Herausforderungen bei der Einführung von Datenbrillen in den Realbetrieb eines Krankenhauses aus Sicht der IT

Ein Erfahrungsbericht aus dem BMBF-Projekt PARCURA

von Arne Reuter, FACT IT GmbH, Bremen

Inhaltsverzeichnis

Münster, Mai 2023

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

ESF Europäischer Sozialfonds für Deutschland

Europäische Union

Zusammen. Zukunft. Gestalten.

1 Einordnung

"Partizipative Einführung von Datenbrillen in der Pflege im Krankenhaus" war der Kurztitel des vom Bundesforschungsministerium (BMBF) und dem Europäischen Sozialfonds (ESF) im Rahmen des BMBF-Förderschwerpunkts "Arbeiten an und mit Menschen" im Zeitraum von 2020 bis 2023 geförderten Forschungsprojekts PARCURA.

"Partizipative Einführung von Datenbrillen in der Pflege im Krankenhaus" war der Kurztitel des vom Bundesforschungsministerium (BMBF) und dem Europäischen Sozialfonds (ESF) im Rahmen des BMBF-Förderschwerpunkts "Arbeiten an und mit Menschen" im Zeitraum von 2020 bis 2023 geförderten Forschungsprojekts PARCURA.

Drei Forschungs- und drei Umsetzungspartner waren an dem Projekt beteiligt. Zu den Umsetzungspartnern gehörten das St. Franziskus-Hospital, Münster, das Maria-Josef-Hospital Greven sowie die FACT IT GmbH, Bremen. Als 100%ige Tochter der St. Franziskus-Stiftung Münster bietet die FACT IT GmbH Rechenzentrums- und Gesundheitsleistungen im Gesundheitswesen an. Das Unternehmen verfügt am Standort Bremen über ein eigenes Rechenzentrum, über das u. a. das Hosting der Krankenhausinformationssysteme von 15 Krankenhäusern der Stiftung erfolgt, darunter die beiden projektbeteiligten Häuser.

Aufgabe der FACT IT im Projekt PARCURA war die Entwicklung eines IT-Schnittstellenkonzepts unter besonderer Berücksichtigung von IT-Sicherheit und Datenschutz sowie die Unterstützung bei der Entwicklung, Erprobung und Einbindung der Datenbrille in die bestehende IT-Infrastruktur.

In dem höchst komplexen Umfeld eines großen Krankenhauses sind diese Themen interdependent und unterliegen in den letzten Jahren immer enger definierten Rahmenbedingungen. Hieraus wird vor dem Hintergrund der Erfahrungen im Projekt PARCURA in diesem Beitrag näher eingegangen.

2 IT-Sicherheit im Krankenhaus

Nach der europaweiten Regelung des Datenschutzes durch die Datenschutz-Grundverordnung (DSGVO)[1] wird im Krankenhaus zusätzlich zu den Daten der Beschäftigten denen der Patienten im Patientendaten-Schutz-Gesetz (PDSG) vom 14.10.2020 eine besondere Schutzwürdigkeit zugeschrieben.[2]

Eine weitere Besonderheit im Krankenhaus liegt in der Vielzahl der notwendigen Schnittstellen, über die Patientendaten zwischen beteiligten Systemen und Akteuren ausgetauscht werden. Aus der Perspektive der IT-Sicherheit stellen alle diese Systemöffnungen auch ein Sicherheitsrisiko dar.

Jegliche Unternehmen stellen in Abhängigkeit ihres potenziellen Wertes und der Qualität ihrer IT-Sicherheit ein Angriffsziel für kommerziell motivierte Cyberkriminalität dar. Das Beispiel des Lukaskrankenhaus der Städtischen Kliniken in Neuss ist nur ein Beispiel dafür, welche Folge

ein erfolgreicher Erpressungsversuch haben kann: Trotz der Hilfe von Spezialisten wurde das Krankenhaus bis zu zwei Wochen lang nahezu lahmgelegt.[3]

Krankenhäuser in Deutschland sind aber nicht nur Wirtschaftsbetriebe, sondern auch ein wichtiger Bestandteil der öffentlichen Ordnung. Man stelle sich vor, wie ein Zusammentreffen eines Massenanfalls von Verletzten (MANV) z. B. durch Terroranschläge in Kombination mit Cyberangriffen wirken könnte. Diese Wirkungen könnten zusammen mit Angriffen auf andere wichtige Ziele verheerende Folgen nach sich ziehen.

Aus diesem Grund sind auch Einrichtungen des Gesundheitswesens unter bestimmten Bedingungen als "Kritische Infrastrukturen" deklariert:

> *"Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."* [4]

Gemäß "§ 6 Sektor Gesundheit" der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) sind alle Krankenhäuser mit mindestens 30.000 vollstationären Fällen pro Jahr Teil der Kritischen Infrastrukturen.[5]

Krankenhäuser müssen umfangreiche organisatorische Maßnahmen zur Sicherung der KRITIS-Anlagen vorsehen und diese zertifizieren. Dies kann z. B. im Rahmen einer ISO 27001- oder BSI IT-Grundschutz-Zertifizierung passieren. Diese Zertifizierungen müssen alle zwei Jahre wiederholt werden.

Inzwischen hat die Deutsche Krankenhausgesellschaft (DKG) dazu einen nach § 8a Abs. 1 BSIG geeigneten branchenspezifischen Sicherheitsstandard B3S erstellt, der inklusive Arbeitshilfen auf den Seiten des DKG abrufbar ist.[6]

Die geforderten Maßnahmen betreffen nicht nur Hardware, Software und Schnittstellen, sondern auch alle sicherheitsrelevanten Prozesse, z. B. den physischen Zugang zu Rechenzentren, die Sicherheitsüberprüfung von Mitarbeitern, dem Berechtigungsmanagement, Update- und Kontrollzyklen von Softwareprodukten und das Erkennen und Melden von Sicherheitsvorfällen an das BSI.

Seit 2022 müssen auch alle anderen deutschen Krankenhäuser laut § 75c des Sozialgesetzbuchs "angemessene organisatorische und technische Vorkehrungen" treffen, um die "Verfügbarkeit, Integrität und Vertraulichkeit" ihrer informationstechnischen Systeme zu gewährleisten.[7]

In keinem der relevanten Gesetze ist allerdings ein zusätzliches Entgelt für Krankenhäuser geregelt. Krankenhäuser müssen diese zusätzlichen Kosten vielmehr aus dem laufenden Geschäftsbetrieb erwirtschaften.

Auf das Projekt PARCURA hatten diese Entwicklungen konkrete Auswirkungen, denn die Bedrohungen sind nicht nur theoretischer Natur, sondern finden als Cyberangriffe regelmäßig statt, ob als E-Mail-Trojaner oder direkte Angriffe auf die Netzwerkknoten der St. Franziskus-Stiftung.

In der Umsetzung der Projekterfordernisse ergaben sich weitere konkrete Hindernisse, die teilweise erst relativ spät im Projektverlauf erkennbar wurden:

- **Personalmangel**
  Die Vorbereitung einer Zertifizierung, die Umstellung von Prozessen und die Umsetzung von erarbeiteten Maßnahmen ist sehr personal- und ressourcenintensiv. Dies erfordert hochqualifizierte Mitarbeiter, die in dieser Zeit nicht für andere Aufgaben zur Verfügung stehen.

- **Prozesse**
  Neue Geräte und Software müssen einer vergleichsweise zeitaufwendigen Sicherheitsprüfung unterzogen werden. Die beispielsweise für das Projekt PARCURA ausgewählte Datenbrille HoloLens 2 greift für ihre Berechtigungen auf die Microsoft-eigene Azure Cloud zurück. Unter den Gesichtspunkten der IT-Sicherheit ist eine solche Cloud-Lösung aber für die St. Franziskus-Stiftung nicht zulässig und kann nur über Umwege gelöst werden.

- **Software**
  Ähnliches gilt für neue Software, die auf dem zugelassenen Gerät verwendet werden soll. Für Software, die nicht bereits auf einer so genannten "White List" vermerkt ist, ist ein umfassender Prüfprozess vorgesehen, in dem üblicherweise die Software-Hersteller einen umfangreichen Fragenkatalog zu sicherheitsrelevanten Themen beantworten müssen, bevor vom letztendlich verantwortlichen Gremium eine Freigabe für die Software erteilt werden kann. Bei einem nichtkommerziellen Produkt wie einer Softwareentwicklung innerhalb des Forschungsprojekts PARCURA ist das problematisch, da jegliche Änderung an der Software zwingend ein Update des Prüfprozesses zur Folge hat.

- **Hardware**
  Auch Beschaffungsprozesse für Hardware unterliegen dem Sicherheitsgedanken. Dies bedeutet, dass nur für Geräte, die eine Freigabe unter ähnlichen Kriterien wie Softwareprodukte erhalten, überhaupt Angebote eingeholt werden dürfen. Bei ausgefalleneren Produkten führt das unter Umständen zu erheblichen zeitlichen Verzögerungen.

- **Priorisierung**
  Die IT eines Krankenhauses ist primär für den laufenden Betrieb eines Unternehmens zuständig, das 24/7 arbeitet. Die dazu erforderlichen Arbeiten wie beispielsweise die Einführung neuer Hard- und Software und damit verbundene Systemumstellungen haben aus diesem Grund Vorrang. Alle weiteren Tätigkeiten müssen sich dieser Priorität unterordnen. Das gilt insbesondere auch für ein Forschungsprojekt wie das Projekt PARCURA.

Für ein Forschungsprojekt wie PARCURA ergeben sich daraus einige Lehren:

- Die für die Bearbeitung von sicherheitsrelevanten Fragen verantwortlichen Mitarbeiterinnen und Mitarbeiter müssen frühzeitig mit ins Boot geholt und als Stakeholder im Projekt behandelt werden.
- Die Prozesse, die im Projektverlauf voraussichtlich berührt werden, sollten möglichst frühzeitig identifiziert werden, damit deren jeweilige Zeitdauer abgeschätzt werden kann. Hier kann z. B. die Critical-Path-Methode[8] verwendet werden.
- Die voraussichtlich in einem Projekt einzusetzende Hard- und Software sollte so früh wie möglich identifiziert werden, damit der Prüfprozess zur IT-Sicherheit möglichst frühzeitig gestartet werden kann.
- Sobald feststeht, dass Hardware- oder Softwarebeschaffungen anstehen, sollte auch der Einkauf als Stakeholder involviert werden.
- Änderungen im Projektverlauf sind alles andere als trivial und können unter den beschriebenen Umständen zu gravierenden Verzögerungen führen. Die Änderungen sind auch unter diesen Gesichtspunkten ob ihrer Notwendigkeit zu bewerten.
- Die Reservierung von notwendigen Ressourcen (z. B. im Rechenzentrum) ist frühzeitig und auf geeigneter Ebene vorzunehmen, vorzugsweise in einem Projektlenkungsausschuss mit Beteiligung der Entscheider.
- Wie "frühzeitig" etwas eingeplant werden kann, ist im Rahmen eines Forschungsprojekts variabel. Da es sich nicht um die Einführung eines fertigen Produkts handelt, sind sämtliche relevanten Parameter bei Projektstart kaum bekannt. Gleichzeitig ist das Projektmanagement eines Krankenhauses selten mit den zunehmend agilen Methoden technischer Entwicklung vertraut. Ein für die frühzeitige Erkennung von Hemmnissen geeignetes Projektmanagement sollte unbedingt von Anfang an etabliert werden, da es sonst passieren kann, dass die zeitliche Komponente aus den Ruder läuft.

Diese vielfältig erfahrenen Hemmnisse haben im Projekt PARCURA immer wieder zu Verzögerungen geführt.

Im Fazit bleibt zum Thema "IT-Sicherheit im Krankenhaus" festzuhalten: Fragestellungen zur IT-Sicherheit haben in Krankenhäusern der stationären Versorgung einen sehr hohen Stellenwert. Projekte, die nicht konkret den laufenden Betrieb des Krankenhauses betreffen sind immer "zusätzlich". Speziell die Projektteile, die IT-sicherheitsrelevant sind, müssen frühzeitig im Sinne eines kritischen Pfades erkannt und geplant werden, da sonst zeitliche Verzögerungen in einem erheblichem Umfang drohen.

3 Datenschutz im Krankenhaus

Neben den technischen Fragen zum Einsatz einer Datenbrille stellt sich vor dem Einsatz insbesondere auch im Krankenhaus die Frage nach der Behandlung der datenschutzrechtlichen Bedingungen.

Mit der Datenbrille sollen im Idealfall nicht nur vorhandene Patientendaten abgerufen werden können, sondern z. B. auch Video- oder Audiodaten vom jeweiligen Status der Patientin oder dem Patienten gespeichert werden, bei denen u. U. auch andere direkt oder indirekt beteiligte Personen erfasst werden, z. B. Angehörige oder auch Pflegepersonal.

Derartige Umstände müssen aus datenschutzrechtlicher Sicht vor dem Einsatz von Datenbrillen geprüft werden. Diese Prüfung kann allerdings erst vollständig erfolgen, wenn die Parameter für die Hard- und Software, die zum Einsatz kommen soll, vollständig bekannt sind – ein Henne-Ei-Problem, denn die Entwicklung kann angepasst werden, wenn die Regelungen für den Datenschutz bekannt sind. Es gilt also, möglichst bereits bei der Projektkonzeption die Rahmenbedingungen für den Datenschutz zu berücksichtigen.

Die Datenschutzregelungen sind 2016 durch die Datenschutz-Grundverordnung (DSGVO)[9] auf europäischer Ebene neu festgelegt und im Anschluss auch auf nationaler Ebene konkretisiert worden, im Jahr 2020 u. a. durch das Patientendaten-Schutz-Gesetz (PDSG)[10]. Letzteres hebt die besondere Schutzwürdigkeit von Patientendaten hervor mit der Folge, dass diese noch einmal anders behandelt werden müssen als bspw. die Kundendaten eines Unternehmens in anderen Branchen.

Während diese Regelungen bestimmen, was erfüllt werden muss, wird nicht erläutert, wie diese Bestimmungen hinreichend erfüllt werden müssen.

Das stellt Datenschützer, speziell, wenn es sich nicht um ausführlich beschriebene Prozesse in einem Unternehmen handelt, grundsätzlich vor ein Problem:

> *Wie finde ich einen rechtssicheren Mittelweg zwischen der gewünschten Nutzung von Daten und der möglicherweise strafbewehrten Verletzung der datenschutzrechtlichen Bestimmungen?*

Im Zweifel wird der Datenschützer den Datenschutz höher bewerten als die "freie" Nutzung der betroffenen Daten.

Für Projektverantwortliche in einem Forschungsprojekt wie PARCURA kann dies problematisch werden, sofern die betroffene Einrichtung und der darin zuständige Datenschutzbeauftragte auf diese Art von Projekten nicht eingestellt ist. Entsprechende datenschutzrechtliche Prüfungen können sehr zeitaufwendig sein und damit den zeitlichen Ablauf des Projekts gefährden.

Im Projekt PARCURA wurde folgerichtig in Zusammenarbeit mit dem Datenschutzbeauftragten ein Projektdokument zu den Rahmenbedingungen für den Datenschutz erstellt. Im

weiteren Verlauf des Projekts wurden dann die bisher verwendeten Verfahren, speziell zur Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO[11] auf die beabsichtigten Teilprojekte angewendet, die ihrerseits in der technischen Machbarkeitsüberprüfung nicht aussortiert werden mussten.

Wie kann man als Projektverantwortlicher diese Problematik beherrschen?

Der erste Schritt besteht darin, sich frühestmöglich mit den relevanten Grundlagen der Datenschutzbestimmungen vertraut zu machen. Zusätzlich zu der bereits erwähnten Datenschutz-Grundverordnung (DSGVO) und dem Patientendaten-Schutz-Gesetz (PDSG) ist auch das Bundesdatenschutzgesetz (BDSG)[12] zu berücksichtigen. Im konkreten Fall von PARCURA, in dem sich die projektbeteiligten beiden Krankenhäuser in Trägerschaft der St. Franziskus-Stiftung Münster befinden – einer kirchlichen Stiftung privaten Rechts[13] – sind außerdem das Gesetz zum Kirchlichen Datenschutz (KDG) und die dazu gehörige Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) zu beachten.[14]

Maßgebliche Beschreibung der Verarbeitungstätigkeit	Ja/Nein
Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen z.B. Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke	Ja
Verarbeitung von genetischen Daten z.B. Früherkennung von Erbkrankheiten Genetische Datenbanken zur Abstammungsforschung	Nein
Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen z.B. Träger von großen sozialen Einrichtungen	
Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	
Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten	Nein
Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen z.B. Analyse / Vorhersage von Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort, Ortswechsel	
Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden z.B. Analyse / Vorhersage von Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort, Ortswechsel	
Verarbeitung von besonderen Kategorien personenbezogener Daten durch Auftragsverarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DSGVO zu exportieren oder offenzulegen z.B. Abwicklung einer Tele-Sprechstunde mit Daten- oder Dokumentenübertragung, Datenverarbeitung in einer öffentlichen Cloud	Nein
Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen	Nein
Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Nein
systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung)	Nein
Verarbeitung von Daten der Personenstands- und Melderegister sowie anderer Stellen, die Daten aus diesen Registern in großem Umfang oder Meldedaten mit Sperrvermerken gemäß § 51 Abs. 1 und 5 Bundesmeldegesetz verarbeiten	Nein
Umfangreiche Verarbeitung von Daten über Kinder z.B,. Schulsozialarbeit, Kinderheime	Nein
Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person)	Nein

Abbildung 1: Beispiel für eine Checkliste zum Erfassung der datenschutzrechtlichen Daten- und Verarbeitungsarten (Auszug)

Im zweiten Schritt muss der Projektverantwortliche für alle im Projekt vorgesehenen Tätigkeiten die verwendeten Daten- und Verarbeitungsarten ermitteln. Mit einer entsprechenden Checkliste als vergleichsweise einfachem Mittel kann geprüft werden, ob überhaupt eine weiterführende Verpflichtung zur Wahrung des Datenschutzes besteht.

Im Beispiel der Abbildung 1 ist die Frage nach der Verarbeitungstätigkeit so formuliert, dass nur ein "Ja" zu einer weitergehenden Behandlung führt. Würden alle Fragen mit einem "Nein" beantwortet, würde die Verpflichtung zu einer Datenschutzfolgeabschätzung entfallen.

Wird eine datenschutzrechtlich relevante Verarbeitung erkannt, müssen alle diesbezüglichen Risiken ausreichend ausführlich beschrieben und bewertet werden. Hierbei bieten sich Methoden des Risikomanagements an, z. B. eine Risikomatrix, die die Eintrittswahrscheinlichkeit zu der möglichen Schadenshöhe in Relation setzt.[15]

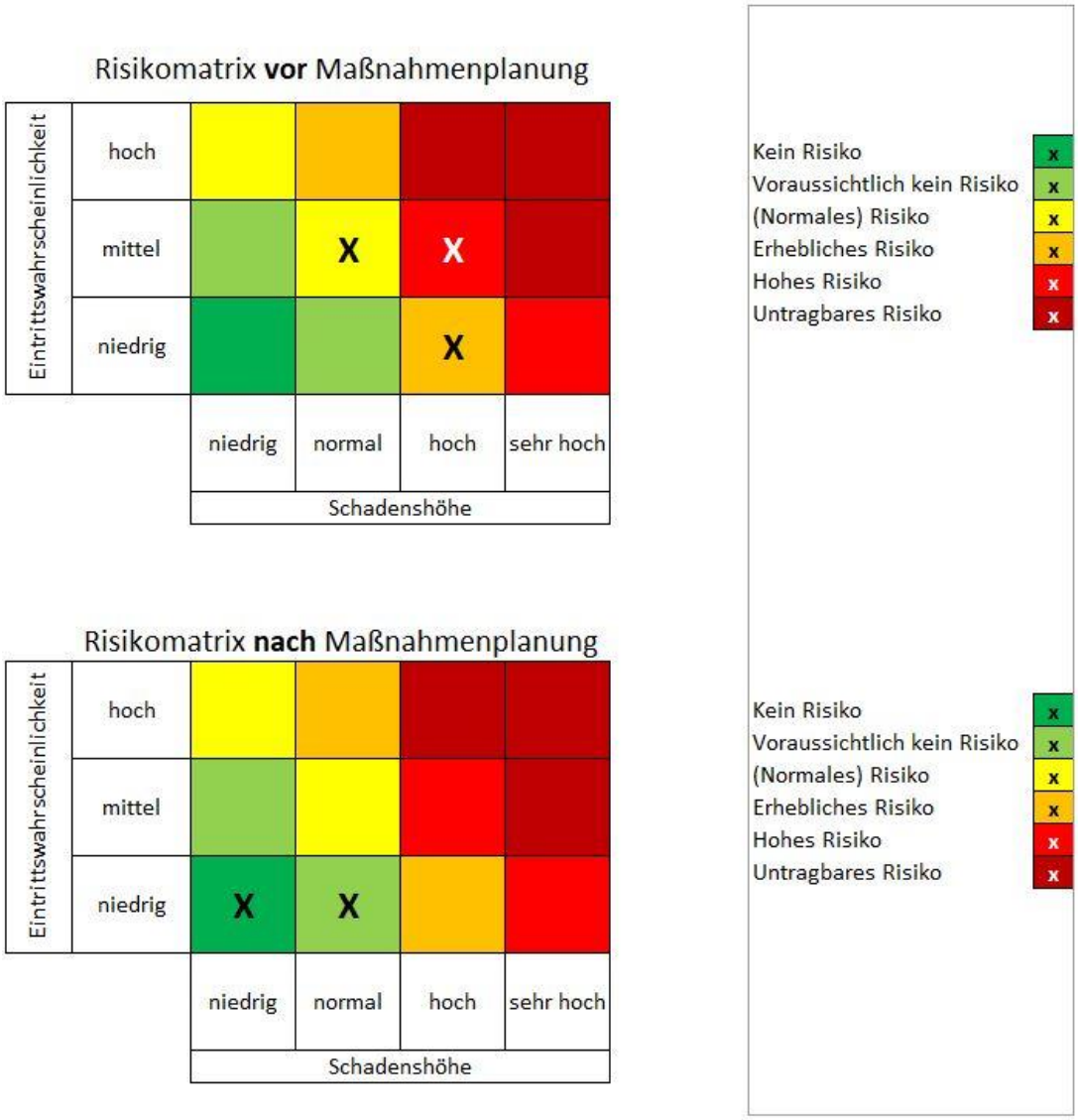

Abbildung 2: Risikomatrix vor und nach der Maßnahmenplanung

Befindet sich ein Risiko nicht in der grünen Zone, muss diese Tätigkeit entweder unterlassen (Risikovermeidung) oder mit geeigneten Maßnahmen abgesichert werden (Risikominderung). Gelingt es mit diesen Maßnahmen nicht, alle Tätigkeiten in die grüne Zone zu verschieben, bleibt üblicherweise (Datenschutzrisiken können meist nicht versichert werden, also scheidet die vierte Möglichkeit des Transfers aus) nur die Möglichkeit übrig, Risiken zu akzeptieren. Diese Variante erfordert mit hoher Wahrscheinlichkeit die explizite Einverständniserklärung eines Vertretungsberechtigten. Diese kann möglicherweise fallabhängig über die Eskalation mit Hilfe des Projektlenkungsausschusses erwirkt werden.

Verarbeitungstätigkeit:						Riskoanalyse VOR Maßnahmenfestlegung				koanalyse NACH Maßnahmenfestleg			Ergebnis
lfd. Nr.	Risiko-Ursprung / Arbeitsschritt	Risiken	sonstige Risiken	Risikobeschreibung	Risiko-Verantwort-licher	Schadens-höhe	Eintritts-wahrschein-lichkeit	Risiko-bewertung	Maß-nahmen	Schadens-höhe	Eintritts-wahrschein-lichkeit	Risiko-bewertung	
						- Niedrig - Normal - Hoch - Sehr hoch	- Niedrig - Mittel - Hoch	- Kein Risiko - Voraussichtlich kein Risiko - (Normales) Risiko		- Niedrig - Normal - Hoch - Sehr hoch	- Niedrig - Mittel - Hoch	- Kein Risiko - Voraussichtlich kein Risiko - (Normales) Risiko - Erhebliches Risiko	- Restrisiko akzeptabel - Weitere Maßnahmen erforderlich - Verfahren kann durchgeführt werden
	Freitext		Freitext		Freitext	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Kennzeichnung folgt automatisch	Freitext	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Kennzeichnung folgt automatisch	Bitte Auswahl anklicken
7.	Allgemein	Sonstiges:	Spracherkennung	Dokumentation der Wundversorgung per Spracheingabe; Fehlerhafte Aufzeichnung der gesprochenen Textes		Hoch	Mittel		Kontrolle durch den Mitarbeiter, Korrektur der Eingaben	Normal	Niedrig		Verfahren kann durchgeführt werden
8.	Allgemein	Sonstiges:	Spracherkennung	Nutzung einer Dolmetscherfunktion (Internet- oder Cloudbasiert) mit und ohne Patientenkontext		Hoch	Hoch		Umsetzbarkeit noch nicht geprüft sorgfältige Auswahl des Anbieters der Dolmetscherfunktion, Betrieb und Hosting ausschließlich innerhalb des EWR				noch nicht beurteilbar

Abbildung 3: Ausschnitt aus der Datenschutzfolgeabschätzung für das Projekt PARCURA

In Abbildung 3 sind beispielhaft zwei ermittelte Tätigkeiten aus der im Projekt PARCURA durchgeführten Datenschutzfolgeabschätzung aus der Rubrik Spracherkennung erfasst. Aus der jeweiligen Einschätzung der Schadenshöhe und der Eintrittswahrscheinlichkeit ergeben sich ein erhebliches (orange) bzw. ein hohes Risiko (rot).

Die Aufgabe der Projektverantwortlichen bestand jetzt darin, geeignete Maßnahmen zu bestimmen, die dieses Risiko ansprechen.

Im ersten Fall (Zeile 7) wurde dies durch ein Maßnahmenbündel erreicht, das sich auf die Registrierung, Benutzeridentifizierung und Regeln für die Aufbewahrung der Datenbrillen bezieht. Bei Befolgung dieser Maßnahmen wird das Risiko anschließend als nur noch "voraussichtlich kein Risiko" eingestuft.

Im zweiten Fall (Zeile 8) ist die Lage komplizierter: Die Inanspruchnahme eines Dolmetscherdienstes über die Brille wird als potenziell risikoreich erkannt, aber es können noch keine geeigneten Maßnahmen getroffen werden, da noch keine Auswahl eines solchen Dienstes getroffen wurde. Die Risikobeurteilung bleibt folglich offen, bis ein solcher Dienst in Anspruch genommen werden soll. Bei der Auswahl eines Dienstes müssen dann auch die Kriterien für den Datenschutz in die Ausschreibung aufgenommen werden.

Alle ermittelten Risko-Schadens-Kombinationen werden in der Risikomatrix automatisch angezeigt – siehe Abbildung 2. Erst wenn nach der Maßnahmenplanung keine erheblichen oder höhere Risiken mehr erkannt werden, kann das Projekt fortgeführt werden.

Die Kunst liegt hierbei darin, die Risiken sowie die Maßnahmen zu erkennen und richtig einzuschätzen. Dies erfordert häufig zum einen die Einschätzung der Stakeholder wie auch eine Kommunikation mit Spezialisten, die dadurch häufig ebenfalls zu Stakeholdern werden.

Mögliche Konflikte bestehen hier in der Einschätzung der Wirksamkeit der gewählten Maßnahmen. Ein Sicherheitsbeauftragter wird eher zu einer geringeren Wirksamkeit der Maßnahme tendieren als der Projektverantwortliche, dessen Ziel es sein muss, das Projekt weiter fortführen zu können.

Wie bei allen möglichen Konflikten im Projektmanagement ist auch hier sinnvoll, möglichst früh, kollegial und zielorientiert mit den relevanten Stakeholdern zu kommunizieren.

Im Fazit bleibt zum Thema "Datenschutz im Krankenhaus" festzuhalten: Der Datenschutz, insbesondere in Bezug auf Patientendaten, genießt im Gesundheitswesen einen sehr hohen Stellenwert. Die zuständigen Datenschutzbeauftragten müssen so früh wie möglich als Stakeholder in das Projekt einbezogen werden. Wenn in einem zeitlich und inhaltlich angemessenen Prozess die Anforderungen an den Datenschutz nicht durch Mittel wie eine Datenschutz-Folgen-Abschätzung erfüllt werden können, bleibt nur das Mittel der Eskalation an den Projektlenkungsausschuss oder ein Verzicht auf den entsprechenden Projektteil. Im äußersten Fall kann ein Projekt am Datenschutz scheitern.

4 Schnittstellen

Zum Thema "Schnittstellen" gehört im Fall des Projekts PARCURA aus rein technischer Sicht des IT-Dienstleisters die Aufgabe, die bidirektionale Übermittlung von Daten von einer Datenbrille aus an andere IT-Systeme im Krankenhaus zu prüfen und ggf. zu ermöglichen. Für die technische Machbarkeit ist dabei zunächst zu ermitteln, welche Daten wie übermittelt werden sollen und ob die beteiligten Systeme diese Daten senden bzw. empfangen können.

Aus der Erfahrung mit früheren Projekten stellt das Herzstück der Krankenhaus-IT dabei das Krankenhausinformationssystem (KIS) die größte Hürde dar. Im konkreten Fall handelt es sich um das Krankenhausinformationssystem ORBIS der Fa. Dedalus[16], das in beiden am Projekt PARCURA beteiligten Krankenhäusern im Einsatz ist.

Die primäre Aufgabe der IT im Krankenhaus ist die Unterstützung klinischer Prozesse. Im Krankenhausinformationssystem werden alle diese Prozesse betreffenden Patientendaten verarbeitet, wie auch die für das wirtschaftliche Überleben des Krankenhauses notwendigen Abrechnungsdaten generiert.

Für den notwendigen Austausch von Daten zwischen diesem System und den beteiligten Subsystemen, z. B. einem Radiologie-Informationssystem (RIS), gibt es Absprachen, die eine Interoperabilität zwischen den Systemen sicherstellen sollen. Diese bestehen grundsätzlich aus drei Pfeilern:

1. **Terminologien**, die sicherstellen sollen, dass die Kommunikationsstellen A und B auch das Gleiche meinen. Die derzeit "beste", aber kostenpflichtige Sammlung ist z. B. SnomedCT[17].

2. **Profile**, die für unterschiedliche fachliche Anwendungsgebiete (Domänen) festlegen, welche Informationen dort ausgetauscht werden müssen. Diese Profile werden von der

internationalen Organisation "Integrating the Healthcare Enterprise" (IHE) verwaltet und gepflegt.[18]

3. **Nachrichtenformate**, die für unterschiedliche Zwecke festlegen, wie spezielle Textnachrichten aufgebaut werden müssen, damit Systeme sie syntaktisch und semantisch korrekt senden und empfangen können. Für diese Nachrichtenformate werden derzeit folgende Versionen gepflegt: das weit verbreitete HL7 v2 sowie HL7 v3, das seinerseits aber weitgehend von dem auf Webtechnologie und Standardformaten (z. B. XML, JSON) basierenden FHIR verdrängt wird. Für alle diese Versionen ist die Organisation "Health Level Seven International" verantwortlich.[19]

Das Krankenhausinformationssystem ORBIS verwendet eine Teilmenge der HL7-Nachrichten, um z. B. Anforderungen an Subsysteme (wie das RIS) zu senden und wertet die zurückkommenden HL7-Nachrichten auf deren Inhalte aus und fügt sie in die Patientenakte ein.

Diese Schnittstellen sind eng definiert, zum einen um den Bestimmungen für den Datenschutz und der Datenintegrität zu genügen, zum anderen aus wirtschaftlichen Interessen des KIS-Herstellers.

Für das Projekt PARCURA hat die FACT IT ermittelt, ob für die angedachten Anwendungsszenarien der Datenbrille der direkte Austausch von Daten mit dem KIS möglich ist. Wie die ausführliche Analyse der Schnittstellen ergeben hat, ist es derzeit nicht ohne Weiteres möglich, Patientendaten aus dem KIS ORBIS abzurufen, da ein Datenexport stets aus ORBIS als patientenführendem System heraus angestoßen werden muss.[20]

Eine direkte Nutzung einer Citrix-Terminalsitzung auf der im Projekt PARCURA verwendeten Microsoft HoloLens 2 wird durch Hardware-Inkompatibilitäten verhindert. Die Nutzung über den Microsoft Edge-Browser scheitert an der im Interface kaum benutzbaren Bedienelemente innerhalb der ORBIS-Anwendung. Die Verwendung der Spracherkennung wird ORBIS-seitig ebenfalls nicht unterstützt.

Hinzu kommt, dass die im Hintergrund verwendete ORACLE-Datenbank aus lizenzrechtlichen Gründen nicht direkt abgefragt werden kann. Ein solcher Zugriff über eine ggf. eigens entwickelte Anwendung scheidet demnach ebenfalls aus.

Für einzelne Anwendungsfälle ist es möglich, einen Datenexport regelbasiert (z. B. in voreingestellten zeitlichen Abständen) über einen Kommunikationsserver bereitzustellen. In einem solchen Fall sind allerdings die anfallenden Datenmengen und vor allem der Datenschutz (unter dem Stichwort der Datensparsamkeit) sorgfältig in die Planung einzubeziehen.

Die Fortführung des Projekts PARCURA wurde von diesen Ergebnissen maßgeblich eingeschränkt. Ein Einsatz der Datenbrillen im Realbetrieb, wie in der Projektkonzeption ursprünglich vorgesehen, ist im Rahmen der Projektlaufzeit ohne die direkte Beteiligung des KIS-Herstellers nicht umsetzbar.

Im Fazit bleibt zum Thema "Schnittstellen" festzuhalten: Der Zugriff auf Daten im Krankenhausinformationssystem ORBIS ist alles andere als trivial. Für die Planung einer Anwendung, die auf Patientendaten im System zugreifen soll, ist es essenziell wichtig, zunächst die limitierenden Möglichkeiten genau zu kennen und anschließend den Umfang der benötigten Daten möglichst exakt festzulegen. Für die Chance der Einbeziehung des KIS-Herstellers im Rahmen eines zeitlich auf drei Jahre begrenzten Förderprojektes ist ein eher längerfristiger Planungshorizont erforderlich.

Quellen und Anmerkungen

[1] Zur DSGVO siehe z. B. die vom Bundesministerium für Wirtschaft und Klimaschutz herausgegebene Serviceseite "Europäische Datenschutz-Grundverordnung", auf der auch ein externer Link zur DSGVO zu finden ist. Online unter https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html.

[2] Zum Patientendaten-Schutz-Gesetz (PDSG) siehe die vom Bundministerium für Gesundheit herausgegebene Serviceseite "Patientendaten-Schutzgesetz (PDSG)" unter https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/patientendaten-schutzgesetz-pdsg.html.

[3] Siehe dazu z.B. den Bericht "Computervirus legt Klinik in Neuss lahm" der Süddeutschen Zeitung vom 12.02.2016 unter https://www.sueddeutsche.de/digital/hackerangriff-computervirus-legt-klinik-in-neuss-lahm-1.2861656.

[4] Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.J.): Was sind Kritische Infrastrukturen? – Online unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html. – Siehe auch § 2 Absatz 10 BSIG unter https://www.gesetze-im-internet.de/bsig_2009/__2.html.

[5] Vgl. https://www.gesetze-im-internet.de/bsi-kritisv/__6.html.

[6] Vgl. https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/.

[7] Vgl. https://www.krankenhaus-it.de/item.1423/2022_neue_regeln_f%C3%BCr_it-sicherheit_im_krankenhaus.html.

[8] Siehe dazu z.B. die von der DATACOM Buchverlag GmbH herausgegebene Serviceseite "Kritische-Pfad-Methode" unter https://www.itwissen.info/Kritische-Pfad-Methode-critical-path-method-PM-CPM.html.

[9] Siehe Endnote 1.

[10] Siehe Endnote 2.

[11] Zu Art. 35 Datenschutz-Folgenabschätzung der DS-GVO vgl. z. B. https://dejure.org/gesetze/DSGVO/35.html. Die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e. V. stellt auf einer von ihr herausgegebenen Serviceseite eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO am Beispiel eines Krankenhaus-Informationssystems inklusive Vorlagen und Erläuterungen auf folgender, von der herausgegebenen Serviceseite bereitgestellt: https://gesundheitsdatenschutz.org/html/dsfa-beispiel.php.

[12] Siehe dazu den Übersichtsbeitrag "Bundesdatenschutzgesetz" in der Wikipedia unter https://de.wikipedia.org/wiki/Bundesdatenschutzgesetz sowie den Text des Gesetzes unter https://www.gesetze-im-internet.de/bdsg_2018/index.html.

[13] Vgl. dazu https://www.sfh-muenster.de/wir-ueber-uns/die-franziskus-stiftung/.

[14] Vgl. dazu die vom Bistum Münster herausgegebene Serviceseite "Rechtliche Grundlagen rund um den kirchlichen Datenschutz" unter https://www.bistum-muenster.de/datenschutz_grundlagen.

[15] Zum Thema "Risikomanagement allgemein" siehe z. B. den entsprechenden Wikipedia-Beitrag unter https://de.wikipedia.org/wiki/Risikomanagement. Zur ISO-Norm 31000 siehe den entsprechenden Wikipedia-Beitrag unter https://de.wikipedia.org/wiki/ISO_31000.

[16] Vgl. https://www.dedalus.com/dach/de/our-offer/products/orbis/.

[17] Siehe dazu den Wikipedia-Beitrag "Systematisierte Nomenklatur der Medizin" unter https://de.wikipedia.org/wiki/Systematisierte_Nomenklatur_der_Medizin sowie die offizielle Website unter https://www.snomed.org/.

[18] Siehe dazu den Wikipedia-Beitrag "Integrating the Healthcare Enterprise" unter https://de.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise.

[19] Siehe dazu den Übersichtsbeitrag "HL7" in der Wikipedia unter https://de.wikipedia.org/wiki/HL7.

[20] Vgl. Banik, Dirk (2023): Beschreibung und Analyse der aktuellen KIS-Schnittstellen. Online: https://parcura.de/pdf/PARCURA_FACT_Banik_KIS-Schnittstellen.pdf.

Der Autor

Arne Reuter ist Mitarbeiter der FACT IT GmbH, einer 100%igen Tochter der St. Franziskus-Stiftung. Das Unternehmen verfügt am Standort Bremen über ein eigenes Rechenzentrum, über das u. a. das Hosting der Krankenhausinformationssysteme von 15 Krankenhäusern der Stiftung erfolgt. Aufgabe im Projekt PARCURA war die Entwicklung eines IT-Schnittstellenkonzepts unter besonderer Berücksichtigung von IT-Sicherheit und Datenschutz sowie die Unterstützung bei der Entwicklung und Erprobung sowie der Einbindung der Datenbrille in die bestehende IT-Infrastruktur.

Schlussredaktion
Jürgen Reckfort, TAT Technik Arbeit Transfer gGmbH

Empfohlene Zitierweise des Beitrags
Reuter, Arne (2023): Der Prozess der partizipativen Auswahl einer geeigneten Datenbrille aus Sicht der Pflege. Online: https://parcura.de/pdf/PARCURA_FACT_Reuter_Erfahrungsbericht.pdf.