Über die Nutzung von Cloud-Services für das Telemonitoring

Cloud-Services – Telemonitoring – Datenschutz

Im Unterschied zu DiGA und Videosprechstunde fordert das Telemonitoring eine asynchrone Kommunikation und eine Verteilung von Aufgaben zwischen Patienten, TMZ, PBA und Dienstleistern. Genau dafür sind Cloud-Dienste prädestiniert. Ein lückenloses Telemonitoring erfordert die ständige Verfügbarkeit und blitzschnelle Skalierung, wie eigentlich nur Cloud-Dienste sie mit ihrer enormen Rechenleistung ermöglichen. In der Cloud wird außerdem ein höherer Schutz vor Hackerangriffen, Datenverlusten und Systemausfällen erreicht als beim Betrieb eines Rechners in der Arztpraxis. Es existieren bereits Hybrid-Cloud-Lösungen für das Telemonitoring, die die Anforderungen des Europäischen Datenschutzausschusses (EDSA) erfüllen.

>> Die Digitalisierung des Gesundheitssystems gilt als wichtiges Instrument, um die Qualität und Effizienz der Versorgung zu verbessern und die Patientenautonomie zu fördern. Das Fraunhofer-ISI nennt in seiner Studie „E-Health in Deutschland" mehrere Beispiele innovativer E-Health-Angebote aus Frankreich, Niederlande und Österreich. Leider fällt Deutschland auf diesem Gebiet im europäischen Vergleich immer weiter zurück. Als Ursachen gelten insbesondere Sicherheitsbedenken und regulatorische Unsicherheiten[1].

Cloud-Services

Große Bedenken bestehen in Deutschland gegen den Einsatz von Cloud Services, obwohl diese gerade für E-Health-Lösungen eine bedeutende Rolle spielen. Als Gründe für die Verwendung im Gesundheitswesen gelten höhere Patientensicherheit, Informationssicherheit und Wirtschaftlichkeit. Zeitgemäße E-Health-Lösungen nutzen die Cloud nicht nur als Datenspeicher, sondern auch als Werkzeug für Softwareentwicklung, IT-Administration, Daten-Transport und Analyse. Als Gründe für die Nutzung von Cloud Services nennt das Bundesamt für Sicherheit in der Informationstechnik (BSI[2]) unter anderem:

- Cloud-Services sind dynamisch und dadurch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar
- Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen

Herkömmliche Prozesse im Gesundheitswesen oder einfache digitale Anwendungen (wie die Videosprechstunde) beruhen auf synchroner Kommunikation: Arzt und Patient sitzen sich gegenüber und kommunizieren miteinander. Dafür braucht es keinen (Cloud-)Server in der Mitte, der Daten (zwischen-)speichert und weiterverarbeitet. Weitergehende digitale Innovationen basieren häufig auf asynchroner Kommunikation und einer Verteilung von Aufgaben zwischen verschiedenen Akteuren (z. B. Patienten, TMZ, PBA, Dienstleister). Genau dafür sind Cloud-Dienste prädestiniert.

Telemonitoring

Beim Telemonitoring erfolgt die Kommunikation zwischen den Geräten des Patienten und den Systemen des telemedizinischen Zentrums (TMZ) ganz überwiegend asynchron. Im TMZ wartet niemand auf den Augenblick, da der Patient auf die Waage steigt oder den Blutdruck misst. Sobald der Patient die Messungen vorgenommen hat, werden die Daten automatisch an eine Datenannahmestelle transportiert, analysiert und gespeichert. Danach werden die Telemonitoringdaten der verschiedenen Geräte zusammengeführt und den Ärzten im TMZ angezeigt. Wesentliche Aufgaben werden von einem technischen Dienstleister oder von Gesundheits- und Krankenpflegern, auch in räumlicher Entfernung von der Arztpraxis, gemäß § 3 Abs. 2 QS-V TmHi[3] wahrgenommen.

Eine Ende-zu-Ende-Verschlüsselung zwischen Patienten und Arzt oder das Verbot der Einsichtnahme in die Daten, wie das für die technischen Verfahren zur Videosprechstunde[4] gefordert ist, würde keine Delegation von Leistungen erlauben. Alle Aufgaben müssten vom Arzt persönlich wahrgenommen werden. Insbesondere wären damit Dienstleistungen ausgeschlossen, die für das Funktionieren der technischen Infrastruktur und die Aufrechterhaltung der Verbindung zur Datenübertragung gemäß § 4 Abs. 4 Satz 2 der Methodenrichtlinie Telemonitoring[5] sorgen. Selbst die Batteriestandsmessung bei den Geräten des Patienten und die Kontaktaufnahme mit dem Patienten für den Versand von Ersatzbatterien wären in diesem absurden Szenario eine persönliche Aufgabe des Arztes.

Die Möglichkeit der Auftragsverarbeitung, auch unter Verwendung von Cloud-Diensten, ist daher unverzichtbar für das Telemonitoring. Beispielsweise werden die Messdaten

„Cloud Computing ist in vielen Bereichen bereits zum Standard avanciert."

Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Thema Cloud Computing

„Deutschland ist zunehmend eines der Schlusslichter."

Fraunhofer ISI-Studie zur Digitalisierung des Gesundheitssystems[1]

von den Cloud-Systemen der Gerätehersteller abgerufen und anschließend über einen Infrastructure-as-a-Service (IaaS)-Cloud-Dienst zur Datenannahmestelle transportiert.

Durch eine kontinuierliche Härtung der Infrastruktur und weitgehende Zertifizierungen können gerade Cloud-Dienste ein hohes Maß an Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) bieten. In solchen Umgebungen wird ein sehr viel höherer Schutz vor Hackerangriffen, Datenverlusten und Systemausfällen erreicht als beim Betrieb eines Rechners in der Arztpraxis.

Die hohe Verfügbarkeit durch 24/7-Infrastruktur-Teams und die schnelle Skalierung durch die enorme Rechenleistung ermöglichen die Sicherstellung einer lückenlosen Patientenbetreuung, insbesondere die in § 4 Abs. 4 der Methodenrichtlinie geforderte und der Patientensicherheit dienende Aufrechterhaltung der Verbindung zur Datenübertragung von den Geräten des Patienten zum TMZ.

Datenschutz

Bei der Datenverarbeitung in der Cloud ist ein Zugriff aus Drittländern nicht denkunmöglich. Daher ist im Einzelfall zu prüfen, ob die Verwendung eines Cloud-Dienstes zulässig ist. Dafür hat der Bundesbeauftragte für den Datenschutz und die Informationsfrei-

Zitationshinweis

Leiter, J.: „Cloud-Services – Telemonitoring – Datenschutz“, in „Monitor Versorgungsforschung“ (03/22), S. 34-35. http://doi.org/10.24945/MVF.03.22.1866-0533.2406

Hybrid-Cloud in der praktischen Anwendung im Telemonitoring bei Herzinsuffizienz

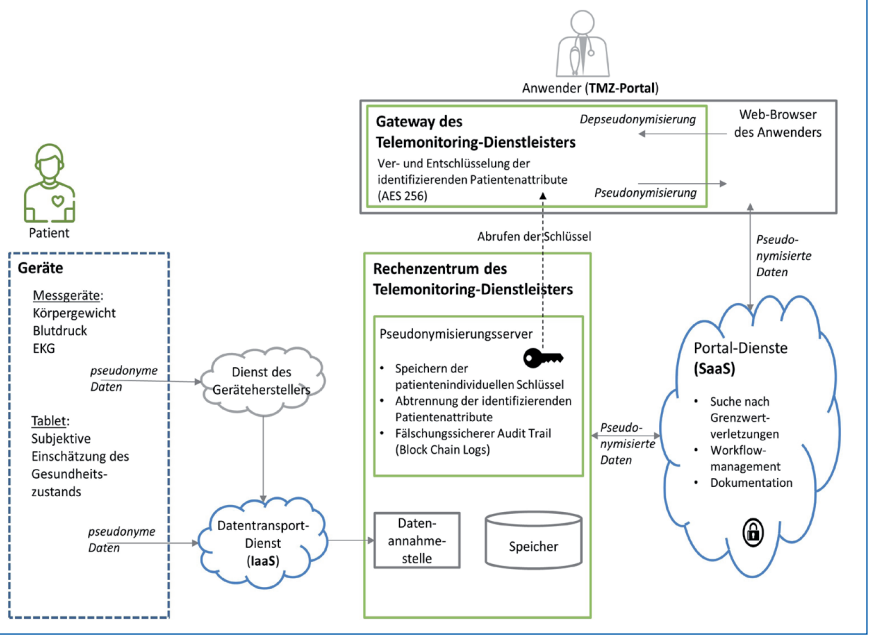

Abb. 1: Hybrid-Cloud in der praktischen Anwendung im Telemonitoring bei Herzinsuffizienz. Eigene Darstellung.

heit (BfDI) ein Prüfschema veröffentlicht[6]. Das BfDI-Prüfschema umfasst alle Schutzmechanismen von Kapitel V (nicht nur Art. 45) DSGVO. Gegebenenfalls sind ergänzende technische Maßnahmen zu ergreifen, um ein ausreichend hohes Datenschutzniveau zu gewährleisten. Die zusätzlichen Maßnahmen müssen wirksam sein und praktisch zur Verfügung stehen.

Auf Grundlage der Rechtsprechung des EU-Gerichtshofs in Sachen „Schrems II“[7] hat der Europäische Datenschutzausschuss (EDSA) Empfehlungen zu ergänzenden Maßnahmen für Übermittlungsinstrumente veröffentlicht[8]. Der EDSA hat bekannt gegeben, dass die Datenschutzaufsichtsbehörden die EDSA-Empfehlungen ihrer Verwaltungspraxis ab dem Zeitpunkt ihrer Veröffentlichung zu Grunde legen werden[9].

Abbildung 1 zeigt eine Hybrid-Cloud-Lösung für das Telemonitoring nach den Empfehlungen des EDSA, wie sie bereits heute praktisch zur Verfügung steht.

Bei dieser Lösung werden in der Cloud nur pseudonyme bzw. pseudonymisierte Daten verarbeitet. Patientenidentifizierende Attribute werden ausschließlich im Rechenzentrum des Telemonitoring-Dienstleisters (on-premises) oder im Webbrowser des Anwenders verarbeitet. Zudem sind alle Daten stets stark verschlüsselt, der Schlüssel befindet sich unter Kontrolle des TMZ und ist in einem Hardware-Kryptomodul auf einem Server in Deutschland hinterlegt. Alle Server befinden sich im Europäischen Wirtschaftraum. Mit der beschriebenen Hybrid-Cloud-Lösung für das Telemonitoring können die im BfDI-Prüfschema geforderten zusätzlichen Maßnahmen wirksam und praktisch zur Verfügung gestellt werden. <<

von:
Dr. med. univ. Josef Leiter,
Lehrbeauftragter für Digital Health an der Universität Heidelberg

Literatur

1: Fraunhofer-Institut für System- und Innovationsforschung (ISI) im Auftrag der Expertenkommission Forschung und Innovation (11.03.2022): Studie zum deutschen Innovationssystem Nr. 12-2022 (https://www.e-fi.de/fileadmin/Assets/Studien/2022/StuDIS_12_2022.pdf)
2: https://www.bsi.bund.de
3: Vereinbarung von Qualitätssicherungsmaßnahmen zwischen der KBV und dem GKV-Spitzenverband nach § 135 Abs. 2 SGB V zum Telemonitoring bei Herzinsuffizienz
4: Vereinbarung zwischen der KBV und dem GKV-Spitzenverband gemäß § 365 Abs. 1 SGB V vom 21.10.2016 i.d.F. vom 25.02.2021
5: BAnzAT 30.3.2021 B4, Richtlinie Methoden vertragsärztliche Versorgung Nr. 37
6: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/EU_UN/Pruefschema-Schrems-II.html
7: Urteil des EuGH (Große Kammer) vom 16. Juli 2020 in der Rechtssache Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559
8: EDSA, Empfehlungen 01/2020 zu ergänzenden Maßnahmen für Übermittlungsinstrumente zur Gewährleistung der Einhaltung des EU-Schutzniveaus für personenbezogene Daten, Version 2.0, verabschiedet am 18.06.2021; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdfsupplementarymeasurestransferstools_en.pdf
9: Vgl. EDSA, Pressemitteilung vom 11. November 2020: https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en

E-Health/Digital Health

Hrsg.: Rehmann, W./Tillmanns, C.
E-Health/Digital Health
Verlag: C.H.BECK, 2022
481 Seiten, in Leinen
ISBN-Print: 978-3-406-76208-6
Preis: 159,00 Euro

>> Diese Neuerscheinung gibt einen Überblick über die gesetzlichen Rahmenbedingungen und erläutert die verschiedenen Anwendungsformen von eHealth und Digital Health. Moderne Informations- oder Kommunikationstechnologien (IKT) haben längst in den Bereich der Behandlung und Betreuung von Patient:innen Einzug gehalten, wobei der Einsatz von IKT im Bereich der Gesundheitsversorgung vielfältig ist. Er erstreckt sich von der reinen Datenverwaltung, der Übermittlung von Daten, der Steuerung von medizinischen Geräten bis hin zum Einsatz intelligenter Systeme bei der Erkennung und Behandlung von Krankheiten und dem Monitoring gesundheitsbezogener Daten im Bereich der telemedizinischen Versorgung. Die zunehmende Digitalisierung im Gesundheitsbereich betrifft dabei alle an der medizinischen Versorgung Beteiligten, also Hersteller, Vertriebsunternehmen (z. B. Groß- und Einzelhandel), Apotheken, Leistungserbringer, die Erstattungsseite sowie insbesondere auch die Patient:innen. Entsprechend breit spannt sich der Bogen der von E-Health/Digital Health berührten Rechtsgebiete, die die Herausgeber – Dr. Wolfgang A. Rehmann und Dr. Christian Tillmanns – in ihrem Rechtshandbuch abarbeiten.

Ebenso geben sie nach einer kurzen Einführung zunächst einen Überblick über die gesetzlichen Rahmenbedingungen, denen E-Health-Anwendungen im Einzelnen unterliegen, und behandeln sodann vertiefend einzelne, nach Auffassung der Herausgeber in der Praxis besonders relevante Anwendungsformen aus rechtlicher Sicht und vor dem Hintergrund des jeweils anwendbaren regulatorischen Umfeldes, der berufsrechtlichen Regelungen und der zu beachtenden Standards. Sie gehen dabei aber auch auf Haftungsfragen und weitere in der Praxis bedeutsame Anwenderfragen ein. <<