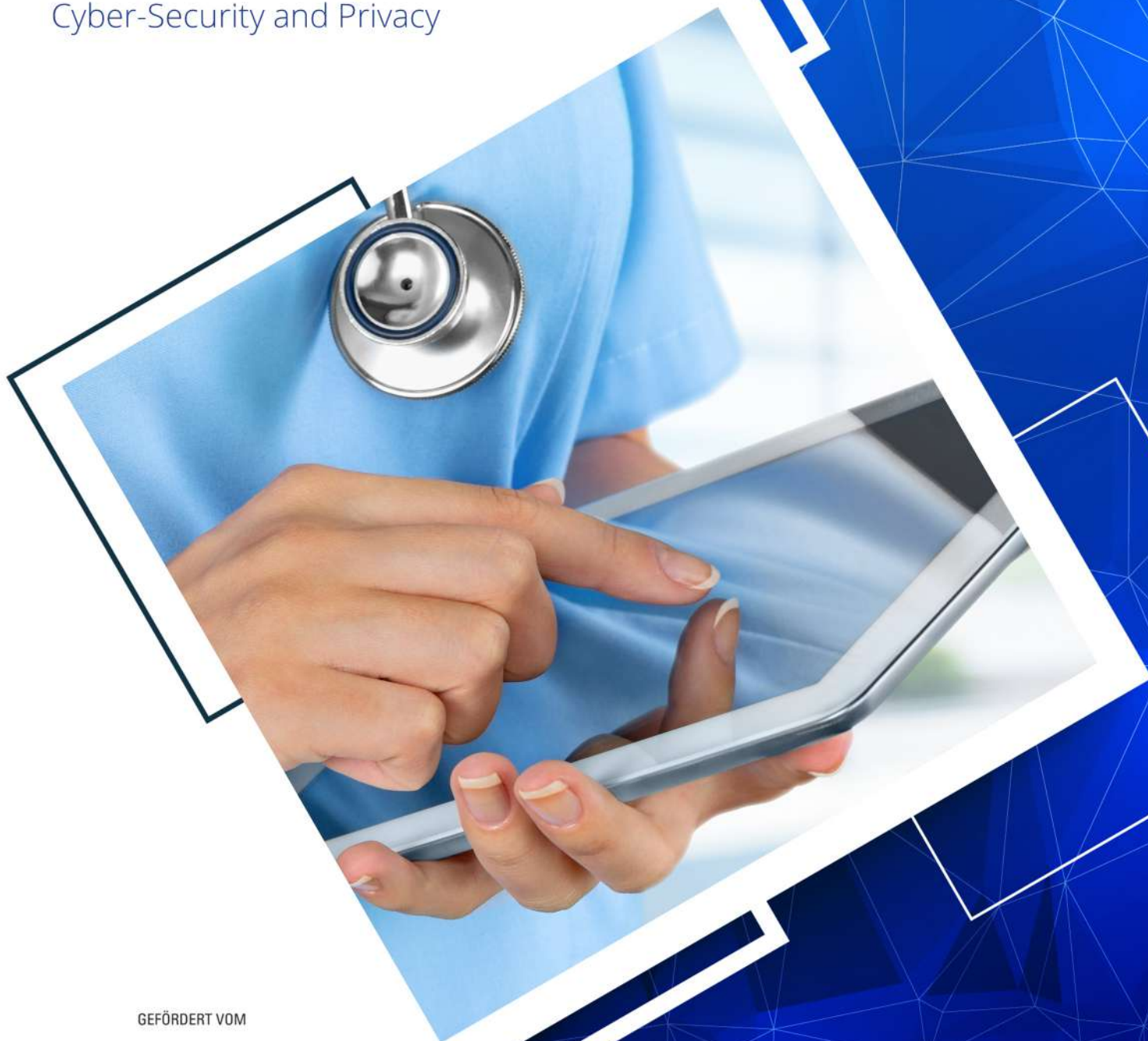


Hospital IT 4.0

Cloud / IT-Service / BigData
Mobile Anwendungen
Daten- / Dokumentenaustausch
Cyber-Security and Privacy

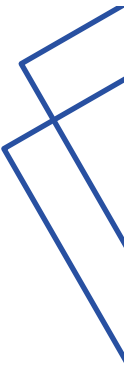


GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Hospital IT 4.0



Der Einsatz von moderner Informationstechnik im Krankenhaus gewinnt immer mehr an Bedeutung. Während die Digitalisierung zunächst darauf abzielt, bestehende Prozesse wie Datenaustausch und Dokumentation zu erleichtern, ergeben sich durch Technologien wie Cloud Computing, Big Data Analysen und medizinische Anwendungen auf mobilen Endgeräten ganz neue Möglichkeiten in der medizinischen Versorgung, der Forschung und der Administration. Durch die Sensibilität medizinischer personenbezogener Patientendaten ergeben sich jedoch durch zunehmende Vernetzung auch neue Herausforderungen an die Sicherheit der Systeme und den Datenschutz.

Cloud-Dienste erlauben es Einrichtungen, den eigenen Bedarf an IT-Infrastruktur, Plattformen oder spezieller Software von außen zu beziehen, was zunächst anfallende Anschaffungskosten, aber auch Wartungs- und Verwaltungsaufwand minimiert. Doch Cloud-Technologien können auch allein innerhalb der eigenen Einrichtung etabliert werden, um verteilte Krankenhausinformationssysteme, Anlagen und Geräte miteinander zu verbinden. Sie erlauben auch die Organisation von großen Datenmengen und deren Nutzung z.B. für eine personalisierte medizinische Behandlung durch Big Data-Analysen.

Durch die Vernetzung mobiler Endgeräte wie Smartphones oder Tablets mit dem Krankenhausinformationssystem ist es den Ärzten und Pflegekräften, aber auch dem Patienten möglich, Zugriff auf die für Sie wichtigen und freigegebenen Daten zu haben und umgekehrt Vorgänge wie die Eintragung von Medikation und

weiteren Daten vor Ort durchzuführen. Damit ergeben sich auch Anwendungen der Telemedizin und der medizinischen Überwachung von Patienten zuhause. Grundlage für diese Anwendungen ist ein strukturierter Datenaustausch, der nach standardisierten Profilen abläuft und Dokumente nach einheitlichen Terminologien erstellt. In einzelnen Bereichen wie der medizinischen Bildgebung werden schon herstellerübergreifende Standards verwendet. Im Falle von Patientendaten bieten Formate wie die elektronische Fallakte eine kontinuierliche Dokumentation zum Beispiel zwischen Praxis und Klinik.

Ziel dieser Entwicklungen ist eine elektronische Patientenakte, in der alle Daten wie Medikation und Befunde hinterlegt sind und dem Arzt, aber auch dem Patienten zur Verfügung stehen. Doch auch bei Vernetzung und Verfügbarkeit muss der Schutz der Daten gewährleistet sein. Dabei ist es wichtig, dass Einrichtungen wie Krankenhäuser Konzepte und Maßnahmen für alle Abteilungen gemeinsam umsetzen, so dass gerade im durch Geräte und Systeme verschiedener Hersteller mit unterschiedlichem Alter und Netzwerkfähigkeiten sehr heterogenen Umfeld Krankenhaus keine Sicherheitslücken entstehen.

Moderne Informationstechnik bietet im Krankenhaus 4.0 viele Möglichkeiten zur Optimierung von Prozessen und Etablierung neuer Anwendungen und Methoden, sowie eine verbesserte Transparenz für den Patienten, der durch die Verfügbarkeit seiner Daten in den Behandlungsablauf mit einbezogen wird.



Cloud / IT-Service / Big Data

Der Begriff „Cloud Computing“, im deutschen auch „Rechnerwolke“ genannt, bezeichnet die Bereitstellung von IT-Infrastruktur und – Diensten über das Internet bzw. über Rechnernetzwerke.

Cloud-Dienste können dabei in drei Kategorien eingeteilt werden. Zunächst das „Infrastructure as a Service“ Modell, kurz IaaS. Mit diesem Service können sich Kunden selbst virtualisierte Computerhardware passend zu ihrem aktuellen Bedarf an Ressourcen wie Speicher und Rechenleistung zusammenstellen und auf dieser dann selbstverantwortlich arbeiten.

Dieses Mieten von Rechnerinfrastruktur hat gegenüber dem direkten Kauf einige Vorteile. Die mit der Anschaffung verbundenen Kosten und Aufwände werden vermieden, seltene Nutzung wird bezahlbar, Bedarfschwankungen, sowohl kurzfristige wie Belastungsspitzen als auch langfristiges Wachstum, können abgefangen werden. Durch die nötige Virtualisierungstechnologie werden weitere Möglichkeiten wie Softwaretests auf unterschiedlichen Plattformen erleichtert.

Möchte ein Anwender Software entwickeln, kann er die dafür benötigten Plattformen wie Laufzeit- und Entwicklungsumgebung ebenfalls ohne die Anschaffung der benötigten Hard- und Software über die Cloud beziehen (Platform as a Service, PaaS). Aber Software kann nicht nur entwickelt, sondern auch als Cloud-Dienst angeboten werden.

Beim „Software as a Service“ Modell (SaaS) betreibt ein externer IT-Dienstleister die Software und die dafür nötige Infrastruktur und der Anwender nutzt diese als Dienstleistung. Hier ist ebenfalls die Kostenersparnis ein bedeutender Vorteil, da Wartung und Aktualisierung an den Dienstleister ausgelagert sind und der Anwender sich auf sein Kerngeschäft konzentrieren kann.

Wie bei jeder Auslagerung begibt sich der Nutzer dieser Services damit in Abhängigkeit zum Anbieter und nimmt einen Grad an Kontrollverlust in Kauf. Daher muss sorgfältig geprüft werden, welche Dienste über die Cloud bezogen werden sollen.

Public und Private Cloud

Doch Cloud ist nicht gleich Cloud. Denn neben den genannten Service-Modellen gibt es auch verschiedene Liefermodelle. Die beiden Hauptkonzepte sind die Public Cloud, in der einer breiten Öffentlichkeit über das Internet abstrahierte IT-Dienste angeboten werden. Am anderen Ende steht die Private Cloud, die nur einer begrenzten Gruppe Zugang ermöglicht und deren Hardware sich innerhalb („on premises“) der jeweiligen Organisation befindet. Dazwischen gibt es verschiedene Kombinations- bzw. Misch-Modelle. Hier sind u.a. die Hybrid-Cloud zu erwähnen, die auf den Nutzer zugeschnittenen kombinierten Zugang sowohl zu Public als auch Private Cloud-Diensten bietet und die Virtual Private Cloud, die öffentliche IT-Infrastruktur nutzt, aber durch geeignete Sicherheitsmaßnahmen wie VPN einen „privaten Bereich“ ermöglicht.

Aus diesem Katalog an Möglichkeiten bieten sich nicht nur für die Industrie, sondern auch in Krankenhäusern viele Einsatzmöglichkeiten. Neben den erwähnten Vorteilen der Einsparungen von Kosten und Einrichtungsaufwand durch Auslagerung kann die Cloud bzw. Cloud-Dienste dazu genutzt werden, große anfallende Datenmengen, die mit klassischen Methoden kaum zu analysieren sind (Big Data) strukturiert auszuwerten. Die so neu gewonnen Erkenntnisse fließen wieder direkt in die eigene Wertschöpfungskette. Die Nutzung dieser Massendaten kann zusätzlich dazu verwendet werden, die eigene Produktion bzw. im Falle eines Krankenhauses die eigene Logistik und weitere Abläufe mit Partnern wie Zulieferern abzustimmen und frühzeitig auf Veränderungen wie Lieferengpässe zu reagieren.

Datenschutz durch Firewalls und Sealed Cloud

In der Industrie, aber im Besonderen auch im Gesundheitsbereich muss die Sicherheit der Daten gewährleistet sein. Gerade bei der Nutzung von Public Cloud-Diensten ist es oft schwer nachvollziehbar, wo genau die jeweiligen Daten gespeichert werden und wer dort Zugriff besitzt bzw. erlangen könnte. Neben Verschlüsselungsmaßnahmen, die verhindern sollen, dass Daten während der Übertragung eingesehen werden können, ist eine besondere

Herausforderung für die Sicherheit, dass der Anbieter der genutzten Cloud-Dienste bzw. der genutzten IT-Infrastruktur grundsätzlich Zugang zu den Daten hat. Die Sealed Cloud (versiegelte Wolke) ermöglicht es durch eine Reihe an organisatorischen und technischen Maßnahmen, dass während der Übermittlung, Verarbeitung und Speicherung von Daten selbst der Betreiber der Infrastruktur keinen Zugriff auf die Daten hat. Diese Technologie wurde u.a. im Zuge des Trusted Cloud Programm des Bundesministeriums für Wirtschaft und Energie weiterentwickelt. Teil dieses Programms ist auch die „HealthCloud“, die dazu dienen soll, medizinische Rohdaten datenschutzgerecht für Fragestellungen aus Forschung, Entwicklung und Gesundheitsökonomie auszuwerten.

Mögliche Anwendungen sind die Auswertung aus anonymisierten Patientendaten, Wirtschaftlichkeitsprüfungen medizinischer Behandlungen und frühzeitige Erkennung von Nebenwirkungen neu eingeführter Medikamente durch automatisierte Verfahren. Diese Services können über eine öffentliche, aber auch über eine private Cloud bereitgestellt werden. Auch über eine interne, durch die eigene Firewall geschützte private Cloud ergeben sich viele weitere Anwendungsmöglichkeiten für Krankenhäuser, wie das Verwalten und die Analyse sowohl medizinischer Daten aus Medical Apps, aber auch logistisch relevanter Daten, wie Raumauslastung und Materialverbrauch durch den Einsatz von IoT-Technologie, über die sogenannte „smart devices“ selbstständig Daten über Gateways an Cloud-Dienste weitergeben können. Auch im Gesundheitswesen spielt „Big Data“ eine Rolle. Neben der erwähnten Nutzung der anonymisierten Daten als Grundlage zur Forschung und Entwicklung können die von einem Patienten anfallenden Daten aus der elektronischen Patientenakte genutzt werden, die Behandlung auf eine personalisierte medizinische Versorgung auszurichten.

Cloud IT im Krankenhaus bietet viele Möglichkeiten, die Digitalisierung und Vernetzung voranzubringen und ganz neue Anwendungen umzusetzen. Dabei ist es jedoch besonders wichtig zu entscheiden, welche Dienste intern über eine sicherere private Cloud bereitgestellt oder über die Public Cloud bezogen werden sollen und wie man diese Systeme miteinander verbindet.





Mobile Anwendungen

Die Digitalisierung und der Einsatz von Informations- und Kommunikationstechnologie (IKT) im Gesundheitswesen, oft als eHealth bezeichnet, umfasst die Bereiche der Vorbeugung, Diagnose, Therapie, Überwachung und auch der Verwaltung. Dabei werden zunehmend auch mobile Endgeräte wie Smartphones und Tablets, sowie tragbare „smart devices“ eingesetzt, um IT-Applikationen am „Point of Care“, also direkt am Patienten, nutzen zu können. Aber auch in den nicht medizinischen Bereichen wie der Logistik und Instandhaltung finden Anwendungen auf mobilen Geräten Verwendung.

Mobile Health

Mobile IKT, wie Smartphones und Tablets, die nicht als Medizingeräte entwickelt wurden, können durch die Verwendung von sogenannten Medical Apps trotzdem als solche fungieren. Dies kann der Darstellung von Röntgenaufnahmen am Krankenbett, der direkten Nachbestellungen von Medikamenten oder aber auch der Unterstützung von medizinischen Entscheidungen durch je nach Anwender festgelegten und sicheren Zugriff auf

weitreichende Daten dienen. Da die mobilen Geräte selbst nur Zugriff auf diese Daten benötigen und sie nicht selbst speichern und verwalten können, bieten sich Cloud-Plattformen zur zentralen Verwaltung der Datenmengen an. Auch die Medical Apps selbst können als Cloud-Dienste dem Anwender zur Verfügung gestellt werden.

Der Bereich der mobilen Anwendungen im Gesundheitswesen, inzwischen auch mit mHealth für „Mobile Health“ bezeichnet, kann in mehrere Einsatzgebiete bzgl. der Anwendergruppen unterteilt werden. So bezeichnet der „Bürgerbereich“ Anwendungen ohne direkten medizinischen Zweck, die freiwillig verwendet werden können und der Wellness und Fitness dienen, wie Laufcomputer oder Ernährungs-Apps. Erfüllt die Anwendungen einen medizinischen Zweck müssen Qualitäts- und Sicherheitsstandards erfüllt werden. Anwender hier sind Patienten mit akuten oder chronischen Erkrankungen, die mit Hilfe der mobilen und tragbaren Geräte Vitalparameter wie z.B. Herzfrequenz und Blutzucker aufzeichnen oder auch direkt

weiterleiten im Rahmen eines „Remote Monitoring“, also der medizinischen Überwachung aus der Ferne.

Abgesehen von den so aufgezeichneten Daten kann das medizinische Fachpersonal ebenfalls von mobilen Anwendungen profitieren. Stehen ein Krankenhausinformationssystem (KIS) und/oder eine elektronische Patientenakte (EPA) zur Verfügung, kann diese vom jeweiligen Endgerät abgerufen oder auch bearbeitet werden. So wird vermieden, dass Patientenakten in bestimmten Situationen nicht zugänglich sind und Lücken durch fehlende Dokumentation oder wechselnde Einrichtungen entstehen. Hierdurch kann der Behandlungspfad besser dokumentiert und organisiert und das Krankenhaus bzw. Praxis-Management unterstützt werden.

Apps als Medizinprodukt

Ein Vorteil vieler mobiler medizinischer Anwendungen ist es, auf schon bestehende Technologien wie dem mobilen Internet zurückgreifen zu können, wodurch die Einführungskosten gesenkt und trotzdem eine Verbesserung der Arbeitsabläufe und der Patientenversorgung erreicht werden kann.

Doch nutzt man schon vorhandene Technologien, muss genau geprüft werden, ob diese den besonderen Anforderungen im medizinischen Kontext an funktioneller Sicherheit und Datenschutz genügen. Denn der Schutz der medizinischen und personenbezogenen Informationen ist eine der Hauptherausforderungen bei der Einführung von mHealth-Anwendungen. Nicht nur aus technischer Sicht, sondern auch als vertrauensbildende Maßnahme gegenüber den Patienten, die oft nicht nachvollziehen können, wo die Daten wirklich gespeichert werden und wer wann Zugriff auf sie hat.

Hilfreich wären Zertifizierungen und Qualitätssiegel. Hier gibt es schon einige Ansätze wie das European Directory of Health Apps, welches über 200 von europäischen Patientengruppen empfohlenen mHealth-Anwendungen auflistet. Zum Thema mHealth veröffentlichte zudem die Europäische

Kommission ein Grünbuch über Mobile-Health-Dienste, in dem der aktuelle rechtliche Rahmen, Potentiale und nächste Schritte behandelt werden.

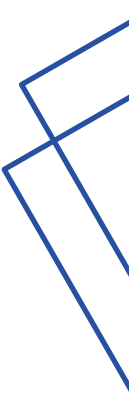
Einbeziehung des Patienten

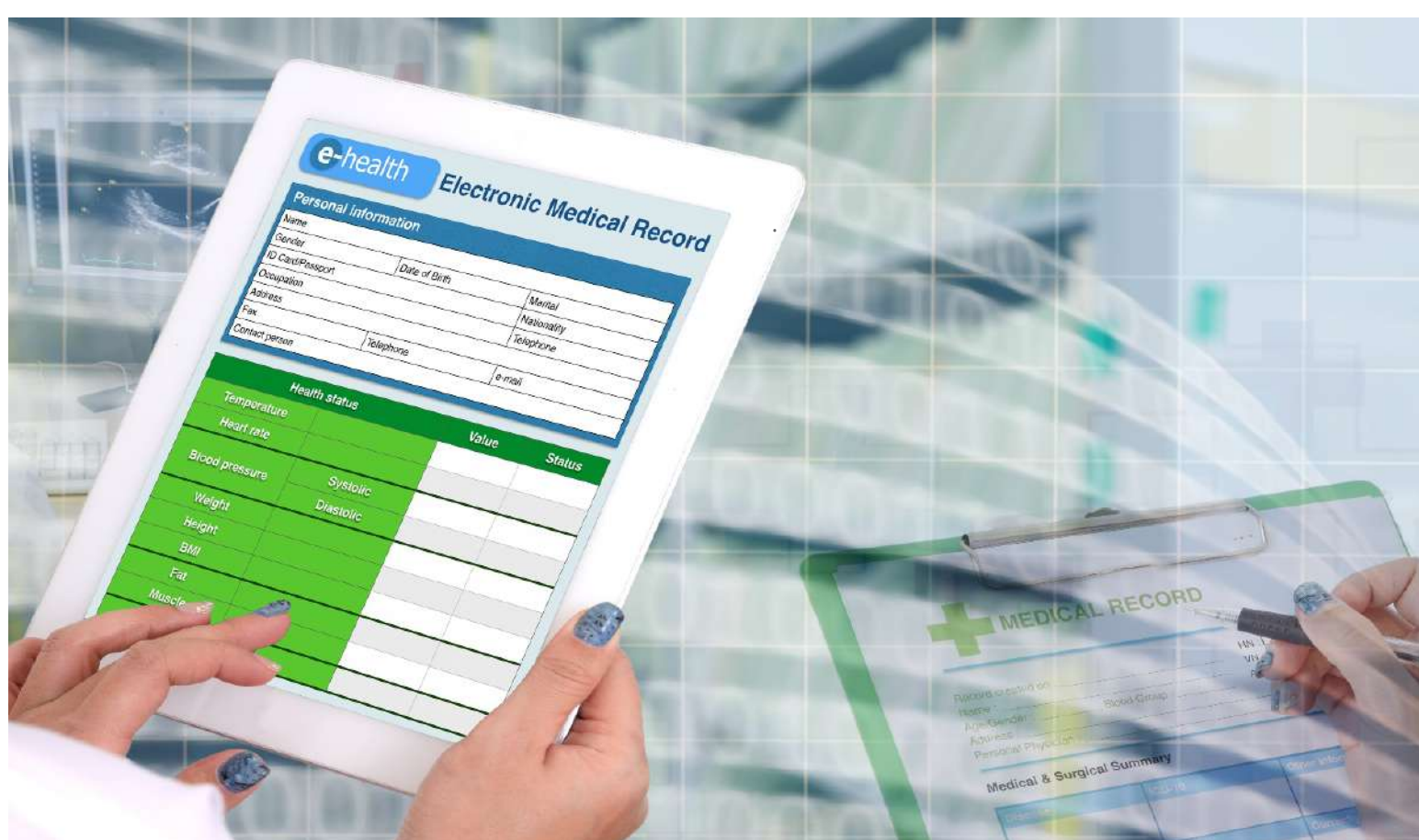
Durch mobile Anwendungen und die Verwendung von Medical Apps werden Patienten besser in den Behandlungsprozess mit einbezogen und haben eine bessere Übersicht über die vom Arzt getroffenen Maßnahmen. Besonders chronisch Erkrankte können von Möglichkeiten wie dem Remote Monitoring profitieren, um die Anzahl nötiger Kontrolltermine zu reduzieren.

Mit Blick auf den demografischen Wandel und die steigende Zahl chronischer Erkrankungen könnten diese und weitere telemedizinischen Anwendungen Versorgungsengpässen entgegenwirken. Aber nicht nur für den Patienten, sondern auch für das medizinische Fachpersonal bringen mobile Anwendungen Vorteile. Bei Visiten können Ärzte direkt neueste Ergebnisse abrufen, dem Patienten visualisieren und sind bei der Einpflege eigener Maßnahmen und Daten nicht mehr auf einen festen Arbeitsplatz und Desktop-Computer angewiesen.

Neben den medizinischen Anwendungen können auch andere Bereiche im Krankenhaus wie die Logistik und die Instandhaltung von mehr Mobilität profitieren. So kann der Verbrauch bestimmter Bedarfsgüter direkt vor Ort eingegeben und an die Lagerbestandsverwaltung weitergeleitet werden. Wartungstechniker können mit geeigneten Schnittstellen an den jeweiligen Geräten Zugriff auf relevante Daten wie Fehlermeldungen oder Störungen erhalten, um nötige Maßnahmen effizienter zu koordinieren und durchführen zu können.

Insgesamt stellen mobile Anwendungen auf Endgeräten wie Smartphones und Tablets eine der Hauptschnittstellen zwischen dem „Krankenhaus 4.0“ und den Anwendern, dem Personal und den Patienten dar und können so seine Vorteile direkt zugänglich machen.





Daten- / Dokumentenaustausch

Im klinischen Umfeld entstehen eine Vielzahl von Daten an, die eine funktionierende Dokumentation unabdingbar machen. Diese dient dabei nicht nur der medizinischen Versorgung direkt, wie Patienteninformationen, Medikation, Arztbriefe, Laborergebnisse, Röntgenaufnahmen etc., sondern ist auch notwendig für die Qualitäts- und Leistungserfassung, die Forschung, sowie für die Patienten- und Personalsicherheit.

Fehlende Standards / Medienbrüche

Durch fehlende Standards und Medienbrüche während der Dokumentation kann es zu Lücken und auch zu Fehlern kommen. Im Gesundheitswesen ist besonders die Vielfältigkeit der anfallenden Informationen eine Herausforderung, um Normen und Standards für verschiedene Einrichtungen dieses Sektors zu erstellen. Doch genau diese sind notwendig und wichtig bei einer fortschreitenden Digitalisierung und Vernetzung, denn die Übermittlung bzw. der Austausch von Informationen bildet die Grundlage für das Krankenhaus 4.0.

Allerdings wird in vielen Bereichen die Dokumentation derzeit noch papierbasiert umgesetzt. Dies kann einige Nachteile nach sich ziehen, wie Übertragungsfehler durch unleserliche Schrift, Unzugänglichkeit durch fehlerhafte Ablage oder lange Wartezeiten bei Anfragen. Innerhalb eines Krankenhauses bieten Krankenhausinformationssysteme (kurz KIS) die Möglichkeit, anfallende Daten und Dokumente zu verwalten und jedem befugten Mitarbeiter Zugang (mobile Anwendungen) zu den für ihn relevanten Informationen zu gewährleisten. Nicht nur medizinische Informationen wie Krankheitsdaten und Arztbriefe, sondern auch administrative und logistische Daten können erfasst werden. Doch bei der Integration von KIS-Strukturen gibt es kaum Standards, nur bei der konkreten Datenübermittlung sind Protokolle und Normen vorhanden, wie HL7 (Health Level 7) oder in Bezug auf die medizinische Bildgebung der offene Standard DICOM (Digital Imaging and Communication in Medicine), der zumindest in diesem Umfeld

herstellerübergreifende Interoperabilität ermöglicht.

Von der Fallakte zur EPA

Beim Austausch von Informationen verschiedener Einrichtungen, wie zwischen der Praxis des Hausarztes und der Klinik ergeben sich zudem weitere Schwierigkeiten. So können bei der Überweisung von Patienten Informationen zur Medikation, der Krankheitsgeschichte und der bisher stattgefundenen Behandlung fehlen, was zu Doppeluntersuchungen, Wartezeiten durch angeforderte Informationen oder sogar zu Behandlungsfehlern wie Fehlmedikation führen kann.

Um Vollständigkeit und Kontinuität der zu übermittelnden Information zu gewährleisten, gibt es für Ärzte die Möglichkeit, für den Patienten bzw. seinen konkreten Behandlungsfall eine elektronische Fallakte (EFA) anzulegen. Diese ersetzt nicht die Dokumentation innerhalb der eigenen Einrichtung, sondern stellt ein Bindeglied zwischen den einzelnen Einrichtungen und Leistungsträgern dar. In ihr vermerkt bzw. überträgt der Arzt mit der Einverständniserklärung des Patienten alle relevanten Informationen, die für eine Weiterbehandlung nötig sind, erstellt Zugangsberechtigungen für die jeweiligen Fachabteilungen und übermittelt die Akte über die EFA-Plattform an die Einrichtung, an die der Patient überwiesen wird.

Die dafür nötige Infrastruktur können die beteiligten Einrichtungen selbst aufbauen oder inzwischen über EFA-Provider beziehen, wodurch sich sowohl technischer als auch finanzieller Aufwand reduzieren. Über standardisierte EFA-Schnittstellen ist die Übertragung unabhängig von den jeweiligen IT-Systemen vor Ort. Unterstützung bei der Integration eines solchen Systems bietet der Verein Elektronische FallAkte e.V.

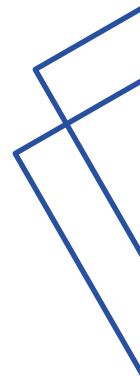
Durch die Kooperation mit weiteren Organisationen und Initiativen zur Einführung von Standards beim Daten- und Dokumentenaustausch im Gesundheitswesen wie dem IHE (Integrating the Healthcare Enterprise) und HL7

werden die Einsatzmöglichkeiten und die Verbreitung weiter vorangetrieben.

Über das Konzept der EFA hinaus könnten zukünftig alle anfallenden Patientendaten zentral in einer elektronischen Patientenakte (EPA) hinterlegt werden. In ihr würden alle Informationen des Patienten, von aktueller Medikation und Unverträglichkeiten bis hin zu einzelnen Befunden erfasst und durch gesteuerte Zugriffsrechte dem Arzt, der Pflegekraft oder dem Patienten selbst jederzeit und unabhängig vom Ort zur Verfügung gestellt werden. Dies ermöglicht einen reibungsloseren Ablauf bei Einweisung und Entlassung sowie bei der Behandlung selbst und sorgt für mehr Transparenz, was sowohl der Qualitäts- und Leistungskontrolle als auch der Sicherheit zu Gute kommt. Auf der anderen Seite ergeben sich mit der EPA neue Anforderungen an den Schutz der Daten.

Basis für die Forschung

Insgesamt bietet die Standardisierung von Erfassung, Dokumentation und Austausch medizinischer Daten die Möglichkeit, klinikübergreifende Datenbanken anzulegen. Auf dieser Menge an Daten (Big Data) könnten z.B. Algorithmen und Data Scientists arbeiten, um Ärzten Behandlungsempfehlungen zu geben oder Studien bzgl. neu eingeführter Medikamente durchgeführt werden. Durch eine gemeinsame Dokumentation und Nutzung der Daten können besonders kleinere Einrichtungen vom Expertenwissen anderer profitieren, wird dem Patienten eine auf ihn besser angepasste, personalisierte medizinische Behandlung ermöglicht und die Grenze zwischen medizinischer Versorgung und Forschung überwunden.





Cyber – Security and Privacy

Bei der Betrachtung von Fragestellungen der IT-Sicherheit müssen mehrere unterschiedliche Aspekte berücksichtigt werden. Zum einen gibt es die sogenannte Funktionssicherheit (Safety), die gewährleisten soll, dass Systeme gemäß ihrer erwarteten Funktion arbeiten. Daneben beschreibt die Informations- bzw. die Datensicherheit den Schutz der Informationen vor unautorisiertem Zugriff (Security). Darauf aufbauend bezieht sich der Datenschutz auf die Sicherheit von Personen, die Kontrolle über die eigenen persönlichen Daten zu behalten (Privacy).


Sicherheit in der Industrie

Eine der am weitesten verbreiteten Bedenken bei der Einführung von neuer Technologie im Rahmen „Industrie 4.0“ ist die Security, also die Datensicherheit. Laut einer Umfrage des VDE unter Entscheidern in der Industrie ist für 7 von 10 Befragten die IT-Sicherheit das größte Hindernis der Industrie 4.0 in Deutschland. Daher kommt der IT-Sicherheit eine Schlüsselrolle bei der Entwicklung hin zur Industrie, aber auch dem Krankenhaus 4.0 zu. Die entsprechenden

Maßnahmen erfüllen damit nicht nur ihren technischen Zweck, sondern wirken vertrauensbildend als Wegbereiter neuer Technologien.

Wenn immer mehr Systeme vernetzt werden und somit einen breiter verteilten Zugang erlauben, steigt auch das Risiko von unautorisierten Zugriffen. Dies gilt für Anlagen wie Kraftwerke, Strom- und Telefonnetze, aber auch für Fabriken, Krankenhäuser und Privathaushalte.

Die Sicherheit von Anlagen wie einer „Smart Factory“ der Industrie 4.0 ist durch die Vernetzung im Unternehmen selbst und die Vernetzung nach außen, sowie durch die Heterogenität der Teilnehmer wie cyber-physischer Systeme (CPS) eine besondere Herausforderung. Dies gilt ebenso für das "Krankenhaus 4.0", das durch die Vielzahl unterschiedlicher Anwender, Geräte und Systeme, sowie die Sensibilität der Informationen besonders geschützt werden muss.



Doch der Einsatz von neuen Technologien im Zusammenhang mit "4.0" bedeutet nicht automatisch den potentiell öffentlichen Zugang zu den eigenen Daten. So können z.B. Cloud-Strukturen auch als „private cloud“ nur innerhalb des eigenen Unternehmens etabliert werden, physisch getrennt oder durch Firewalls und weitere Systeme und Module geschützt werden.

Security Engineering

Um diese Sicherheit der IT in sogenannten soziotechnischen Systemen, in denen die IT verschiedenste Zwecke erfüllt und die Anwender bzw. Mitarbeiter über unterschiedliches Know-How verfügen zu gewährleisten, bedarf es eines methodischen und systematischen Vorgehens (Security Engineering). Um Unternehmen bei Maßnahmen zur Verbesserung der Sicherheit wie Bedrohungsanalyse, Modellierung und Bewertung zu unterstützen, hat das Bundesministerium für Sicherheit und Informationstechnik (BSI) mehrere Ansätze entwickelt. Das „ICS-Security-Kompodium“ (ICS für Industrial Control Systems) stellt eine Art Grundlagenwerk für die IT-Sicherheit in Automatisierungs-, Prozesssteuerungs- und Prozessleitsystemen dar und richtet sich an IT-Sicherheitsexperten, aber auch als Informationsquelle für Betreiber mit weniger Erfahrung. Ergänzend steht mit dem „Light and Right Security ICS, kurz LARS ICS ein Werkzeug für einen einfachen Einstieg für kleinere und mittlere Unternehmen in das Thema der Cyber-Security zur Verfügung.

Sicherheit im Krankenhaus

Im Krankenhaus 4.0 ergeben sich ähnliche Probleme bezüglich vernetzter Systeme. Doch hier können Angriffe auf die IT eines Krankenhauses mehr als nur wirtschaftlichen Schaden, sondern auch direkt gesundheitliche Konsequenzen für die Patienten bedeuten. Laut einer IBM Studie war das Gesundheitswesen 2015 der am häufigsten von Cyber-Angriffen betroffene Sektor. Über verbundene Medizingeräte wie Messgeräte auf der Intensivstation kann Zugriff auf das Krankenhausnetzwerk erlangt und Malware eingeschleust werden. Ziele der Hacker sind oft die Patientendaten und weitere wichtige und vertrauliche Daten

des Krankenhauses, um diese weiter zu verkaufen oder zu sperren, um das Krankenhaus zu erpressen. Auch nach einem Angriff kann die verwendete Malware zu Fehlfunktionen der infizierten Geräte führen.

Ein Grund für erfolgreiche Angriffe ist oft die veraltete Software der Geräte, die durch vernachlässigte oder durch rechtliche Hürden blockierte Updates für neue Bedrohungen angreifbar werden. Daher ist es besonders wichtig, genau zu wissen, welche Geräte verbunden sind und über welche Sicherheitsmaßnahmen diese verfügen, um so das Krankenhaus sowohl im Sinne der Funktionssicherheit als auch der Informationssicherheit und des Datenschutzes zu schützen.

Die elektronische Gesundheitskarte

Ein prominentes Beispiel bezüglich des Datenschutzes im Gesundheitswesen ist die deutsche elektronische Gesundheitskarte (eGK). Auf dieser Smartcard sind neben dem Namen und Adressdaten des Versicherten auch Informationen gespeichert, die besonderen Schutz vor unautorisierten Zugriff bedürfen, wie Daten über den sozialen Status, Rezepte oder zukünftig auch weitere medizinische Daten. Die eGK verfügt über verschiedene Verschlüsselungsverfahren und -Ebenen. Neben einer sechs- bis achtstelligen PIN unterstützt die eGK zur Erstellung digitaler Signaturen und Zertifikate das RSA-Verfahren, den X.509 Standard und verwendet Verschlüsselungsalgorithmen wie SHA-1 und 3DES.

Ein wichtiger Schritt hin zu mehr IT-Sicherheit ist die Sensibilisierung der Hersteller, Betreiber und Anwender für das Thema Cyber-Security. Zudem ist es wichtig, dass Abteilungen, die bisher eigenständig agierten, wie Office-, Infrastruktur- und Medizingeräte-IT ein gemeinsames Sicherheitskonzept etablieren, um Schwachstellen in der umfassenden Vernetzung des Krankenhauses zu verhindern.

Partner



UNIVERSITÄT ZU LÜBECK



Impressum

UniTransferKlinik Lübeck
Maria-Goeppert-Straße 1
23562 Lübeck
E-Mail: info@unitransferklinik.de

Autoren der Arbeitsgruppe Innovationsforum Krankenhaus 4.0

Dr. Raimund Mildner
Prof. Dr. J.-Uwe Meyer
Nils Eckardt
Lina Hartung
Julia Kahlisch
Juljan Bouchagiar
Martin Mildner

Gestaltung

Niclas Apitz
Bjarne Anderse

Bildnachweis

in chronologischer Reihenfolge:
Great Bergens, www.BillionPhotos.com,
Sergey Nivens, dolgachov,
pandpstock001, Khakimullin
- alle Bigstock.com

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung