conversol®

Beratung Planung Ausführung

Unternehmensberatung für Tele-, Daten & Bildkommunikation

WLAN IM GESUNDHEITSWESEN

Aufgaben und Lösungen im medizinischen Umfeld

convergence solutions GmbH
Schulte-Hinsel-Str. 33
45277 Essen
Telefon (02 01) 847 388-0
Telefax: (02 01) 847 388-9

E-Mail: info@conversol.de
Internet: www.conversol.de

Inhalt

Vorbetrachtung

Das Gesundheitswesen befindet sich in einer Restrukturierungsphase, die durch verschiedene Einflüsse und Strömungen gekennzeichnet ist. Diese sind neben dem medizinischen Fortschritt die Integration der technischen Ausrüstung, die Transparenz der Geschäftsprozesse sowie unterschiedliche Anwendungsbereiche durch verschiedene Nutzergruppen.

Nach Aussagen von Marktforschungsunternehmen wird die Entwicklung des Marktes in den kommenden Jahren wesentlich durch die Bevölkerungsentwicklung, dem daraus resultierenden Kostendruck der privaten und öffentlichen Versicherer, sowie einer Konsolidierung des Marktes bestimmt.

Informationen müssen auch im mobilen Umfeld von Kliniken jederzeit verfügbar und trotzdem sicher sein. Um einzelne Geschäftsprozesse zu optimieren, werden völlig neue Lösungen benötigt, die in dieser Forum bislang nicht oder nur schwer realisierbar waren. Daher steigt die Akzeptanz für die Anwendung drahtloser Übertragungstechniken auch im medizinischen Bereich ständig.

Veränderte Anforderungen im Gesundheitswesen

Auch im medizinischen Bereich stehen sich die neuen technischen Lösungen und die Forderung nach höherer Produktivität dem Aufruf zur Kostensenkung gegenüber. Gefordert werden:

Informationsbereitstellung : Individuelle Zugriffsmöglichkeiten auf Patientendaten, je nach Berechtigung und Möglichkeit.

- Hochverfügbarkeit: Stabile Datennetze, die einen ständigen Zugriff auf die Patientendaten sicherstellen.
- Qualitätsgarantie der Übertragung: Für effektiv nutzbare Sprachnetze.
- Flexibilität ohne Verlust von Sicherheit: Einsatz von WLAN-Techniken, um ausgewählte Anwendungen mit höherer Flexibilität nutzen zu können.
- Zugriffsberechtigungen, Autorisierung von Personen und Gruppen: Zugriff auf spezielle Patienteninformationen, um verschiedene Dienstleister wie z.B. Pflegedienste effektiv in die Patientenbetreuung einbinden zu können.
- Datensicherheit: Absicherung der Daten-Übertragungswege, um unberechtigte Zugriffe zu verhindern.
- Schutz vor Manipulationen: Gewährleistung der Datenintegrität.
- Ganzheitliche Lösungskonzepte: Einbeziehung medizinischer Geräte und Ausrüstung in das Sicherheitskonzept.
- Investitionssicherheit: Skalierbare Lösungen, um auf veränderte Anforderungen effektiv reagieren zu können.

DRG zur Kostenoptimierung

Die Auswirkungen der Umstellung auf *Diagnosis Related Groups (DRG)* sind für Krankenhäuser und Kliniken deutlich spürbar:

- sinkende Behandlungsdauer
- zunehmende Untersuchungsdichte
- Patient als Kunde
- Annäherung von Medizin und Ökonomie
- Infragestellung gewohnter Abläufe, Zuständigkeiten und Qualifikationsprofile

Die Klinikleitung steht vor schwierigen Fragen. Ihre Beantwortung entscheidet über die Zukunft des Hauses. Beispiele:

- Wo liegen die Stärken des Krankenhauses? Wie können diese erweitert werden?
- Wie kann mit exzellenter Medizin ein wirtschaftliches Ergebnis erzielt werden?
- Ist es möglich, die Leistungsbreite des Krankenhauses zu erhalten oder auszubauen, ohne seine finanzielle Leistungsfähigkeit zu gefährden?
- Gibt es Bereiche, die die Kooperationen mit Mitbewerbern nahelegen (Stichwort: Integrierte Versorgung)?
- Ist es sinnvoll, Krankheitsgebiete in den ambulanten Bereich auszulagern?
- Welche Investitionen in die IT-Struktur sind sinnvoll?

Entscheidend für den Erfolg sind nicht nur Strategien, Kennzahlen und Leistungscontrolling. Entscheidend sind auch Kommunikation und mentale Veränderungsarbeit. Beides wird viel zu oft vernachlässigt.

Gerade bei der Einführung von DRGs wird explizit auf die IT als Investitionsthema mit dem Hinweis auf Sinnfälligkeit Bezug genommen.

KIS/ RIS/ PACS /EPA

Um langfristig wettbewerbsfähig zu bleiben, sind Kliniken gezwungen, Patienten auch weiterhin die bestmögliche Versorgung zu bieten. Zu einer optimalen Betreuung der Patienten und einer effektiveren Verknüpfung aller Patientendaten werden in den Gesundheitseinrichtungen zunehmend Systeme installiert. Dazu zählen:

- KIS (Krankenhaus-Informationssystem)
- RIS (Radiologie-Informationssystem)
- PACS (*Picture Archiving and Communication System* = Bild-Archivierungs- und Kommunikations-System)
- EPA (Elektronische Patientenakte) und Pflegedokumentation

Diese Systeme stellen verteilte Gesundheitsinformationssysteme dar und bieten dem medizinischen Personal in unterschiedlichen Gesundheitsorganisationen völlig neue Möglichkeiten der Patientenbetreuung.

Ein wichtiger Faktor für die Absicherung einer entsprechenden Qualität ist der Einsatz einer effizienten und hochverfügbaren Kommunikationsinfrastruktur. Mit ihrer Hilfe soll das betreuende Personal in der Lage sein, die erforderlichen Patientendaten schnell, effizient und sicher bei Bedarf zu erhalten.

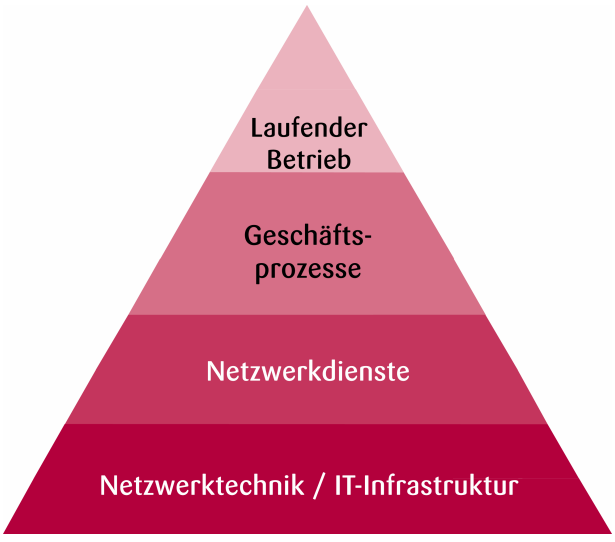
Alle genannten erfordern eine stabile IT-Infrastruktur, da alle darauf aufbauenden Abläufe von dieser abhängig sind. Sie benötigen nicht nur hochperformante Netzwerke für schnelle Datenübertragung, sondern auch eine sichere Übertragung der sensiblen Daten.

Transparenz oder Datenschutz?

Gefordert ist eine hohe Verfügbarkeit der Patientendaten an unterschiedlichsten Orten und zu sehr differenzierten Zwecken. Der behandelnde Arzt braucht volle Sicht auf die Anamnesedaten. Die Patientendaten dürfen unbefugten Personen keinesfalls zugänglich gemacht werden und müssen vor unbefugtem Zugriff – auch innerhalb der Klinik – geschützt werden. Wenn diese Patientendaten übertragen werden, so muss dafür gesorgt sein, dass der Datenverkehr mit externen Partnern, wie beispielsweise mit Versicherungen, Apotheken und anderen Dienstleistern, sicher ist. Nur mit höchster Datensicherheit gewinnen die Kliniken das Vertrauen des Patienten und arbeiten überdies gesetzeskonform. Die Vertraulichkeit der Patientenakten ist also für alle Beteiligten ein wichtiges Anliegen. Das Gesundheitswesen fordert Netzwerk-Lösungen, die die Sicherheit und den Datenschutz in jedem Fall gewährleisten. Die Antwort heißt also eindeutig „Transparenz und trotzdem voller Datenschutz“.

IT-Infrastruktur: Basis für effiziente Geschäftsprozesse

Eine wichtige Rolle spielt die IT-Infrastruktur, die zunehmend immer neuen und höheren Anforderungen gerecht werden muss.



Die Pyramide verdeutlicht die einzelnen Ebenen einer Kommunikationsinfrastruktur und ihre aufeinander aufbauenden Anwendungs- bzw. Geschäftsebenen. Die höheren Ebenen basieren jeweils auf einer stabilen und zuverlässigen darunter liegenden Schicht.

Mobilität durch flexible WLAN-Lösungen

Ärzte, Pflegepersonal und auch Patienten wollen zunehmend äußerst flexibel auf die für sie relevanten Informationen zugreifen. Dabei müssen klar definierte Sicherheitsanforderungen eingehalten und sichergestellt werden. Nur so kann gewährleistet werden, dass lebenswichtige Patientendaten während der medizinischen Versorgung stets zur Verfügung stehen und zugleich die Sicherheit im Umgang mit diesen Daten garantiert ist. Nur so können die unterschiedlichen Anwendergruppen auch spezifische Dienste ohne sicherheitstechnische Probleme erhalten.

Die WLAN-Technik (*Wireless Local Area Network*) stellt den flexiblen Teil der Kommunikationsinfrastruktur dar, bietet völlig neue Möglichkeiten der Kommunikation und ist ebenso zuverlässig und sicher wie die bisherige verkabelte Infrastruktur.

Vielfältige Vorteile durch WLAN-Lösungen

Die Forderung nach flexiblen mobilen Anwendungen kann mit herkömmlicher Infrastruktur nicht mehr erfüllt werden. WLAN-Techniken ermöglichen eine effiziente Gestaltung klinischer Prozesse und die Erschließung neuer Anwendungsfelder in medizinisch-pflegerischen, administrativen und in Leistungs- und Funktionsbereichen für Klinikmitarbeiter.

Anwendungsbeispiele:

- Die mobile Visite sowie Patientenüberwachung (z.B. mittels RFID-Armbändern) mit Zugriff auf Patientendaten und Datenaustausch mit klinischen Funktions-/Leistungsbereichen für
  - + Diagnostik (Labor, Radiologie u.a.)
  - + Therapie (Dialyse, OP, Physiotherapie u.a.),
- Beratung/Untersuchung/Konsilien am Patientenbett, auf Stationen und/oder in diversen Funktions- und Leistungsbereichen
- mobile KIS-/RIS-/Labor-/Funktionsdiagnostikanwendungen inklusive mobile Bild- und Signalverarbeitung
- Unterstützung administrativer Prozesse in der Materialwirtschaft/ Lagerhaltung (auf RFID-Basis)

An erster Stelle stehen die Vereinfachung und/oder Erweiterung der IT-Nutzungsmöglichkeiten für das in der Klinik tätige Personal (Ärzte, Pflege, Verwaltung). Dies gilt insbesondere für

- *Roaming User* zum Zugriff auf benötigte Datenbestände an externen oder Heimatstandorten sowie zur Integration/Teilnahme am E-Mail-Betrieb. Auch Dienste, wie beispielsweise der Zugriff auf Daten in Intranet/Internet-Portalen, zur Zentralbibliothek, zum Research Center sowie für Aus- und Weiterbildungszwecke sind möglich.
- Externe Partner (beispielsweise Gastärzte) zur Beratung/Untersuchung/ Konsilien am Patientenbett, auf Stationen oder in diversen Funktions- und Leistungsbereichen. Dabei stehen diesem nicht nur die internen Daten im Haus, sondern auch die eigenen, extern gelagerten Daten zur Verfügung.

Außerdem kann eine Steigerung des Niveaus der Patientenbetreuung durch Bereitstellung weiterer Dienstleistungen für Patienten und Besucher erreicht werden. Die möglichen Einsatzschwerpunkte liegen hier in

- der Bereitstellung von Internetdiensten für Patienten
- der Schaffung von Meetingpoints mit diversen Klinikinfo-Systemen für Patienten und Besucher

WLAN ist nicht gleich WLAN

WLAN-Techniken sind erst seit etwa dem Jahr 2000 sinnvoll nutzbar. Hier hat eine beeindruckende Entwicklung der Komponenten, Einsatzszenarien und Lösungsvarianten stattgefunden, die sich durch die Einführung controllergesteuerter Systeme etwa seit dem Jahr 2003 zeigt. Die meisten aktuell installierten WLAN-Netze basieren dennoch auf inzwischen veralteten Techniken, die einen hohen administrativen Aufwand und somit auch einen unnötigen Kostenfaktor bedeuten.

Ein weiterer Nachteil besteht in der ungenügenden Kontrolle des Verhaltens und der Wechselwirkungen eines solchen Netzwerkes. Definierte Eigenschaften können hier nicht gewährleistet werden. Aus heutiger Sicht ist die Installation von flächendeckenden WLANs für den professionellen Einsatz mit sogenannten FAT-APs nicht zu empfehlen.

Aktuell wird dem Nutzer mit der WLAN-Switching-Technologie eine Lösung geboten, die einerseits diese existierenden Mängel auf ein Mindestmaß reduziert, andererseits aber auch neue Einsatzgebiete erschließt. Derartige Netzwerke sind durch zentrale Komponenten beispielsweise in der Lage, auf Störungen aktiv zu reagieren und den Netzwerkbetrieb je nach Vorgabe zu modifizieren.

Höhere Sicherheitsanforderungen im WLAN-Umfeld

Gerade im WLAN-Umfeld muss der verbindungssuchende Client höhere Sicherheitsüberprüfungen durchlaufen als im verkabelten Netz. Folgende Aspekte müssen berücksichtigt werden:

- Authentifizierung *(Authentication)*
- Autorisierung *(Authorization)*
- Abrechnung *(Accounting)*

Während die Abrechnung für den Einsatz im Klinikumfeld durchaus noch als optional betrachtet werden kann (Internet am Patientenbett), sind die ersten beiden Aspekte unbedingt zu berücksichtigen.

In diesem Zusammenhang wird auch von NAC-Lösungen (*Network Admission Control*) gesprochen. Darunter sind Lösungen zu verstehen, die den Zugriff eines Clients erst dann auf die Res-

sourcen des Netzwerkes zulassen, wenn der Client vordefinierte Sicherheitsregeln erfüllt. Sonst darf er keinen Zugang zum Netzwerk erhalten oder muss sich in einer definierten Umgebung wiederfinden, in der er die erforderlichen Prozeduren durchlaufen kann.

Authentifizierung und Autorisierung der Clients

Die Authentifizierung beginnt vor der ersten Verbindungsaufnahme, da der Empfang des WLAN-Signals physikalisch auch außerhalb des Unternehmens möglich ist. Somit können theoretisch auch Unberechtigte Kontakt zum Netzwerk aufnehmen. Das muss in jedem Fall unterbunden werden. **Eine starke Authentifizierung als erste Sicherheitsstufe ist ein absolutes Muss.** Ist diese Stufe durchlaufen, werden den Clients eindeutige Berechtigungen zugewiesen. Dadurch sind sie in der Lage, sich in einem vordefinierten Netzwerkumfeld zu bewegen, aus dem sie nicht „ausbrechen“ können. conversol empfiehlt Anwendern einen umfassenden Schutz, der auch internationalen Sicherheitsstandards entspricht.

NAC-Implementierung

Gängige Schutzmaßnahmen sind:

- Virenschutzsysteme
- Firewallsysteme
- ID- und IP-Systeme

Einige am Markt befindliche Lösungen beinhalten für ihre Nutzer jedoch erhebliche Nachteile. Den Virenschutz von Rechnersystemen aktuell zu halten (Updates, Patches), bedeutet einen hohen administrativen und dadurch auch finanziellen Aufwand. Rechnernetze werden durch sie zudem nur ungenügend geschützt, weil sie anfällig für Sicherheitslücken sind – beispielsweise durch mobile Rechner.

conversol empfiehlt, in einem Unternehmen Regeln bzw. Automatismen einzuführen, die einerseits die Sicherheitsaspekte voll berücksichtigen und andererseits den administrativen (und somit kostenintensiven) Teil in überschaubaren Grenzen halten.

conversol plant mit zu diesem Zweck individuell ausgewählten Software-Systemen zur Überprüfung und zum Schutz der WLAN-Endgeräte. Dazu gehören u.a. die Überprüfung auf aktuelle Antivirensoftware, die Konfiguration der lokalen Firewall, die Verbindungskontrolle auf Trojaner, die Erkennung von Keyloggern und die Unterbindung des Auslesens von Monitordarstellungen.

Die NAC-Implementierung besteht aus sechs Modulen:

- Virtual Desktop
- Host Integrity
- Malicious Code Protection

- Connection Control
- Cache Cleaner
- Adaptive Policies

Erfüllt ein Modul den Sicherheitscheck nicht, so unterbindet der WLAN-Switch (Controller) den weiteren Datenverkehr.

Einbruchserkennung: Als **Intrusion Detection System (IDS)** wird die aktive Überwachung von Computersystemen und -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Intrusion Detection Systeme analysieren jedoch nur eine Kopie des Netzwerkverkehrs. Mögliche Aktionen bei Erkennen von Einbruchsversuchen müssen nach ihrer Entdeckung administrativ geregelt werden. Da ID-Systeme Missbrauch nur analysieren und nicht verhindern können, benötigen sie eine geeignete Einbindung in den organisatorischen Ablauf sowie technische Unterstützung durch geeignete Werkzeuge. Dies bedeutet einen zusätzlichen administrativen und personellen Aufwand, ohne ein aktives Handeln bei der Erkennung von Eindringlingen zu garantieren.

Einbruchsverhinderung: Anders sieht es mit so genannten IP-Systemen aus, wie sie von conversol empfohlen werden. Ein **Intrusion Prevention System (IPS)** arbeitet ähnlich wie ein Intrusion Detection System, ist jedoch aufgrund seiner Positionierung im Netzwerk in der Lage, erkannte Angriffe und schädliche Pakete auf Wunsch zu blocken und somit den Netzwerkverkehr durch Filterung **aktiv zu säubern**.

Ein weiterer Vorteil von IPS-Lösungen besteht in der grundsätzlichen Einrichtungsmöglichkeit an unterschiedlichen Positionen im Netzwerk. conversol erstellt aufgrund der erhöhten Kosten, die dabei entstehen können, auf Wunsch eine Kosten-Nutzen-Analyse.

Sicherheit

Die Sicherheit von Netzwerken ist ein sehr komplexes Thema und umfasst nicht nur rein technische, sondern auch viele organisatorische Aspekte. Dazu sollen einige Begriffe im Zusammenhang mit Datensicherheit definiert werden, um festzulegen, wo Schutzmaßnahmen ergriffen werden müssen:

- Integrität
- Verfügbarkeit
- Vertraulichkeit
- Verbindlichkeit
- Authentizität

Nachfolgend werden ausschließlich Fragen bezüglich der zu schützenden Daten betrachtet:

1. Welche Daten müssen geschützt werden?

- Persönliche Daten
- Geschäftliche Daten
- Besonders schützenswerte Daten (z.B. Patientendaten)

2. Wovor müssen diese Daten geschützt werden?

- Vor unerlaubten Zugriffen
- Vor missbräuchlicher Manipulation
- Vor Verlusten
- Übertragung „unerlaubter" Daten

3. Wie müssen Daten geschützt werden?

- Restriktive Zugriffsdefinition
- Abgestufte/selektive Zugriffsberechtigungen
- Ungehinderte Zugriffe aber Authentizitätsgarantie

Dem IT-Verantwortlichen stellen sich daher folgende Fragen:

- Wie kann sichergestellt werden, dass nur berechtigte Anwender Zugriff auf interne Daten je nach Berechtigungsebene erhalten?
- Welche technische Maßnahme hilft, eine erkannte Sicherheitsverletzung schnell und effizient zu beheben?
- Mit welchem organisatorischen und finanziellen Aufwand muss gerechnet werden?

Viele dieser Themen können durch administrative Festlegung z.B. mittels Mechanismen durch die Berechtigungssteuerungen auf Betriebssystemebene geregelt werden. Weitere Informationen zum Thema Sicherheit können auch dem IT-Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik) entnommen werden. [www.bsi.bund.de]

Anwendungen im klinischen Umfeld

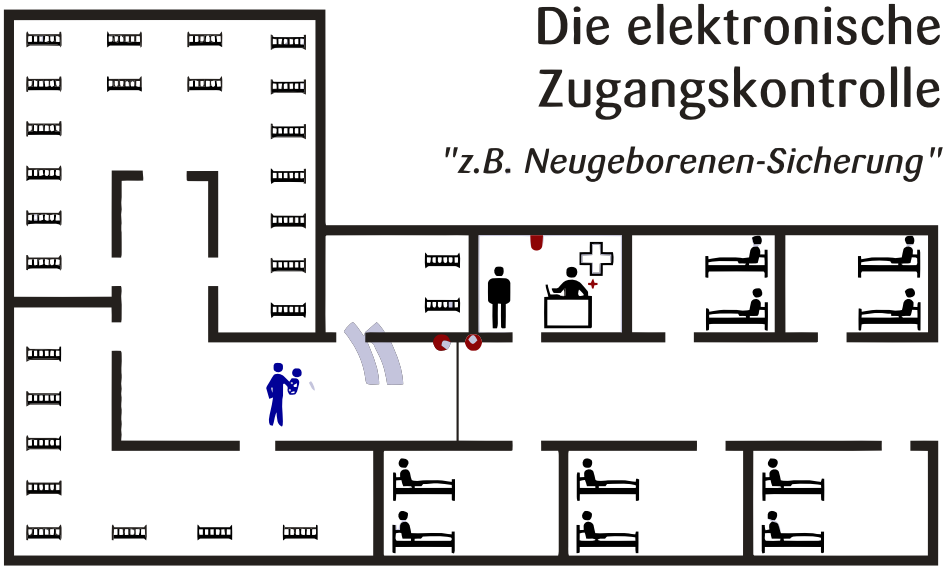
Die mobile Visite

Immer häufiger wird die Anforderung gestellt, beim Kontakt mit dem Patienten auf alle relevanten Patientendaten zugreifen zu können, um eine gesicherte Diagnose zu erstellen und eine effektive Weiterbehandlung festlegen zu können. Unter dem Begriff der *mobilen Visite* ist die Möglichkeit zu verstehen, dem Arzt an jedem Behandlungsort, Zugriff auf dessen elektronische Patientenakte zu geben.

Dabei handelt es sich um alle Daten, die im Krankenhaus-Informationssystem (KIS) hinterlegt wurden und auf die der Arzt zugriffsberechtigt ist. Dafür eignen sich neben herkömmlichen PCs auch PDAs (*Personal Digital Assistants*), Notebooks oder auch Tablett-PCs.

Drahtlose Patientenidentifizierung

RFID (*Radio Frequency Identification* – Funkfrequenzidentifizierung) stellt eine Methode zur berührungslosen und sogar sichtkontaktfreien Datenübermittlung dar (induktiv oder per Funk).



Der Begriff RFID bezeichnet die komplette Infrastruktur, die es möglich macht, Informationen drahtlos aus dem RFID-Etikett auszulesen. Das RFID-Etikett wird auch RFID-Tag oder RFID-Transponder genannt.

Diese Technik umfasst:

- RFID-Tag
- Sende- und Empfangseinheit, mit welcher der RFID-Tag angesprochen wird
- Integration mit Servern, Diensten und sonstigen Systemen wie z. B. Kassensystemen oder Warenwirtschaftsystemen.

Die Anwendungen sind auch im medizinischen Umfeld bereits etabliert und im täglichen Einsatz.

Lokalisierung von Ausrüstungsgegenständen

Gegenüber verdrahteten Netzwerken können mit Funktechniken in Verbindung mit entsprechend konzipierten WLAN-Netzwerken völlig neue Anwendungen realisiert werden, die bisher unmöglich umzusetzen waren. Dazu gehören Anwendungen, bei denen mobile Einrichtungen, Gegenstände oder auch Personen durch ihre Position im Gelände/Gebäude wichtige Informationen bereit stellen können (*Location Based System*):

- Lokalisierung von medizinischen Geräten
- Lokalisierung von wichtigem beweglichen Mobiliar (z.B. Bettenmanagement)

- Überprüfung, ob bestimmte Ausrüstungen durch „Tore“ bewegt wurden, hinter denen beispielsweise keine Lokalisierung mehr möglich ist
- Verfügbarkeit von patientenspezifischen Daten (am Krankenbett)

Um diese Dienste zu realisieren, sind erforderlich:

- eine geeignete WLAN-Infrastruktur
- Transponder, zur Informationsbereitstellung
- RFID-Komponenten zur „Markierung“ der Ausrüstungsgegenstände
- RFID-Empfänger (Reader) zum Empfang und zur Verarbeitung der Signale

Rechtliches

Vorschriften und Regularien

Für den Einsatz elektrischer Geräte in Europa müssen generell folgende Gesetze und Vorschriften beachtet und eingehalten werden.

- Die Geräte müssen alle über ein **CE-Zeichen** verfügen
- Die EMV-Bestimmungen, wie sie in der **EN 60 601** – “Sicherheit Medizinischer Elektrischer Geräte” – definiert sind (Grundzüge der neuen Norm **IEC 60601-1**)
- Die WLAN-Geräte müssen **Wi-Fi**-geprüft sein (*Wireless Fidelity*)

WLAN-Technik im Krankenhaus

Grundlage der WLAN-Technik bildet der Standardset IEEE 802.11, auf den sich das Institute of Electrical and Electronics Engineers (IEEE) und die Wireless Ethernet Compatibility Alliance (WiFi-Alliance13) geeinigt haben. Das 2,4-GHz-ISM-Band (ISM, Industrial, Scientific and Medical) wurde auch von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen freigegeben und ist speziell für den Einsatz im medizinischen Umfeld geeignet. Die Verordnung erlaubt jedoch die grundstücksübergreifende Anwendung von Funk-LANs für den internen Unternehmensbedarf. Somit steht dem Einsatz von Funk-LANs gemäß IEEE 802.11 nichts im Wege.

Relevant für den Einsatz im Klinik-Umfeld sind auch folgende Aspekte:
Die Personensicherheit (Patienten, Klinikpersonal, Besucher u.a.), die maximal zulässigen Effektivwerte nach DIN VDE 0848, Teil 2, E/10/91 Expositionsbereich 1 und die 26. Verordnung zum Bundes-Immissionsschutzgesetz werden durch die Standards nicht nur eingehalten, sondern weisen weitere Sicherheitsreserven auf.
Dies ist durch die in den IEEE-Standards (IEEE 802.11b/802.11g) festgelegte WLAN-Geräte-sendeleistung von maximal 100 mW. Im Vergleich dazu senden Mobilfunktelefone mit einer Leistung bis zu 2, d. h. mit der 60-fachen Leistung. Auch die Sendeleistung von herkömmlichen DECT-Telefonen liegt mit 250 mW noch um ein 2,5-faches höher. Bei Beachtung der vorgegebenen Grenzwerte bzgl. Einhaltung des Mindestabstands von 50 cm zwischen Antenne und WLAN-

Nutzern ist damit die Sicherheit von Menschen im elektromagnetischen WLAN-Umfeld in hohem Maße sichergestellt. Der Betrieb von ISM-basierten WLAN-Systemen ist in Deutschland anmelde-, genehmigungs- und gebührenfrei. Die Nutzung technischer Geräte im medizinischen Bereich nach DIN EN 60601-1 (Allgemeine Festlegung für die Sicherheit medizinischer elektrischer Geräte) und DIN EN 60601-1-2 (Ergänzung: Elektromagnetische Verträglichkeit) und dafür zertifizierter WLAN-Systeme von führenden Herstellern ist unbedenklich.

Funktechniken: Vorteile und Risiken im Klinikumfeld

Eine umfangreiche Untersuchung des Fraunhofer-Instituts für Integrierte Schaltungen (Fraunhofer IIS) am Klinikum Nürnberg Ende 2006 erzielte eine Reihe von relevanten Erkenntnissen. Es wurden unterschiedliche WLAN-Techniken (DECT, GSM, Bluetooth, WLAN im ISM-Band: 2,4-2,4835GHz) im Intensivbereich des Klinikum getestet.
Zusammengefasst wurden folgende Beobachtungen gemacht:

- DECT: leichte Störungen im EEG sichtbar
- GSM: weitaus größere Störungen als bei DECT (höhere Sendeleistung)
- WLAN: sehr begrenztes Störungspotential, welches nur unter extremen Bedingungen und auch dort nur bei ausgewählten Gerätetypen nachgewiesen wurde.

Kernaussage des Fraunhofer IIS: "Die WLAN-Technik ist ungefährlich, doch die Gefahr droht aus einer ganz anderen Richtung. DECT- und Handy-Telefonie stellen hohe Gefahrquellen dar."

Weitere Forderungen sind:

- WLAN-Geräte müssen eine CE-Kennzeichnung haben
- EMV-Werte sind nach gültigen Vorschriften einzuhalten (z.B. EN 60 601)

Die Systeme und Lösungen von conversol bieten eine vollständige Lösung für die Erkennung und Verhinderung nicht autorisierter Zugriffe oder Angriffe auf WLANs:

- Kontinuierliche WLAN-Überwachung
- Definition und Steuerung strenger Regeln für Datenzugriffe
- Klassifizierung von Ereignissen
- Lokalisierung und Eindämmung

Ein wesentlicher Faktor ist eine starke Authentifizierung der WLAN-Teilnehmer und Verschlüsselung der übertragenen Daten (Patientendaten). Mittels einer leistungsstarken Reportgenerierung kann sich der Administrator je nach Situation einen schnellen Überblick über das System verschaffen und das zukünftige Netzwerkverhalten durch Trendanalysen während des Netzwerkbetriebes einschätzen.

Fazit

Um im mobilen Umfeld der Kliniken auf lebenswichtige ebenso wie auf rein administrative Daten jederzeit sicher zugreifen zu können, ist die WLAN Technologie zum aktuellen Zeitpunkt unverzichtbar. Sie wird den seit einigen Jahren veränderten Anforderungen im Gesundheitswesen gerecht, ohne den finanziell eng gesteckten Rahmen der Unternehmen und Institutionen in dieser Branche zu strapazieren.

Auf der Basis einer stabilen IT-Infrastruktur können die erforderlichen Netzwerkdienste aufsetzen und damit einen reibungslosen Ablauf der Geschäftsprozesse für den laufenden Betrieb ermöglichen. Durch ihre Mobilität und Flexibiltät bietet die WLAN-Technologie eine effiziente Gestaltung der Prozesse und erschließt sogar neue Anwendungsfelder in den medizinisch-pflegerischen, den administrativen und den Leistungs- sowie Funktionsbereichen der Klinikmitarbeiter.

Die von conversol® herstellerunabhängig und individuell konzipierten Lösungen berücksichtigen die erhöhten Sicherheitsanforderungen, die die Unternehmen der Gesundheitsbranche an mobile Netzwerke haben. Selbstverständlich werden rechtliche und gesundheitliche Vorschriften und Regularien (Stichworte beispielsweise: Datensicherheit und Strahlungsschutz) bei der Komponentenauswahl berücksichtigt. Neben den bereits entwickelten Lösungen zur mobilen Visite, elektronischer Zugangskontrolle und Ressourcenmanagement entwickelt conversol® maßgeschneiderte Lösungen für die individuellen Anforderungen der Unternehmen und Kliniken.