



Anforderungen an eine iPaaS Cloud Lösung zum sicheren Betrieb von Gesundheitsdaten in Schweizer Spitälern

Christian Russ · Philipp Stalder · Joachim Steinwendner ·
Tibor Pimentel · James Kavakopoulos

Eingegangen: 29. April 2023 / Angenommen: 6. August 2023 / Online publiziert: 13. September 2023
© The Author(s) 2023

Zusammenfassung Wie viele Cloud Computing Angebote, erfreuen sich „Integration Plattform as a Service“ (iPaaS) immer grösserer Beliebtheit. In verschiedenen Branchen bereits etabliert, stellen sie in der Schweizer Gesundheitsbranche und speziell in den Spitälern noch eine Minderheit dar. Dies, obwohl das Datenmanagement und die Datenintegration der administrativen und medizinischen Daten essenziell sind, um die Digitalisierung in Spitälern erfolgreich voranzutreiben. Es zeigt sich jedoch schnell, dass die Anforderungen und Voraussetzungen für den Einsatz von iPaaS im sensiblen Gesundheitsdatenbereich sehr umfassend sind und potenzielle Hürden beinhalten. Im Zuge des Innosuisse Flagship Multi-Forschungsprojekts SHIFT wurde diese Fragestellung aufgegriffen und nun die erste Phase mit den Anforderungen an eine iPaaS Lösung erarbeitet. In der vorliegenden Arbeit werden auf Basis der Situation der Schweizer Spitäler auf die einzelnen allgemeinen, rechtlichen, organisatorischen, technischen und speziellen Anforderungen eingegangen, welche abschliessend grafisch zusammenfasst werden. Dies kann als initiale Hilfestellung für konkrete Handlungsfelder in der Praxis und neue wissenschaftliche Fragestellungen bzgl. der Nutzung von iPaaS in der Schweizer Gesundheitsbranche dienen. Es wird ersichtlich, dass es sowohl einen systemischen als auch interdisziplinären Ansatz benötigt, um den sicheren Betrieb von Gesundheitsdaten in der Public Cloud in Schweizer Spitälern zu ermöglichen.

✉ Christian Russ · Philipp Stalder · Tibor Pimentel
Institut für Wirtschaftsinformatik, Züricher Hochschule für Angewandte Wissenschaften, Zürich,
Schweiz
E-Mail: christian.russ@zhaw.ch

Joachim Steinwendner
Laboratory of Web Science, Fernfachhochschule Schweiz, Brig, Schweiz

James Kavakopoulos
Big Data & Security, Eviden AG, München, Deutschland

Schlüsselwörter Cloud Computing · iPaaS · Datenintegration · Gesundheitsdaten · Compliance · Krankenhaus

Requirements for an iPaaS cloud solution for the secure operation of health data in Swiss hospitals

Abstract Like many cloud computing offerings, “Integration Platform as a Service” (iPaaS) are becoming increasingly popular. Already established in various industries, they still represent a minority in the Swiss healthcare industry, especially in hospitals. This is despite the fact that data management and data integration of administrative and medical data are essential to successfully drive digitization in hospitals. However, it quickly becomes apparent that the requirements and prerequisites for the use of iPaaS in the sensitive healthcare data area are very comprehensive and include potential challenges. In the course of the Innosuisse Flagship Multi-Research Project SHIFT, this issue has been addressed and now the first phase with the requirements for an iPaaS solution has been developed. In this paper, based on the situation of Swiss hospitals, the individual general, legal, organizational, technical and special requirements are addressed, which are summarized graphically at the end. This can serve as initial support for concrete fields of action in practice and new scientific questions regarding the use of iPaaS in the Swiss healthcare industry. It becomes apparent that both a systemic and interdisciplinary approach is needed to enable the secure operation of healthcare data in the public cloud in Swiss hospitals.

Keywords Cloud Computing · iPaaS · Data integration · Health data · Compliance · Hospital

1 Einleitung und Ausgangslage

Das aktuelle Gesundheitswesen unterliegt dem permanenten Druck, verbesserte Behandlungsformen und Leistungsangebote für die Patienten zu bieten und gleichzeitig möglichst wirtschaftlich und effizient zu arbeiten. Da die Behandlungs- und Therapiemöglichkeiten immer umfassender und tiefgreifender werden, stehen die meisten Gesundheitssysteme jedoch vor einem kontinuierlichen Kostenwachstum. Darüber hinaus werden immer mehr Datensilos produziert, welche aus den vielen, teils isolierten oder technisch unzureichend integrierten IT-Systemen entstehen. Schweizer Spitäler sind einer der grössten wirtschaftlichen Leistungserbringer und Datenproduzenten im Gesundheitswesen. Unzureichendes Datenmanagement und -integration erzeugt unnötige Datenredundanzen und erhöhten Verwaltungsaufwand. Zudem verhindert es eine einfache End-to-End-Entwicklung von digitalen Anwendungen, welche z.B. das Patientenerlebnis verbessern oder die Arbeit des Spitalpersonals erleichtert.

In anderen Branchen wie Finanzwesen, Handel und Logistik haben sich bereits seit längerem Daten- und Systemintegrationsplattformen etabliert, welche mittlerweile auch in der Cloud als sogenannte „Integration Plattform as a Service“ (iPaaS)

angeboten werden. Optimistische Schätzungen gehen davon aus, dass der iPaaS Markt bis 2026 auf bis zu 13,9 Mrd. USD ansteigen wird (Markets und Markets 2023).

Neben dem generellen „Cloud Trend“ sind die Gründe für den Einsatz von iPaaS vielfältig. Obwohl extern gehostete Datenplattformen auch unterschiedlichste Risiken beinhalten, kommen folgende Vorteile zum Tragen (Ebert et al. 2017; Gartner 2023; Markets und Markets 2023):

- Schnellere Inbetriebnahme, da die iPaaS Lösung bereits besteht und ad-hoc konsumiert werden kann
- Einfachere und sichere Datenintegration durch bereits bestehende Daten-Konnektoren
- Einfache, teilweise „code-less“ Integration mit anderen Cloud Provider APIs
- Schnellere Entwicklung von digitalen Anwendungen, da auf die Business Logik fokussiert werden kann
- Zumeist sicherer IT-Betrieb und Wartung, sowie kontinuierlicher Ausbau neuer Funktionen
- Nutzung von Economy of Scale und geringere Investitionskosten

In der Gesundheitsbranche sind solche iPaaS Plattformen, und speziell in Schweizer Spitälern, noch nicht so häufig anzutreffen. Daher stellt sich mit der weiter voranschreitenden „Cloudifizierung“ der IT die Frage, welche Anforderungen und Voraussetzungen für den sicheren iPaaS Einsatz in der Spitalwelt notwendig sind. Im Weiteren wird diese Frage für den Schweizer Markt erörtert, und die verschiedenen Herausforderungs- und Anforderungsperspektiven werden adressiert.

Das 3,5 Jahre laufende Innosuisse Projekt „Smart Hospital: Integrated Framework, Tools and Solutions“ (SHIFT¹) hat das Ziel, die digitale Transformation in Spitälern voranzutreiben. Das Optimierungspotential durch Digitalisierungsmöglichkeiten soll daher ausgeschöpft und ineffiziente analoge Prozesse durch intelligente digitale Lösungen ersetzt werden (SHIFT n.d.).

Für eine einheitliche Integration der erarbeiteten Lösungen bzw. Anwendungen und einen nahtlosen Datenfluss erarbeitet ein übergeordnetes Teilprojekt eine gehostete Daten- und Integrationsmiddleware (iPaaS), die sogenannte Tech-Foundation. Mit einer Hybriden Cloud-Architektur iPaaS, welche die Vorteile von „private“ und „public“ Cloud-Modellen kombiniert, folgt die Tech-Foundation einem strategischen IT-Ansatz.

Schlussendlich hat die Tech-Foundation das Ziel, Schweizer Spitälern bei der Bewältigung der Herausforderungen der Datenintegration und des Datenmanagements zu unterstützen und dafür eine skalierbare und kostengünstige Lösung für Krankenhäuser unter Berücksichtigung strenger medizinrechtlicher und technischer Vorschriften anzubieten.

In der ersten Phase wurde eine Anforderungsanalyse für eine solche iPaaS Lösung durchgeführt. Dabei wurden wissenschaftliche und Fachquellen gesammelt, Experteninterviews geführt, Informationen mit dem SHIFT Sounding Board ausgetauscht, als auch Gesetzestexte und Vorschriften durchforstet. In den folgenden Kapiteln

¹ Mehr Details zu den Innosuisse Flagship Projekt SHIFT: <https://future.hospital/>.

wird aufgezeigt, welche Anforderungen notwendig sind, um die Realisierung einer erfolgreichen iPaaS Lösung voranzutreiben.

1.1 Stand der Digitalen Transformation im Schweizer Gesundheitswesen

Der Digitalisierungsgrad der verschiedenen Schweizer Industrien ist sehr unterschiedlich. Die Gesundheitsbranche ist mit nur 44 % Digitalisierungsgrad in 2019 eher ein Schlusslicht (Angerer et al. 2021). Während der Covid19-Pandemie wurde durchaus ein Digitalisierungsschub im Gesundheitswesen wahrgenommen. Diese Welle ist jedoch unterschiedlich nachhaltig und variiert pro Schweizer Kanton und Leistungserbringer. Die finalen Aussagen zur Nachhaltigkeit der Veränderung müssen noch genauer untersucht werden.

Generell wird das Optimierungspotenzial im Schweizer Gesundheitssystem auf bis zu 8,2 Mrd. CHF in 2019 geschätzt (Hämmerli et al. 2021). So könnten durch die erweiterte Einführung von digitalen Anwendungen und Tools, in Kombination mit klassischen Versorgungsmodellen, die Ausgaben für chronische Krankheiten gesenkt und gleichzeitig die Sicherheit und Zufriedenheit von Patienten und Leistungserbringern verbessert werden.

1.2 Ein grosser Leistungserbringer, die Spitäler

Im Jahr 2021 wurden in der Schweiz 1,44 Mio. stationäre Fälle und mehr als 23 Mio. ambulante Konsultationen in den Spitälern durchgeführt (Hauser et al. 2023). Diese Patientenkontakte, ärztliche Zuweisungen und Interaktionspunkte werden noch immer hauptsächlich analog oder bestenfalls per E-Mail organisiert und kommuniziert (Wicht und Exner 2020).

Aktuell scheint sich die Digitalisierung in Schweizer Spitälern somit noch auf die zwei Themen Krankenhausinformationssystem (KIS) und E-Patientendossier (EPD) zu fokussieren. In der Studie von Synpulse (Wicht und Exner 2020) gaben 72 % der Spitäler an, dass die klinische Dokumentation bereits digital erfolgt oder sich bei zusätzlichen 12 % der Spitäler in Planung befindet, jedoch nur knapp ein Drittel verwendete mobile Endgeräte. Interessant dabei ist, dass die Befragten aus der Unternehmensentwicklung ihr Spital deutlich innovativer bzgl. digitaler Umsetzung einschätzten als Angestellte aus anderen Spitalsbereichen. Ähnlich fraktioniert ist die Sichtweise auf die Hemmnisse bzgl. spitalinterner Digitalisierungsvorhaben: Befragte aus der IT/Medizintechnik favorisierten ein fehlendes digitales Mindset (60 %) und personellen Ressourcenmangel (83 %), während Angestellte aus anderen Bereichen diese zwei Faktoren lediglich zu 45 % respektive 57 % als wichtige Hinderungsgründe einschätzten (Wicht und Exner 2020).

Der Nutzen der Digitalisierung für die Patienten zeigt sich an den Interaktionspunkten entlang der Patientenpfade, welcher von D'Onofrio auch als Nutzungspotenzial der Intersektoralen Vernetzung beschrieben wurde (D'Onofrio 2022). Gemäss der Studie von Synpulse sind dazu für den Spitalertritt bei gerade mal 4 % der Schweizer Spitäler Lösungen für die Anamnese oder Self-Services (Datenerfassung, Terminverwaltung) vorhanden, ganze 40 % sehen diesbezüglich keinen Handlungsbedarf. Für die Zeit nach dem Spitalaufenthalt scheint sich die Digitalisierung im

Wesentlichen darauf zu beschränken, verfasste Dokumente (Behandlungsberichte, Laborwerte) verfügbar zu machen (52 % der Spitäler). Jedoch werden in dieser Phase zunehmend Tools für die Terminverwaltung und die medizinische Ergebnismessung eingesetzt, bei 20 % der Spitäler wurden diese bereits eingesetzt, bei weiteren rund 20 % waren sie in der Umsetzung. Die Vernetzung mit weiteren Sektoren des Gesundheitswesens oder paramedizinischen Dienstleistern scheint jedoch noch kein Thema zu sein (25 %), die digitale Unterstützung der Nachversorgung wurde erst bei 4 % der Befragten umgesetzt (Wicht und Exner 2020). Daraus lässt sich schließen, dass eine Grundproblematik der End-to-End-Digitalisierung in der fehlenden oder nicht vollständigen Datenintegration und in den vorhandenen Datensilos liegt.

2 Herausforderungen der Schweizer Spital-IT in der Digitalen Transformation

Die Schweizer Gesundheitsbranche und damit auch das Spitalwesen unterliegt gewissen helvetischen Besonderheiten. Diese Spezifika müssen die IT-Organisationen und die IT-Dienstleister der Spitäler Rechnung tragen. Ebenso können sie für die Nutzung einer iPaaS Lösung relevant sein. Daher werden im Folgenden die verschiedenen Perspektiven kurz angeführt.

2.1 Allgemeine Herausforderungen

Beobachtungen aus der Spital-IT haben gezeigt, dass die IT von der Spitalleitung noch sehr stark als „Kostentreiber“ wahrgenommen wird. Diesbezüglich ist die Spital-IT besonders gefordert, ihre Wertgenerierung so zu verdeutlichen, dass diese im klinischen Umfeld auch wahrgenommen wird. Denn schweizweit werden ambulante Leistungen über ein einheitliches Tarifsystem mit Taxpunkten (Tarmed) abgerechnet. Im stationären Bereich kommt ein fallbasiertes System (SwissDRG) zum Einsatz, welches sehr ähnlich zu den deutschen Diagnosis Related Groups (DRG) oder zur österreichischen leistungsorientierten Krankenanstaltenfinanzierung (LKF) funktioniert. Doch in einem derartig finanziell regulierten Umfeld sind förderliche Massnahmen auf den Umsatz schwierig zu realisieren (Vettori et al. 2010). Vielversprechender sind da positive Effekte bei den Aspekten Zeitaufwand, Effektivität und Kundenzufriedenheit, welche im klinischen Alltag einen hohen Stellenwert besitzen. Diese Aspekte setzen einen reibungslosen und übergreifenden Datenaustausch voraus, damit die klinischen Prozesse mit weniger (Zeit-) Aufwand und ohne Umwege oder Medienbrüche (effektiver) ausgeführt werden können (Baumgartner 2023; Urech 2019). Dies gilt auch für die Kundenseite. Niemand will mehr die Ultraschallbilder als CD-ROM zugesandt bekommen, nur weil diese in einer Klinik erstellt wurden und nicht weiter digital verfügbar sind. Dass die jeweils spitaleigene, mosaikartige Applikationslandschaft, welche für die Schweizer Spitäler sehr typisch ist, dabei zusätzlich den übergreifenden Datenaustausch erschwert, ist sowohl für das medizinische Personal wie auch für die Patienten kaum einsichtig. Für alle Digitalisierungsinitiativen wird das dafür notwendige Datenmanagement als wichtiger Erfolgsfaktoren für die Spitäler gesehen (Harvey 2023). Folglich ist zwar ein

ganzheitliches Datenintegrationskonzept notwendig, welche jedoch in-house oftmals hohe Investitionskosten beansprucht und wiederum nicht so einfach verargumentiert werden kann.

2.2 Organisatorische und rechtliche Herausforderungen

Das Schweizer Gesundheitssystem ist ein Konglomerat aus Föderalismus, Liberalismus, Korporatismus und direkter Demokratie (Brock 2022). Obschon sich der Bund für die rechtlichen Rahmenbedingungen verantwortlich zeichnet, liegt die Hauptlast der Verantwortung im Gesundheitswesen bei den Kantonen. Der Föderalismus drückt sich im Schweizer Spitalbetriebsgesetz aus, wobei jeder Kanton seine eigene Gesetzgebung und Regelung in Bezug auf Organisation, Finanzierung und Qualitätskontrolle von Krankenhäusern besitzt. Gesundheitspolitik ist zwischen Kantonen, Ärzteschaft und Bund aufgeteilt, die lokal ihre Interessen verfolgen (Thiel et al. 2018) und somit technische Entwicklungen in der Bedeutung eher in den Hintergrund rücken. Aufgrund der Machtverhältnisse zwischen Gesundheitspersonal und technischem Personal ist die Umsetzung von Digitalisierungsprojekten in einer Expertenorganisation, jedoch auch vielerorts wegen fehlender oder eingeschränkter digitaler Gesundheitskompetenz (D’Onofrio 2022), besonderen Herausforderungen unterworfen.

Medizinische Fachpersonen sind dem Berufsgeheimnis verpflichtet, das im Strafgesetzbuch Art. 321 geregelt ist. Konsequenterweise findet das auch im neuen Datenschutzgesetz (nDSG) seinen Niederschlag, da man es hier mit besonders schützenswerten Daten zu tun hat.

Da IT-Abteilungen mit Vertragspartnern zusammenarbeiten, welche Leistungen via IT-Lösungen und -Services zur Verfügung stellen, ist es notwendig, die gesetzlichen Anforderungen in die Vertragsgestaltung der Service Level Agreements (SLA) einfließen zu lassen.

2.3 Technische Herausforderungen

Neben den typischen Herausforderungen und technologischen Altlasten sind Spital-IT Organisationen normalerweise auf Stabilität und Robustheit konditioniert. Dadurch besteht oftmals eine risikoaverse Änderungsphilosophie, welche sich in bürokratischen und langwierigen IT-Systemlebenszyklen, überbordenden Datenschutzregeln und -sicherheitsvorschriften, Langzeit-Archivierungsvorschriften und externen Regulierungen widerspiegelt (D’Onofrio 2022; Palvia et al. 2012).

Darüber hinaus hat die Covid19-Pandemie alte Schwächen und neue Herausforderungen an den Tag gebracht. Dies sind, um nur ein paar ausgewählte Beispiele im iPaaS Kontext zu nennen (Hämmerli et al. 2021; Hansen 2022):

- *Daten-Management & Integration:* Die IT-Spitallandschaft kann aus sehr vielen Einzellösungen bestehen, oft existiert auch ein KIS welches, ähnlich einem ERP-System, bei den medizinischen Prozessen als Datenverwaltungssystem dient. Diese Lösungen besitzen aber zumeist proprietäre Schnittstellen und die Integration

mit weiteren medizinischen, fachabteilungs- und administrativen Systemen kann aufwendig und somit kostspielig werden.

- *Ausbau neuer Formen der Patienteninteraktion:* Dies kann der Einsatz von Telemedizin ausserhalb des Spitäles sein oder der generelle Trend, dass die Patienten sich selbst befähigen wollen, um ihre Gesundheit aktiver in die Hand zu nehmen (D’Onofrio 2022). Ebenso explodieren die Angebote im Digital- und im Mobile Health Bereich.
- *Erhöhte Compliance Vorschriften:* Durch die verstärkte digitale Öffnung hin zum Patienten, in die Gesundheitsökosysteme und die Forschung, wie auch dem Einsatz von innovativen Technologien wie Künstliche Intelligenz (KI), eröffnen sich neuartige und komplexere Fragestellungen zu Ethik und der Einhaltung von Verhaltensformen und Regulatorien (D’Onofrio 2022).

Zusätzlich entstehen immer kurzfristiger neue soziale und ethische Fragestellungen, z.B. Algorithmic Fairness, Aging Digital Divide, Gender Specific Medicine, welche schlussendlich auch in der Spital-IT ihre Spuren hinterlassen, und technologische, prozessuale und datenbasierte Antworten benötigen.

3 Spezielle Anforderungen im Data- & Integration Management

Wie bereits in der Einleitung erwähnt, sind die Anforderungen beim Umgang mit Patienten- und Gesundheitsdaten in einer iPaaS Lösung besonders sensibel und schützenswert. Zusätzlich zeigt die heterogene System- und Datenlandschaft in den Spitälern einen hohen Komplexitätsgrad an Datenarten, -semantiken und formaten auf. Daraus ergeben sich besondere Anforderungen, welche hier nun kurz angerissen werden.

3.1 Anforderungen an iPaaS und – Cloud basierten Datenintegrationslösungen

Mit iPaaS wird die konsequente Weiterentwicklung der Bestrebungen von Enterprise Application Integration (EAI) gesehen. Dabei werden die technische Middleware-Lösungen nicht On-Premises sondern in einer Cloud Computing Umgebung zur Verfügung gestellt (Ebert et al. 2017). Wesentliche Unterscheidungsmerkmale einer iPaaS Lösung sind das IT-Betriebs- und Auslieferungsmodell auf Basis eines Cloud Service Providers und die „pay per use“ Zahlungsmodelle. Der Kunde der iPaaS Lösung sollte sich auf die Kernaufgabe, das Integrieren von Applikationen und deren Daten, fokussieren können. Dafür wird eine Vielzahl von Daten-Konnektoren/-Adaptern und die Unterstützung führender Datenaustauschstandards angeboten.

Generell unterliegen iPaaS Lösungen in der Gesundheitsbranche ebenso den nicht-funktionalen Anforderungen wie Sicherheit, Skalierbarkeit, Wartbarkeit, Kosten usw. Besonderes Augenmerk wird bei den funktionalen Anforderungen auf die Einhaltung der notwendigen Datenschutz- und Datensicherheitsvorschriften bis hin zu Abgrenzung zu den Regulatorien von medizinischen Softwareprodukten (MepV, MDR) gelegt. Diese domänenspezifischen Anforderungen werden nachfolgend und in den Folgekapiteln etwas genauer behandelt:

- *Offene Daten- und Integrationsstandards und APIs auf syntaktischer Ebene:* Für den einfachen technischen und strukturierten Datenaustausch, wie auch für die Anbindung von Applikationen, empfiehlt es sich, wiederverwendbare und stabile Datenschnittstellenstandards zu verwenden. Im Speziellen wird hier der HL7 Fast Healthcare Interoperability Resources (FHIR) Datenaustauschstandard hervorgehoben. Dieser sollte sich durch die einfache Datenstruktur (sogenannter Ressourcen) und der Nutzung von Web-basierten Programmiersprachen besonders einfach integrieren lassen. Ein weiterer internationaler Standard wird in ISO 13606 zusammengefasst, welcher mit einem dualen Ansatz eines Datenreferenz- und Archetypen Modells operiert (Brandstätter 2020; Pedrera-Jiménez et al. 2022).
- *Definitionen, Terminologien und Klassifizierung auf semantischer Ebene:* Syntaktische Datenformate und Standards sind erst dann vollständig interoperabel, wenn auch die Inhalte, also die Semantik, zwischen den Systemen verstanden wird. Dafür existieren als erster Schritt verschiedenste sogenannte Terminologien und Klassifizierungen. Dazu zählen z. B. Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT), Logical Observation Identifiers Names and Codes (LOINC), Digital Imaging and Communications in Medicine (DICOM) oder International Classification of Diseases (ICD). Zusätzlich sind zur Verständigung eines Datenaustausches auf semantischer Ebene z. B. sogenannte Integrating the Healthcare Enterprise (IHE) Profile hilfreich (Brandstätter 2020; de Mello et al. 2022).
- *Einheitliches Informationsmodell für die Datenrepräsentation der Spitaldomäne:* Idealerweise bietet eine iPaaS Lösung auch ein universelles und wiederverwendbares Informationsmodell zur Zwischenspeicherung oder dem Mapping von Spitaldaten an. Hier spielt seit geraumer Zeit OpenEHR² als offenes und freies Electronical Health Repository eine zunehmend wichtige Rolle. Wird OpenEHR eingesetzt, wird die Interoperabilität zwischen verschiedenen medizinischen IT-Systemen wesentlich erleichtert (Pedrera-Jiménez et al. 2022).
- *Vordefinierte Plug-and-Play-Konnektoren und Adapter:* Sie sind für die Anbindung von branchenspezifischen Systemen wie KIS, Patienten Daten Management Systeme (PDMS), Elektronisches Patienten Dossier (EPD), Picture Archiving and Communication System (PACS), Dokumenten Management System (DMS) usw hilfreich.

3.2 Anforderungen an die IT-, Cyber- und Datensicherheit

Die Bedrohungsszenarien aus dem Internet erfordern speziell in Spitälern erhöhte Sicherheitsvorgaben. Die typischen Sicherheitsziele sind unter der Abkürzung CIA (Confidentiality, Integrity, Availability) für IT-Dienste und Daten zusammengefasst. Hierfür bestehen Normen aus der ISO 2700x Familie, Minimalstandards und IT-Sicherheitsrahmenwerke z. B. in Anlehnung an BSI, NIST Cybersecurity Framework, welche die jeweilige nationalen Cybersicherheitsstellen zur Verfügung stellen (BWL 2018). Am Beispiel des US CyberSecurity Framework NIST (NIST 2018) beschreibt dieses die fünf Schutzphasen: Identifizieren, Schützen, Erkennen, Re-

² <https://openehr.org/>.

agieren auf Sicherheitsrisiken und Wiederherstellen des Normalzustandes. Darüber hinaus existieren branchenspezifische Empfehlungen und Leitfäden für den Schweizer Gesundheitsbereich und deren Spitäler (FMH 2020; H+ 2020). Im Speziellen sind hier die besonders sensiblen persönlichen und eindeutigen Gesundheits- und Vitaldaten als auch die Einhaltung des strengen Berufsgeheimnisses zu berücksichtigen. Darüber hinaus muss der 24/7 Dauerbetrieb und die Business Continuity bei den systemkritischen Krankenhaussystemen gewährleistet werden. Weite Detailanforderungen werden im letzten Kapitel in Abb. 1 aufgezeigt.

Es zeigt sich, dass grundsätzlich ein systemischer und ganzheitlicher Ansatz notwendig ist. Die Vorgaben zu „Security by Design“ müssen durch konkrete und proaktive Designansätze, Security- und Disaster Recovery Tests realisiert werden, um ein hohes Mass an IT- und Datensicherheit gewährleisten zu können.

3.3 Anforderungen durch das neue Schweizer Datenschutz Gesetz (nDSG)

Das neue Schweizer Datenschutzgesetz (nDSG) und die Datenschutzverordnung (DSV) treten am 1. September 2023 in Kraft. Diese Totalrevision wurde auf aktuelle Anforderungen und stärker an die europäische DSGVO Verordnung angeglichen (EU Monitor 2016). Dabei wurden insbesondere die Anforderungen zur Transparenz von Datenverarbeitungen verbessert und die Selbstbestimmung der betroffenen Personen über ihre Daten gestärkt. Zudem muss nachgewiesen werden, dass die erforderlichen Massnahmen auch aktiv bewirtschaftet und regelmässig auf ihre Wirksamkeit kontrolliert werden (Bundesamt für Justiz 2022).

Hinzu kommen die Pflicht, eine Datenschutz-Folgeabschätzung durchzuführen (Fock et al. 2019) und die Aspekte „Privacy by Design“ und „Privacy by Default“ zu berücksichtigen. Das Prinzip „Privacy by Default“ bedeutet die Umsetzung von datenschutzfreundlichen Voreinstellungen für die betroffenen Personen, damit ohne weitere Eingriffe die Privatsphäre auf bestmöglichem Niveau eingehalten wird. Beim Prinzip „Privacy by Design“ sind aus organisatorischer Sicht v. a. zwei Aspekte zu beachten: Jede datenverarbeitende und datenkontrollierende Organisation muss ein Informationssicherheitskonzept und entsprechende Prozesse zur Umsetzung vorweisen (Bundesamt für Justiz 2022).

Da in einem Spital generell besonders schützenswerten Personendaten (BSPD) bearbeitet werden, muss eine vertragliche Grundlage für die Bearbeitung dieser personenbezogenen Daten vorhanden sein, ebenso muss die Zweckbindung und Verhältnismässigkeit erfüllt sein. Bei der Bearbeitung von BSPD muss eine Datenschutz-Folgeabschätzung erstellt werden, bei besonderen Risiken ist zudem eine Vorabkontrolle durch den Datenschutzbeauftragten erforderlich. Die vorgängige und nachweisbare Informationspflicht der betroffenen Person und deren explizite Einwilligung ist zwingend erforderlich. Da die klinisch relevanten Gesundheitsdaten unter das ärztliche Berufsgeheimnis fallen, gelten weitere rechtliche Bedingungen. Wer entsprechend im Spital eine IT-Infrastruktur oder Services zur Verfügung stellt, wartet oder betreut und das medizinische Personal damit bei seiner Berufstätigkeit unterstützt, gilt als Hilfsperson (Schwaninger und Latmann 2013). Befindet sich jedoch der Cloud Computing Anbieter ausserhalb der Schweiz, gilt das „Hilfsperson“ Prinzip nicht mehr, da dieser nicht der schweizerischen Strafgesetzgebung untersteht.

Werden Patientendaten in einen ausländischen Cloud-Service ausgelagert, bedarf es daher der expliziten Einwilligung der betroffenen Person, ansonsten stellt eine solche Datenweitergabe eine Verletzung des Arztgeheimnisses dar (Schwaninger und Latmann 2013). Daraus ist ersichtlich, dass es ein enges Zusammenspiel der Datensicherheit mit dem Datenschutz benötigt, um allen Anforderungen und Vorschriften gerecht zu werden.

3.4 Implikationen zur Medizin Produkte Verordnung (MepV)

Die Entwicklung oder Einführung von Medizinprodukten ist in der Schweiz im Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG) geregelt. Eine der Verordnungen, die vor allem die Angleichung zur europäischen MDR³ zum Ziel hat, ist die Medizinprodukteverordnung (MepV). Dies gilt auch für reine digitale Medizinprodukte, welche einen medizinischen Zweck verfolgen und damit unter die Regulierung fallen können.

Somit gelten prinzipiell für alle Software-Lösungen im Gesundheitswesen mit einem medizinischen Zweck die gleichen regulatorischen Anforderungen. Dabei ist es grundsätzlich unerheblich, ob es eine On-Premises Lösung ist oder Teile an einen Cloud-Computing Anbieter ausgelagert werden. Das bedeutet, es muss zuerst festgestellt werden, ob das Produkt in eine der folgenden Kategorien fällt (MepV 2020):

- Software als Teil eines Medizinprodukts (Medical Device Software)
- Software als eigenständiges Medizinprodukt (Software as a Medical Device)
- Software als Zubehör zu einem Medizinprodukt

Wenn die iPaaS-Lösung in eine der Kategorien qualifiziert, so muss die Risikoklasse (I, IIa, IIb, III) bestimmt werden. Die Klasse III beschreibt das höchste (Patienten-)Risiko und je nach Klasse ist es notwendig, ein umfassenderes Risiko- und Qualitätsmanagementsystem (QMS) zu implementieren. Besonders die ISO 13485:2016 (Zertifizierung der QMS von Medizinprodukteherstellern) erfordert, dass auch der Cloud Anbieter die entsprechende Konformität nachweisen muss.

Von besonderer Bedeutung im Zusammenhang mit MepV ist die IT-Sicherheit. Hier kommt vor allem die Norm IEC 81001-5-1 (Sicherheit, Effektivität und Sicherheit von Gesundheitssoftware und Gesundheits-IT-Systemen – Aktivitäten im Produktlebenszyklus) und die IEC TR 60601-4-5 (Medizinische elektrische Geräte – Sicherheitsbezogene technische Anforderungen) zur Anwendung und zusätzlich müssen die nDSG-Regeln sowohl seitens des QMS als auch bzgl. Sicherheit berücksichtigt werden.

Damit verlangt MepV den Nachweis, dass genügend Sicherheitsmassnahmen umgesetzt werden, damit die spezifizizierte medizinische Leistung, wie auch der Schutz von sensiblen Daten, gewährleistet ist (MepV 2020). Somit sind bereits im Entwicklungsprozess mehrere Anforderungen zu berücksichtigen (eHealth Suisse 2022):

³ Europäische Medical Device Regulation.

- beim Definieren der Produkthanforderungen
- beim Entwickeln der Produktarchitektur
- beim Erstellen der Risikoanalyse
- bei der Verifizierung und Validierung
- bei der Produktpflege (Aktualisierungen, Bugfixes, etc.)

Schlussendlich ist die wesentliche Frage, ob die technische iPaaS Plattform selbst einen medizinischen Zweck verfolgt und damit sich als MepV qualifiziert (Swissmedic 2021). Zudem, ob eine geeignete Modularisierung der Architektur vorgenommen werden kann, damit nur ein möglichst kleiner Teil der Lösung zertifiziert werden muss. Ein geeignetes Risikomanagement und intelligente API-Schnittstellenansätze können die Modularisierung erleichtern und die Komplexität der Lösung aus MepV Sicht reduzieren.

4 Fazit und Ausblick

Das Betreiben und Nutzen einer iPaaS Lösung für Gesundheitsdaten in Schweizer Spitälern ist heute noch Neuland. Wie in den vorherigen Kapiteln versucht wurde aufzuzeigen, müssen verschiedene Dimensionen und Aspekte betrachtet werden, um diese rechtskonform, sicher und nachhaltig betreiben zu können. Die aus der Forschung wichtigsten identifizierten Anforderungsdimensionen sind dabei:

- *Allgemeine Anforderungen:* Erfüllung von generellen Anordnungen und Fragestellungen bis hin zu einer professionellen und skalierbaren Cloud Infrastruktur Basis.
- *Technisch und funktionale Anforderungen:* Unterstützung der spezifischen iPaaS Kernfunktionen zum schnellen, einfachen und umfassenden, sowie interoperablen Datenmanagement.
- *Organisatorisch und rechtliche Anforderungen:* Alle Compliance relevanten Punkte von organisatorischen bis hin zu gesetzlichen als auch vertraglichen Aspekten.
- *Im Speziellen für die Handhabung von Gesundheitsdaten:* Unter Berücksichtigung des Datenschutzes bezgl. der Nutzung besonders schützenswerter Daten wird hier speziell auf folgende Vertiefungspunkte geachtet:
 - *IT-Sicherheit und Cybersecurity:* Massnahmen und Kontrollen zur Sicherung und Abwehr jeglicher Form von Sicherheitsrisiken
 - *Schweizer Datenschutzgesetz (nDSG):* Umfassende Einhaltung und Schutz von besonders schützenswerten Gesundheitsdaten
 - *Schweizer Medizinprodukte Verordnung (MepV):* Qualifizierung und Klassifikation von möglichen medizinischen Zwecken und der damit verbundenen Zertifizierungsmassnahmen

In Abb. 1 werden die verschiedenen Anforderungen für den Einsatz einer iPaaS Lösung in der Spital-IT nochmals zusammengefasst. Ziel dieser Darstellungsform ist es, die Vielfältigkeit, Komplexität und Abhängigkeit zwischen den einzelnen Dimen-

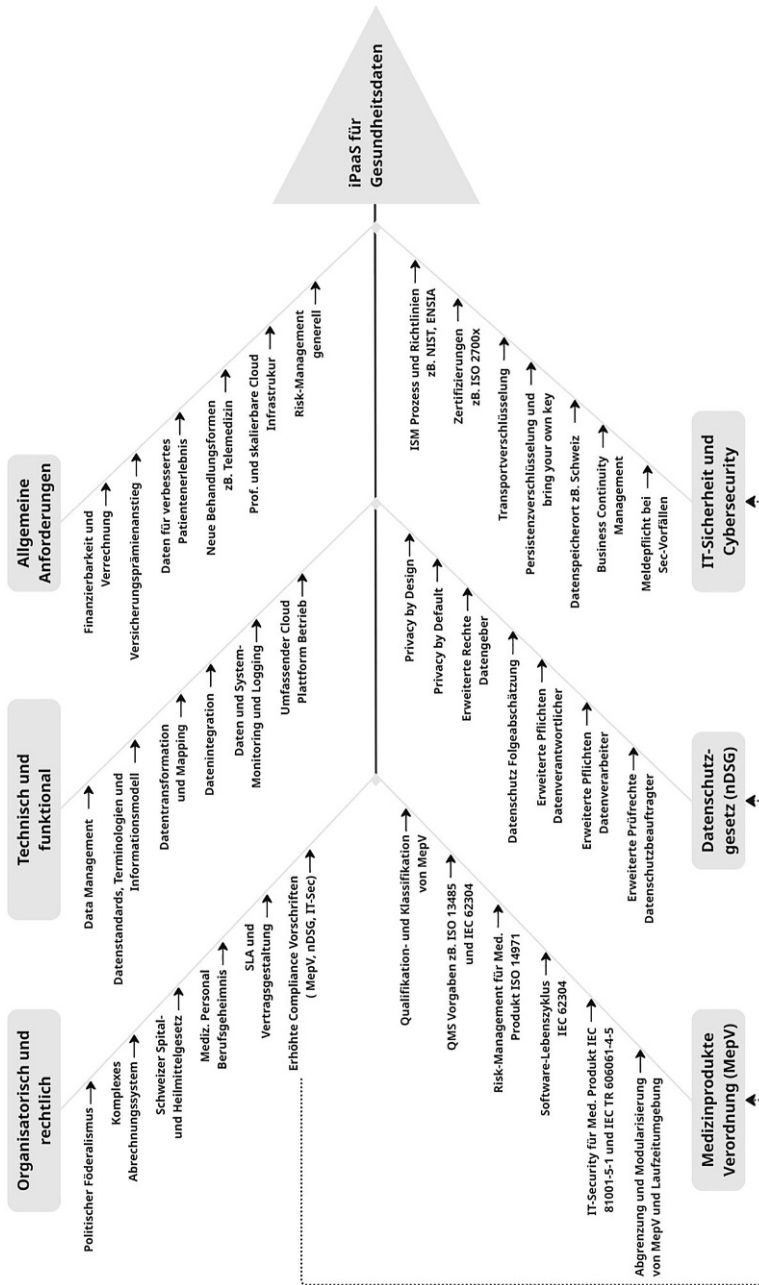


Abb. 1 Zusammenfassung der iPaaS Anforderungen anhand der sechs Hauptdimensionen

sionen aufzuzeigen und Einstiegspunkte zu benennen. Daraus entstanden 6 Anforderungsdimensionen, welche zur Lösung der Fragestellung mit ihren Unterpunkten beitragen. Besonders zu beachten sind die drei spezifischen und erhöhten Com-

pliance Dimensionen, deren Abhängigkeit mit der gepunkteten Linie im unteren Bereich aufgezeigt werden.

So wie in anderen Branchen werden sich über kurz oder lang auch iPaaS Lösungen in Spitälern verbreiten und einen Beitrag zur verbesserten Interoperabilität innerhalb und über die Spitäler hinaus leisten. Zudem wird durch neue Technologien wie IoT, Big-Data und Mobile Health Lösungen der Druck in Spitälern steigen, die Datenflut und -vielfalt besser zu beherrschen (Neft et al. 2021). Erst mit einfachen, nahtlosen, medienbruchfreien und konsistenten Datenflüssen können die Potentiale der Digitalisierung im Spitalbetrieb voll ausgereizt werden.

Es bleibt jedoch immer in der Verantwortung der Spital-IT und der Spitalleitung, das notwendige und kontinuierliche Risk-Management bei den eingesetzten Cloud Lösungen wie iPaaS wahrzunehmen. Risiken wie z.B. Vendor lock-in, Cybersecurity Lücken und -Angriffe, Kostenmanagement und Single-Point of Failure müssten regelmässig geprüft und mitigiert werden.

Das Innosuisse SHIFT Projekt ist bestrebt, mit der Tech-Foundation als iPaaS Ansatz, hier einen Beitrag zu leisten und über die nächsten 2 Jahre konkrete Lösungsvorschläge zu entwickeln. Es bleibt somit zu klären, wie die konkreten und praktischen Handlungsempfehlungen gestaltet werden und ob die Akzeptanz und der Nutzen in Schweizer Spitälern mit konkreten Fallbeispielen nachgewiesen werden kann. Dafür muss noch einiges an Validierungsforschung durchgeführt werden und anhand der SHIFT Anwendungsteilprojekte in den Spitalsalltag pilotisch nachgewiesen werden.

Danksagung Diese Arbeit entstand im Rahmen des Flagship Forschungsprojektes SHIFT (Smart Hospital: Integrated Framework, Tools & Solutions), gefördert durch die Innosuisse – Schweizerische Agentur für Innovationsförderung.

Funding Open access funding provided by ZHAW Zurich University of Applied Sciences

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Literatur

- (2020) Medizinprodukteverordnung (MepV), Pub. L. No. SR 812.213.1. <https://www.fedlex.admin.ch/eli/oc/2020/552/de>. Zugegriffen: 01.07.2023.
- Angerer A et al (2021) Der Digital Health Report 21/22—Die Zukunft des Schweizer Gesundheitswesens. ZHAW WIG. <https://www.zhaw.ch/storage/hochschule/medien/news/2021/210914-digital-health-report-2021.pdf>. Zugegriffen: 01.07.2023.

- Baumgartner N Gefahr für Patienten: Grosser Nachholbedarf in Spital-IT. Inside IT. <https://www.inside-it.ch/gefahr-fuer-patienten-grosser-nachholbedarf-in-spital-it-20230303> (Erstellt: 3. Juni 2023). Zugegriffen: 01.07.2023.
- Brandstätter J (2020) IHE / HL7 / FHIR – Auslegeordnung (V1.3; p. 41). eHealth Suisse. https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/auslegeordnung-ihe-hl7-fhir.pdf. Zugegriffen: 01.07.2023.
- Brock H (2022) Das Gesundheitssystem der Schweiz – Teuer, aber gut. *Österr Krankenhausz* 63(3–4):22–24. <https://doi.org/10.1007/s43830-022-0087-1>
- Bundesamt für Justiz (2022) Totalrevision des Datenschutzgesetzes (DSG) – Übersicht zu den wichtigsten Änderungen für die Erarbeitung der Rechtsgrundlagen betreffend Datenbearbeitungen durch Bundesorgane. Eidgenössisches Justiz- und Polizeidepartement EJPD
- BWL (2018) Minimalstandard zur Verbesserung der IKT-Resilienz. Bundesamt für wirtschaftliche Landesversorgung BWL. https://www.bwl.admin.ch/dam/bwl/de/dokumente/themen/ikt/broschuere_minimalstandard.pdf.download.pdf/IKT_DE_2018_Web.pdf. Zugegriffen: 01.07.2023.
- D’Onofrio S (2022) Der digitale Wandel im Gesundheitswesen: Grundlagen, Nutzungspotenziale und Herausforderungen von e-Health. *HMD* 59(6):1448–1460. <https://doi.org/10.1365/s40702-022-00930-4>
- Ebert N, Weber K, Koruna S (2017) Integration Platform as a Service. *Bus Inf Syst Eng* 59(5):375–379. <https://doi.org/10.1007/s12599-017-0486-0>
- eHealth Suisse (2022) Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer. eHealth Suisse. https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/Leitfaden_e-Health_Suisse_fuer_App_Entwickler.pdf. Zugegriffen: 01.07.2023.
- FMH (2020) Technische und organisatorische Anforderungen an Cloud-Dienste. FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern (<https://www.fmh.ch/files/pdf24/fmh-technische-und-organisatorische-anforderungen-an-cloud-dienste.pdf>)
- Fock S, Isele C, Kaufmann P, Letter M (2019) Beispielhafter Umgang mit der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) am Beispiel eines Krankenhaus-Informationssystems. Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie/Bundesverband Gesundheits-IT
- Gartner (2023) Magic quadrant for integration platform as a service, worldwide [market report]. Gartner.com. <https://www.gartner.com/document/4023272>. Zugegriffen: 01.07.2023.
- H+ (2020) Informationssicherheit und Datenschutz – Anforderungen zur ICT-Sicherheit von Fremdsystemen. H+: Spitäler, Kliniken und Pflegeinstitutionen. https://www.hplus.ch/fileadmin/hplus.ch/public/Politik/Cyber_Security/Leitfaden_Cyber_Security_D_V1.2.pdf. Zugegriffen: 01.07.2023.
- Hämmerli M et al (2021) Digitalisierung im Gesundheitswesen – Die 8,2-Mrd.-CHF-Chance für die Schweiz. McKinsey Digital. <https://www.mckinsey.com/ch/~/media/mckinsey/locations/europe%20and%20middle%20east/switzerland/our%20insights/digitalization%20in%20healthcare/digitalisierung%20im%20gesundheitswesen%20%20die%2082mrdchance%20fr%20die%20schweiz%20de.pdf>. Zugegriffen: 01.07.2023.
- Hansen L (2022) Top 6 IT Challenges in Healthcare. CIOInsight. <https://www.cioinsight.com/news-trends/it-challenges-in-healthcare/>. Zugegriffen: 01.07.2023.
- Harvey D Six key objectives for hospitals in 2023, and how digital health solutions can support them | David Harvey. OncLive. <https://www.chiefhealthcareexecutive.com/view/six-key-objectives-for-hospitals-in-2023-and-how-digital-health-solutions-can-support-them-david-harvey> (Erstellt: 5. März 2023). Zugegriffen: 01.07.2023.
- Hauser T, Menoud L, Bachmann M (2023) Kennzahlen der Schweizer Spitäler 2021. Bundesamt für Gesundheit (BAG)
- Markets and Markets (2023) Integration Plattform as a Service (iPaaS) Market by Service Type, Deployment Model, Organization Size, Vertical and Region (2022–2026). Markets and Markets. <https://www.marketsandmarkets.com/Market-Reports/integration-platform-as-a-service-market-134216323.html>. Zugegriffen: 01.07.2023.
- de Mello BH, Rigo SJ, da Costa CA, da Rosa Righi R, Donida B, Bez MR, Schunke LC (2022) Semantic interoperability in health records standards: A systematic literature review. *Health Technol* 12(2):255–272. <https://doi.org/10.1007/s12553-022-00639-w>
- Monitor EU (2016) Regulation 2016/679—Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)—EU monitor. EU Monitor. https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lbczq. Zugegriffen: 01.07.2023.

- Neft F, Kappler KE, Smolnik S (2021) Der Einfluss von IoT-, Big-Data- und Mobile-Health-Lösungen auf die Wertschöpfung in Krankenhäusern: Gap-Analyse und Handlungsempfehlungen. *HMD* 58(1):50–63. <https://doi.org/10.1365/s40702-020-00682-z>
- NIST (2018) CSF Cybersecurity Framework Documents. NIST.Gov. <https://www.nist.gov/cyberframework/framework>. Zugegriffen: 01.07.2023.
- Palvia P, Lowe K, Nemati H, Jacks T (2012) Information technology issues in healthcare: hospital CEO and CIO perspectives. *Commun Assoc Inf Syst*. <https://doi.org/10.17705/1CAIS.03019>
- Pedrera-Jiménez M, Spanish Expert Group on EHR standards, Kalra D, Beale T, Muñoz-Carrero A, Serrano-Balazote P (2022) Can OpenEHR, ISO 13606 and HL7 FHIR work together? An agnostic perspective for the selection and application of EHR standards from Spain <https://doi.org/10.36227/techrxiv.19746484.v1> (Preprint)
- Schwaninger D, Latmann S (2013) Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke. *Jusletter*, 1071. <https://doi.org/10.38023/622c3a33-9a87-454e-844e-b88c37e4e46e>
- SHIFT Blaupause für die Digitalisierung im Gesundheitswesen—SHIFT | Smart Hospital—Integrated Framework, Tools & Solutions. ZHAW SHIFT Projekt. <https://future.hospital/>. Zugegriffen: 22. März 2023
- Swissmedic (2021) Merkblatt Medizinprodukte-Software. Swissmedic. https://www.swissmedic.ch/dam/swissmedic/de/dokumente/medizinprodukte/mep_urr/bw630_30_007d_mbmedizinprodukte-software.pdf.download.pdf/BW630_30_007d_MB%20Medizinprodukte-Software.pdf. Zugegriffen: 01.07.2023.
- Thiel R et al (2018) SmartHealthSystems—Digitalisierungsstrategien im internationalen Vergleich. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/Der_digitale_Patient/VV_SHS-Gesamtstudie_dt.pdf. Zugegriffen: 01.07.2023.
- Urech M Veraltet, proprietär und zu komplex: Wie die IT Schweizer Spitälern zu schaffen macht. *Netzwoche*. <https://www.netzwoche.ch/news/2019-04-08/veraltet-proprietar-und-zu-komplex-wie-die-it-schweizer-spitaelem-zu-schaffen> (Erstellt: 8. Apr. 2019). Zugegriffen: 01.07.2023.
- Vettori A, Schmid S, von Stokar T (2010) Evaluation Tarmed: Fallbeispiele. Eidg. Finanzkontrolle (EFK)
- Wicht A, Exner A (2020) Auf dem Weg zum „digitalen Spital“ Marktstudie zum Stand der Digitalisierung in der Schweizer Spitallandschaft. Synpulse Schweiz