

# Sicherheitskonzept Version 4.3



## Siemens Remote Service

Die neue Service-Dimension. Online.

[www.siemens.de/medical](http://www.siemens.de/medical)

**SIEMENS**  
medical

<b>1. Allgemeines Betriebskonzept</b>	<b>4</b>
<b>1.1. Einleitung</b>	<b>4</b>
1.1.1. Zweck und Anwendung des Dokuments	4
1.1.2. Datenschutz als Grundvoraussetzung	4
1.1.3. Wartung an medizintechnischen Systemen	4
1.1.4. Verwendung einer standardisierten Lösung	4
<b>1.2. Fernzugriffe im Siemens Service-Prozess</b>	<b>5</b>
<b>1.3. Die technischen Möglichkeiten der Siemens-Produkte</b>	<b>6</b>
1.3.1. Sicherheit und Vertraulichkeit ist unser Ziel	6
1.3.2. Applikationssoftware <i>syngo</i>	6
1.3.3. Produktklassen, die <i>syngo</i> nicht nutzen	6
1.3.4. Besonderheiten bei Online-Hilfestellungen	6
1.3.5. Proaktive Serviceleistungen	6
<b>2. Technisches und organisatorisches Konzept</b>	<b>7</b>
<b>2.1. Überblick</b>	<b>7</b>
2.1.1. Verbindungsaufbau	7
2.1.2. Zugriffskontrolle	8
2.1.3. Vier-Augen-Prinzip	8
2.1.4. Protokollierung	8
2.1.5. Vertraulichkeit auf dem Übertragungsweg	8
2.1.6. Organisatorische Maßnahmen	8
<b>2.2. Sicherheitsinfrastruktur von Siemens Remote Service</b>	<b>9</b>
2.2.1. Authentifizierung und Autorisierung unserer Service-Ingenieure	9
2.2.2. Demilitarisierte Zone	9
2.2.3. Sicherung der Übertragungsstrecke	9
2.2.4. Sicherheitsmaßnahmen im Kundennetzwerk	11
<b>2.3. Schutz vor böswilligen Angriffen</b>	<b>11</b>
2.3.1. Geschützter SRS-Server	11
2.3.2. Schutz der Kunden-Systeme	11

# Siemens Remote Service

**Die neue Service-Dimension. Online.**

**Mehr Service. Mehr Komfort. Damit Sie den Kopf frei haben, sich auf das Wesentliche zu konzentrieren – Ihre klinische Arbeit.**

Hohe Systemverfügbarkeit, sichere Diagnosen, optimaler Workflow – um Ihre Performance-Erwartungen jederzeit erfüllen zu können, setzen wir konsequent auf Proaktivität. Auf Echtzeit-Überwachung und präventive Fernwartung medizinischer Hard- und Software. Auf proaktive Analytik und vorausschauende Logistik für die Planung und Durchführung von Service-Einsätzen. Und auf intelligente Prozesse, die uns helfen, von Tag zu Tag besser zu werden. So verhindern wir Systemausfälle und Qualitätsschwankungen, bevor sie auftreten. So ermöglichen wir mehr Systemauslastung, Prozesseffizienz und Produktivität – und verschaffen Ihnen den entscheidenden Vorsprung vor dem Wettbewerb. Proaktiv.

Dabei haben wir den Themen Datensicherheit und Zugriffsschutz von Anfang an höchste Priorität gegeben. Kein Klick in Ihr System erfolgt ohne Ihre Zustimmung, keine Maßnahme im Gerät ohne Ihre Kenntnis.

Unser Sicherheitskonzept besteht aus zwei Teilen. Im ersten Teil, dem allgemeinen Betriebskonzept, geben wir Antworten auf Fragen zur Wartung mit Siemens Remote Service, zu unseren Service-Prozessen und den technischen Möglichkeiten unserer Produkte. Dieser Teil richtet sich vor allem an Radiologen, Krankenhausadministratoren und technische Leiter.

Der zweite Teil, das technische und organisatorische Konzept, richtet sich an IT-Spezialisten und Datenschutzbeauftragte, die im Detail erfahren möchten, welche technischen und organisatorischen Maßnahmen wir treffen, um den hohen Anforderungen an Datensicherheit und Zugriffsschutz gerecht zu werden. In diesem Teil erklären wir, auf welche Weise die Verbindung von Ihrem Netzwerk zu Siemens Remote Service hergestellt wird, wie unsere Sicherheitsinfrastruktur aufgebaut ist und was wir tun, um böswillige Angriffe abzuwehren.

## Life

Siemens Remote Service ist ein Bestandteil von Life. Mit Life bieten wir Ihnen Unterstützung, damit Sie Ihre Investition von heute über den gesamten Lebenszyklus optimal nutzen und eine maximale Rendite erzielen können. Nach dem Kauf stellen wir Ihnen verschiedene Programme und Dienstleistungen zur Verfügung, wie Weiterbildungen, Services zur Maximierung der Produktivität oder Zugang zu neuen technologischen Entwicklungen.

Für die kontinuierliche Weiterentwicklung von Know-how, Produktivität und Technologie. Life. Kundenbetreuung so individuell wie Ihre Bedürfnisse.

## 1. Allgemeines Betriebskonzept

### 1.1. Einleitung

#### 1.1.1. Zweck und Anwendung des Dokuments

Dieses Sicherheitskonzept beschreibt, welche Maßnahmen Siemens ergreift, um Patientendaten bei der Durchführung von Siemens Remote Service an medizintechnischen Produkten der Siemens AG, Medical Solutions zu schützen. Es wird bei sämtlichen Produkten, bei denen Siemens Remote Service angeboten wird, angewendet.

#### 1.1.2. Datenschutz als Grundvoraussetzung

Ein Patient erwartet beim Arztbesuch, dass die gesetzlichen Regelungen zum Schutz seiner persönlichen Daten eingehalten werden. Im Falle der Fernwartung haben sowohl der behandelnde Arzt als auch Siemens hierzu gewisse Verpflichtungen einzuhalten. Welche technischen und organisatorischen Maßnahmen Siemens zum Schutz personenbezogener Daten sowie zur Sicherung der für Siemens Remote Service genutzten Infrastruktur ergreift, beschreibt dieses Sicherheitskonzept.

#### 1.1.3. Wartung an medizintechnischen Systemen

Die zunehmende Komplexität medizintechnischer Systeme stellt auch deren Wartung vor ständig neue Herausforderungen. Mit Siemens Remote Service haben wir eine Lösung entwickelt, die dieser Entwicklung Rechnung trägt. So können die Ursachen für Systemstörungen oftmals bereits per Ferndiagnose ermittelt und per Fernreparatur behoben werden. Und falls eine Fernreparatur nicht möglich ist, liefern die per Ferndiagnose ermittelten Informationen unseren Service-Ingenieuren vor Ort wertvolle Unterstützung.

Das ist aber noch nicht alles: Mit unseren proaktiven Services arbeiten wir präventiv, statt erst im Störfall zu reagieren. Dabei überwacht unsere Software selbstständig wichtige Parameter Ihrer Systeme. Werden vorher definierte Werte über- oder unterschritten, sendet Ihr System automatisch eine Meldung an unsere Service-Zentrale, das UPTIME Service Center. Hier wird anschließend die eingehende Meldung analysiert und – falls notwendig – eine präventive Fernreparatur eingeleitet. Ganz ohne Ihren Patien-

tenbetrieb zu beeinflussen. Oder wir beheben die sich ankündigende Störung im Rahmen des nächsten geplanten Service-Einsatzes bzw. innerhalb der vertraglich vereinbarten Reaktionszeit.

Ob vor Ort oder per Fernwartung: Viele Fehler lassen sich bereits auf Grundlage von technischen Daten des Systems erkennen und beheben. Der Zugriff auf Patientendaten ist dann nicht notwendig. Falls der Zugriff auf Datensätze oder Bilder, die Patientendaten enthalten, dennoch einmal notwendig sein sollte, haben wir für die meisten unserer Produktklassen sichergestellt, dass patientenbezogene Daten vor der Übertragung automatisch und zuverlässig ausgeblendet werden.

Im Fall von Produktklassen, bei denen dies technisch noch nicht möglich ist bzw. bei denen die Aufgabenstellung dies nicht erlaubt (z. B. beim Zugriff auf Datenbanken), schränken wir die Zugriffe auf Patientendaten so weit wie möglich ein und treffen besondere technische und organisatorische Sicherheitsmaßnahmen (siehe Kapitel 2.), um die Vertraulichkeit dieser Daten nicht zu gefährden.

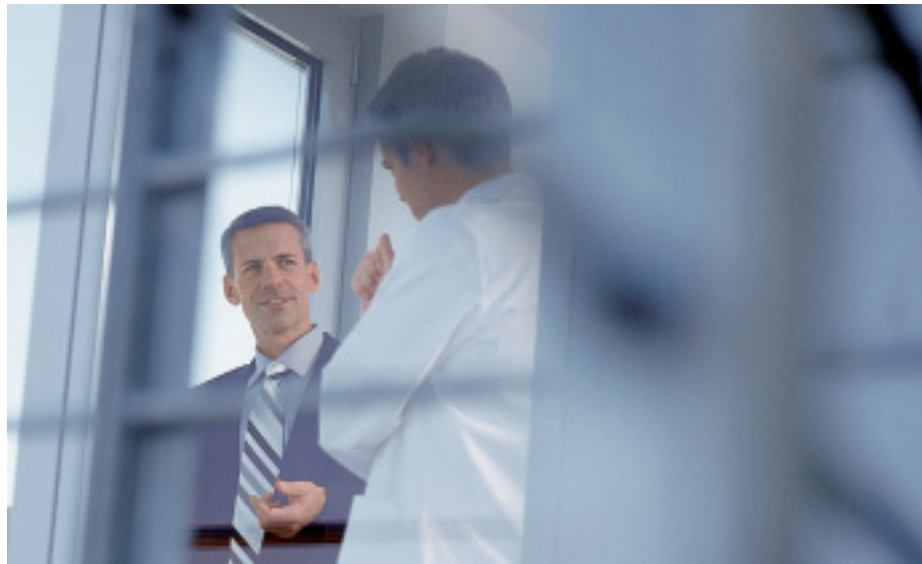
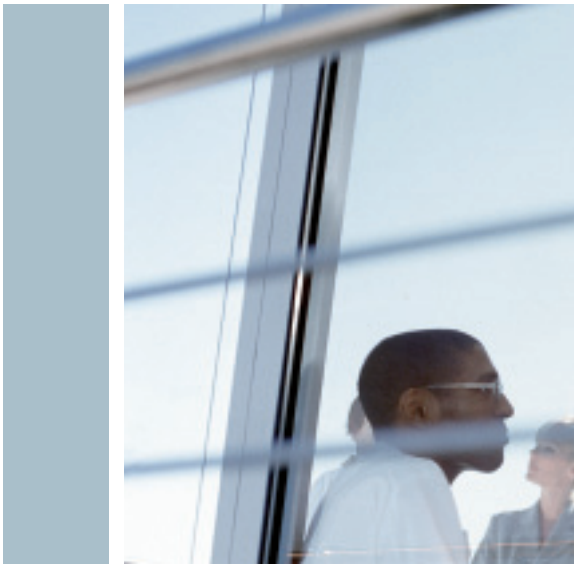
#### 1.1.4. Verwendung einer standardisierten Lösung

Immer mehr Hersteller bieten unterschiedlich konfigurierte Fernservices für ihre Produkte an. Damit steigt zunächst einmal auch die Anzahl der unterschiedlichen Remote-Verbindungen zwischen Kunden und Produktherstellern und der damit verbundene Administrationsaufwand beim Kunden. Vermehrter Administrationsaufwand kann aber auch die Wahrscheinlichkeit von Sicherheitslücken erhöhen. Diese Entwicklung wollen wir vermeiden. Deshalb bieten wir eine Lösung an, die von Herstellern aus den drei Märkten USA, Europa und Japan im Joint NEMA/COCIR/JIRA Security and Privacy Committee ([www.nema.org/medical/spc](http://www.nema.org/medical/spc)) gemeinsam erarbeitet und verabschiedet wurde.

Sie berücksichtigt sowohl die technische Machbarkeit für unterschiedlich komplexe Kundenorganisationen als auch die gesetzlichen Rahmenbedingungen in Deutschland. Damit erleichtern wir es unseren Kunden erheblich, die für sie geltenden gesetzlichen Rahmenbedingungen einzuhalten.



Um medizintechnische Geräte sicher aus der Ferne überwachen zu können, setzt Siemens Medical Solutions als einer der ersten Hersteller in der Medizintechnik ein Informationssicherheits-Managementsystem ein. Dieses wurde in Deutschland vom TÜV Süd nach der international gültigen Norm ISO 27001 zertifiziert.



## 1.2. Fernzugriffe im Siemens Service-Prozess

Abbildung 1 zeigt schematisch zunächst den gesamten Eskalationsprozess für Service-Calls, inklusive der üblicherweise vor Ort durchgeführten Arbeitsschritte: Nach Aufnahme der Störungsmeldung wird zunächst per Ferndiagnose vom UPTIME Service Center geklärt, um welche Art von Störung es sich handelt und welche Ursache sie haben könnte.

Falls möglich, wird die Störung gleich per Fernreparatur behoben. Ansonsten wird ein Service-Ingenieur das Problem vor Ort und mit Hilfe der aus der Ferndiagnose gewonnenen Informationen beseitigen (Eskalationsstufe 1).

Sollte dies nicht gelingen, eskalieren wir die Störung ins Regional Support Center (Eskalationsstufe 2) zu Experten, die sich auf ein ganz bestimmtes System bzw. auf eine Systemgruppe spezialisiert haben und somit tiefgehendes Fachwissen besitzen.

Falls das Problem auch hier nicht beseitigt werden kann, wird es in der 3. Eskalationsstufe an das Headquarters Support Center bzw. die produktspezifischen Entwicklungsabteilungen weitergeleitet. Jetzt arbeiten die Experten an Ihrem Problem, die auch schon an der Entwicklung des Systems mitgearbeitet haben.

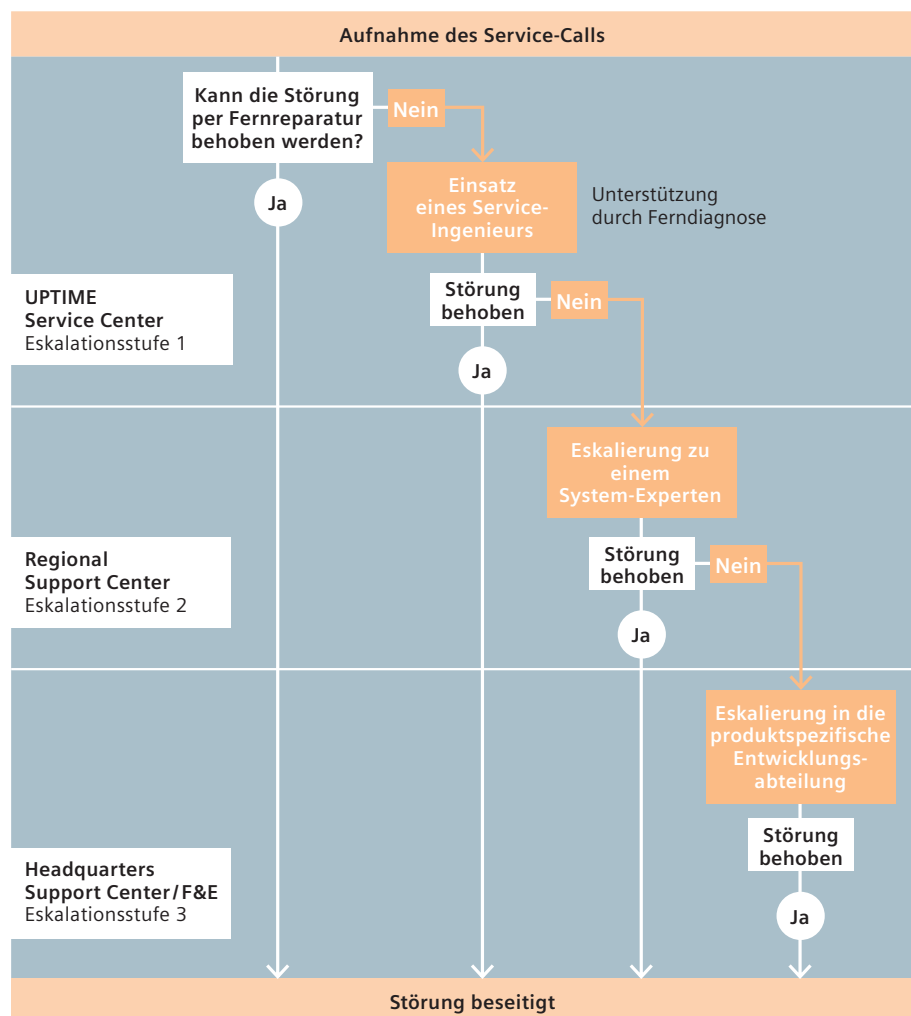


Abb. 1: Eskalationsprozess zur Bearbeitung von Service-Calls

### 1.3. Die technischen Möglichkeiten der Siemens-Produkte

#### 1.3.1. Sicherheit und Vertraulichkeit ist unser Ziel

Bei allen Siemens Remote Service-Aktivitäten ist es unser Ziel, nur in zwingend notwendigen Fällen und nur im technisch notwendigen Ausmaß auf Patientendaten zuzugreifen. Durch konsequente Umsetzung dieser Anforderung haben wir dies auch schon bei den meisten Produktklassen erreicht. Dabei sorgt die sichere und vertrauenswürdige Infrastruktur von Siemens Remote Service zusammen mit den organisatorischen Maßnahmen dafür, dass die Vertraulichkeit von Patientendaten sichergestellt wird. Diese Infrastruktur setzt auf eine Anbindung der Kundenanlagen an den Siemens Remote Server über VPN-Verbindungen (Internet, DSL etc.) oder über Telefonverbindung (analog oder ISDN) unter Verwendung zukunftsweisender Wartungssoftware. Abhängig vom Stand der Wartungssoftware und vom Produkt unterscheiden sich die verfügbaren Funktionen. Im Detail unterscheiden wir hier zwischen Produkten, die auf unserer *syngo*<sup>®</sup>-Applikationssoftware basieren, und Produkten, die diese Software nicht nutzen.

#### 1.3.2. Applikationssoftware *syngo*

Mit *syngo* haben wir eine Software entwickelt, die Patientendaten vor der Übertragung in unser UPTIME Service Center automatisch ausblendet.

Zusätzlich kann bei der aktuellen *syngo*-Version\* vorab vom Kunden an seinem Gerät eingestellt werden, welche Anwender Zugang zu welchen Daten erhalten.

So haben Sie es in der Hand, wann Service-Ingenieure oder Ihre eigenen Mitarbeiter auf Patientendaten zugreifen dürfen – und Sie können es jederzeit unterbinden.

#### 1.3.3. Produktklassen, die *syngo* nicht nutzen

Zu den Produkten, die *syngo* nicht nutzen, gehören z. B. einige PACS-Systeme. Hauptfunktionalität dieser Produkte ist die Verwaltung von Datenbanken, weshalb uns hier bei der Ausblendung bzw. Unterdrückung patientenbezogener Daten technische Grenzen gesetzt sind. Denn je nach Fragestellung erfordern Wartungsarbeiten an Datenbanken den Zugriff auf die darin enthaltenen Daten. Auch in diesen Fällen sorgen die technischen und organisatorischen Maßnahmen (siehe Kapitel 2.) zusammen mit der sicheren Infrastruktur von Siemens Remote Service (siehe Kapitel 2.2.) dafür, dass die Vertraulichkeit von Patientendaten sichergestellt ist.

#### 1.3.4. Besonderheiten bei Online-Hilfestellungen

Fernzugriff auf Kundensysteme zur Online-Hilfestellung (z. B. für Anwenderfragen zur Bedienung) erfolgt mit spezieller Desktop-Management-Software. Diese erlauben eine 1:1-Darstellung des Kundenbildschirms im UPTIME Service Center und damit eine direkte Hilfestellung durch einen Service-Ingenieur. Dies ist jedoch nur dann technisch möglich, wenn der Kunde den Zugriff explizit freigegeben hat, was er für jede Sitzung gesondert tun muss. Außerdem hat der Kunde auch in diesem Fall die Möglichkeit, den Verlauf der Online-Hilfestellung zu verfolgen und gegebenenfalls den Zugriff des UPTIME Service Centers zu unterbrechen.

#### 1.3.5. Proaktive Serviceleistungen

Bei unseren proaktiven Services senden Ihre Geräte automatisch vorab definierte Systemdaten an unser UPTIME Service Center. Hierbei handelt es sich um technische Daten wie Systemlogs, statistische Daten (z. B. die Anzahl der Restarts, Scans etc.) oder Systemzuverlässigkeitsdaten. Der Zugriff bzw. die Übertragung patientenbezogener Daten sind bei diesen Services ausgeschlossen.

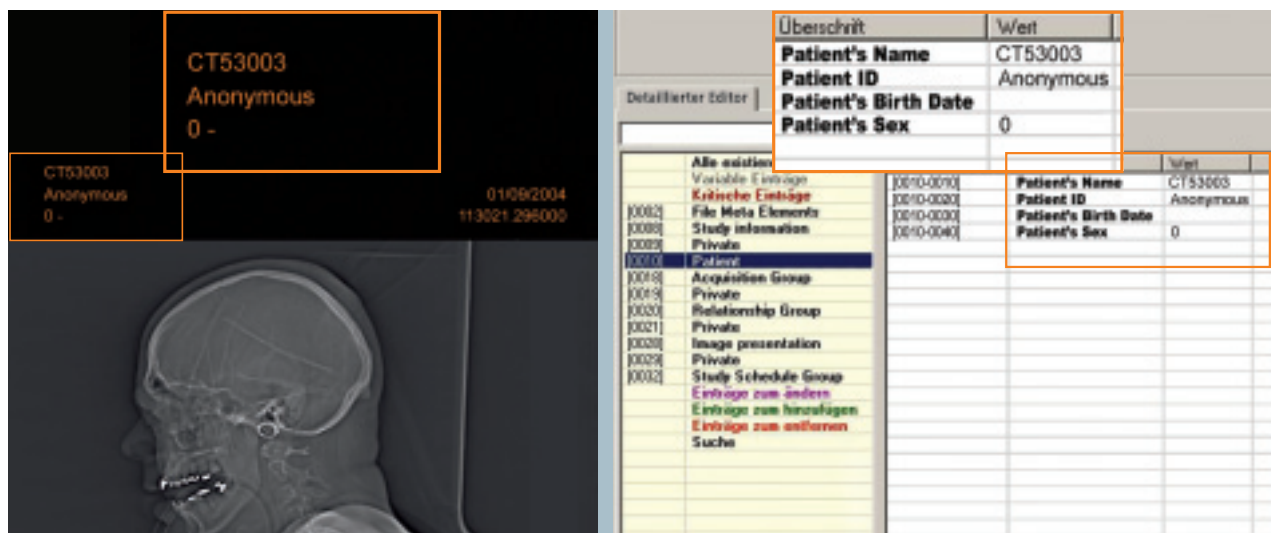
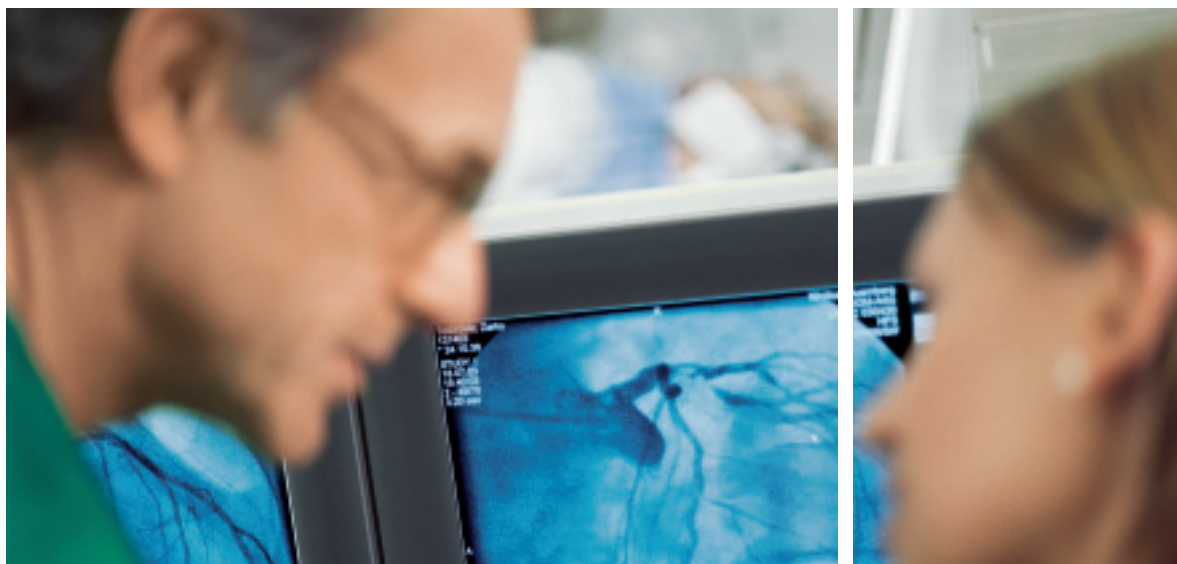


Abb. 2: Die *syngo*-Oberfläche: Patientendaten werden automatisch ausgeblendet

\* Informationen bezüglich der auf Ihrem Gerät installierten Software-Version erhalten Sie von Ihrem Siemens-Ansprechpartner. *syngo* ist ein eingetragenes Warenzeichen der Siemens AG.

## 2. Technisches und organisatorisches Konzept



### 2.1. Überblick

Im Folgenden beschreiben wir, mit welchen technischen und organisatorischen Maßnahmen wir dafür sorgen, dass die Vertraulichkeit von Patientendaten nicht gefährdet wird. Detaillierte Informationen zu den einzelnen Elementen der Sicherheitsinfrastruktur des Siemens Remote Service erhalten Sie in Kapitel 2.2.

#### 2.1.1. Verbindungsaufbau

Grundsätzlich gilt: Die Art und Dauer eines Service-Zugriffs auf Ihre Systeme, die unsere *syngo*-Software nutzen, wird von Ihnen bestimmt und kann jederzeit von Ihnen unterbunden werden. Bevor eine Verbindung zu Ihren Systemen hergestellt wird, können Sie eine von vier Zugriffsarten festlegen:

##### › Kein Zugang

Bei dieser Einstellung haben wir grundsätzlich keinen Zugang zum Kundensystem. Bei einer Störung schalten Sie Ihre Anlage für unseren Service-Ingenieur fallweise frei. Nach Behebung der Störung wird die Verbindung wieder gesperrt. Patientenuntersuchungen sind in diesem Modus jederzeit möglich.

##### › Begrenzter Zugang

In diesem Modus haben unsere Service-Ingenieure einen zeitlich limitierten und funktionell eingeschränkten Zugang zum Kundensystem. Patientenuntersuchungen sind möglich.

##### › Permanenter begrenzter Zugang

In diesem Modus haben unsere Service-Ingenieure einen funktionell eingeschränkten Zugang zum Kundensystem. Es besteht kein Zeitlimit. Auch hier sind Patientenuntersuchungen jederzeit möglich.

##### › Voller Zugang

In diesem Modus haben unsere Service-Ingenieure vollen Zugang zum Kundensystem. Hier können wir z. B. diverse Tests durchführen oder die Konfiguration einstellen und verändern. Patientenuntersuchungen sind nicht möglich.

Mit der Wahl einer Zugriffsart legen Sie fest, in welchem Umfang und für welche Zeitspanne Sie uns Zugriff auf Ihre Systeme gewähren. Unabhängig davon, für welchen Modus Sie sich entscheiden, gilt: Ihre Patientendaten werden vor der Übertragung automatisch ausgeblendet.

Die meisten unserer Kunden entscheiden sich für den permanenten begrenzten Zugang. Natürlich haben Sie jederzeit die Möglichkeit, die Art des Zugriffs zu ändern. Im Fall der ersten Zugriffsart, kein Zugang, läuft der in Abb. 3 dargestellte Prozess ab.

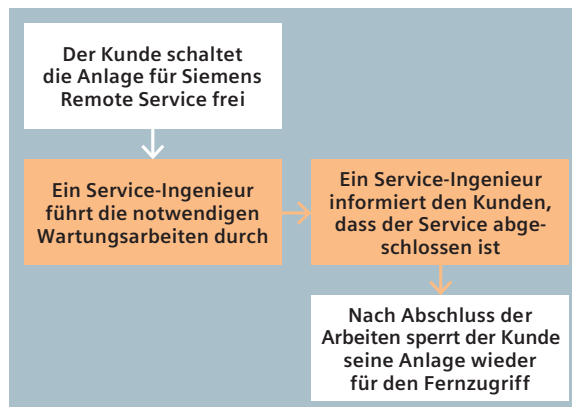


Abb. 3: Ablauf einer Siemens Remote Service-Aktion, Modus „kein Zugang“

In Abhängigkeit von den technischen Möglichkeiten kann die tatsächliche geräte- und/oder kundenspezifische Realisierung hiervon abweichen.



#### 2.1.2. Zugriffskontrolle

Voraussetzung für jede Fernwartungsaktivität ist, dass der Kunde den Siemens Remote Service-Zugriff zuvor ausdrücklich vertraglich erlaubt hat und dass er kontrollieren kann, wer auf seine Anlage zugreifen will. Zugriffe finden stets nur zur Fehleridentifizierung bzw. -behebung statt. Verstellungen von Messparametern, wie z. B. der Zugriff auf Scanprotokolle, sind nicht möglich. Nach Ablauf einer definierten Zeitdauer, in der keine Aktion erfolgt, wird die Siemens Remote Service-Sitzung am System des Kunden automatisch beendet.

#### 2.1.3. Vier-Augen-Prinzip

Am Bildschirm des zu wartenden Systems wird dem Kunden mit Hilfe eines Symbols angezeigt, dass eine Siemens Remote Service-Sitzung durchgeführt wird. Ergänzend dazu kann unser Service-Ingenieur dem Kunden-Mitarbeiter über eine simultane Telefonverbindung die Aktionen erläutern, die er gerade durchführt. Weiterhin hat der Kunde bei jeder Siemens Remote Service-Sitzung die Möglichkeit, den Zugriff des Service-Ingenieurs auf sein System jederzeit so zu beenden, dass alle laufenden Service-Programme unmittelbar kontrolliert abgeschlossen werden, ohne den weiteren sicheren Betrieb des zu wartenden Systems zu gefährden.

#### 2.1.4. Protokollierung

Alle Zugriffe auf Ihre Anlagen werden bei uns lückenlos mit Zeitstempel aufgezeichnet. Hierbei wird der zugreifende Service-Ingenieur eindeutig zugeordnet. So können wir Ihnen innerhalb einer angemessenen Zeit (drei Werktage (Mo – Fr) ab Eintreffen der Anfrage) mitteilen, welcher Service-Ingenieur wann Zugriff auf die Daten hatte und welche Aktionen er an welchem System durchgeführt hat. Diese Protokolle bewahren wir mindestens ein Jahr auf.

#### 2.1.5. Vertraulichkeit auf dem Übertragungsweg

Wir setzen modernste Verschlüsselungsverfahren ein, um Ihre Daten auf dem Übertragungsweg vor unberechtigtem Zugriff zu schützen. Optional wird für den gesamten Datenverkehr auf öffentlichen Leitungen eine Router-Router-Verschlüsselung angeboten. Weiterführende Informationen hierzu erhalten Sie in Kapitel 2.2.

#### 2.1.6. Organisatorische Maßnahmen

Unsere Service-Ingenieure sind sich der Vertraulichkeit der Patientendaten bewusst, kennen die rechtlichen Grundlagen und wissen, dass bei Nichtbeachtung der rechtlichen Regelungen harte Konsequenzen drohen. Für den Remote Service an medizintechnischen Systemen sind nur die Service-Ingenieure zugelassen, die im Datenschutz unterwiesen und darauf verpflichtet wurden. Am Siemens Remote Server werden elektronisch Listen geführt, wer zum ausgewählten Servicepersonal gehört und wer die entsprechenden Zugriffsrechte erhalten darf.

## 2.2. Sicherheitsinfrastruktur von Siemens Remote Service

In diesem Kapitel bieten wir Ihnen weiterführende technische Informationen zu den folgenden Elementen der Sicherheitsinfrastruktur des Siemens Remote Service an: Authentifizierung und Autorisierung der Service-Ingenieure an der Siemens Remote Service-Einwahlplattform, die „demilitarisierte Zone“ (DMZ) zwischen dem Siemens-Intranet und dem Internet bzw. der Telefonleitung, die für die Übertragung verwendeten Protokolle und Services sowie mögliche Sicherheitsmaßnahmen im Kundennetzwerk.

### 2.2.1. Authentifizierung und Autorisierung unserer Service-Ingenieure

Die vom UPTIME Service Center genutzte zentrale Wartungs- und Einwahlplattform (das SRS-Portal) befindet sich im firmeneigenen Intranet und ist von außen nicht zugänglich. Der Zugang zum Siemens Remote Service-Portal ist nur aus dem Siemens-Intranet und nur mit gültiger Siemens Remote Service-Benutzerkennung und gültigem Passwort möglich. Derzeit müssen die Passwörter mindestens acht Zeichen lang sein und aus unterschiedlichen Zeichenarten (Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen) bestehen.

Ein mehrstufiges „Service Domain Concept“ legt fest, welcher Benutzer auf welche Anlage zugreifen darf. So ist sichergestellt, dass jeder Service-Ingenieur nur Zugriff auf diejenigen Kunden-Systeme erhält, für die er ausdrücklich berechtigt ist. Außerdem sind nur diejenigen Siemens Remote Service-Funktionen für ihn frei geschaltet, für die er explizit autorisiert ist. Andere Anlagen im Kundennetzwerk, die nicht von Siemens Medical Solutions gewartet werden, können über diese Plattform nicht erreicht werden.

### 2.2.2. Demilitarisierte Zone

Um einerseits das Siemens-interne Intranet, andererseits aber auch die Kunden-Seite vor gegenseitigen Störungen und Angriffen zu schützen, haben wir den SRS-Server (Linux) in einer demilitarisierten Zone (DMZ) abgesichert. Verbindungen vom Service-Ingenieur zum Kundensystem und umgekehrt werden nicht „durchgeschaltet“, sondern im SRS-Server durch eine „Reverse-Proxy“-Funktionalität unterbrochen. Das heißt, eine aus dem Siemens-Intranet aufgebaute Verbindung wird im SRS-Server terminiert. Dieser Server baut dann die eigentliche Verbindung zum Kundensystem auf und spiegelt umgekehrt die vom Kunden kommende Kommunikation ins Intranet.

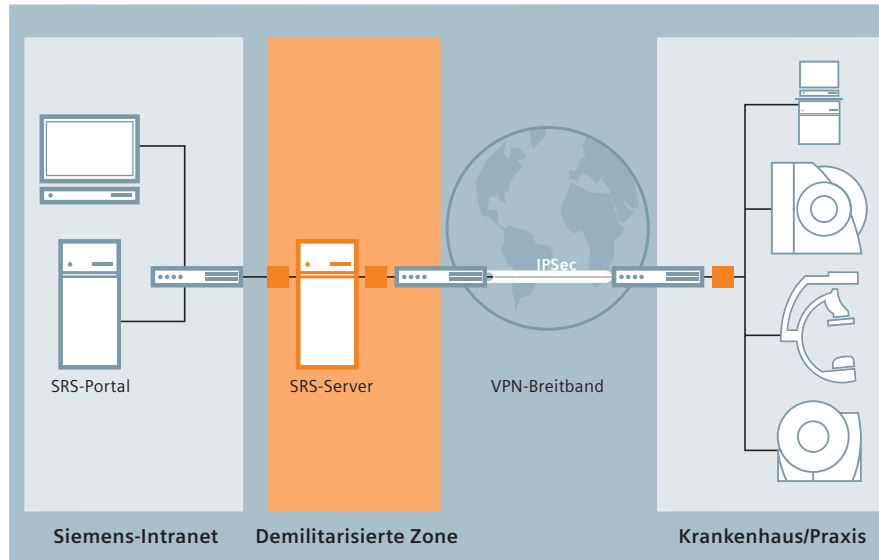


Abb. 4: Die Sicherheitsinfrastruktur von Siemens Remote Service

Diese Spiegelung findet jedoch nur für vordefinierte Protokolle statt. Damit wird gewährleistet, dass eine Kommunikation zwischen dem Siemens-Intranet und dem Kundennetzwerk nur über explizit erlaubte Protokolle stattfindet. Diese Architektur bietet einen zuverlässigen Schutz vor:

- › nicht-autorisierten Zugriffen von einem Netz in das jeweils andere Netz (Hacker)
- › Zugriffen aus dritten Netzen (z. B. aus dem Internet)
- › Übertragung von Viren und ähnlichen Schadensprogrammen aus dem einen Netz ins andere.

Darüber hinaus speichern wir in der DMZ keine kritischen Daten – insbesondere keine Zugangsdaten zu Kunden.

### 2.2.3. Sicherung der Übertragungsstrecke

#### Virtual Private Network (VPN) über das Internet

Wir empfehlen eine breitbandige und sichere Verbindung über das Internet. Ihre Vorteile: Mehr Sicherheit, erheblich schnellere Transferzeiten sowie eine permanente Verfügbarkeit der Verbindung. Stand der Technik ist ein mit IPSec gesichertes Virtual Private Network (VPN) zwischen der Siemens-DMZ und Ihrem Netzzugang. Haben Sie bereits die erforderliche Infrastruktur? Dann stehen Ihnen die Mitarbeiter von Siemens Remote Service gerne zur Verfügung, um mit Ihnen die zum Verbindungsaufbau nötigen Parameter abzustimmen, die Sie anschließend vor unbefugter Veränderung zuverlässig schützen müssen. Falls Sie keinen VPN-Endpunkt haben, stellt Ihnen Siemens einen VPN-Endpunkt zur Nutzung von Siemens Remote Service zur Verfügung (Cisco PIX Firewall).

Der VPN-Endpunkt auf unserer Seite ist ebenfalls ein Router der Firma Cisco. Bitte beachten Sie, dass es in seltenen Fällen aus Gründen mangelnder Systemkompatibilität nicht möglich ist, mit Modellen anderer Hersteller eine funktionierende Verbindung herzustellen. Sollte dies bei Ihnen der Fall sein, wenden Sie sich bitte an Ihren Siemens-Ansprechpartner.

#### **Virtual Private Network über Dial-Up-Verbindungen**

Sofern eine breitbandige VPN-Verbindung über das Internet nicht realisierbar ist, kann ein VPN auch über eine Dial-Up-Verbindung aufgebaut werden. Verfügen Sie bereits über eigene Einwahlmöglichkeiten, so stimmen Sie in Zusammenarbeit mit Ihrem Siemens-Ansprechpartner die genaue Konfiguration ab.

Sollten Sie keine eigene Einwahlinfrastruktur haben, stellen wir Ihnen einen Router zur Nutzung von Siemens Remote Service zur Verfügung (diverse Cisco-Produkte).

#### **Technische Sicherheitsmaßnahmen**

Zur weiteren Absicherung bieten wir die folgenden technischen Sicherheitsmaßnahmen:

##### **› Sichere Passwortübertragung mit CHAP**

Zur Übermittlung von Passwörtern verwenden wir nur das Challenge Handshake Protocol (CHAP), das die verschlüsselte Übertragung des Passwortes sicherstellt. Das CHAP-Passwort sowie die Passwörter für Telnetzugriff und den Zugriff auf den Konfigurationsmodus werden zufällig aus großen und kleinen alphanumerischen und Sonderzeichen generiert und sind mindestens zehn Zeichen lang.

##### **› Sicherer Verbindungsaufbau mit PPP-Callback (optional)**

Bei der Nutzung von Wählverbindungen setzen wir das „Point-to-Point Protocol“ ein. Dieses kann optional um eine Rückruf-Funktion (Callback) erweitert werden. Es stellt sicher, dass Ihr Service-Router nach der Authentifizierung des anrufenden Siemens-Routers die gespeicherte Telefonnummer des Siemens-Routers zurückruft. Dies verhindert zuverlässig den unwahrscheinlichen Fall, dass ein unautorisiertes Dritter gleichzeitig den Benutzernamen, das Passwort und die Telefonnummer herausfindet und sich mit diesen Daten bei Ihnen einwählt.

##### **› Anruferauthentifizierung mit CLI (optional)**

Mit Hilfe von „Calling Line Identification“ (CLI) überprüft Ihr angerufener Service-Router die „Multiple Subscriber Number“ (MSN) des anrufenden Routers. Dadurch wird sichergestellt, dass ein Zugriff auf den Service-Router nur dann stattfinden kann, wenn die übertragene MSN mit der auf dem Service-Router hinterlegten Telefonnummer von Siemens Medical Solutions übereinstimmt. Diese Funktion ist nur bei ISDN-Service-Routern möglich.

##### **› Zugriffsregelung über Access Control Lists (optional)**

Access Control Lists (ACLs) auf Ihrem Service-Router bieten eine ähnliche Funktion wie Firewalls, indem sie Datenverkehr nur von und zu bekannten IP-Adressen zulassen. So können Sie sicherstellen, dass Ihre Service-Router nur Datenverkehr zwischen dem UPTIME Service Center und den gewarteten medizinischen Anlagen passieren lassen. Ein Zugriff von Siemens Medical Solutions auf andere Teile Ihres Netzes oder Zugriff von Dritten auf Ihre medizinischen Anlagen ist somit ausgeschlossen.

##### **› IPSec schützt Daten vor Mitlesen und Verfälschen (optional)**

Zur verschlüsselten und authentifizierten Datenübertragung setzt Siemens Medical Solutions den etablierten Standard IP Security (IPSec) mit Preshared Secrets ein. Die Preshared Secrets bestehen aus mindestens 12 Zeichen, die wiederum zufällig gewählt werden. Zum Austausch der Schlüsselinformationen wird das Internet Security Association and Key Management Protocol (ISAKMP) eingesetzt. Die Verwendung eines Authentication Headers (AH) stellt die Integrität der Daten mit den Hash-Verfahren MD5 oder SHA1 sicher. Encrypted Secure Payload (ESP) sichert die Vertraulichkeit der Daten durch Verschlüsselung mit den Algorithmen DES oder 3DES. Als symmetrische „Session Keys“ können Diffie-Hellmann-Schlüssel mit 768, 1024 oder 1536 bit Schlüssellänge verwendet werden.

##### **› Erweiterte Kontrollmöglichkeiten durch Debugging (optional)**

Möchten Sie SNMP- oder Syslog-Meldungen des Service-Routers auf einem Ihrer Server empfangen oder möchten Sie die aktuelle Konfiguration auf dem Service-Router ansehen, wenden Sie sich bitte an Ihren Siemens-Ansprechpartner.

## 2.2.4. Sicherheitsmaßnahmen im Kundennetzwerk

### Firewall

Da keine End-to-End-Verschlüsselung stattfindet, haben Sie jederzeit die Möglichkeit, zusätzlich zu den bisher geschilderten Sicherheitsmaßnahmen die gesamte Kommunikation bei Ihrem Netzwerkzugang über eine selbstadministrierte Firewall zu leiten. Dies ermöglicht Ihnen die volle Kontrolle über die Kommunikation.

### Systemzugriff

Ist der Zugriff zum Kundensystem vom Kunden freigeschaltet, so muss sich der Service-Ingenieur am Kundensystem noch mit einem zeitabhängigen Service-Passwort authentifizieren, bevor er die Anlage in den Servicemodus schalten kann. Es gelten die Passwortregelungen der Siemens AG, die den derzeitigen internationalen Standards entsprechen und fortlaufend aktualisiert werden.

### Protokolle

Für den Service auf Ihrem System können – abhängig von den Möglichkeiten der Software auf Ihrem System – die Protokolle http bzw. vorzugsweise https sowie die Dienste der Tools Telnet, TeraTerm-Pro, PuTTY, WinVNC, pcAnywhere, Netmeeting, Citrix, Timbuktu, MS Terminal Server genutzt werden.

### Datenübertragung von Ihren Systemen zum SRS-Server

Bei einigen unserer proaktiven Services werden Diagnose-Daten von Ihren Geräten entweder automatisch (gemäß Konfigurierung Ihres Systems) oder auf explizite Anforderung des Service-Ingenieurs zum SRS-Server verschickt. Dabei werden ausschließlich technische Daten und niemals Patientendaten übertragen. Abhängig von den Möglichkeiten der Software werden hierbei die folgenden Dienste genutzt:

- › ftp (File Transfer Protocol)
- › scp (Secure Copy)
- bzw. die System Management Tools
- › CA Unicenter
- › HP Open View

### Datenübertragung vom SRS-Server zu Ihren Systemen

Bei unseren Services „Software Updates“ und „Virus Protection“ werden Daten vom SRS-Server automatisch auf Ihre Systeme übertragen. Dabei handelt es sich z. B. um Virus Pattern oder Microsoft Hotfixes. Diese Art der Übertragung erfolgt nur nach vorheriger Abstimmung mit Ihnen.

## 2.3. Schutz vor böswilligen Angriffen

### 2.3.1. Geschützter SRS-Server

Die SRS-Server sind Linux-Server. Ein Befall durch Würmer, Viren, trojanische Pferde und andere Attacken ist daher äußerst unwahrscheinlich und bisher nicht vorgekommen. Trotzdem sorgen wir dafür, dass die SRS-Server nach dem neuesten Stand der Technik geschützt sind.

### 2.3.2. Schutz der Kunden-Systeme

#### Keine Gefahr vom SRS-Server direkt

Ein Virenbefall Ihres Systems durch die SRS-Server bzw. eine Verbreitung von Viren von den SRS-Servern in Richtung Ihres Systems ist aufgrund der in Kapitel 2.2.2. beschriebenen Reverse-Proxy-Funktionalität nicht möglich.

#### Gefährdung bei Internet-Anschluss

Kundensysteme, die über das Internet mit dem zugehörigen SRS-Server verbunden sind, sind – wie jeder Anschluss über das Internet – über diesen Anschluss einer gewissen Gefährdung ausgesetzt. Solange Sie Ihren Internet-Zugang nur für Siemens Remote Service nutzen, ist eine Infizierung mit Viren über unsere Sicherheitsinfrastruktur ausgeschlossen. Falls Sie Ihren Internet-Anschluss auch für andere Zwecke nutzen, sollten Sie entsprechende Vorkehrungen treffen, um diese Gefährdung zu vermeiden.

#### Keine Gefahr durch E-Mail-Verkehr

Bestimmte Typen von Kundensystemen versenden E-Mails (ohne Anlagen) an den zugehörigen SRS-Server, und nur in diese Richtung. E-Mails, die ein Kundensystem an den SRS-Server sendet, werden an den zuständigen Siemens Mail Server weitergeleitet und von dort aus an den Empfänger geschickt. Die Siemens Mail Server scannen alle E-Mails auf Viren und reagieren entsprechend den Vorgaben des Siemens Chief Information Officer, um eine Gefährdung des Siemens-Intranets auszuschließen. Da keine E-Mails in die Gegenrichtung (zum Kundensystem) verschickt werden, ist eine Infizierung der Kundensysteme über diesen Weg ausgeschlossen.

#### Infektion der Kunden-Systeme durch Kontakt mit einem infizierten Kundensystem

Eine Infektion der SRS-Server selbst durch Kontakt mit einem infizierten Kundensystem ist nicht möglich, da keine direkte IP-Routbarkeit zwischen diesen beiden Systemen besteht (siehe Reverse-Proxy-Funktionalität in Kapitel 2.2.2.).

Aufgrund lokaler Einschränkungen von Vertriebsrechten und Serviceverfügbarkeiten können wir leider nicht gewährleisten, dass alle in dieser Broschüre aufgeführten Produkte weltweit gleichermaßen durch Siemens vertrieben werden können.

Die Informationen in diesem Dokument beinhalten allgemeine technische Beschreibungen von Leistungen und Ausstattungsmöglichkeiten, die nicht in jedem Einzelfall vorliegen müssen. Verfügbarkeit und Ausstattungspakete können sich von Land zu Land unterscheiden. Aus diesem Grund sind die gewünschten Leistungen und Ausstattungen im Einzelfall bei Vertragsschluss festzulegen.

Siemens behält sich das Recht vor, Konstruktion, Ausstattungspakete, Leistungsmerkmale und Ausstattungsmöglichkeiten ohne vorherige Bekanntgabe zu ändern. Bitte wenden Sie sich für die neuesten Informationen an Ihre Siemens-Vertretung.

Hinweis: Innerhalb definierter Toleranzen kann es Abweichungen von den technischen Beschreibungen in diesem Dokument geben. Bei der Reproduktion verlieren Originalaufnahmen immer ein gewisses Maß an Detailtreue.

Das passende Zubehör finden Sie unter:  
[www.siemens.de/medizinisches-zubehoer](http://www.siemens.de/medizinisches-zubehoer)

© 07.2007 Siemens Medical Solutions  
Bestell-Nr. A91CS-00007-10C-3  
Gedruckt in Deutschland  
PUBLICIS 009102/2845 WS 07071.

**Kontaktadresse**

Siemens AG, Medical Solutions  
European Sales and Service  
Customer Services  
Karlheinz-Kaske-Straße 2  
D-91052 Erlangen  
[Service.Med@siemens.com](mailto:Service.Med@siemens.com)  
Hotline 0180 311 22 44

**Siemens AG**  
Wittelsbacherplatz 2  
D-80333 München  
Deutschland

**Headquarters**  
Siemens AG  
Medical Solutions  
Henkestr. 127  
D-91052 Erlangen  
Deutschland  
Telefon: +49 9131 84-0  
[www.siemens.de/medical](http://www.siemens.de/medical)

[www.siemens.de/medical](http://www.siemens.de/medical)