BLOCKCHAIN™ IN HEALTHCARE TODAY

VOM TEILEN ZUM VERKAUFEN: HERAUSFORDERUNGEN UND CHANCEN BEIM AUFBAU EINES DIGITALEN GESUNDHEITSDATENMARKTPLATZES MIT BLOCKCHAIN-TECHNOLOGIEN

Mohamed A. Maher, MBA[1,2*] und Imtiaz A. Khan, PhD[(1)]

[1]Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, Vereinigtes Königreich; [2]Balsamee LTD, Cardiff, Vereinigtes Königreich

Zusammenfassung

Während der COVID-19-Pandemie haben wir erlebt, wie die gemeinsame Nutzung biologischer und biomedizinischer Daten Forschern, Medizinern und politischen Entscheidungsträgern die Bekämpfung der Pandemie auf globaler Ebene erleichtert hat. Trotz der zunehmenden Nutzung elektronischer Gesundheitsakten (EHR) durch Ärzte und tragbarer digitaler Geräte durch Privatpersonen bleiben 80 % der Gesundheits- und medizinischen Daten ungenutzt, was für die Arbeit von Forschern und Ärzten nur einen geringen Mehrwert bedeutet. Gesetzliche Einschränkungen im Zusammenhang mit der gemeinsamen Nutzung von Gesundheitsdaten, der zentralisierte, siloartige Aufbau herkömmlicher Datenverwaltungssysteme und vor allem fehlende Anreizmodelle werden als Engpässe für die gemeinsame Nutzung von Gesundheitsdaten angesehen.

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (GDPR) der Europäischen Union (EU) und der Entwicklung von Technologien wie Blockchain und Distributed-Ledger-Technologien (DLT) ist es nun möglich, ein neues Paradigma für die gemeinsame Nutzung von Daten zu schaffen, indem das Anreizmodell von der derzeitigen autoritativen oder altruistischen Form zu einem gemeinsamen Wirtschaftsmodell geändert wird, bei dem finanzielle Anreize die Hauptantriebskraft für die gemeinsame Nutzung von Daten sein werden. Dies kann durch die Einrichtung eines digitalen Marktplatzes für Gesundheitsdaten (DHDM) erreicht werden.

In diesem Artikel werden technische Modelle oder implementierte Frameworks vorgestellt, die Blockchain-ähnliche Technologien für Gesundheitsdaten nutzen. Wir versuchen, die verschiedenen technischen Herausforderungen zu verstehen und zu vergleichen, die mit der Implementierung und Optimierung des in diesen Artikeln beschriebenen DHDM-Betriebs verbunden sind. Wir untersuchen auch die rechtlichen Beschränkungen im Kontext der EU und anderer Länder wie den USA, um die Compliance-Anforderungen für einen solchen Marktplatz zu erfüllen. Zu guter Letzt überprüfen wir Arbeiten, die die kurz-, mittel- und langfristigen sozioökonomischen Auswirkungen eines solchen Marktplatzes auf eine Vielzahl von Interessengruppen untersucht haben.

Stichworte: *Blockchain*; *EHR*; *Marktplatz*; *GDPR*; *allgemeine Datenschutzverordnung*; *Anreize*

Abschnitt: Narrative/Systematische Übersichten/Meta-Analysen

Eingereicht am: 22 September 2021; Überarbeitet: 27 September 2021; Angenommen: 30. Dezember 2021; Veröffentlicht: 28. Januar 2022

Seit der Einführung des digitalen Gesundheitswesens hatten die Entwickler von Informations- und Kommunikationstechnologien (IKT) den Eindruck, dass der Einsatz digitaler Technologie bei der Handhabung und Verarbeitung von Gesundheitsinformationen eine Fülle von Daten generieren wird, die die Gesundheitsbranche verändern können. Durch die Einspeisung dieser Daten in Algorithmen des maschinellen Lernens werden wir in der Lage sein, die medizinische Praxis zu entschlacken und neue Diagnose- und Behandlungsverfahren vorzuschlagen. Projekte wie DeepMind Health sind ein aktuelles Beispiel, bei dem ein in London ansässiges Unternehmen für künstliche Intelligenz, das zu Alphabet gehört, mobile App-Streams (1) entwickelt hat, die die EHR-Daten des Londoner Royal Free Hospital Daten des Londoner Royal-Free-Krankenhauses zur Vorhersage und Identifizierung von Patienten, die kurz vor einer akuten Nierenschädigung stehen - eine Erkrankung, die im Vereinigten Königreich jedes Jahr zu 100 000 Todesfällen führt (2). Darüber hinaus haben Portale wie Patients-LikeMe (3), über die Patienten mit ähnlichen Erkrankungen und/oder Problemen Informationen über ihre Behandlungen austauschen können, nachweislich Vorteile für ihre Nutzer (4, 5).

Als diese Projekte begannen, den Wert der gemeinsamen Nutzung von Daten zu zeigen, hat die Allgemeine Datenschutzverordnung (GDPR) (6) der Europäischen Union (EU), die 2018 eingeführt wurde, das Paradigma der gemeinsamen Nutzung und Verwendung von Patientendaten grundlegend verändert, indem sie das Eigentum und die Verantwortung neu positioniert

*Korrespondenz: Mohamed A. Maher. Email:m.maher2@outlook.cardiffmet.ac.uk ; mohamed.maher@balsamee.co.uk

Citation: Blockchain in Healthcare Today 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

Tabelle 1. Die allgemeine Datenschutzverordnung der EU hat das Paradigma der gemeinsamen Nutzung von Patientendaten grundlegend verändert, indem sie das Eigentum und die Verantwortung für medizinische Daten von den Dienstleistern auf den Patienten überträgt und ihm die folgenden Rechte einräumt (6)

Allgemeine Datenschutzverordnung	Definiert
GDPR Artikel 12 und 13	Das Recht, informiert zu werden • Das Recht des Einzelnen, über die Erhebung und Verwendung seiner Daten informiert zu werden.
GDPR Artikel 15	Das Recht auf Auskunft: • Einzelpersonen haben das Recht, auf ihre Daten zuzugreifen.
GDPR Artikel 16	Das Recht auf Berichtigung: • Personen haben das Recht, unrichtige personenbezogene Daten zu ändern oder zu vervollständigen, wenn diese unvollständig waren.
GDPR Artikel 17	Das Recht auf Löschung: • Das Recht des Einzelnen, personenbezogene Daten löschen zu lassen, auch "Recht auf Vergessenwerden" genannt.
GDRP Art 18	Das Recht auf Einschränkung der Verarbeitung: • Das Recht des Einzelnen, die Einschränkung oder Löschung seiner Daten zu verlangen.
GDPR Artikel 20	Das Recht auf Datenübertragbarkeit • Ermöglicht es Personen, ihre Daten einfach und sicher von einem IT-System in ein anderes zu übertragen, zu verschieben, zu kopieren oder zu senden, ohne dass die Verwendbarkeit der Daten beeinträchtigt wird.
GDPR Artikel 21	Das Recht auf Widerspruch: • Einzelpersonen haben das Recht, der Verarbeitung ihrer Daten unter bestimmten Umständen zu widersprechen.
GDPR Artikel 22	Rechte in Bezug auf automatisierte Entscheidungsfindung und Profiling: • Regeln zum Schutz des Einzelnen, wenn eine Organisation eine automatisierte Entscheidungsfindung durchführt, die erhebliche Auswirkungen auf ihn hat

von medizinischen Daten vom Diensteanbieter an den Patienten, zusammen mit der Gewährung der folgenden Rechte, wie in Tabelle 1 aufgeführt.

Hätte DeepMind nicht vor der Einführung der Datenschutz-Grundverordnung (DSGVO) begonnen oder wäre PatientsLikeMe innerhalb des Europäischen Wirtschaftsraums (EWR) angesiedelt gewesen, hätte keines der oben genannten Projekte überhaupt gestartet werden können. Es ist nun offensichtlicher, dass die Daten einen einzigen Eigentümer und Pförtner in Bezug auf die Zugangs- und Verteilungsrechte haben. Selbst in anonymer Form hat nur der Patient das Recht, Zugang zu seinen Daten zu gewähren und die Informationen so zu nutzen, dass alle davon profitieren. Ironischerweise haben die Patienten den Wert dieses neuen Eigentumsrechts noch nicht erkannt und wissen nicht, wie sie es verwalten sollen. Das liegt daran, dass es keine direkten Vorteile für sie gibt und auch keine indirekten Vorteile, die nicht deutlich genug sind, um die berechtigte Sorge vor einem Datenverlust und der damit verbundenen Gefährdung der Privatsphäre zu überwinden. Daher gilt es, einen neuen Ansatz und neue Instrumente zu finden, die ein Gleichgewicht zwischen dem Schutz der Privatsphäre des Einzelnen und dem transparenten Datenzugang zu Forschungszwecken herstellen (7).

Dieser Paradigmenwechsel, den die Datenschutz-Grundverordnung den Dienstleistern auferlegt, bietet auch Möglichkeiten für Einzelpersonen, ihre medizinischen Daten zu Geld zu machen, indem sie sie an medizinische Forscher oder Technologieunternehmen verkaufen. Ähnlich wie Airbnb, das es Einzelpersonen ermöglichte, ihre freien Unterkünfte zu Geld zu machen, können Patienten mit ihren neuen Eigentums- und anderen Rechten, die ihnen durch die Datenschutz-Grundverordnung verliehen wurden, nun ihre persönlichen Gesundheitsdaten über einen "Marktplatz für digitale Gesundheitsdaten" (DHDM) unter Verwendung eines gemeinsamen Wirtschaftsmodells zu Geld machen. Abbildung 1 veranschaulicht den Arbeitsablauf des DHDM. Bei der derzeitigen zentralisierten Datenverwaltung, bei der die elektronischen Patientenakten auf verschiedene Dienste verteilt sind, ist es jedoch so, dass

Bei Anbietern, bei denen die Vorschriften für verschiedene Organisationen und geografische Zuständigkeitsbereiche unterschiedlich sind, ist es schwierig, den Zugang und die Verwaltung zu regeln, insbesondere die Mikrotransaktionen in einer solchen verteilten Umgebung. In diesem Zusammenhang werden die Blockchain und die damit verbundenen intelligenten Verträge als eine bahnbrechende Technologie angesehen, die über eine eingebaute verteilte Architektur und die Fähigkeit verfügt, die Verwaltung von Informationen auf dezentralisierte Weise für verschiedene Arten von transaktionsbasierten digitalen Dienstleistungen zu verwalten.

Der Rest des Papiers ist wie folgt gegliedert: Zunächst wurden 36 Arbeiten zu den technischen Herausforderungen untersucht, wobei der Schwerpunkt auf drei Bereichen lag: Dateneigentum und Zugangskontrolle, Dateninteroperabilität und Datensicherheit. Anschließend wurden sieben Beiträge zu rechtlichen Fragen und schließlich neun Beiträge zu sozioökonomischen Fragen untersucht.

TECHNISCHE HERAUSFORDERUNGEN

DATENEIGENTUM UND ZUGANGSKONTROLLE

Wer ist Eigentümer der Gesundheitsdaten? Eine Frage, die seit jeher fasziniert und aus technischer, rechtlicher und philosophischer Sicht für Debatten sorgt. Kostkova et al. haben sich mit diesem Thema auseinandergesetzt und die Frage gestellt, ob Gesundheitsdaten für die Forschung freigegeben werden sollten, um ein Gleichgewicht zwischen der Privatsphäre des Einzelnen und dem Wert der datengestützten Forschung für das Leben von Millionen Menschen auf der ganzen Welt herzustellen (7). Abschließend forderten die Autoren die politischen Entscheidungsträger auf internationaler Ebene auf, einen Rechtsrahmen zu entwickeln, der personenbezogene Daten schützt, die geschäftliche Verwertung einschränkt und gleichzeitig die Nutzung von Daten für die Forschung und die kommerzielle Nutzung ermöglicht.

Bei der Entwicklung von Blockchain-basierten Zugangskontrollinstrumenten und -modellen wurde bereits viel Arbeit geleistet,

Zitat: Blockchain im Gesundheitswesen heute 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

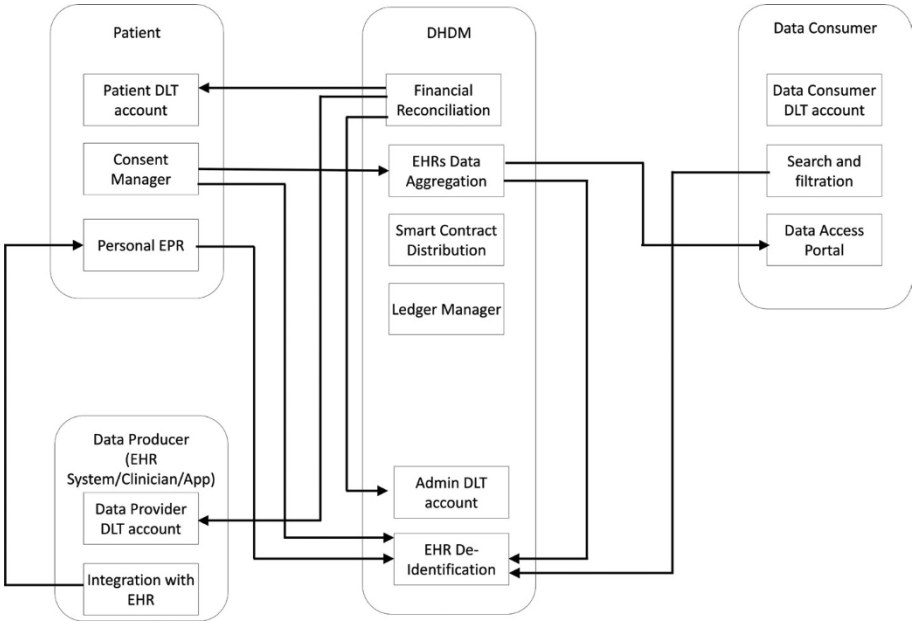

Abbildung 1. Vier Schnittstellen des Arbeitsablaufs des DHDM: Über die Patientenschnittstelle (oben links) richtet der Patient seine Konten ein, vervollständigt seine elektronische Gesundheitsakte (EHR) und verwaltet die Zugangskontrolle, indem er seine Zustimmung zur Weitergabe seiner Daten an Forscher seiner Wahl erteilt. Über die Schnittstelle für Datenproduzenten (unten links) können Pflegedienstleister und andere Datenproduzenten ihre Konten anlegen und die Verknüpfung von Patienten mit ihren lokalen Dateien über das Informationssystem des Pflegedienstleisters verwalten. Forscher richten ihre Konten ein, suchen nach Datensätzen, beantragen den Zugang zu Daten und zahlen für die Daten, auf die sie zugreifen, über die Schnittstelle für Datenkonsumenten (oben rechts). Die Back-End-Verwaltung des Marktplatzes wird über die DHDM-Schnittstelle, EPR (elektronische Patientenakte) und DLT (Distributed Ledger Technologies) erfolgen.

die den Patienten in den Fahrersitz setzt und ihm die volle Kontrolle über die Gewährung oder Verweigerung des Zugriffs auf Teile oder die Gesamtheit seines EHR gibt. In den meisten Studien wurde versucht, dem Patienten diese Kontrolle aus klinischen und betrieblichen Gründen zu übertragen. Dieselben vorgeschlagenen Modelle können jedoch auch für die Datenkontrolle aus Sicht der Vermögensverwaltung von Nutzen sein. Bahar et al. bieten eine spezifische Literaturübersicht, die den Großteil der Arbeiten in diesem Bereich abdeckt. In dieser Übersicht haben die Autoren vor allem Arbeiten zur Verwaltung digitaler Identitätsdatensätze und zur Selbstsouveränität von EHR-Daten behandelt und diskutiert (8). Sie erstellten eine Liste von Lösungen für soziale Daten, die mit Ethereum-Smart Contracts implementiert wurden, und verglichen sie auf der Grundlage von Anreizen, Datenmarkt, PHR, dezentraler Vermögensverfolgung, Web-/Mobilanwendungen, IoT, EHR-Kompatibilität/Interoperabilität und Proof-of-Concept-Implementierung.

Wie bereits erwähnt, stellte Nguyen ein Modell für eine sichere Zugangskontrolle für elektronische Patientenakten vor, die in einer InterPlanatery File System (IPFS)-Konfiguration gespeichert sind (9). Das Modell schlug einen auf einem intelligenten Vertrag basierenden EHR-Manager vor, der Zugriffsanfragen und Datentransaktionen verwaltet und dem Patienten eine auf einer Blockchain-Schnittstelle basierende mobile App zur Verfügung stellt, mit der er seine Rechte zur Kontrolle des Zugriffs ausüben kann. Obwohl dieses Modell eine faszinierende Lösung sein könnte, um die Deen-tralisierung von EHR anzugehen und gleichzeitig sichere und nachvollziehbare Tools für die Datenzugriffskontrolle und den Eingabeprüfpfad bereitzustellen, zeigten alle praktischen Versuche dieser Konfiguration sehr hohe Latenzzeiten im Betrieb. Rifi et al. befassten sich mit demselben Konzept der Verwendung von Blockchain zur Verwaltung von Transaktionen in EHR(10). Die Autoren befassten sich mit der Kontrolle von Daten, die von persönlichen medizinischen Geräten und Sensoren erfasst wurden, und schlugen eine DApp eHealth Blockchain vor, um Lese- und Schreibvorgänge in der EHR-Datenbank zu kontrollieren, die sich in der Cloud oder im IPFS befindet.

Nortey et al. bieten ein weiteres Beispiel für einen Blockchain-Rahmenvorschlag für das EHR-Datenmanagement, indem sie Patienten die Kontrolle darüber geben, wer auf ihre EHRs zugreift (11). Die Autoren führten einen Channeling-Mechanismus ein, der sicherstellt, dass die Patienten den Zugriff auf ihre Daten durch Stellen innerhalb des verteilten Netzwerks genehmigen. Andere verfolgen einen anderen Ansatz, bei dem die Autoren ein Zustimmungsmodell für die gemeinsame Nutzung von Daten entwickeln wollten (12, 13). Sie schlugen einen Transaktionsworkflow vor und erstellten Ethereum-Smart Contracts auf der Grundlage von LUCE (14). Eine Blockchain-Lösung für die Überwachung der Datenlizenzen AccoUntability und ComplianceE und bauten darauf aufbauend ein zustimmungsbasiertes Architekturmodell und implementierten es auf D1NAMO-Datensätzen (15) von 29 Teilnehmern. Darüber hinaus wird ein halbdezentraler Ansatz vorgeschlagen, bei dem das Blockchain-Netzwerk für die einzelnen Aufträge auf mehrere Organisationen verteilt ist (13). Die Zugangskontrollregeln werden in Smart Contracts kodiert, die über das Blockchain-Netzwerk verteilt sind. Denselben Weg beschreiten Guo et al., schlagen aber eine hybride Blockchain-Edge-Architektur vor (16).

EHR-Daten werden auf Edge-Knoten gespeichert, die auf Attributen basierende Zugangskontrollrichtlinien auferlegen. Die Autoren verwendeten die Hyperledger Composer Fabric-Blockchain, die mit intelligenten Verträgen und Zugriffskontrolllisten programmiert wurde, um die Leistung zu bewerten, indem sie die Transaktionsverarbeitung und die Reaktionszeit gegen unbefugte Wiederabrufversuche maßen. Die Experimente haben gezeigt, dass das System Ergebnisse in Millisekunden liefert, wodurch es sich für die Einbindung in Echtzeit- und sichere EHR-Datenzugriffskontrollsysteme eignet. Das wichtigste Ergebnis ist, dass die Implementierung in allen Versuchen über die verschiedenen Größen hinweg konsistent war. Dieses Ergebnis deutet darauf hin, dass diese Architektur das am besten skalierbare Modell für die EHR-Zustimmungsverwaltung sein könnte.

Andere haben ebenfalls attributbasierte Blockchain-Signaturmodelle entwickelt, um die Vertraulichkeit, Integrität und Authentifizierung von Patientendaten zu gewährleisten und gleichzeitig den Datenaustausch zwischen den Beteiligten zu unterstützen (17-20). Seol et al. bereiteten ihre Studie so vor, dass das Modell aus der Sicht verschiedener Entscheidungsträger betrachtet wird, und bauten ihr Modell in zwei Stufen auf (Zugangskontrolle und digitale Signatur), wobei Smart Contracts jede Regel der Reihe nach durchsetzen können
(20). Yang et al. (21) bauten auf dem attributbasierten Modell von Wang et al. (17) auf und erstellten eine Demonstration zur Messung der Leistung, insbesondere der Verschlüsselungs- und Suchzeit, und wiesen nach, dass die Zeit unabhängig von der Anzahl der Attribute ist.

Guang et al. stellten ein Modell vor, bei dem die Kontrolle der EHR-Transaktionen vom Leistungserbringer abhängt (22). Interessant an diesem Modell ist, dass die Autoren eine Architektur vorschlagen, die die Blockchain-Technologie mit dem bestehenden EHR-System implementiert. In Anbetracht der Tatsache, dass ein EHR-System über ein System mit Mehrfachzugriff verfügen muss und dass Gesundheitsdienstleister gemäß dem Prozessdesign der Autoren individuell Datensätze pflegen, wurden in dem Modell den Dienstleistern primäre Verantwortlichkeiten zugewiesen, darunter das Erstellen, Überprüfen und Anhängen neuer Blöcke. Das Design verwendet intelligente Verträge, wobei diese Architektur unabhängig von bestimmten Blockchain-Plattformen ist und ihre Variationen potenziell auf jedes EHR-System angewendet werden können.

DATENINTEROPERABILITÄT

Die Interoperabilität von Daten ist eine der größten Herausforderungen für die Gesundheitsinformatik, da die Daten sehr heterogen sind und die verschiedenen EHR-Systeme nicht standardisiert sind.

MedRec (23) war die Grundlage, die viele Blockchain-Forscher für den sicheren Austausch/Transfer von Daten aus verteilten Systemen in eine einheitliche Patienten-EHR nutzten. MedRec hat ein industrielles Whitepaper herausgegeben, in dem ein Open-Source-Blockchain-Modell für die sichere Übertragung von EHR-Dateneinträgen von Systemen von Gesundheitsdienstleistern zu Patientenknoten und umgekehrt erläutert wird. Ziel ist es, die in einer lokalen Patientenakte angelegten Daten in einer beliebigen Anzahl von Krankenhäusern sicher zu sammeln Krankenhäusern erstellt wurden, sicher zu sammeln und in einer konsolidierten Datei unter der Kontrolle des Patienten zusammenzufassen. Die Tatsache, dass das Modell als Open Source zur Verfügung steht, hat viele Forscher dazu ermutigt, es in Versuchsimplementierungen zu verwenden, und auch die Industrie wurde ermutigt, ihr Modell zu übernehmen. Dieses Whitepaper-Modell ist eines der wenigen Blockchain-Modelle im Gesundheitswesen, die bereits umgesetzt wurden. Die Arbeit von Yang et al. ist ein Beispiel für einen akademischen Aufbau auf dem MedRec-Framework (24).

MedShare (25) ist eines der ersten vorgeschlagenen Modelle zur Kontrolle des EHR-Datenaustauschs mit Blockchain. Die Autoren schlugen zunächst eine Verarbeitungsebene zur Verwaltung des Informationsaustauschs zwischen den bestehenden Cloud-Infrastrukturen der Gesundheitsdienstleister vor. Die Simulation zeigte jedoch, dass die Latenzzeit relativ hoch ist und mit zunehmender Nutzerzahl steigt. MedBlock (26) ist ein ähnliches Modell. Hier schlugen die Autoren vor, nicht-traditionelle Blockchain-Einheiten wie Authentifizierungsdienstleister und Zertifizierungsstellen zu verwenden, um Mittel zur Ausstellung von Identitäten und zur Sicherung des kryptografischen Materials bereitzustellen, das zur Verschlüsselung aller Daten auf der Blockchain verwendet wird. Obwohl MedBloc auf die IT-Infrastruktur des neuseeländischen Gesundheitswesens zugeschnitten ist, konnten die Forscher keine Besonderheiten feststellen, die eine Implementierung in anderen Ländern behindern würden.

Xiaoguang et al. (27) stellten eine aktuelle Anpassung des MedRec-Modells vor. Diesmal bestand das Ziel darin, ein manipulationssicheres Schema für die gemeinsame Nutzung medizinischer Daten bereitzustellen und zu implementieren - einen delegierten Zustandsnachweismechanismus, der als leichtgewichtiger und zuverlässiger Konsensmechanismus fungiert. Die Analyseergebnisse haben gezeigt, dass das System zufriedenstellend ist und geringe Rechen- und Kommunikationskosten verursacht. Dieses System passt perfekt in den Bereich der Datenmarktplatzforschung, mit der Ausnahme, dass es sich um ein Nicht-Bezahlungssystem handelt.

Zhuang et al. (28) haben einen anderen Rahmen geschaffen, der sich vom MedRec-Modell unterscheidet. Obwohl es auf denselben Zweck abzielt, nämlich den patientenorientierten Austausch von Gesundheitsinformationen, konzentrierte sich dieser Rahmen auf die Befähigung der Patienten zur Kontrolle durch Werkzeuge. Es wurde eine DApp für den Patienten erstellt, in der er Parameter in den intelligenten Verträgen anpassen kann, indem er Berechtigungen erteilt, Berührungspunkte zulässt und Zugriffsanfragen durch Verknüpfungs- und Anforderungsmodule verwaltet. Dieses Framework bietet praktische Eigenschaften für das System: einen Blockchain-Adapter, der für die Kommunikation, das Senden/Empfangen von Gesundheitsdaten und die Erstellung einer grafischen Präsentation für Benutzer mit einfacher Interaktion eingerichtet wurde, zwei Sicherheitsebenen, um sicherzustellen, dass nur autorisierte Smart-Contract-Funktionen ausgeführt werden, um das Risiko einer Datenverletzung zu minimieren, Hashing für die Datenkonsistenz, Datensegmentierung, die eine teilweise Datenfreigabe ermöglicht, und die Auswahl von Berührungspunkten für Ärzte, um das relevante Datensegment für das Fachgebiet auszuwählen.

DATENSICHERHEIT

Die De-Identifizierung der Patientenakte ist von grundlegender Bedeutung, um den Datenschutz und die Sicherheit zu gewährleisten. Dies muss an zwei Fronten

Zitat: Blockchain im Gesundheitswesen heute 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

parallel angegangen werden. Zum einen müssen die identifizierbaren Parameter des Patienten von den klinischen Daten getrennt werden. Die Trennung muss in den Anwendungs-, Kommunikations- und Speicherschichten erfolgen. Die andere betrifft die klinischen Daten selbst. So enthält beispielsweise jedes DICOM-Bild (Digital Imaging and Communications in Medicine) von vornherein identifizierbare Daten wie den Namen des Patienten, sein Geburtsdatum und die überweisende Stelle. Daher muss eine De-Identifizierung und Anonymisierung vorgenommen werden, bevor die Daten in ein unveränderliches Blockchain-Netzwerk eingestellt werden.

In mehreren Forschungsarbeiten wurde das Modell der Speicherung von EHR in einer Blockchain (29, 30) angenommen. Dieser Ansatz wurde im Laufe der Zeit aus technischen und rechtlichen Gründen verworfen. Technisch gesehen lag dies an der Größe des Blocks und der Kapazität, eine große Menge an Daten in einer Kette zu speichern, die über viele Knoten repliziert wird. Rechtlich gesehen erfüllt sie kaum die Anforderungen von Artikel 17 (6) der Datenschutz-Grundverordnung (DSGVO) bezüglich des Rechts auf Vergessenwerden, da es nicht möglich ist, einen Datensatz zu ändern oder zu löschen, sobald er in der Kette gespeichert ist. Eine der Studien, die den EHR on the chain-Ansatz gewählt haben, ist die von Tang et al. (30). Natürlich wäre sie für diese Untersuchung nicht relevant gewesen. Die Autoren schlagen jedoch ein interessantes Modell für die Authentifizierung vor, indem sie ein identitätsbasiertes Signaturschema mit mehreren Instanzen für das Blockchain-basierte EHR-System de-signieren. Das Schema bietet effiziente Signatur- und Verifizierungsalgorithmen.

In zahlreichen Veröffentlichungen wurde vorgeschlagen, was zumeist als Cloud-gestützte EHR-Blockchain-Sicherheit bezeichnet wird. Wang et al. (31) stellten ein Cloud-gestütztes sicheres und datenschutzfreundliches EHR-Sharing-Protokoll vor, das auf einer Konsortialblockchain basiert. Mit anderen Worten: Die EHR werden in der Cloud gespeichert, während die EHR-Indizes (Protokollierung) in der Blockchain aufbewahrt werden. In ihrer Arbeit schlugen die Autoren ein Blockchain-basiertes EHR-Sharing-Schema mit konjunktiver Verschlüsselung mit Schlüsselwortsuche und bedingter Proxy-Wiederverschlüsselung vor, um die Datensicherheit und den Schutz der Privatsphäre beim Datenaustausch zwischen verschiedenen medizinischen Organisationen zu gewährleisten.

Darüber hinaus stellten Kim et al. (32) ein Modell und einen simulierten Versuch für ein sicheres Protokoll für ein Cloud-gestütztes EHR-System mit Blockchain vor. Sie demonstrierten die Sicherheit des vorgeschlagenen Systems gegen Man-in-the-Middle- (MITM) und Replay-Angriffe mit Hilfe der Simulation der automatisierten Validierung von Internet-Sicherheitsprotokollen und -anwendungen (AVISPA). In ähnlicher Weise haben Vora et al. (33) ein Modell vor, das Blockchain nutzt, um die Sicherheit von EHR-Datenbanken zu verbessern. Hier setzten die Autoren auf intelligente Verträge von Ethereum, um Zustimmungen, Berechtigungen, Klassifizierungen und Dienste zu verwalten. Das Modell sieht vielversprechend aus und schlägt sechs Algorithmen vor, um die Transaktionssicherheit und den Schutz der Privatsphäre zu gewährleisten. Dennoch hat das Modell gezeigt, dass es unmöglich wäre, alle Informationen vollständig zu verbergen und ein zugängliches und interoperables System zu erhalten. Durch die Verwendung von intelligenten Verträgen zur Trennung von Informationen bietet das vorgeschlagene Modell jedoch immer noch einen erheblichen Schutz der Privatsphäre und der Datenintegrität. Darüber hinaus kann man mit einem intelligenten Vertrag den Grad des Informationszugriffs bestimmen, aber bei einer öffentlichen Blockchain ist die Integration mit dem intelligenten Vertrag schwierig und nicht praktikabel.

Obwohl es sich um eine ungarische Studie handelt, haben Magyar et al. (34) ein auf Blockchain-Signaturen basierendes Modell vor, das die amerikanischen Health Insurance Portability and Accountability Act (HIPAA)-Vorschriften aufgreift. Das Modell verwendet intelligente Verträge und die Innovationen der Kryptographieindustrie, blinde Signaturen, Mehrfachsignaturen, hierarchische Signaturen und andere Sicherheitsverfahren, die den Zugang zu den Informationen gewährleisten. Gleichzeitig kann auf dem Weg dorthin niemand offene Textdaten lesen.

In den oben genannten Studien wurde das EHR als eine einzige Datenbank betrachtet, die entweder lokal oder in der Cloud gespeichert ist, und es wurden verschiedene Ansätze für die Verwendung von Blockchain zum sicheren Hinzufügen, Löschen und Ändern von Einträgen im EHR erörtert. Einer der Hauptgründe, warum Blockchain als potenzielle Technologie zur Erhöhung der Robustheit von EHR und der damit verbundenen Transaktionen identifiziert wurde, ist jedoch, dass EHRs von Natur aus dezentralisiert sind. Ein typischer Patient hat verschiedene EHRs in der Primär-, Sekundär- und Tertiärversorgung. Allein auf diesen drei Ebenen können im Laufe des Lebens eines Patienten Zehntausende von Datensätzen anfallen, die zu einer vollständigen Patienten-EHR zusammengeführt werden müssen.

Im Gegensatz dazu erörterten Ayesha et al. (35) eine alternative Architektur, die ebenfalls das Prinzip der Speicherung von EHR in der Cloud in Frage stellt. Die Autoren schlugen einen Rahmen vor, der Maßnahmen vorsieht, um sicherzustellen, dass das System das Problem der Datenspeicherung angeht, da es den Off-Chain-Speichermechanismus des IPFS nutzt. In ihrem Beitrag wird die Leistung der verschiedenen Topologien in Bezug auf Ausführungszeit, Durchsatz und Latenzzeit bewertet. Es wird ein Rahmenwerk vorgeschlagen, das eine Kombination aus sicherer Datenspeicherung und Blockchain-Zugriffsregeln für EHRs darstellt.

Ein weiteres Modell von Nguyen et al. (9) zielt auf eine sichere Zugangskontrolle für EHR ab und schlägt auch eine IPFS-Konfiguration (InterPlanetary File System) für die EHR-Speicherung vor. Die Idee besteht darin, bei jedem Leistungserbringer einen IPFS-Knoten zu bilden und einen EHR-Manager (Server) zu schaffen, der die Rolle übernimmt, die ursprünglich die Cloud-EHR gespielt hat. Das Modell verwendet dann die Blockchain, um den Transaktionspfad zu indizieren und mit dem EHR-Manager als Cloud-Service umzugehen. Intern ist der EHR-Manager dafür verantwortlich, die Patientenakte von allen IPFS-Knoten auf Anfrage zu aggregieren und weitere Knoten zu erstellen, wenn der Patient zwischen verschiedenen Leistungserbringern wechselt. Das Modell schlägt vor, dass der EHR-Manager selbst auf einem intelligenten Vertrag basiert, um Anfragen für den Zugang und Datentransaktionen zu verwalten, während dem Patienten eine mobile App mit Blockchain-Schnittstelle zur Verfügung gestellt wird, mit der er seine Rechte zur Kontrolle des Zugangs ausüben kann.

RECHTLICHE UND ETHISCHE HERAUSFORDERUNGEN

Die rechtliche Auseinandersetzung beginnt immer mit der Frage, wer Eigentümer der Daten ist. Das Eigentum wird oft mit dem Zugang verwechselt. Kostkova et al. (7) haben versucht, zwischen Dateneigentum und Zugangsrecht zu unterscheiden und neue, ausgewogene Ansätze zu finden, um die Interessen der Unternehmen zu befriedigen und die Öffentlichkeit aktiv einzubeziehen und gleichzeitig einen transparenten Datenzugang für Forschungszwecke und groß angelegte Integrationen unter Wahrung der Privatsphäre des Einzelnen zu gewährleisten. Eine Studie von Castillo et al. (36) versucht, Hindernisse für den Informationsaustausch im Rahmen des Health Information Technology for Economic and Clin-ical Health (HITECH) Act zu ermitteln, um ein effizienteres und effektiveres Gesundheitssystem zu schaffen. Die Ergebnisse deuten darauf hin, dass ein Krankenhaus mit größerer Wahrscheinlichkeit klinische Daten mit Krankenhäusern außerhalb seines Gesundheitssystems austauscht, wenn das andere Krankenhaus denselben EHR-Anbieter verwendet. Die Autoren betonen die Bedeutung der EHR-Anbieterneutralität und daher die Bedeutung der Interoperabilität von EHR-Systemen.

In einer kritischen Übersicht von Yadav et al. (37) über das Mining klinischer Daten aus der elektronischen Patientenakte untersuchen, diskutieren und präsentieren die Autoren neue Erkenntnisse darüber, wie Data-Mining-Techniken für die elektronische Patientenakte genutzt wurden. In dieser systematischen Übersichtsarbeit erörtern sie die Anwendung, das Studiendesign und die Data-Mining-Methodik zahlreicher Initiativen zum klinischen Data-Mining. Darüber hinaus erörtern die Autoren die Hindernisse, die einer weit verbreiteten Nutzung von Data Mining in der klinischen Praxis entgegenstehen. Der Bericht selbst geht nicht auf die rechtlichen und regulatorischen Anforderungen des DHDM ein. Sie befasst sich jedoch mit den ethischen Aspekten und der Einhaltung von Vorschriften bei der Data-Mining-Forschung (KI, ML usw.), die durch das DHDM erleichtert wird.

Mello Michellem präsentierte ein umfassendes Handbuch zu den Hindernissen für das Wachstum des Gesundheitsdatenaustauschs im Rahmen der nordamerikanischen Gesetze (38). Die Autoren analysierten die bundes- und einzelstaatlichen Datenschutzgesetze und -vorschriften für Gesundheitsdaten sowie sekundäre Materialien und kamen zu dem Schluss, dass einige kritische rechtliche Hindernisse fortbestehen, dass aber viele Probleme, die von den Leistungserbringern als Hindernisse wahrgenommen werden, eher illusorisch sind. Die Autoren betonten, dass die Gesundheitsdienstleister die Datenschutzgesetze als Hindernis für den elektronischen Austausch von Gesundheitsdaten wahrnehmen, und machten dafür verschiedene Faktoren verantwortlich, wie z. B. die Uneinheitlichkeit der Gesetze über die Einwilligung der Patienten, die Sonderbehandlung sensibler Gesundheitsdaten und die fehlende Einführung eines einheitlichen Patientenindexierungssystems.

In einem technisch-regulatorischen Dokument werden die Unterschiede zwischen den Standards für die Übermittlung von Gesundheitsdaten (ISO/IEEE 11073, IHE PCD-01 und HL7 DoF) verglichen und Vorschläge für die am besten geeignete Umgebung zur Verwendung der einzelnen Standards gemacht (39). Die Autoren kommen zu dem Schluss, dass ISO/IEEE 11073-Nachrichten keine Patienteninformationen enthalten können, dass IHE PCD-01-Nachrichten nur begrenzte Geräteinformationen enthalten und dass HL7 DoF in allen vier Parametern der Studie (menschliche Lesbarkeit, Erlernbarkeit, Implementierung und Erweiterbarkeit) die umfassendste Informationsabdeckung aufweist.

SOZIOÖKONOMISCHE HERAUSFORDERUNGEN

Der von Joseph Schumacher geprägte Begriff der "schöpferischen Zerstörung" erklärt, wie der Prozess der industriellen Umgestaltung die Wirtschaftsstruktur von innen heraus revolutioniert, indem die bestehende Struktur zerstört und gleichzeitig eine neue geschaffen wird (40). Bei disruptiven Technologien wie der Blockchain und in Branchen wie dem Gesundheitswesen ist die Struktur in Bezug auf die Beteiligung von Interessengruppen und wirtschaftliche Impulse äußerst kompliziert.

Das in einer Studie vorgestellte Modell ist zwar nicht medizinisch, aber (41) lieferte eine vielversprechende Marktplatz-Implementierung auf der Grundlage eines bestehenden Modells für einen Nutzfahrzeugdatenmarktplatz in Japan. ID-Link war ein erfolgreiches Modell, als die japanische Regierung den Aufbau einer Informationsinfrastruktur zur gemeinsamen Nutzung von Daten in verschiedenen Geschäftsbereichen initiierte. Einer dieser Bereiche war die gemeinsame Nutzung von Daten aus individuellen EHR. In ihrer Studie ersetzen die Autoren Kfz-Daten wie Geschwindigkeit, Zeit, Reichweite, Emissionen usw. durch medizinische Daten aus der elektronischen Patientenakte. In der Studie werden Einbindungsoptionen (Opt-In vs. Opt-Out), Zugriffskontrollprivilegien und die Standardisierung von Daten erörtert, insbesondere die Übernahme spezifischer Formate wie HL7 (das Papier schlug V2.5. vor, FHIR HL7-V3.0 ist jedoch derzeit weltweit weit verbreitet), WHO ICD-10 und SNOMED-CT als klinische Terminologiebibliothek. Das Papier bietet auch eine medizinische Anpassung an die au-tomotive ID-Link Prozess-Workflow in eine machbare sieben-Schritt-Modell von Patienten Zustimmung, Arzt Interaktion, ID-Check, kommerzielle Nutzung, Zahlung und Gewinnbeteiligung. ID-Link ist in vier architektonischen Schichten aufgebaut: Geschäfts-, Funktions-, Daten- und Technologieebene.

Guo et al. (42) kritisieren die Prozesse, die Innovatoren im Bereich der digitalen Gesundheit anwenden, um Ergebnisse für ihre Lösungen und Implementierungen zu erzielen. Die Autoren betonen auch, dass es bei digitalen Gesundheitslösungen an der Umsetzung mangelt und es daher nicht einfach ist, evidenzbasierte Ergebnisse zu erzielen. In der Studie wurden einige der wichtigsten Umsetzungen von Lösungen für die digitale Gesundheit anhand der Auswahl nicht ausschließlicher relevanter Regulierungsstandards und der von den Innovatoren bei der Bewertung ihrer Lösungen angewandten Methoden analysiert. Nichtsdestotrotz räumen die Autoren ein, dass die Innovatoren keine Barrieren schaffen und dass die Innovatoren in dem Paradoxon "keine Evidenz, keine Implementierung - keine Implementierung, keine Evidenz" in der digitalen Gesundheit feststecken. Die Autoren schlagen vor, dass Ansätze wie die simulationsbasierte Forschung qualitativ hochwertigere, kostengünstigere und zeitnähere Erkenntnisse liefern können.

Die Umfrage von Affinito et al. (43) zielt dagegen darauf ab, zu verstehen, welche digitalen Mittel Ärzte nutzen, um mit ihren Patienten in Kontakt zu treten, und welche Auswirkungen die Ärzte auf die klinischen Gesundheitsergebnisse wahrnehmen. Die Ergebnisse der Umfrage deuten darauf hin, dass die wichtigsten Erfolgsfaktoren für die Befähigung der Patienten zum Einsatz digitaler Hilfsmittel und die Verbesserung der Gesundheitsergebnisse die klinische Evidenz und die Beteiligung der tatsächlichen Nutzer (Patienten und Pflegekräfte) an der Gestaltung der digitalen Lösungen sind. Die Studie

Zitat: Blockchain im Gesundheitswesen heute 2022, **5**: 184 - http://dx.doi.org/10.30953/bhty.v5.184

kommt zu dem Schluss, dass der Einsatz digitaler Hilfsmittel die Eigenverantwortung der Patienten durchaus verbessern würde. Bislang gibt es jedoch keine Belege für eine Verbesserung der gesundheitlichen Ergebnisse.

Nachdem festgestellt wurde, dass es keine Belege dafür gibt, dass sich die Ergebnisse für die Patienten durch den Einsatz digitaler Hilfsmittel verbessern, führten Angeline und Sharon (44) eine Studie durch, um zu untersuchen, ob das Niveau der digitalen Kompetenz des Gesundheitspersonals dafür verantwortlich ist. Diese Studie zeigte, dass die Mehrheit des Personals Vertrauen in die Nutzung von IKT zeigte. Es versteht sich jedoch von selbst, dass der Standort der Studie (Australien) die Ergebnisse der Studie beeinflusst haben könnte und dass wir andere Ergebnisse in anderen Gebieten erwarten sollten. Electronic Health Records for Clinical Research EH-R4CR ist ein europäisches Projekt, das darauf abzielt, patientenorientierte Studien zu verbessern, indem eine Plattform entwickelt wird, die den Zugang zu bestehenden elektronischen Patientenakten ermöglicht (45), wodurch das Projekt dem DHDM-Forschungsprojekt sehr ähnlich ist. Es sieht jedoch keine Entschädigung der Patienten für die Nutzung ihrer EHR-Daten vor. Dupont et al. (46) ist eine Studie, in der die finanziellen Ergebnisse des Projekts untersucht werden. Die Studie verglich EHR4CR mit bestehenden Praktiken und kam zu dem Schluss, dass EHR4CR-Lösungen für die Hauptsponsoren klinischer Studien kostensparend zu sein scheinen. Die Ergebnisse der Studie deuten darauf hin, dass das Einsparungspotenzial mit einer breiteren Einführung von EHR4CR-Lösungen in Europa und darüber hinaus steigen würde. Die Ergebnisse deuten wiederum darauf hin, dass ein medizinischer Datenmarktplatz, auf dem Patienten den Zugang zu ihren EHR-Datensätzen zu ihrem eigenen Nutzen verkaufen können, auf lange Sicht Kosteneinsparungen bei industrielle und klinische Versuche.

Timo und Harri (47) haben in einem Beitrag versucht, ein Ecosystem Evaluation Framework (EEF) zu entwickeln, um die Überlebenschancen einer digitalen Geschäftsplattform zu verstehen. Die Autoren beschrieben das EEF-Modell anhand von sechs Parametern (die Plattform, das Problem, das die Plattform zu lösen versucht, den Zweck der Plattform, das Ökosystem, die durch die Plattform ermöglichten Transaktionen und das Ertragsmodell der Plattform). Die Autoren betonten die Wichtigkeit der Berücksichtigung des Vergütungsmodells, das perfekt zu den Zielen unserer Studie passt. Sie sehen in der Vernachlässigung der Anreizkomponente den Hauptgrund dafür, dass das regionale Gesundheitsinformationssystem RHIS in der finnischen Region Pirkanmaa, in der sie ihr Modell angewandt haben, keine kritische Masse erreicht hat.

Alina und Jose Luis (48) erörterten, was die Autoren einen FAIR-Marktplatz nannten. Sie stellten fest, dass die Daten auffindbar, zugänglich, interoperabel und wiederverwendbar sein müssen, woraus der Begriff FAIR entstand. Die Autoren stellten eine Architektur vor, die Schichten zur Erfassung von Informationen von Patienten, Leistungserbringern und anderen Plattformen wie EHR4CR umfasst.

Die Kreditwürdigkeit war schon immer die größte Hürde für die DHDM-Forschung. In fast allen Umfragen, Meinungsumfragen und sogar in freundschaftlichen Gesprächen wurde dieses Thema angesprochen. Die Leute fragen sich, ob sie durch das Projekt genauso bloßgestellt werden Kreditwürdigkeit mit ihren Finanzen zu tun hat. Die Menschen sind immer besorgt, dass ihnen Leistungen verweigert werden oder sie mehr für Leistungen zahlen müssen, die sie jetzt ohne nennenswerten Einfluss auf die Gesundheitshistorie erhalten, z. B. bei der Erneuerung einer Kfz-Versicherung. Sie befürchten höhere Prämien, wenn die Versicherung mehr Details über ihren Gesundheitszustand erfährt, oder, schlimmer noch, dass ihnen Leistungen verweigert werden, wenn sie den Zugang zu ihren Daten verweigern, wie es beim Kreditscore der Fall ist.

Die Architektur der Kreditwürdigkeitsprüfung ist jedoch ein perfektes Beispiel für die Zusammenführung von Daten und die genehmigte gemeinsame Nutzung aus einer technisch-gewerblichen Perspektive. Dumitru und Gatti (49) erörterten die Beschränkungen und Möglichkeiten im Zusammenhang mit der gemeinsamen Nutzung von Gesundheitsdaten und der Verwendung der Daten für die Kreditwürdigkeitsprüfung. Die Autoren haben eine Architektur für einen vertrauenswürdigen Datenmarktplatz vorgeschlagen, der als Wiegesystem im DHDM-Projekt sehr nützlich sein kann. Das Wiegesystem berechnet den Beitrag eines jeden EHR zu einem gesamten Datensatz. Es soll dazu dienen, die Zahlungen von medizinischen Forschern gerecht zwischen den Dateneigentümern aufzuteilen, und zwar in einer Weise, die Anreize für die EHR auf der Grundlage ihres Engagements für das Wohlergehen und ihre Verpflichtung, die EHR auf dem neuesten Stand zu halten, schafft.

Eine von Roman und Stefano (50) durchgeführte Studie ist ein praktisches Beispiel für die Nutzung des erfolgreichen Kreditscoring-Modells zur Berechnung der Gewichtung/des Wertes jedes EHR-Eintrags. Die Gewichtungskomponente ist von großem Wert für eine gerechte Verteilung des Reichtums zwischen den EHR-Eigentümern auf der Grundlage des Beitrags jedes Eintrags und jedes EHR in der Forschung, für die der Reichtum gezahlt wurde.

Die Studie von Ryuji (41) ist ein weiteres praktisches Beispiel, das dem DHDM-Forschungsprojekt zugute kommen könnte. Sie bietet ein praktikables Modell für den kommerziellen Austausch von Geldern gegen Daten, das auf bereits in der Automobilindustrie eingeführten Techniken aufbaut.

SCHLUSSFOLGERUNGEN

Obwohl Milliarden von Dollar ausgegeben werden, um die derzeitigen Systeme zur Verwaltung von Gesundheitsdaten effizienter zu machen, bleibt die gemeinsame Nutzung von Daten im Gesundheitssektor ein schwer erreichbares Ziel. Da die Datenschutz-Grundverordnung einen Paradigmenwechsel in Bezug auf Dateneigentümerschaft und -kontrolle zusammen mit Blockchain-ähnlichen Technologien eingeleitet hat, die die technologischen Möglichkeiten einer dezentralen Datenverwaltung bieten, ist es an der Zeit, das nicht mehr zeitgemäße Anreizmodell durch ein DHDM-ähnliches offenes Marktmodell zu ändern.

Auf der Grundlage dieses Überblicks ist es offensichtlich, dass Blockchain-basierte Lösungen wie MedRec (23) als separate Schicht implementiert und über Anwendungsprogrammierschnittstellen (APIs) in native Datenbanken integriert werden können, ohne die nativen Datenverwaltungssysteme und -kulturen zu beeinträchtigen, was dem Technologieanpassungsprozess definitiv zugute kommen wird. Da es sich um Open-Source-Lösungen handelt, werden MedRec-ähnliche Lösungen außerdem eine wichtige Rolle bei der sicheren Datenerfassung aus bestehenden Datenverwaltungssystemen spielen und

ein aggregiertes EHR unter der Kontrolle des Patienten. Intelligente Verträge und IPFS-/Wolkenspeichersysteme werden den Patienten die Möglichkeit geben, den Zugriff auf verschiedene Arten und die Dauer de-identifizierter Daten auf sichere Weise zu gewähren. Die Überprüfung zeigte verschiedene Vorschläge für den Datenzugang und die sichere gemeinsame Nutzung von Daten durch Datenproduzenten und -verbraucher. Es müssen jedoch noch weitere Studien über die Reproduktion digitaler Daten durchgeführt werden und darüber, wie die Rechte des Herstellers gesichert werden können, wenn der Verbraucher die Daten ohne seine Zustimmung reproduziert. Weitere Studien sind auch erforderlich, um herauszufinden, wie der Prozess der gemeinsamen Datennutzung mit unterschiedlichen Vorschriften in verschiedenen geografischen Zuständigkeitsbereichen und zu unterschiedlichen Zeiten angepasst werden kann.

Das auf der Sharing Economy basierende Anreizmodell, das für den DHDM-Kontext als am besten geeignet erachtet wird, muss ebenfalls eingehend evaluiert werden. Obwohl ein Unternehmen wie Airbnb nachweislich wirtschaftliche Vorteile sowohl für den Anbieter als auch für den Verbraucher hat, kann der Austausch persönlicher Gesundheitsdaten einen anderen sozialen und emotionalen Kontext haben als eine persönliche Unterkunft. Trotz dieser Bedenken ist es fast sicher, dass ein offener Markt den Wettbewerb um die Produktion und den Austausch hochwertiger Daten entsprechend der Verbrauchernachfrage fördern wird. Dies wiederum wird Forschern und Ärzten den Zugang zu Daten erleichtern, die ihren Anforderungen entsprechen.

Finanzielle Unterstützung

Für die Erstellung dieses Artikels wurden keine Mittel bereitgestellt.

Finanzielle und nichtfinanzielle Beziehungen und Aktivitäten

Die Autoren erklären, dass keine potenziellen Interessenkonflikte bestehen.

Beiträge der Autoren

Beide Autoren des Artikels leisteten einen wesentlichen Beitrag zu dieser Arbeit. Mohamed Maher konzipierte das Modell, führte die Literaturrecherche durch und schrieb den Artikel. Imtiaz Khan unterstützte den Entwurf, schrieb und formatierte den Artikel.

REFERENZEN

1. Heather B. Google DeepMind und Royal Free schließen einen Fünfjahresvertrag. Digitalhealth; 2016. Verfügbar unter: https://www.digitalhealth. net/2016/11/google-deepmind-and-royal-free-in-five-year-deal/ [zitiert am 19. September 2021].
2. Kowelle J. NHS data is worth billion-but who should have access to it? The Guardian. 2019. Verfügbar unter: https://www.theguardian.com/society/2019/jun/10/nhs-data-google-alpha-bet-tech- [zitiert am 19. September 2021].
3. PatientsLikeMe. patientslikeme.com. 2021.
4. Jeana HF, Michael PM. Soziale Nutzung von persönlichen Gesundheitsinformationen in PatientsLikeMe, einer Online-Patientengemeinschaft: Was passieren kann, wenn Patienten Zugang zu den Daten der anderen haben. J Med Internet Res. 2008;10(3):e15. doi: 10.2196/jmir.1053
5. Paul W, Michael M, Jeana F, et al. Sharing health data for better outcomes on PatientsLikeMe. J Med Internet Res. 2010;12(2):e19. doi: 10.2196/jmir.1549
6. GDPR. Allgemeine Datenschutzverordnung. Intersoft Consult-ing. 2016. Verfügbar unter: https://gdpr-info.eu [zitiert am 19. September 2021].
7. Kostkova P, Brewer H, de Lusignan S, et al. Who owns the data? Offene Daten für das Gesundheitswesen. Front Public Health. 2016;4:7. doi: 10.3389/fpubh.2016.00007
8. Bahar H, Abdelhakim Senhaji H, Dimitrios M. A sur-vey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access. 2020;8:90478-94. doi: 10.1109/ access.2020.2994090
9. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access. 2019;7:66792-806. doi: 10.1109/ ACCESS.2019.2917555
10. Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. IEEE; 2017, S. 1-4.
11. Nortey RN, Yue L, Agdedanu PR, Adjeisah M, editors. Privacy module for distributed electronic health records(EHRs) using the blockchain. 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), 15-18 März 2019.
12. Jaiman V, Urovi V. A consent model for blockchain-based health data sharing platforms. IEEE Access 2020;8:143734-45. doi: 10.1109/ACCESS.2020.3014565
13. Ryno A, Bertram H. A permissioned blockchain approach to the authorisation process in electronic health records. 2019 In-ternational Multidisciplinary Information Technology and En-gineering Conference (IMITEC). 2020.
14. Havelange A, Dumontier M, Wouters B, et al. LUCE: A blockchain solution for monitoring data License accoUnt-ability and ComplianceE. 2019. Verfügbar unter: https://arxiv.org/ abs/1908.02287 [zitiert am 19. September 2021].
15. Fabien D, Jean-Eudes R, Stefano B, Jean-Paul C, Juan R, Mi-chael S. The open D1NAMO dataset: Ein multimodaler Datensatz für die Forschung zum nicht-invasiven Management von Typ-1-Diabetes. Informat Med Unlocked. 2018;13:92-100. doi: 10.1016/j.imu.2018.09.003
16. Guo H, Li W, Nejad M, Shen C, editors. Zugriffskontrolle für elektronische Gesundheitsakten mit hybrider Blockchain-Edge-Architektur. 2019 IEEE International Conference on Blockchain (Blockchain), 14-17 Juli 2019.
17. Wang H, Song Y. Secure cloud-based EHR system using at-tribute-based cryptosystem and blockchain. J Med Syst. 2018;42(8):1-9. doi: 10.1007/s10916-018-0994-6
18. Guo R, Shi H, Zhao Q, Zheng D. Secure attribute-based sig-nature scheme with multiple authorities for blockchain in elec-tronic health records systems. IEEE Access. 2018;6:11676-86. doi: 10.1109/ACCESS.2018.2801266
19. Sun Y, Zhang R, Wang X, Gao K, Liu L, Editors. Eine dezentralisierende, attributbasierte Signatur für die Blockchain im Gesundheitswesen. 2018 27th International Conference on Computer Communication and Networks (ICCCN), 30. Juli-2. August 2018.
20. Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Datenschutzerhaltendes, attributbasiertes Zugriffskontrollmodell für XML-basiertes elektronisches Gesundheitsdatensystem. IEEE Access. 2018;6(99):9114-28. doi: 10.1109/ACCESS.2018.2800288
21. Yang X, Li T, Rui L, et al. Blockchain-based secure and search-able ehr sharing scheme. 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 24-26 October 2019.
22. Guang Y, Chunlei L. Ein Entwurf einer Blockchain-basierten Architektur für die Sicherheit von elektronischen Gesundheitsakten (EHR). 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). 2018.

23. Azaria A, Ekblaw A, Vieira T, Lippman A, editors. MedRec: Using blockchain for medical data access and permission man-management. 2016 2nd International Conference on Open and Big Data (OBD), 22-24 August 2016.
24. Yang H, Yang B, editors. A blockchain-based approach to the secure sharing of healthcare data. Proceedings of the Norwe-gian Information Security Conference; 2017.
25. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeD-Share: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017;5:14757-67. doi: 10.1109/ACCESS.2017.2730843
26. Huang J, Qi YW, Asghar MR, Meads A, Tu Y, editors. Med-Bloc: A blockchain-based secure EHR system for sharing and accessing medical data. 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE); 5-8 August 2019.
27. Xiaoguang L, Ziqing W, Chunhua J, Fagen L, Gaoping L. Ein Blockchain-basiertes System zum Austausch und Schutz medizinischer Daten. IEEE Access. 2019;7:118943-53. doi: 10.1109/ access.2019.2937685
28. Zhuang Y, Sheets LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR. A patient-centric health information exchange framework using blockchain technology. IEEE J Biomed Health Informat 2020;24(8):2169-76. doi: 10.1109/JBHI.2020.2993072
29. Xu L, Bagula A, Isafiade O, Ma K, Chiwewe T, editors. Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) platform. 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K), 4-6 Dezember 2019.
30. Tang F, Ma S, Xiang Y, Lin C. An efficient authentication scheme for blockchain-based electronic health records. IEEE Access. 2019;7:41678-89. doi: 10.1109/ACCESS.2019.2904300
31. Wang Y, Zhang A, Zhang P, Wang H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access. 2019;7:136704-19. doi: 10.1109/ ACCESS.2019.2943153
32. Kim M, Yu S, Lee J, Park Y, Park Y. Entwurf eines sicheren Proto-Col für ein Cloud-gestütztes elektronisches Gesundheitsaufzeichnungssystem unter Verwendung von Blockchain. Sensors (Basel, Switzerland) 2020;20(10):2913. doi: 10.3390/s20102913
33. Vora J, Nayyar A, Tanwar S, et al. (Hrsg.). BHEEM: A block-chain-based framework for securing electronic health records. 2018 IEEE Globecom Workshops (GC Wkshps); 9-13 Decem-ber 2018.
34. Magyar G, Herausgeber. Blockchain: Lösung des Kompromisses zwischen Datenschutz und Verfügbarkeit von EHR-Daten für die Forschung: A new disruptive technology in health data management. 2017 IEEE 30th Neu-mann Colloquium (NC); 24-25 November 2017. doi: 10.1109/ NC.2017.8263269
35. Ayesha S, Usman Q, Ayesha K. Using blockchain for electronic health records. IEEE Access. 2019;7:147782-95. doi: 10.1109/ access.2019.2946373
36. Castillo AF, Sirbu M, Davis AL. Vendor of choice and the effectiveness of policies to promote health information ex-change. BMC Health Serv Res 2018;18(1):405-12. doi: 10.1186/ s12913-018-3230-7
37. Yadav P. Mining electronic health records (EHRs): A survey. ACM Comput Surv. 2017;50(6):1-41. doi: 10.1145/3127881
38. Michellem M. Legal barriers to the growth of health information exchange-Boulders or pebbles? Milbank Q 2018;96(1):110-44. doi: 10.1111/1468-0009.12313
39. Lee S, Do H. Comparison and analysis of ISO/IEEE 11073, IHE PCD-01, and HL7 FHIR messages for personal health devices. Healthc Inform Res. 2018;24(1):46-52. doi: 10.4258/ hir.2018.24.1.46
40. Schumpeter JA, Stiglitz JE. Capitalism, socialism and democ-racy. Florence, SC: Taylor & Francis Group; 2010.
41. Ryuji I. ID-link, an enabler for medical data marketplace. IEEE. 2016. doi: 10.1109/ICDMW.2016.0117
42. Guo C, Ashrafian H, Ghafur S, Fontana G, Gardner C, Prime M. Herausforderungen für die Bewertung digitaler Gesundheitslösungen - Aufruf zu innovativen Ansätzen für die Evidenzgenerierung. NPJ Digit Med. 2020;3(1):1-14. doi: 10.1038/s41746-020-00314-2
43. Affinito L, Fontanella A, Montano N, Brucato A. How physi-cians can empower patients with digital tools. J Public Health. 2020:1–13.doi: 10.1007/s10389-020-01370-4
44. Kuek A, Hakkennes S. Das Niveau der digitalen Kompetenz des Gesundheitspersonals und seine Einstellung zu Informationssystemen. Gesundheitsinformatik J. 2020 Mar;26(1):592-612. doi: 10.1177/1460458219839613
45. EHR4CR | Elektronische Patientendatensysteme für die klinische Forschung. Innovative Medicines Initiative. 2016. Verfügbar unter: https://www.imi.europa.eu/projects-results/project-factsheets/ ehr4cr [zitiert am 19. September 2021].
46. Dupont D, Beresniak A, Schmidt A, Proeve J, Bolanos E. Assessing the financial impact of reusing electronic health re-cords data for clinical research: Ergebnisse aus dem europäischen Projekt EHR4CR. J Health Med Informat. 2016;7(3):235. doi: 10.4172/2157-7420.1000235
47. Timo I, Harri T. Difficult business models of digital business platforms for health data: A framework for evaluation of the ecosystem viability. 2017 IEEE 19th Conference on Business In-formatics (CBI); 2017. doi: 10.1109/cbi.2017.6
48. Alina T, Jose Luis O. A FAIR marketplace for biomedical data custodians and clinical researchers. 2018 IEEE 31st In-ternational Symposium on Computer-Based Medical Systems (CBMS); 2018. doi: 10.1109/cbms.2018.00040
49. Dumitru R, Gatti S. Towards a reference architecture for trusted data marketplaces: The credit scoring perspective. 2016 2nd In-ternational Conference on Open and Big Data (OBD). 2016. doi: 10.1109/obd.2016.21
50. Roman D, Stefano G, Editors. Towards a reference architecture for trusted data marketplaces: The credit scoring perspective. 2016 2nd International Conference on Open and Big Data (OBD); 22-24 August 2016. doi: 10.1109/OBD.2016.21