Von der Digitalisierung in der Medizin profitieren - HealthCare 2.0 und MedTec- Industrie 4.0:

Connectivity und Cybersecurity bei Medizinprodukten im MDR- & IVDR- Zeitalter (Teil 1: Stakeholder-Anforderungen)

Die Digitalisierung in der Medizin ist nicht nur die Schlüsseltechnologie zur Effizienzsteigerung und Schonung der Personalressourcen in der medizinischen Versorgung – Stichwort Pflegenotstand – , sondern eine wesentliche Voraussetzung zur Weiterentwicklung der Evidenzbasierten Medizin (EbM) und damit zur Steigerung und Sicherung der Versorgungsqualität. Evidence-adaptive clinical decision support systems (CDSS) unterstützen nicht nur die Therapieentscheidung, sondern auch die Delegation der Therapiesteuerung vom verantwortlichen Arzt auf das medizinische Assistenzpersonal. Medizin braucht digitale Lösungen. „Cybersicherheit ist eine wesentliche Voraussetzung für die Medizinproduktesicherheit und den Patientenschutz." sagte das BfArM.

Dieser dreiteilige Praxisbericht zeigt die Bedeutung der Connectivity und Cybersecurity bei der Entwicklung und Vermarktung zukunftsweisender Medizintechnischer Geräte und Verbrauchsmaterialien.

Dabei beleuchten wir die praktische Umsetzung im Lichte der MDR/IVDR, der ISO 13485 (QMS), der ISO 14971:2019 (Risiko Management), der IEC 62304 & IEC 82304-1 (Software Lebenszyklus), der IEC 81001-5-1:2021 (Cyber-Sicherheit) und der europäischen Datenschutzgrundverordnung (DSGVO).

In diesem „**Teil 1: Stakeholder-Anforderungen**" skizzieren wir die Use- und Business Cases der Connectivity von zukunftsfähigen Medizinprodukten und Verbrauchsmaterialien.

Business Development-, Produkt Manager und Entwicklungsingenieure finden in diesem Whitepaper eine Übersicht über die Use Cases und Business Cases zur Digitalisierung von Medizinprodukten.

Damit kann dieser Erfahrungsbericht als Checkliste dienen, um die Vollständigkeit der Stakeholder Anforderungen / des Lastenheftes für die Neu- oder Weiterentwicklung von Medizinprodukten und Verbrauchsmaterialien zu überprüfen.

Im „**Teil 2: R&D Best Practices**" berichten wir über die Erweiterung von ISO 13485 QM Systemen um die regulatorischen und normativen Vorgabe zur Integration von Cyber-Security Maßnahmen entlang des Entwicklungs- & Product Lifecycle- Prozesses.

Außerdem bietet Ihnen der Teil zwei eine kompakte Einführung in die Grundlagen und Begriffe der Cyber-Sicherheit mit Fokus auf Medical Devices in TCP/IP und IoMT Netzen.

Wer im Sinne einer agilen Entwicklung von Medizinprodukten die Spezifikation oder Architektur für die Plattform der nächsten Gerätegenerationen entwickeln möchte, findet im „Teil 2: R&D Best Practices" konkrete Vorschläge aus unserer Beratungspraxis.

Mit dem „**Teil 3: IoMT & Künstliche Intelligenz**" schließen wir unsere [wissenswert] Serie Connectivity & Cybersecurity von Medizinprodukten ab. Im Fokus stehen die Themen **Internet-of-Medical-Things (IoMT)** / **Medical Cloud** und das zukunftsweisende Thema der **Künstlichen Intelligenz** bei Medizinprodukten. ■

1 Connectivity – der unterschätze Erfolgsfaktor

Die historische Lösung die Kundenanforderung an eine IT-Schnittstelle bei Medizinprodukten zu erfüllen war und ist, Statusänderungen der Geräte einfach auf eine serielle Schnittstelle zu legen. In der Regel wurden das mangels herstellerunabhängiger Standards durch proprietäre Protokolle realisiert.

Irgendwann waren dann keine single-board Computer mit RS-232 Schnittstelle mehr verfügbar und der RJ-45 Ethernet Port wurde zum Stand der Technik und möglicherweise zur Sicherheitslücke.

Praxisbeispiel: Änderung von Geräteeinstellungen bei Insulinpumpen und Sterilisatoren durch nicht authentifizierten Fernzugriff über das Netzwerk.

Der Aufwand der Implementierung von herstellerspezifischen Protokollen, das Problem der sicheren Patientenidentifikation und die geringe Fehlertoleranz unidirektionaler Geräteschnittstellen hat dazu geführt, dass ein sehr geringer Anteil der heute in Krankenhäusern genutzten medizintechnischen Geräte in die Krankenhaus-IT-Infrastruktur eingebunden ist.

Das etablierte Modell, um den Digitalisierungsgrad innerhalb eines Krankenhauses zu messen, ist das Electronic Medical Record Adoption Model (kurz EMRAM). Hier werden Krankenhäuser anhand einer Skala von 0 (keine Digitalisierung) bis 7 (papierloses Krankenhaus) bewertet. Krankenhäuser in Deutschland erreichen im Durchschnitt einen Wert von 2,3 (n=~400). Damit liegt Deutschland unter dem europäischen Mittelwert von 3,7. Kein Krankenhaus in Deutschland erreichte 2019 die Stufe 7.

Der Krankenhaus-Report 2019 „Das digitale Krankenhaus“, kommt zu dem Fazit, dass der Anteil der Krankenhäuser in Deutschland, die im klinischen Bereich noch gar nicht beziehungsweise kaum digital arbeiten (Stufe 0 EMRAM) bei etwa 40 Prozent liegt.

Wer daraus das Fazit zieht, dass die IT-Integration von Medizinprodukten nur eine untergeordnete Rolle spielt, nimmt sich die Chance (a) sein Produkt durch Value-Added Funktionen für die (potentiellen) Kunden aufzuwerten und sich in der Healthcare 2.0 zu positionieren sowie (b), das Internet-of-Things nicht nur als Hebelarm der Effizienzsteigerung und Kostensenkung, sondern als Wettbewerbsfaktor zu nutzen.

Schlimmer noch: Durch Zögern gewinnt der Wettbewerb wertvolle Zeit, seine durchgängigen IT-Plattformen in Kliniken auszubauen, seine Produkte in den klinischen Workflows und der IT-Infrastruktur der Krankenhäuser zu verwurzeln, und so Wettbewerb von zukünftigen Aufträgen auszuschließen.

Inhalt

Links:

(1) EU Datenschutz-Grundverordnung (PDF)
(2) BfArM: Cybersicherheit von Medizinprodukten
(3) BSI: Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte (PDF)

Stichworte: Datenschutz, Privacy by Design, Patientenschutz, Datensicherheit, MDR, IVDR, IEC 60601-1:2005+A1:2012, DIN EN 61010-1:2020, IEC 62304, IEC 82304-1, IEC 81001-5-1:2021, Secure by Design, FDA Cybersecurity in Medical Devices, Defense in Depth, UL 2900-2-1:2017, IEC 8001, Risiko Management, ISO 14971:2019 / ISO 24971, MDCG 2019-16, Medizinprodukte-Sicherheitsplanverordnung (MPSV), Vigilanz, Remote Service, Medical Devices, Cyber-Security, Cyber-Sicherheit,Medizinprodukte

2 Regulatorische und normative Anforderungen

Im Gegensatz zur MDD Richtlinie aus dem Jahr 1993 geben die aktuelle Medical Device Regulation (MDR) und auch die In-vitro-Diagnostic Device Regulation (IVDR) Herstellern von Medizinprodukten seit 2017 konkrete Vorgaben zur Cybersecurity vor, z.B.:

- MDR Anhang I, # 14.2 bzw. IVDR Anhang 1, #13.2: Die Produkte werden so ausgelegt und hergestellt, dass folgende Risiken ausgeschlossen oder so weit wie möglich reduziert werden: (…) d) Risiken minimieren im Zusammenhang mit der möglichen negativen Wechselwirkung zwischen Software und IT-Umgebung, in der sie eingesetzt wird und mit der sie in Wechselwirkung steht.
- MDR Anhang 1, # 16.4 / 17.4 bzw. IVDR Anhang 1 # 16.4: Die Hersteller legen Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT- Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff fest, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind.

Auch die 3rd Edition der ISO 14971:2019-12 zur Anwendung des Risikomanagements auf Medizinprodukte nimmt das Thema Cybersecurity (risks related to data and systems security) in den Scope. Die 3rd Edition ist zwar bisher noch nicht harmonisiert, empfiehlt sich jedoch schon jetzt. Nach dem 25. Dezember 2022 wird die FDA auf die Erfüllung der Anforderungen aus der 3rd Edition bestehen.

Ebenso finden sich in der IEC 60601-1:2005+A1:2012 (Medizinische elektrische Geräte) bzw. der DIN EN 61010-1:2020 (Elektrische Laborgeräte) und IEC 62304 (Software) die Forderung, Risiken im Zusammenhang mit Cybersecurity zu beherrschen.

Zwar gesetzlich nicht bindend aber spannend wie aktuell ist das Medical Device Coordination Group Document (MDCG 2019-16) „Guidance on Cybersecurity for medical devices“ z.B. für Audits durch Benannte Stellen. Das FDA Guidance Dokument „Cybersecurity in Medical Devices“ gilt als Voraussetzung für Zulassung. Die IEC 81001-5-1:2021 konkretisiert die Anforderungen entlang des Product Lifecycle.

In QM Systemen nach ISO 13485:2016 wird im Abschnitt 4.2.5 der „Schutz von vertraulichen Angaben zur Gesundheit“ gefordert.

Die Neu- und Weiterentwicklung von Medizinprodukten unterliegt klaren regulatorischen und normativen Vorgaben zur Cybersecurity. Das Thema ist hochaktuell und nicht nur im Fokus der FDA. Best Practices zur effizienten Umsetzung der Vorgaben finden Sie im Teil 2 dieses Whitepapers.

3 Patienten-Identifikation und EU Datenschutzgrundverordnung (DSGVO)

Die eindeutige Patientenidentifikation ist die Grundvoraussetzung zur Erfüllung der ärztlichen Dokumentationspflicht und der Patientensicherheit, wie z.B. aus der gemeinsamen Initiative der The-Joint-Commission und der WHO hervorgeht.

Auch wenn ein Großteil der medizinischen Geräte auch heute noch keine Patientenidentifikationsdaten z.B. über eine HL7 Patient Demographics Query von Mastersystemen abrufen, bieten viele Geräte die Eingabe von Patienten-Informationen an.

Seit dem 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (DSGVO), die Gesundheitsdaten als besonders schutzwürdig einstuft.

Die DSGVO betrifft die Hersteller von Medizinprodukten nicht nur direkt, wenn sie in Europa personenbezogene Daten oder Daten von Europäern z.B. in IoT Kundenportalen oder Apps verwalten, sondern auch als Kundenanforderung an Medizinprodukte.

Die Anforderung, mit einem Medizinprodukt datenschutz-konform arbeiten zu können wird zunehmend zum grundlegenden Beschaffungskriterium von Krankenhäusern, Arztpraxen und Pflegeeinrichtungen.

„Privacy by Design“ bedeutet, das bei der (Weiter-) Entwicklung von Medizinprodukten die Grundsätze des Datenschutzes umgesetzt werden:

- Sobald ein Gerät die Eingabe der Patienten ID, Vor-/Nachnamen, des Patientengewichtes- oder der Körpergröße ermöglicht, gelten die Vorgaben des Datenschutzes.
- Einmal eingegebene Patientendaten dürfen nicht für jedermann zu jederzeit im Gerätespeicher oder den Geräte-Log Files sichtbar sein. Das gilt insbesondere auch für ortsveränderliche / mobile Medizinprodukte, die z.B. in Gerätepools eingesetzt werden.
- Der Artikel 32 der DSGVO fordert die Pseudonymisierung und Verschlüsselung personenbezogener Daten, was damit zur Anforderung an die Datenbank auf Medizinprodukten wird.
- Der U.S. Health Insurance Portability and Accountability Act (HIPAA) definiert konkrete Anforderungen an die Pseudonymisierung personenbezogener Daten. Er eignet sich für die Implementierung und Zertifizierung der Lösungen.
- Die Löschung der Daten bzw. aller identifizierenden Merkmale (=Anonymisierung) auf (Software) Medizinprodukten muss regelbasiert erfolgen,

um die Einhaltung der Datenschutz Vorgaben sicherstellen zu können. Regeln, wie das automatische Löschen nach Abschluss der Therapie, dem Ausschalten des Gerätes oder der erfolgreichen Datenübertragung an ein Mastersystem haben sich in unserer Beratungspraxis bewährt.

- Über die im technischen Service beliebten Remote Desktop / Control Tools lassen sich die Anforderungen des Datenschutzes in der Regel nicht sicherstellen. Connected Services müssen transparent gestaltet sein.
- Medizinprodukte sollten im „Privacy by Default" Modus ausgeliefert werden, d.h. alle Funktionen des Datenschutzes müssen per Default aktiviert sein.

Beim Datenschutz gilt: Alles, was nicht explizit erlaubt ist, ist verboten! Allein durch den Artikel 82 der DSGVO „Haftung und Recht auf Schadensersatz" wird „Privacy by Design" zur wichtigen und vielleicht kaufentscheidenden Kundenanforderung.

Damit gehört „Privacy by Design" als Stakeholder-Anforderung heute in jedes Lastenheft für die (Weiter-) Entwicklung von Medizintechnischen Geräten.

4 Use- & Business Cases der MedTec Industrie 4.0 für Gegenwart und Zukunft

Die Digitalisierung in der Medizin ist einer der Schlüsseltechnologien zur Effizienzsteigerung und damit zur Kosteneinsparung in der medizinischen Versorgung.

Die Workflow- und IT-Integration von Medizinprodukten entlastet medizinisches Assistenz- & Fachpersonal bei administrativen und organisatorischen Prozessen und hilft sich auf die wertschöpfenden Kernprozesse der Versorgung von Patientinnen und Patienten zu fokussieren.

In der Vergangenheit stand deshalb die automatische Dokumentation, d.h. die Datenübergabe an Krankenhausinformationssysteme (KIS), Laborinformationssysteme (LIS), Patienten-Datenmanagement-Systeme (PDMS) und Radiologie- Informationssysteme (RIS) im Vordergrund. HL7 und DICOM sind die Sprachen der HealthCare 1.0.

Heute sehen Medizinprodukte-Hersteller das zusätzliche Wachstumspotential in der Intraoperabilität, der Workflow Integration und der IoMT-Technologie.

Auf den folgenden Seiten berichten wir über vielleicht inspirierende Praxisbeispiele aus der HealthCare 2.0 und aus der MedTec-, BioTec- und Pharma-Industrie 4.0.

4.1 Professionalisierung und Profitabilitätssteigerung des Verbrauchsmaterial Geschäftes

IoMT und die automatische Erkennung von Verbrauchsmaterial und Reagenzien (Barcodes, RFID, NFC,…) steigern nicht nur die Patientensicherheit und das **Verbrauchsmaterial-Geschäft** durch die Überwachung der max. Standzeit, Sterilisation, Wiederverwendung und Ausschluss der Produktpiraterie.

Die Digitalisierung des Verbrauchsmaterial Geschäftes erlaubt auch **Pay-By-Use Zusatzgeschäfte.** So lässt sich im Sinne der Kliniken der Investitionsanteil reduzieren und die Budgetsicherheit erhöhen.

Transparenz und eine automatische Nachbestellung (Abo Funktion) schützen vor Produkt-Piraterie und Wettbewerbsangeboten und verbessern die exakte Prognose des individuellen Kundenbedarfs.

Selbst wenn sich beim Verbrauchsmaterial keine echte Differenzierung zu preisgünstigen Alternativen realisieren lässt, kann die Anzeige „Möglicherweise nicht kompatibles Schlauchsystem" oder eben die automatische Freischaltung von Geräte-Zusatzfunktionen durch das Originalzubehör oder das Medikament eine wertvolle Differenzierung bieten.

Praxisbeispiel: Überwachung der Benutzung steriler chirurgischer Instrumente in der Roboterchirurgie.

4.2 Umsatzsteigerung durch Kostendruck dank Modularität und Medical Apps

Viele Kunden erwarten eine universelle Einsetzbarkeit des technischen Equipments. Diese Anforderung und das z.B. durch Ausschreibungen getriebene Wettrüsten bei den Produkt Features lässt den Funktionsumfang moderner Geräte und damit die R&D Kosten immer weiter steigen.

Kunden kaufen und bezahlen heute Gerätefunktionen, die sie vermutlich nie selbst nutzen werden. Das kann schnell zur Preisfalle für den Vertrieb werden.

IoMT macht es möglich Funktionspakete bedarfsgerecht über online verfügbare Lizenzen anzubieten und aus dem Standard Lieferumfang heraus zu nehmen.

So wird der Wert des Produktes, und nicht nur der Preis reduziert. Dabei bleibt für den Kunden die Zukunftssicherheit des Gerätes erhalten. Dem Hersteller bleibt die Hoffnung die Funktionspakete in der Zukunft vermieten oder verkaufen zu können und nicht durch einen Rabatt verschenkt zu haben.

Es gab mal eine Zeit, in der wurden Anbieter von Apps auf Telefonen müde belächelt. Der Erfolg dieses

neuen Geschäftsmodells hat Skeptiker mittlerweile verstummen lassen.

In unserer Beratungspraxis haben wir mehrfach zeigen können, dass sich modulare Software auf Medizinprodukten durch smartes Risikomanagement und den Beleg der Gebrauchstauglichkeit ohne weiteres regulatorisch beherrschen lässt.

Praxisbeispiel: Lizenzcodes zur Erweiterung der Funktionen der Oxymetrie.

4.3 Mehrwert und Kundenbindung durch Training, Simulation und Augmented Reality

Der Funktionsumfang universell einsetzbarer medizintechnischer Geräte stellt nicht nur die Entwicklungsabteilung des Herstellers, sondern auch die Kunden selbst vor eine große Herausforderung.

So gesehen profitieren durchaus auch Anwender von der bedarfsgerechten Reduktion des Funktionsumfangs und damit der Komplexität der Geräte.

Insbesondere auch bei komplexeren Geräten und in Bereichen, in denen das Personal interdisziplinär zusammenarbeitet oder eine überdurchschnittliche Personalfluktuation herrscht, wird die Geräteschulung der Anwender zu einer Herausforderung.

Smarte Konzepte zur Anwenderschulung erzeugen für Krankenhäuser nicht nur einen Mehrwert dadurch, dass die (technischen) Möglichkeiten der angeschafften Geräte auch wirklich ausgenutzt werden, sondern sind auch aus Sicht der Steigerung der Anwender- und Patientensicherheit und den gesetzlichen Vorgaben aus der Haftung und dem Medizinproduktegesetz relevant.

So schafft ein Simulations- & Trainingsmodus von Geräten und interaktive web-basierte E-Learnings einen großen Mehrwert für die Anwender und das Krankenhaus als verantwortlicher Betreiber.

Selbst der Implementierungsaufwand von Augmented Reality Lösungen als unterstützendes Trainingswerkzeug z.B. über die Microsoft HoloLens 2 ist überschaubar, wenn die Anwendung bereits während der Entwicklung der Software Architektur des Medizinproduktes berücksichtigt wurde.

Praxisbeispiel: Simulationsmodus eines Beatmungsgerätes zum Trainieren des Komplikationsmanagements.

4.4 Wirtschaftlichkeit und zusätzliches Umsatzpotential durch Geräte Pool Management

Insbesondere bei mobilen Geräten, die klinikweit eingesetzt werden (können), ist die objektive Bewertung der Verwendungshäufigkeit der Schlüssel zur Optimierung der Wirtschaftlichkeit.

Geräte Pool Management heißt im Digitalen Zeitalter nicht nur, den Gerätestandort und die zugeordnete Kostenstellen online verfolgen zu können, sondern auch den Datenschutz und das (stationsspezifische) Konfigurationsmanagement vollständig zu automatisieren.

Smarte Implementierungen machen Versorgungsengpässe beim Kunden auch für den Hersteller sichtbar. Die Bereitstellung von Geräten zur Abdeckung von Bedarfsspitzen, der Betriebswirt spricht von Konsignationslägern, lässt sich dank IoMT so automatisieren, dass dem Pflegepersonal kein administrativer Mehraufwand entsteht.

Auch zum Vorteil des Kunden kann der Kundenberater so Verbesserungs- und Einsparungspotentiale basierend auf Daten und Fakten des individuellen Kunden aufzeigen. Beratungskompetenz schafft Kundenbindung.

Praxisbeispiel: Deutliche Steigerung der Verwendung von Dekubitus-Präventions-Systemen und Chirurgischen Spezialinstrumenten durch vollautomatisierte Abwicklung des Pay-by-Use Mietvorgangs.

4.5 Alarm- / Echtzeitanwendungen & Personalruf

Verschiedene Studien zeigen, dass jeder Intensivpatient und dessen Behandlung mehr als sechs Alarme pro Stunde verursachen. Die Mehrheit dieser Alarme, bis zu 90%, ist jedoch falsch positiv, also ein Fehlalarm. Diese Fehlalarme führt oftmals zu einer Unterbrechung der Arbeit und begünstigen Fehler. Das Emergency Care Research Institute benennt zwei Jahre in Folge diese „Alarm-Fatigue“ als größte medizintechnologische Gefahr.

Bidirektionale Geräteschnittstellen und Intraoperabilität erlauben nicht nur ein smartes zentrales Management von Alarmgrenzen und die schnelle Quittierung akustischer Alarme, sondern auch die Vermeidung von Alarmen durch Trendanalysen und der Anzeige der Restlaufzeit, bis ein Alarm ausgelöst wird bzw. vermeidbar ist.

Praxisbeispiel: Zentrale Anzeige der Prognose der Restlaufzeit bis zu vermeidbaren Alarmen bei Infusionspumpen.

4.6 Einzelprodukte durch Systemlösung schützen

Durch Intraoperabilität (DIN EN ISO IEEE 11073 Service-oriented Device Connectivity (SDC) / Vital Standard) und die Integration der Geräte in den klinischen Workflows entsteht nicht nur wertvoller Zusatznutzen für den Kunden, sondern auch eine kaum überwindbare Hürde für den Wettbewerb.

Werden Einzelgeräte durch Intraoperabilität und nicht nur das gleiche Firmenlogo miteinander verbunden, schützt die Systemlösung das Einzelprodukt.

So lassen sich modulare Systeme entwickeln, die sich an den Bedarf und das Budget des Kunden flexibel anpassen lassen.

Intraoperabilität wird insbesondere im OP (siehe OR.net) und der Notfall- & Intensivmedizin das Pseudonym für die Zukunftsfähigkeit von Medizingeräten und Value-Added Systemlösungen werden.

Praxisbeispiel: Gerätetyp übergreifende IT-Plattformstrategie eines chinesischen Systemanbieters.

4.7 Effizienzsteigerungen in der medizinischen Versorgung durch Workflow Modellierung

Intraoperabilität und Real Time Location Services (RTLS) erlauben es, den Patientenfluss in Funktionsbereichen wie dem OP oder der Notaufnahme zu modellieren und zu optimieren.

Insbesondere bei Medizinprodukten, die den Patienten auf seinem Clinical Pathway durch den Funktionsbereich (z.B. OP) begleiten, lassen sich pseudonymisierte Daten zur Workflow Analyse oder auch zur Steuerung z.B. in einem digitalen OP-Plan nutzen. Ein Mehraufwand für das Pflegepersonal durch Dokumentation dürfte weitgehend vermeidbar sein.

So leisten Hersteller durch die Bereitstellung von Daten eine Wertschöpfung z.B. für das OP Management.

Praxisbeispiel: Mobiler OP-Tisch mit SDC Interface & elektronischem OP-Plan.

4.8 Digitalisierung als Schlüssel zur Evidenz basierten Medizin (EbM)

Die Digitalisierung in der Medizin gilt auch als die Schlüsseltechnologie zur kontinuierlichen Steigerung der Versorgungsqualität bei gleichzeitiger Kostensenkung im Sinne der Evidenzbasierten Medizin (EbM).

Die EbM fordert, dass bei einer medizinischen Behandlung patientenorientierte Entscheidungen nach Möglichkeit auf der Grundlage von empirisch nachgewiesener Wirksamkeit getroffen werden sollen.

Der wissenschaftliche Nachweis der Wirkung erfordert in der Regel eine sehr umfassende Datenerhebung und Auswertung mit den Werkzeugen der Statistik und Künstlichen Intelligenz.

Im Hinblick auf die knappen Ressourcen beim medizinischen Assistenz- & Fachpersonal ist schon aus Sicht der EbM eine vollautomatisierte Datenerfassung und Therapiedokumentation zu fordern um multifaktorielle Therapieverläufe erfassen und bewerten zu können.

Praxisbeispiel: Validierung der Algorithmen zum Automated Weaning (Entwöhnung von der Beatmung).

4.9 Evidence-adaptive clinical decision support systems (CDSS) und Telemedizin Konsil

Gleichzeit entsteht durch Intraoperabilität / Cockpits zusätzlicher Kundennutzen in der Reduktion von Komplexität, Steigerung der Sicherheit und Usability:

Evidence-adaptive Clinical Decision Support Systems (CDSS) können im Zusammenspiel mit der Telemedizin helfen, den scheinbaren Widerspruch zwischen Ressourcenknappheit / Pflegenotstand auf der einen, und dem Anspruch der Qualitätssicherung / Evidenzbasierter Medizin auf der anderen Seite aufzulösen.

Schon einfache web-basierte (telemedizinische) Cockpits können die engmaschige Therapiesteuerung z.B. in der Intensivmedizin und die Delegation an Assistenzpersonal vereinfachen.

Smarte Implementierungen machen über streng pseudonymisierte Daten den **klinischen Nutzen** für Kunden, wissenschaftliche Fachverbände und den Hersteller belegbar. Ein echter Mehrwert auch für Marketing und Vertrieb.

Die Anforderungen an ein CDSS Cockpit sind meist spezifischer als an die standardisierte Therapiedokumentation im PDMS. Deshalb stehen beide Ansätze auch nicht im Wettbewerb zueinander.

Web-based Lösungen für den mobilen Einsatz auf dem Smartphone, dem Tablet oder PC können heute schon über ein einzelnes Gerät, in jedem Fall aber über eine Gateway Software elegant gelöst werden. Dazu sind die Use Cases nur bei der Geräteentwicklung und dem Risiko Management zu berücksichtigen.

Solche Lösungen können Pflegepersonal dabei unterstützen, Abweichungen von den gewünschten Therapiezielen frühestmöglich zu erkennen.

Praxisbeispiel: Trenddarstellung der lungenprotektiven Beatmung mit Kapnographie und Blutgasen auf dem Tablet (PC)

4.10 Service Geschäft und Kundennähe professionalisieren

Kundenzufriedenheit und Kundennähe bleiben bei einem so umkämpften Markt wie der Medizintechnik ein wichtiger Erfolgsfaktor. IoMT Kundenportale ermöglichen ganz neue Möglichkeiten der Kundenbindung.

Hersteller können die online Registrierung ihrer Geräte zur Voraussetzung zur Inanspruchnahme der -marktüblichen- zweijährigen Herstellergarantie statt der gesetzlichen einjährigen Gewährleistung machen. Das wird in den meisten Fällen dazu führen, dass sich die Geräteverantwortlichen mit Ihren Kontaktdaten beim Hersteller registrieren.

Der Download der aktuellsten Gebrauchsanweisungen, online Hilfe und Newsletter zu neuen Software Versionen sind kostengünstige Value-Added Dienstleistungen und Werkzeuge der Kundenbindung. Die online Störungsmeldung mit Logfile Upload oder auch eine „Rückruf Taste“ sind schnell realisiert.

Smarte IoMT Implementierungen erlauben es Service Spezialisten und Entwicklungs-Ingenieuren (!) technische Daten und Logs von Ihren Geräten im Feld abzurufen. So können Sie die Werkzeuge zur Fehleranalyse und rechtzeitigen Vorhersage von drohenden Störungen an einer zentralen Stelle weiterentwickeln. Kunden und Ihr Service profitieren von einem Remote Service und Remote Device Monitoring, von dem sich auch Datenschutzbeauftragte leicht überzeugen lassen.

4.11 Der gläserne Kunde oder Post-Market Surveillance (PMS)

Die Forderung nach einer Überwachung nach der Inverkehrbringung (PMS) bzw. dem Post-Market Performance Follow-up (PMPF) findet sich in der MDR, der IVDR, der ISO 13485:2016, der ISO 14971:2012, dem 21 CFR part 822 und dem FDA Guide aus dem Mai 2016.

IoMT Kundenportale bieten die wohl effizienteste Möglichkeit Gerätedaten wie auch Kundenfeedback systematisch zu erfassen und auszuwerten.

5 Best Practice für die Systemarchitektur

Ob die IT-Integration wirklich als Mehrwert vom Kunden wahrgenommen wird, zeigt sich schon bei der ersten Störung der Datenübertragung.

Das medizinische Personal erwartet dann eine Hochverfügbarkeit der gewohnten IT gestützten Funktionen.

Neben all den Funktionen rund um die Dokumentation der Diagnostik und Therapie in der elektronischen Patientenakte gilt dies insbesondere auch bei Value-Added Gerätefunktionen, die mit der Steigerung der Patienten Sicherheit verbunden sind.

Der Best Practice ist nicht, die falsche Einstellung / Bedienung / Dosierung unmöglich zu machen, sondern den Bedienerfehler erst vor der Ausführung abzufangen. Nur dann wird sichtbar wie häufig wie schwerwiegende Fehler durch das System verhindert wurden. Das hilft nicht nur dem Qualitätsmanagement und Critical Incident Reporting System (CIRS) im Krankenhaus, sondern auch dem Vertrieb des Herstellers.

Im Gegensatz zur IT-Integration von Großgeräten wie z.B. in der Radiologie, der Zentralsterilisation oder dem Labor kann die Robustheit der Datenübertragung bei mobilen Geräten in den unterschiedlichen Funktionsbereichen und Stationen zur Herausforderung werden. Ein häufig unterschätzter Fakt.

Der klassische Ansatz auf dem Gerät eine RS232-, USB- oder Ethernet Schnittstelle anzubieten und im Störungsfall auf die klinikeigene Medizintechnik & IT-Abteilung oder den Software Hersteller zu verweisen ist selten zielführend. Weder für den Kunden noch den technischen Service des Herstellers.

Die Zuständigkeit des Geräteherstellers auf die Geräteschnittstelle zu beschränken erscheint nur auf den ersten Blick die einfachste Lösung zu sein. In der Praxis wird dann schnell die Abhängigkeit spürbar, in die diese Strategie den Hersteller (Service) führt.

Die profitabelsten Business Cases scheitern an der Serviceability der IT-Integration und der Abhängigkeit von 3rd Party Softwareanbietern.

Auch hier ist der vielleicht naheliegendste Lösungsansatz, die Installation einer Remote Control Software (z.B. die Freeware VNC, Remote Desktop, ….) schon aus Gründen des Datenschutzes schwer in die Praxis umzusetzen. Das gilt erst recht bei „firewall friendly“ Lösungen, also die Datenübertragung die den normalen http port (80) benutzt und damit versuchen die Sicherheitsfunktionen des Krankenausnetzwerkes zu umgehen. Ein Thema der Cybersecurity.

Als den Best Practice beim Entwurf der Funktionalen Architektur sehen wir ein dreistufiges Konzept:

(1) **Point-of-Care Connectivity:** Der Verbindungsstatus und die Verbindungsqualität sollten wie beim

Smartphone (Netzqualität und WLAN) für den Nutzer von Medizintechnischen Geräten jederzeit als Statusicon sichtbar sein. Zur Einrichtung der Netzwerkverbindung und zur Ursachenanalyse im Störungsfall solle eine interaktive Bedienerführung so realisiert werden, dass die Handhabung für technische Laien möglich ist. Wer die Unterbrechung der Datenübertragung als normalen Betriebszustand bewertet und entsprechende IO-Buffer und Synchronisationsmechanismen implementiert, wird durch eine hohe Robustheit der Lösung auch im klinischen Routinebetrieb überzeugen.

(2) **(HL7) Gateway:** Die direkte Datenübertragung von einem mobilen Medizingerät zu einer 3rd Party Software sollte wo immer möglich vermieden werden. Erst eine im Netzwerk des Kunden installierte Hersteller spezifische Gateway Lösung (als Medizinprodukt) bietet die Möglichkeit der zentralen Konfiguration, des Monitorings und Troubleshootings der Geräte Connectivity. Im Auslieferzustand können Geräte selbst die Verbindung zum Gateway aufnehmen und die kundenspezifische Konfiguration zu übernehmen. Im Gegensatz zur Einzelverbindung behält der Hersteller bei der Gateway Lösung die Kontrolle über das Connectivity Geschäft, wenn er z.B. ein bidirektionales HL7 Gateway oder das Geräte Pool & Service Management lizensiert. Web basierte Telemedizin Anwendungen lassen sich so mit geringem Aufwand und Risiko realisieren. Quasi- Echtzeit Anwendungen im Status- & Alarmmanagement inkl. der Fernsteuerung (Alarmquittierung) werden möglich. Protokollkonverter und vor allem die Funktionen zur Analyse, dem Troubleshooting und Customizing von z.B. HL7 Nachrichten müssen so nicht mehr auf jedem Gerät entwickelt werden.

(3) **Connected Services:** Ein zentrales Gateway im Netzwerk des Kunden dürfte die beste Voraussetzung bieten IT-Security und Datenschutz Experten in Krankenhäusern von dem Nutzen des Internet-of-Medical-Things (IoMT) zu überzeugen. Die zentrale Einstellung der „Privacy by Default“ aller Geräte wird sicherlich von jedem Datenschutzbeauftragten positiv bewertet. Die Einstellung welche Daten automatisch oder manuell an den Hersteller übertragen werden und die volle Transparenz der Datenübertragung dürften selbst die letzten Zweifel aus dem Weg räumen. So profitieren Krankenhäuser von der Effizienzsteigerung und Kostensenkung, die die Digitalisierung der Medizintechnik bietet.

Hat ein Krankenhaus erstmal in die Beschaffung, Installation und die HL7 / DICOM Interfaces zu den Mastersystemen investiert, wird die Motivation und das Budget gering sein, weitere vergleichbare Systeme zusätzlich in Betrieb zu nehmen. Die Erweiterung der vorhandenen Installation durch die Neubeschaffung weiter System kompatibler Geräte wird fast immer wirtschaftlicher sein, als weitere Insellösungen. Der Hersteller profitiert von der Verwurzelung seiner Geräteplattform in den klinischen Workflows und der IT-Infrastruktur.

Praxisbeispiel: Zentrales Management aller dezentralen mobilen Geräte der Point-of-Care Diagnostik

6 Zusammenfassung des ersten Teils

Dieser erste Teil bot Ihnen nicht nur eine Übersicht über die gesetzlichen und regulatorischen Vorgaben zum Datenschutz und der Cybersecurity. Die Liste der Use- und Business Cases für das HealthCare 2.0 und MedTec Industrie 4.0 Zeitalter ermöglicht einen schnellen Abgleich mit Ihren Lastenheften.

Autoren & Feedback

Herr Samim Azizi, MSc, Herr Dr. Philipp Babel und Dipl.-Ing. (FH) Bernd Schleimer sind (Senior) Berater bei der Grünewald GmbH.

Wir freuen uns über Ihr Feedback.