PHILIPS

Remote Services

Schutz Ihrer medizinischen Systeme und der Patientendaten

Philips Remote Services
Häufig gestellte Fragen zu Konnektivität und Datensicherheit

Um Sie bei der effizienten Erbringung einer qualitativ hochwertigen Patientenversorgung und dem Schutz sensibler Patientendaten zu unterstützen, bieten wir Ihnen sichere Remote-Support-Lösungen und -Systeme. In diesem Dokument finden Sie Informationen zu unserer Technologie für Remote-Verbindungen und unseren Sicherheitsvorkehrungen.

Datensicherheit

Senkung des Risikos

Hohe Systemverfügbarkeit

Kurze Reaktionszeiten

Kontrolle

Dienstleistungen und Verbindungsmethoden

1. Was sind Philips Remote Services?
Philips Remote Services bieten technischen und klinischen Remote-Support, damit Sie Ihre medizinischen Systeme optimal nutzen können. Unsere innovativen, proaktiven Dienstleistungen sollen den kontinuierlichen Betrieb Ihrer Systeme über eine Remote-Verbindung sicherstellen, ohne Ihre täglichen Arbeitsabläufe zu stören. Dadurch können wir für eine hohe Systemverfügbarkeit sorgen und Ihrer Einrichtung innovative neue Dienstleistungen anbieten. Philips Remote Services werden über eine hochmoderne, sichere B2B-VPN-Verbindung (virtuelles Privatnetzwerk) oder eine ausgehende SSL-Verbindung (Secure Socket Layer) zwischen Ihren klinischen Lösungen und unserem Remote Services Data Center bereitgestellt.

2. Welche Verbindungsmethoden werden für den Remote Support genutzt?
Zur Erfüllung der Anforderungen von unterschiedlichen IT-Infrastrukturen stellen die Philips Remote Services über ein VPN mittels IPSec (Internet Protocol Security) und/oder eine ausgehende SSL-Direktverbindung (je nach klinischer Lösung) die gewünschte Verbindung her. Bei VPN- und SSL-Verbindungen werden die über das Internet übertragenen Kundendaten verschlüsselt.

Ihre Einrichtung kann die jeweils bevorzugte Verbindungsart wählen, wobei im Regelfall eine SSL-Verbindung empfohlen wird. Diese zeichnet sich durch höhere Geschwindigkeit und Qualität aus und bietet Ihnen auch eine bessere Kontrolle über die Verbindung. In diesem Dokument finden Sie weitere Einzelheiten über die verschiedenen Optionen, damit Sie leichter eine fundierte Entscheidung treffen können.

3. Worin besteht der Unterschied zwischen einer VPN- und einer SSL-basierten Verbindung bei Philips Remote Services? Was bedeutet das für meine Einrichtung?
Bei der Philips VPN-Verbindung muss Ihre Einrichtung über einen IPSec-kompatiblen VPN-Router verfügen; die durch Fernzugriff unterstützten Medizinprodukte müssen mit statischen IP-Adressen konfiguriert sein. Eine SSL-basierte Verbindung nutzt das in Ihrer Einrichtung vorhandene Netzwerk zur Herstellung einer sicheren Verbindung über das Internet und unterstützt den Fernzugriff auf die mit dynamischen IP-Adressen bereitgestellten Medizinprodukte über DHCP. Der IPSec-VPN-Tunnel ermöglicht Punkt-zu-Punkt-Verschlüsselung. Je nach verwendetem Remote-Tool werden die innerhalb des Netzwerks der medizinischen Einrichtung übertragenen Daten nicht verschlüsselt. Eine SSL-basierte Verbindung ermöglicht die Verschlüsselung zwischen zwei Endpunkten, z.B. zwischen einem Medizinprodukt und dem Philips Remote Services Data Center.

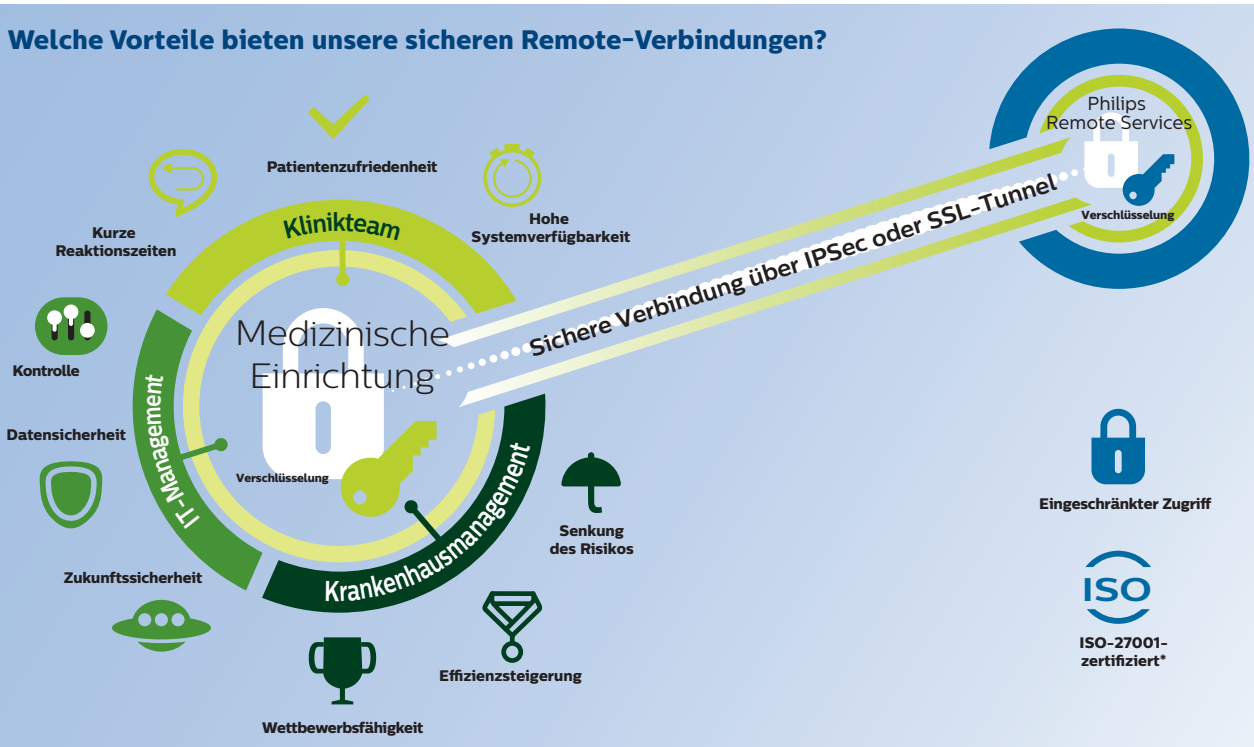
4. Wie oft stellt das medizinische Gerät eine Verbindung zum Philips Remote Services Server her und wie viel Bandbreite benötigt die SSL-basierte Verbindung?
Ob und wie häufig Daten zum Gerätestatus an Philips weitergeleitet werden, hängt von den jeweils aktivierten Produkt- und Remote-Service-Optionen ab. Beispielsweise werden Daten bei proaktiven Dienstleistungen in der Regel alle 5 Minuten übertragen; das Übertragungsintervall kann jedoch von 30 Sekunden bis 15 Minuten reichen. Normalerweise beträgt das Datenpaket mit Angaben zum Gerätestatus nur wenige Bytes. Das Volumen des anwendungsbezogenen Datenverkehrs hängt jedoch von der Modalität (CT, MRT, konventionelle und interventionelle Radiologie, Ultraschall, Nuklearmedizin und Lösungen für die Patientenüberwachung) und der jeweiligen Nutzung (Statusaktualisierung, Herunterladen von Antivirus-Dateien, Hochladen von täglichen Protokolldateien usw.) ab.

Kann ich die SSL-basierte Verbindung auch dann nutzen, wenn bereits eine VPN-Verbindung zwischen meiner Einrichtung und Philips Remote Services besteht?
Ja, Sie können die SSL-basierte Verbindung nutzen. Geräte, die eine SSL-basierte Verbindung unterstützen, beeinträchtigen in keiner Weise Geräte, die über das VPN der Philips Remote Services betrieben werden. SSL-basierte Geräte können direkt über das Internet (über Ihr bestehendes Netzwerk) verbunden und betrieben oder über das VPN der Philips Remote Services geroutet werden.

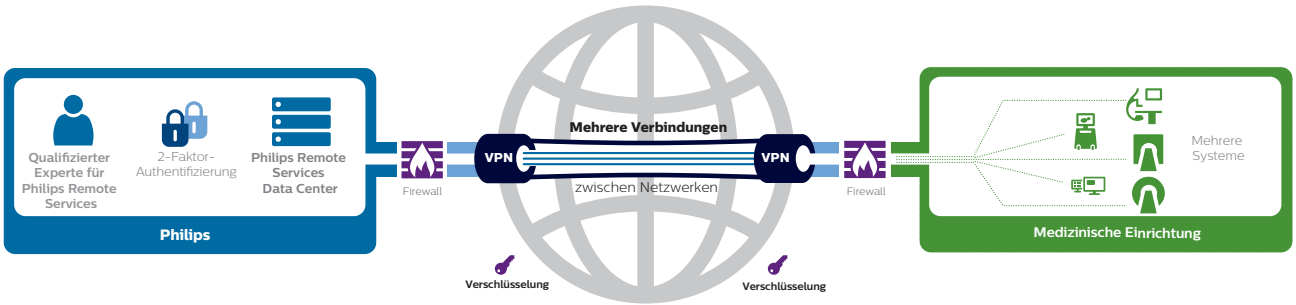
Unterstützt Philips die Nutzung von Drittanbieter-VPNs in meiner medizinischen Einrichtung für den Fernzugriff?

Um Ihnen jederzeit den bestmöglichen Service und umfassende Lösungen für den Remote-Support bereitstellen zu können, unterstützen wir keine VPN-Clients des Krankenhauses für den Remote-Support. Die Philips Remote Services nutzen eine sichere Umgebung, die erweiterte Sicherheits- und Managementfunktionen bietet. Weitere Informationen finden Sie im Abschnitt zu den Sicherheitsvorkehrungen.

Welche Vorteile bieten unsere sicheren Remote-Verbindungen?



Lösungen von Philips für sichere Verbindungen



IPSec-VPN-Tunnel

Zwischen Ihrer Einrichtung und dem Philips Remote Service Data Center kann über einen VPN-Tunnel eine sichere Verbindung mit Punkt-zu-Punkt-Verschlüsselung hergestellt werden.

Ausgehende SSL-Verbindung

Mit dieser Lösung wird der Tunnel zwischen den beiden Endpunkten vollständig verschlüsselt. Der Vorteil einer ausgehenden SSL-Verbindung vom Medizinprodukt zum Philips Remote Services Data Center besteht darin, dass vom Medizinprodukt lediglich eine Verbindung zum Internet hergestellt werden muss. Zusätzliche Routerkonfigurationen sind nicht erforderlich.

Sicherheitsvorkehrungen

5. Welche Datensicherheitsstandards werden von Philips Remote Services eingehalten?

Der gesetzlich geregelte Datenschutz und proaktive Datensicherheit stehen bei Philips an oberster Stelle. Die Philips Remote Services arbeiten auf einer umfassenden Sicherheitsinfrastruktur sowie unter strengen Anforderungen und Kontrollmechanismen der gesetzlichen Auflagen. Verbindliche Verhaltensrichtlinien stellen den weltweit einheitlich hohen Datenschutzstandard in der gesamten Philips Gruppe sicher.

Einzelheiten zu unseren Datenschutzbestimmungen stellen wir Ihnen bei Bedarf gerne zur Verfügung.

6. Welche Kontrolle habe ich über meine Systeme und Daten?

Zur Erfüllung der grundlegenden Anforderungen Ihrer Einrichtung bieten wir eine große Palette an Funktionen für die Remote-Verbindung und für die Zugriffskontrolle an, mit denen Sie den Fernzugriff von Philips auf Ihre Lösung flexibel verwalten und überwachen können. Je nach Produktfunktionen und/oder lokalen Bestimmungen können Sie entscheiden, ob Ihre Geräte proaktiv rund um die Uhr überwacht werden sollen. Technische Protokolldateien für die Systemanalyse können automatisch heruntergeladen und Sicherheitspatches können hochgeladen werden.

Sofern technisch möglich, können wir von Ihnen gemeldete Störungen auch per Fernzugriff beheben oder zumindest eine Vorabdiagnose durchführen. Ebenso steht eine Anwendung für den Fernzugriff zwecks Remote-Support, klinischer Unterstützung und zu Schulungszwecken zur Verfügung. Auf Wunsch ist auch die Aktivierung bestimmter Funktionen pro Sitzung möglich.

Damit die Datensicherheit jederzeit gegeben ist, verfügen unsere Lösungen über integrierte Sicherheitsmechanismen, die den Fernzugriff für Benutzer auf bestimmte Gerätefunktionen bei der Ferndiagnose beschränken. Ihre medizinische Einrichtung kann die Aktivitäten der Remote Services überwachen. Nachstehend finden Sie dazu weitere Informationen.

7. Wie kann ich überwachen, wer über Philips Remote Services auf mein System zugreift?

Die über Philips Remote Services vorgenommenen Remote-Support-Aktivitäten werden protokolliert und lassen sich zu jedem einzelnen Benutzer bei Philips zurückverfolgen. Die Prozessprotokolle werden ein Jahr lang bei Philips gespeichert. Per Fernzugriff vorgenommene Anwendungs- oder Konfigurationsänderungen werden nicht im Philips Remote System, sondern in der Registry/den Prüfprotokollen des Produkts aufgeführt. Über die Philips Remote Services Audit Internetseite können Kunden jederzeit auf die detaillierten Prüfprotokolle zu den Aktivitäten der Philips Remote Services zugreifen. Für Aktivitäten der Remote Services, die über eine Philips SSL-Verbindung durchgeführt werden, kann Philips Ihrer medizinischen Einrichtung auf Wunsch Protokolle zur Verfügung stellen.

8. Wie schützt Philips die sensiblen, vertraulichen Patientendaten?
Nur Philips Mitarbeiter mit zwingend erforderlichem Zugriff und entsprechender Autorisierung erhalten Zugriff zu Ihren Medizinprodukten (mittels Zwei-Faktor-Authentifizierung). Mittels mehrerer Maßnahmen verringert Philips das Risiko der Erfassung und unbefugten Offenlegung personenbezogener Daten, die über die Remote Services an Philips weitergeleitet werden können, beispielsweise durch die Entwicklung von Philips Produkten, die die Erfassung personenbezogener und sensibler Daten (ePHI) in Systemprotokolldateien einschränken, und/oder durch automatische Löschung personenbezogener Informationen bei Abruf von Protokolldaten über das Remote Services Netzwerk.

9. Welche Informationen werden von den Philips Mitarbeitern geprüft und wie werden sie verwaltet?
Die Art der geprüften Informationen hängt vom jeweiligen Gerät ab. Im Allgemeinen handelt es sich dabei um Berichte zum Gerätestatus und -zustand in Form von kritischen Parametern wie Heliumstand, Temperatur, CPU- und Speicherauslastung. Nach dem Erkennen eines Fehlers kann das Gerät in regelmäßigen Abständen oder umgehend Protokolldateien an Philips senden. Falls zu Wartungs- oder Instandhaltungszwecken aktiv auf Ihr System zugegriffen werden muss, kann die Systemsoftware des Geräts die Ausführung von Service-Anwendungen wie Remote Desktop gestatten, um Philips den Fernzugriff zu ermöglichen. Über Remote-Konsolenanwendungen wird einem Philips Spezialisten eine Live-Ansicht Ihres Bildschirms angezeigt und der Fernzugriff auf das System ermöglicht, sofern Sie dies wünschen.

10. Wo kann ich weitere Informationen erhalten?
Allgemeine Informationen zu Philips Remote Services oder Informationen zu bestimmen Netzwerkeigenschaften Ihres Geräts erhalten Sie bei Ihrem Philips Customer Care Center.

Liste der Abkürzungen und Akronyme

CPU	Central Processing Unit, Zentraleinheit
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol (Internetprotokoll)
IPSec	Internet Protocol Security
ISO 27001	Norm für Informationssicherheits-Managementsysteme
IT	Informationstechnologie
(e)PHI	(Electronic) Protected Health Information; (elektronische) geschützte Gesundheitsdaten
RSN	Remote Services Network
SSL	Secure Sockets Layer
VPN	Virtuelles Privatnetzwerk

Proaktiver Support

Wir entwickeln ständig innovative neue Dienstleistungen, um die Leistung, Auslastung und Verfügbarkeit Ihrer klinischen Lösungen von Philips zu optimieren und Ihnen eine noch bessere Kontrolle zu ermöglichen. Zur Erbringung dieser Leistungen überwachen wir permanent wichtige Parameter, informieren Sie über potenzielle Probleme und erfassen leistungsspezifische Trenddaten zur proaktiven Wartung Ihrer Lösung.

Anhand der Leistungsdaten werden mittels fortschrittlicher Algorithmen über einen längeren Zeitraum Trendanalysen erstellt. Auf der Grundlage dieser Informationen können Schlussfolgerungen gezogen werden, die eine Ferndiagnose zu Ihren Philips Geräten ermöglichen. Auf diese Weise können wir in vielen Fällen die Entstehung eines Problems erkennen, bevor für den Benutzer überhaupt Auswirkungen zu erkennen sind. Das Datenvolumen und die Häufigkeit der Datenübertragung hängen vom jeweiligen Produkt ab.

4522 991 07513 * JUN 2015