



Der Datenschutz ist eine wichtige Voraussetzung für die Akzeptanz der Telemedizin



Patienten von zuhause aus via Mobilfunk oder Internet zu betreuen kann den Weg zum Arzt und somit Zeit und Kosten sparen. Beim Entwickeln von Geräten, mit denen Patientendaten übertragen werden, gilt es, von Anfang an auch die Datensicherheit zu berücksichtigen.

Informationssicherheit in der Telemedizin

Wie in anderen Branchen schon vollzogen, hält die moderne Informationstechnologie auch Einzug in die Medizintechnik und somit in die traditionsbehaftete Welt der Medizin. Besonders in der Telemedizin hat sich in den vergangenen Jahren viel getan. Telekonsile mittels Internet oder Bildtelefon, zwischen Chirurgen über große Distanzen hinweg, in Echtzeit und sowohl unter beiderseitiger Einbeziehung der Ergebnisse bildgebender Verfahren (Endoskopie oder Sonografie) als auch mit Live-Kameraaufnahmen des Operationsfelds: Das alles ermöglicht heute eine gemeinsame Betrachtung des Falls und die zeitnahe Diskussion von Fragestellungen. Auch innerhalb eines Krankenhauses oder zwischen den verschiedenen arbeitsteilig agierenden Heilberufen werden diagnostische und therapeutische Daten auf unterschiedlichen Wegen ausgetauscht. Manchmal liefert der Patient die Daten auch selbst, denn



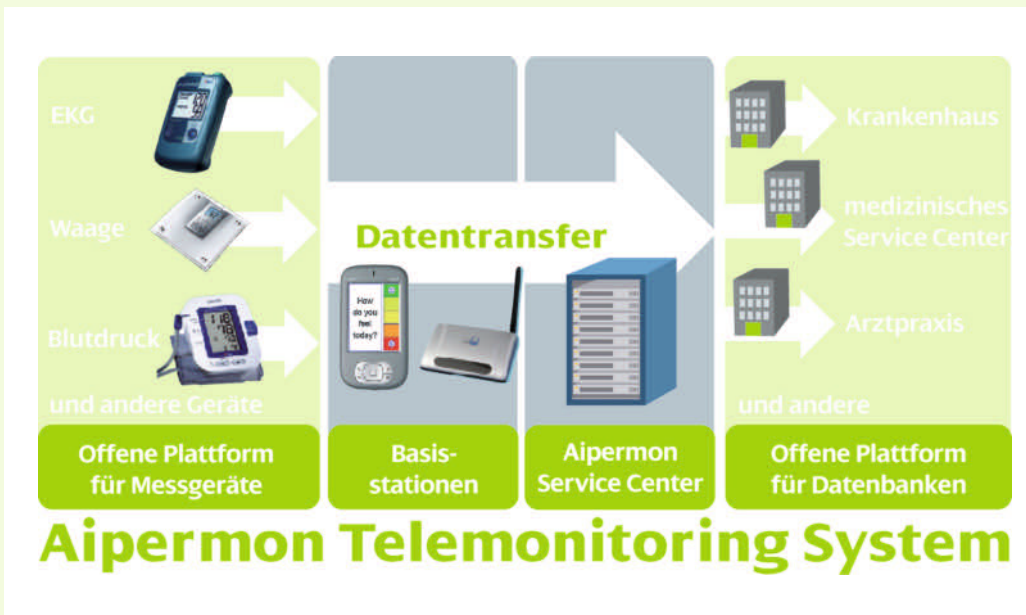
KONTAKT

TÜV SÜD
80339 München
Tel. +49 (0)89 57915000
Fax +49 (0)89 51551097
www.tuev-sued.de

auch in den eigenen vier Wänden hält die Telemedizin mittels Medical Homecare Einzug. Dabei werden Vitalparameter mit unterschiedlichen Geräten gesammelt und mittels Telefon- oder Internetverbindung an einen medizinischen Dienst weitergegeben. All diese Anwendungsmöglichkeiten der modernen Medizintechnik haben sicherlich ihren Reiz und werden in Zukunft noch an Bedeutung gewinnen, doch darüber hinaus verbindet sie auch ein wichtiger Aspekt, der vielen Medizintechnikentwicklern noch neu ist: die Sorge um die Sicherheit der anvertrauten Information. Sich dieser Herausforderung zu stellen, ist zwar in erster Linie die Aufgabe der Anwender (tele)medizinischer Geräte – also der Ärzte und anderen medizinischen Personals –, doch schon in der Produktentwicklung werden die Weichen gestellt, die die Integration und Anwendung von Sicherheitsaspekten erleichtern.

Vertrauen mit Sicherheit verbinden

Wenn man Informationssicherheit gewährleisten will, müssen die drei Schutzziele nämlich: Vertraulichkeit, Verfügbarkeit und Integrität von Information gewährleistet sein. Das bedeutet, dass



1 Patientendaten lassen sich dank moderner IT-Technologie unkompliziert vom Patienten zum Arzt oder in die Klinik übertragen. Eine gute Sache, wenn das Sicherheitskonzept bei der Datenübertragung stimmt

- + Informationen nicht unberechtigten Personen, Einheiten oder Prozessen verfügbar gemacht oder enthüllt werden dürfen (Vertraulichkeit),
- + die Daten für eine berechtigte Einheit im Bedarfsfall auch zugänglich und nutzbar sind (Verfügbarkeit) und
- + die Richtigkeit und Vollständigkeit der Daten gewährleistet ist (Integrität).

Diese Schutzziele lassen sich mit technischen und organisatorischen Maßnahmen erreichen und ihre Aufrechterhaltung nachhaltig sicherstellen. Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch die internationale Normenreihe ISO/IEC 27000 bieten die

Statt Klarnamen lieber Pseudonyme

normative Basis für die Implementierung eines Informationssicherheitsmanagements in Organisationen. Während im klinischen Alltag immer noch die Papiere für die medizinische Dokumentation vorherrscht, bringt die bereits laufende Verlagerung auf elektronische Medien zusätzliche Anforderungen an die Technik mit sich. Denn auch nur temporär nicht verfügbare oder anwendungsintern verfälschte oder verlorene Gesundheitsdaten bergen hohe Risiken für Arzt und Patient. Gerade bei der Verordnung eines zusätzlichen Medikaments mit bekannten Wechselwirkungen oder bei möglichen Vorerkrankungen sind verfügbare und integre Daten unerlässlich. Und damit die mittels Medical Homecare in der eigenen Wohnung aufgezeichneten Werte den Arzt bei seinem Vorgehen unterstützen können, müssen diese Daten bei Bedarf in unverfälschter Form zur Auswertung auch verfügbar sein.

Genauso wesentlich ist allerdings, dass die Daten nicht versehentlich unberechtigten Personen zugänglich gemacht werden – der Arzt ist in seiner Funktion als Berufsgeheimnisträger schon seit jeher zur Verschwiegenheit verpflichtet. Besonders geregelt ist der Aspekt der Vertraulichkeit unter anderem im Bundesdatenschutzgesetz. Das Gesetz behandelt wichtige datenschutzrechtliche

Grundlagen, die auch auf telemedizinische Anwendungen und die Übermittlung personenbezogener Daten zwischen den Teilnehmern angewendet werden müssen.

» Ein Sicherheitscheck durch einen externen Dritten ist bei Web-Applikationen dringend anzuraten.«

Prof. Dr. Peter Schaff, CEO TÜV SÜD Management Service

In telemedizinischen Anwendungen handelt es sich dabei um Gesundheitsdaten, die als „besondere personenbezogene Daten“ gelten. Damit unterliegt deren Verarbeitung laut dem Bundesdatenschutzgesetz erhöhten Anforderungen. Solche besonderen personenbezogene Daten dürfen in der Regel nicht ohne die Einwilligung des Betroffenen – also des Patienten – erhoben und verarbeitet werden. Ferner haben sich Datenverarbeitungssysteme – zu denen auch telemedizinische Anwendungen zählen – im Allgemeinen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder ▶

Datenstrukturen und -banken richtig konzipieren



2 Vitalparameter werden mit unterschiedlichen Messgeräten gesammelt und anschließend übertragen, wie hier von Getemed auf der MedTel in Luxemburg vorgestellt wurde

zu nutzen. Daher ist es meist sinnvoll, wenn die telemedizinischen Anwendungen bereits in ihrer grundsätzlichen inhaltlichen Ausgestaltung die Vorgaben des Datenschutzes erfüllen, denn so können sie den Anwendern vom Datenschutz auferlegte Pflichten aufzeigen oder deren Umsetzung erleichtern.

Verschlüsselte Datenübertragung und der Einsatz von Firewalls sind deshalb heute schon zur Selbstverständlichkeit geworden. Für fast alle Bereiche gibt es kostengünstige und schlüsselfertige Lösungen. Bei aller Notwendigkeit der Implementierung gesetzlicher Anforderungen an das Design von Produkten und Servern ergeben sich jedoch in der konkreten Umsetzung durch unerfahrene Programmierer und Administratoren oft sicherheitskritische Unachtsamkeiten, die in der Onlinewelt, aber auch in Hackerkreisen schon lange als mögliche Angriffspunkte bekannt sind.

Eine sinnvolle und dabei sehr wirkungsvolle Schutzmaßnahme ist das Verschlüsseln der Klarnamen. Für viele telemedizinische Anwendungen ist ein Zugriff auf den vollständigen Namen des Patienten nicht nötig, die Darstellung eines Pseudonyms oder einer Identifikationsnummer reicht häufig aus. Im Sinne des Datenschutzes sollte deshalb schon bei der Konzeption von Datenstrukturen und Datenbanken der Patientename stets von den Restdaten separiert werden. Die zur Rückverwandlung vom Pseu-

donym in Klartext notwendigen Daten können dann in einer besonders geschützten, möglicherweise sogar verschlüsselten Datenbanktabelle vorgehalten werden. Maßnahmen wie diese bieten inhärenten Schutz vor feindlicher Umgebung: Ohne direkten Personenbezug ist eine Kompromittierung des Patienten durch eine Datenpanne bei Weitem weniger wahrscheinlich.

Ebenso bedeutsam ist ein wirksamer Schutz der Serverinfrastruktur. Dieser sollte von Anfang an so konzipiert werden, dass die Datenhaltung und die Präsentationsschichten für Arzt und Patient voneinander getrennt liegen. Von außen sollte nur die Präsentationsschicht zu erreichen sein, was einen direkten Zugriff auf die Daten verhindert. Ein weiterer kritischer Punkt sind die für Patienten, Anwender und Administratoren zugänglichen Oberflächen sowie die Softwareschnittstellen zwischen den einzelnen Komponenten. Dort gilt es beispielsweise, alle Nutzereingaben über eine Abstraktionsschicht zu filtern und erst dann an die zentralen Server und Datenbanken weiterzuleiten.

Geprüfter Datenschutz

Soll die Anwendung per Browser zugänglich sein oder im Internet veröffentlicht werden, sollten Entwickler applikationsspezifische Probleme wie Cross-Site Scripting, SQL-Injection oder Schwächen im Handling authentifizierter Sitzungen in Betracht ziehen. Ein in der Webentwicklung versiertes Entwicklerteam, die Einführung und Umsetzung von Programmierrichtlinien und ein anschließender Sicherheitscheck – sinnvollerweise durch einen externen Dritten – sind für Web-Applikationen dringend anzuraten. Nur so lassen sich Schwachstellen noch vor dem Rollout einer Anwendung erkennen und korrigieren.

Dies ist nur ein geringes Spektrum an Möglichkeiten, Informationssicherheit durch die systematische Implementierung technischer und organisatorischer Maßnahmen für Anwendungen im telemedizinischen Bereich zu etablieren. De jure ist zwar nicht der Entwickler hierfür verantwortlich, doch kann er anhand der genannten Beispiele den späteren Anwender – also seinen Kunden – durch vorausschauendes Produktdesign dabei unterstützen, Sicherheitsprobleme zu antizipieren und bestmöglich zu eliminieren. Das erzeugt einen Mehrwert für den Kunden und kann als Alleinstellungsmerkmal zur Differenzierung im Wettbewerb dienen.



3 Wie auf der MedTel in Luxemburg gezeigt, ermöglichen Kameras und Video-Equipment die Kommunikation zwischen Ärzten, die sich an beliebigen Orten auf der Welt aufhalten können



PROF. DR. PETER SCHAFF
ist Leiter des Geschäftsbereichs Management Service beim TÜV SÜD.

RAINER SEIDLITZ
ist Leiter Strategische Geschäftseinheit IT und Internet des Geschäftsbereichs Management Service beim TÜV SÜD.
Rainer.Seidlitz@tuev-sued.de

ANDREAS SPECKMANN
ist Mitarbeiter bei TÜV SÜD Management Service in München.



MD110075
www.med-eng.de