visible to the Internet. This feature allows healthcare IT administrators to filter or block traffic by source IP addresses, which reduces the risk of unauthorized access or harmful traffic.

Access control

Monitoring and controlling the activities of users while they access your medical systems is another critical security measure.

Role-based and user-based access. User access to Philips Remote Services is tightly controlled by rigorous internal policies and procedures, with privileges assigned on a role and user basis. Each Philips user must connect to the Philips Remote Services Network using a secure token device as well as a unique account and password for two factor authentication and access control. The user's defined profile is activated automatically, permitting access only to preassigned customer facilities and systems.

Remote access logging. Philips Remote Services was designed to provide the tracking that assists customers in monitoring security. For example, Philips tracks, identifies and logs all access attempts and activities during remote service sessions. Online access to a real-time audit trail report allows you to view the details of remote access and activity on your systems.

Screen sharing for problem identification. Many Philips diagnostic services are noninvasive and do not impact the operation of a medical device. However, for utilities such as screen sharing that can impact customer operations, Philips has implemented a request/grant system where the customer must grant permission to establish a remote session. This capability puts access control into your hands, avoids interruptions of patient procedures and allows for a smooth workflow.

Data transfer and encryption

Philips adheres to procedures and controls over system access and data transfer as well as advanced encryption technologies to maintain the confidentiality of your networks, systems and sensitive data.

No Internet connection. Unlike other remote service solutions, Philips does not allow access to or from the Internet via the Philips Remote Services infrastructure. Tunneling of connections to reach Internet content is not supported, which significantly reduces the risk of exposure to hacker attacks or external virus injection.

No email interface. Email interfaces are cumbersome to administer and represent significant security risks. Philips does not deploy email interfaces in the Philips Remote Services environment. Instead, Philips uses agent-based connectivity for gathering alerts from customer systems. This design allows customer-based call initiation from the site or device to signal the delivery of alerts, services and other features through an existing connection to the Philips Remote Services environment.

Data encryption. Philips has made significant investments in its remote services to protect sensitive data and encrypts all transmissions to and from the customer site. Philips deploys the 3DES encryption protocol, which is compliant with the FIPS 2.0 government standard for encrypted data transmissions.

Antivirus solution

Philips antivirus protection uses defense-in-depth measures, with the antivirus solution deployed and active at every tier of a remote connection. The tiers consist of the field service engineers' laptop PC, the Remote Services Network and the final destination, the medical device. The laptop PC and the Philips Remote Services infrastructure are protected via an antivirus solution that is updated automatically. Many of the medical devices installed in hospitals include the Philips Anti Virus Solution, which updates the medical systems in a controlled manner with the latest virus definition files.

Securing the advantages of Philips Remote Services

With Philips Remote Services, your healthcare facility will gain the advantages of proactive support and enhanced service performance—all while protecting the security of medical systems and monitoring systems and patient privacy.

The worldwide Philips Remote Services network links your Philips Healthcare equipment to our global Philips Customer Care Centers. The Philips Remote Services Network provides fast, reliable and secure communications links.

The result is rapid, advanced support delivered 24 x 7 by authorized Philips Remote Services resources.

For more information

Visit our internet security page at **www.healthcare.philips.com/main/support/productsecurity/index.wpd.**

Philips Customer Services provides innovative solutions that can help you meet your challenges, simplify your business and focus more on patient care.

Start-up
Peak Usage
Renewal
Planning
Seasons of Ownership

Philips Healthcare is part of
Royal Philips Electronics

How to reach us
www.philips.com/healthcare
healthcare@philips.com
fax: +31 40 27 64 887

Asia
+852 2821 5888

Europe, Middle East, Africa
+49 7031 463 2254

Latin America
+55 11 2125 0744

North America
+1 425 487 7000
800 285 5585 (toll free, US only)

Philips Healthcare
Global Information Center
P.O. Box 1286
5602 BG Eindhoven
The Netherlands

Philips Healthcare reserves the right to make changes in specifications and/or to discontinue any product at any time without notice or obligation and will not be liable for any consequences resulting from the use of this publication.

Printed in The Netherlands.
4522 962 34601/800 * DEC 2008