HAW HAMBURG

BACHELORARBEIT

Die elektronische Patientenakte in Deutschland: Eine Analyse zur Datensicherheitslage im internationalen Vergleich

vorgelegt am 13. Oktober 2025

Khatera Naser

Erstprüfer: Prof. Dr. Nils Martini
Zweitprüfer: Prof. Dr. Larissa Putzar

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Department Medientechnik
Finkenau 35
20081 Hamburg

Zusammenfassung

Diese Bachelorarbeit befasst sich mit der Datensicherheit der elektronischen Patientenakte als zentraler Baustein des Gesundheitswesens und analysiert ihre Stellung im internationalen Vergleich. Das Ziel der Arbeit ist die Analyse darüber inwiefern die ePA einen sicheren und effizienteren Austausch von Patientendaten gewährleistet und ob dieser Fortschritt mit bereits existierenden Modellen im Ausland mithalten kann. Hierzu wurde umfassend Wissen aus Literatur, internetbasierten behördlichen Quellen, Artikeln zu aktuellen Entwicklungen und Vorfällen analysiert, aufbereitet und in ermittelten Erkenntnissen aufgezeigt.

Abstract

This bachelor thesis deals with the data security of electronic patient record in Germany as a central component of the healthcare system and analyzes its position in an international comparison. The aim of the thesis is to analyze the extent to which the electronic patient record ensures a secure and efficient exchange of patient data and whether this progress can keep pace with existing models abroad. To this end, comprehensive knowledge from literature, internet-based official sources, articles on current developments, and incidents was analyzed, processed, and presented in the findings.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit und Information
DSGVO	Datenschutzgrundverordnung
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
FDZ	Forschungsdatenzentrum Gesundheit
TI	Telematikinfrastruktur
VAU	Vertrauenswürdige Ausführungsumgebung
E2EE	Ende-zu-Ende-Verschlüsselung
AES	Advanced Encryption Standard
2FA	Zwei-Faktor-Authentifizierung
FHIR	Fast Healthcare Interoperability Resources

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

„Wissen ist Macht“ – ist ein berühmtes Zitat von dem englischen Philosophen Francis Bacon, welches sich in den meisten Situationen bewahrheitet. Je mehr Wissen zu einem Thema, einer Situation oder einer Person existiert, desto leichter fällt die Wahl der Entscheidung über die zu erfolgende Handlung. Besonders in Fragen, welche die Gesundheit eines Menschen betreffen, führt jede weitere Information zu einem korrekteren Handeln für das medizinische Personal, aber auch den Patienten selbst. Die moderne Gesellschaft läuft – mal gleichauf, mal hinterher – mit den technologischen Errungenschaften der heutigen Zeit, um die Effizienz in allen Lebensbereichen zu steigern. Ein wichtiger Sektor ist das Gesundheitswesen, welches noch nicht das volle Potenzial der digitalen Medizin ausschöpft, und deshalb auf der Agenda der Bundesregierung zur Digitalisierung Deutschlands geführt ist. Die vielversprechenden Vorteile, die aus der Verfügbarkeit von Gesundheitsdaten zur Vereinfachung von Bürokratie, Erleichterung für das medizinische Personal und fortschriftlichen medizinischen Behandlungsverfahren entstehen, sprechen dafür die Digitalisierung voranzutreiben. Mit der COVID-19-Pandemie im Jahr 2020 hat der Bereich eHealth (electronic health) einen deutlichen Mehrwert gezeigt und einen Sprung in das Bewusstsein von Politik und Bevölkerung gemacht. Die Relevanz von Gesundheitsdaten hat zu dieser Phase einen besonderen Höhepunkt an Bedeutung erreicht zum Eindämmen von Fallzahlen und zum Bewältigen der Krisensituation. Gesetze sind im Eilbeschluss verabschiedet und Gesundheitsanwendungen in Höchstgeschwindigkeit entwickelt worden. Seither ist ein Vorantreiben der Digitalisierung der Medizin ein Ziel, das es so bald wie möglich umzusetzen gilt. Zum Erreichen dieses Ziels stehen digitale Gesundheitsanwendungen im Mittelpunkt, im Besonderen die „ePA für alle“, nachfolgend nur ePA genannt. Die Idee dazu besteht schon seit 2003 in Deutschland, aber trotz erwähnter Vorteile und Einführung im Jahr 2021 auf freiwilliger Basis hat es sehr lange gedauert, bis sie in den medizinischen Alltag einzieht. Die Gründe sind vielseitiger Natur, nicht zuletzt aber auch aufgrund von Datenschutzbedenken und Datensicherheit. Es ist nun so weit, denn seit dem 15. Januar 2025 bis Mitte Februar 2025 ist für jeden gesetzlich versicherten Kassenpatienten eine ePA angelegt worden mit dem Vorsatz bis Ende 2025 diese zu einem neuen und festen Bestandteil eines modernen digitalen Gesundheitswesens werden zu lassen. Ab dem 1. Oktober 2025 sind Praxen und Kliniken dazu verpflichtet die ePA zu pflegen und zu führen.

Ziel dieser Arbeit ist es die gegenwärtigen Lösungen zur Datensicherheit der elektronischen Patientenakte in Deutschland, sowie Hürden und Vorfälle zu analysieren und mit Modellen und Vorfällen aus anderen Ländern zu vergleichen.

Diese Arbeit basiert auf einer beschreibenden und vergleichenden Analyse. Hierzu ist das Vorgehen folgendermaßen festgelegt:

- Aufarbeitung von Grundlagen und Definitionen zur deutschen Patientenakte, Recht, Technik und Cyberangriffen

- Vorstellung der elektronischen Patientenakte und zugehörigen Infrastrukturen und Schwachstellen
- Vorstellung von sicherheitsrelevanten Vorfällen im Ausland
- Analyse und Vergleich anhand gewählter Kriterien
- Auswertung der Erkenntnisse und Handlungsempfehlungen

2 Grundlagen und Begriffsdefinitionen

2.1 Die Patientenakte und die Rolle von Gesundheitsdaten

2.1.1 Die elektronische Patientenakte

Per Definition gemäß Fünftem Sozialgesetzbuch (SGB V) § 341 ist die ePA eine vom Patienten verwaltete elektronische Akte, die dem Patienten auf seinen Wunsch seitens Krankenkassen bereitgestellt wird und die eine Ansammlung von medizinischen Unterlagen und Informationen zum Patienten in digitaler Form enthält. Sie zählt zu den sogenannten digitalen Gesundheitsanwendungen, welche der Kategorie E-Health unterliegen und dient zur einrichtungsübergreifenden und barrierefreien Einsicht und Verwendung von Patientendaten zu dessen bessere Anamnese, Diagnose, Behandlung und Verlaufsbeobachtung (Rashid et al., 2022). Außerdem enthält die Akte, welche auch als Gesundheitsakte erachtet wird, relevante Informationen für Notfallsituationen, Impfangaben oder den Organspenderstatus.

2.1.2 Ursprünge und Bedeutung der Patientenakte

Eine Patientenakte, wie sie gegenwärtig den meisten Menschen ein Begriff ist, enthält alle medizinisch notwendigen Informationen zu einem Patienten und ist der ständige Begleiter bei gesundheitsrelevanten Zusammenkünften zwischen medizinischem Personal und Patienten. Sie ist die Dokumentation der Anamnese, also die sogenannte Vorgeschichte, eines Patienten und ist essenziell für die richtige Beurteilung des behandelnden Arztes und damit zielführend für die korrekte Diagnose und Behandlung des Patienten. Schon in der Antike haben medizinische Dokumentationen einen besonderen Wert gehabt, wenn auch eher zu Zwecken der Wissensteilung und -erweiterung für Mediziner zu Behandlungsverfahren. Dies haben bereits Schriftstücke aus Papyrusrollen von vor 1600 Jahren vor Christi Geburt bewiesen, welche beispielsweise Informationen zu Operationen festgehalten haben (Al-Awqati, 2006). Eine lange Zeit später im 19. Jahrhundert haben französische und deutsche Mediziner den Anstoß gegeben auch die körperlichen Konditionen eines Patienten und seine familiäre Vorgeschichte in seiner Gesamtheit zu berücksichtigen und festzuhalten, und nicht nur die Symptome seiner Beschwerden. Mit der Einführung von Krankenversicherungen im Gesundheitswesen im Jahr 1883 in Deutschland (Bundesministerium für Gesundheit (BMG), 2025a), und zu ähnlicher Zeit in

anderen Teilen der Welt, hat sich die handschriftliche Dokumentation von Patientenakten in Krankenhäusern etabliert. Ab dem 20. Jahrhundert hat sich die systematisierte Dokumentation von Patientendaten etabliert mit dem Hintergrund eine verlässliche Informationsquelle zu schaffen für die Weiterbehandlung des Patienten und zur Erforschung von Krankheiten und ihren Verläufen. Das Zeitalter der Computerrechner hat dann dazu geführt die in Papierform geführte Patientenakte mit besonderem Druck von einer Vielzahl an medizinischen Organisationen, wie Krankenhäusern, Universitätskliniken, Kassenärztlichen Vereinigungen, Krankenversicherungen, IT-Unternehmen für Praxis- und Krankenhaussoftware und Gesellschaften für Standardisierungen, wie die Health Level 7 Deutschland (HL7) oder die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS), in digitale Akten zu übertragen (Gillum, 2013). Die Bedeutung und der Nutzen der Patientenakte haben sich stark weiterentwickelt, sodass die alleinige Dokumentation in digitaler Form nicht ausreicht, sondern mit den heutigen technologischen Mitteln die größtmögliche Wertschöpfung für alle Parteien gezogen werden soll.

2.1.3 Motivation zur ePA und Vorteile für das Gesundheitswesen

Die Gründe für eine gemeinsame Datenbank, welche die ePA prinzipiell darstellt, sind sowohl auf Patientenseite als auch das medizinische Personal betreffend zu finden. Das Bundesgesundheitsministerium, welche die Digitalisierung des Gesundheitswesens vorantreiben möchte, sieht vor allem entscheidende Vorteile, die durch eine digital verfügbare Patientenakte entstehen würden.

Nicht selten möchte ein Patient seine ärztlichen Unterlagen griffbereit haben für die persönliche Überwachung, aber auch zum Vorlegen bei einem Arztbesuch. Dahinter verbirgt sich ein Aufwand, der das Erfassen, Sortieren, Aufbewahren und speziell Mitführen benötigter Dokumente in analoger Form einschließt. Aber nur nach größeren Behandlungsverfahren bei Fachärzten wird eine Dokumentation ausgehändigt und das Risiko diese Dokumente zu verlegen oder zu verlieren, besteht immer.

Hinzu kommt, dass Ärzte ihre Aufzeichnungen nicht ohne Einverständnis des Patienten und bürokratischem Aufwand untereinander bereitstellen dürfen und somit auf die Sorgfalt des Patienten angewiesen sind. Eine Patientenakte, die Befunde, Hinweise, verordnete Medikationen und Behandlungsmaßnahmen enthält, gibt jedem Arzt ein umfassendes Bild zu einem Patienten und erlaubt ihm eine auf ihn zugeschnittene Behandlung zu wählen. So passiert es häufig, dass Patienten wiederholt untersucht werden müssen, um eine Diagnose stellen zu können. Dies führt zu einem höheren Zeit- und Kostenaufwand und einer Verzögerung des Behandlungsbeginns, zu Lasten des Gesundheitssystems.

Der schnelle Überblick über bestehende Erkrankungen und einzunehmende Medikamente kann Wechselwirkungen, Allergien oder bekannte Unverträglichkeiten bei Arzneien vermeiden und führt zu einer höheren Therapiesicherheit und Gesundheitsversorgung. Gerade in Notsituationen ist schnelles und präzises Handeln ein unverzichtbares Muss, um Leben retten und größere Schäden vermeiden zu

können. Jedoch sind Patienten in solchen Situationen selten gut ansprechbar oder sind imstande die erforderlichen Dokumente sofort zur Verfügung stellen zu können.

Dies ist auch eine Entlastung für (pflegende) Angehörige, die gegebenenfalls nicht immer alle Unterlagen vorliegen haben oder nicht auf dem aktuellen Stand sein könnten.

Der bürokratische Aufwand, der mit einem Arztbesuch zusammenliegt, führt zu langen Wartezeiten im Wartezimmer und verhindert, dass der Arzt sich viel Zeit für den Patienten nehmen kann. Fremdbefunde werden einzeln ins System eingepflegt, um auf dem Laufenden zu sein und die Patientenakte im eigenen System zu vervollständigen. Der Zeitaufwand durch Informationszusammenlegung aus zum Teil analogen Dokumenten und Untersuchungsergebnissen ist nicht nur ein kostspieliger Faktor, sondern es bleibt auch weniger Zeit für den einzelnen Patienten. Dies führt wiederum zu erheblichem Stress möglichst effizient Patienten zu behandeln, indem schnell und präzise korrekte Diagnosen gestellt und effektive Behandlungsverfahren eingeleitet werden. Mit einer vollständig verfügbaren Patientenakte, die bedenkenlos aufrufbar, eindeutig zuzuordnen und gut lesbar ist, entfallen bürokratische Hürden, die allen voran dem Patienten zugutekommen. Ein Behandlungsverlauf oder auch eine Krankengeschichte lässt sich detailliert im medizinischen Kontext erfassen.

Patienten mit „Seltener Erkrankung“ (SE) profitieren von einer gebündelten, sortierten und evaluierten Ansammlung von Daten sehr, da die Diagnose ihrer Erkrankung schneller und einfacher gestellt werden kann und sie somit eher versorgt werden und in Behandlung kommen können (Rashid et al., 2022). Jegliche Forschung zu Krankheiten – ob selten oder nicht selten – und der Gesundheit profitiert sehr, da sich aus den gesammelten Daten von Patienten Muster und Zusammenhänge erkennen und erschließen lassen für verschiedene Erkrankungen und eine bessere Gesundheit. Die Anzahl der Daten für eine Studie wäre um ein Vielfaches größer und ermöglicht damit genauere Ergebnisse. Dies ebnet den Weg zu einer frühzeitigen Erkennung von Veränderungen im Körper und besseren Präventivmaßnahmen sowie Behandlungsverfahren.

Die veranschaulichten Gründe lassen verstehen, dass digitale Medizin großes Potenzial hat mithilfe einer gemeinsam genutzten und vernetzten Datenbank existierende Probleme zu reduzieren, das Gesundheitssystem zu entlasten und Ressourcen effizienter einzusetzen. Der Koalitionsvertrag der Ampelregierung von 2021 hat diverse Bestrebungen zur Digitalisierung in verschiedenen Bereichen ausführlich beschrieben, worunter auch die Digitalisierung des Gesundheitswesens und damit verbunden auch die Einführung der elektronischen Patientenakte fällt (SPD et al., 2021).

2.1.4 Die Relevanz von Gesundheitsdaten

<u>Gesundheitswesen und Politik</u>

Aus den Gesundheitsdaten eines Patienten lassen sich wesentliche Informationen schließen zu seinem körperlichen und geistigen Zustand, genetischen Merkmalen, aber auch medizinische Versorgung und

Rückschlüsse auf soziale und erziehungs- sowie bildungsbezogene Faktoren. Gesundheitsdaten haben außerdem einen hohen Stellenwert in der Forschung, geben Auskunft über die Qualität und Sicherheit der erbrachten medizinischen Leistungen und tragen zu ihrer Optimierung bei. Außerdem lassen sich genauere regionale und überregionale Statistiken ermitteln zur Gesundheit, zu Erkrankungen und angewandten Therapieformen sowie deren Erfolg. Politische und finanzielle Entscheidungen zu Gesundheitsleistungen und -verhalten hängen davon ab, welche Informationen zur Gesundheitslage und möglichen Bedrohungen vorliegen. Dies hat sich während der COVID-19-Pandemie maßgeblich erwiesen, indem viel in die Gesundheitsversorgung eingegriffen worden ist und verschiedene Maßnahmen zur Eindämmung der Bedrohung insbesondere über Datenerhebungen beschlossen worden sind.

Cyberkriminelle Aktivitäten

Gesundheitsdaten können auch für eine völlig andere Kategorie von Interessenten lukrativ sein: Cyberkriminelle. Gesundheitsdaten enthalten meistens persönliche Informationen, wie die Adresse, das Geburtsdatum, die Sozialversicherungsnummer und Versicherungsnummern, mit denen betrügerische Handlungen im Namen der bestohlenen Person begangen werden können. Meistens bedeutet dies für die Opfer große finanzielle Schäden durch Verschuldung mit Krediten beispielsweise und rechtliche Konsequenzen, wie die ungerechtfertigte Strafverfolgung. Eine weitere Gefahr stellt der Versicherungsbetrug dar, wenn im Namen des Patienten teure Behandlungen oder Medikamente bezogen oder andere Leistungen der Krankenkassen beansprucht werden. Bestohlene können leicht erpresst werden, indem bei Patienten mit der Veröffentlichung sensibler Informationen, wie psychischen Erkrankungen oder Suchterkrankungen, gedroht wird. Personen des öffentlichen Lebens könnte eine Enthüllung über gesellschaftlich verpönte Erkrankungen, wie HIV oder Suchterkrankungen, den Ruf derart schädigen, dass ihre Karriere zerstört wird. Gesundheitseinrichtungen, die Datenlecks aufweisen, können mit Angriffen bedroht werden und damit einen herben Verlust auf finanzieller Ebene und zu ihrem Ruf erleiden. Auf dem Schwarzmarkt des Internets, dem sogenannten Darknet, werden Gesundheitsdaten teuer verkauft, da sie umfangreicheren Inhalt haben und, anders als bei einer Kreditkarte, Gesundheitsdaten nicht gesperrt werden und damit länger gültig sind. Unter den Interessenten können sich auch Fremdstaaten mit geopolitischen Motiven verbergen, die entweder Informationen zu technologischen Fortschritten in der Medizin und Forschung erlangen wollen für ihren eigenen Fortschritt und wirtschaftlichen Nutzen oder um den Gesundheitszustand von relevanten politisch aktiven Personen zu herauszufinden. Die absichtliche Sabotage von medizinischer Versorgung durch Manipulation von Patientenakten ist ebenfalls ein potenzielles Angreiferziel, um einer Zielperson zu schaden oder schlimmeres. Mit geleakten Daten über psychische Erkrankungen, Suchterkrankungen, Behinderungen oder auch genetischen Merkmalen, können Betroffene diskriminiert werden, indem sie Probleme bei der Arbeitsfindung oder Schwierigkeiten mit ihrer Stellung und Leistungsbezug bei ihrer Versicherung haben. Der Diebstahl großer Datenmengen, an die auf legalem Wege nicht heranzukommen wäre, bietet mehrere Verwendungsmöglichkeiten an. Es können KI-Modelle trainiert

werden für medizinische Zwecke, mittels Analyseverfahren wertvolle Informationen zu Krankheitsentwicklungen und Forschung entnommen werden und in Verbindung mit Informationen aus anderen Quellen zum Verkauf gestellt werden. Auch Personen des Gesundheitswesens sind potenzielle Täter, da sie mit Gesundheitsdaten Rezepte fälschen oder nicht stattgefundene Behandlungen abrechnen können.

Zusammenfassend wird von Kriminellen mit gestohlenen Gesundheitsdaten Erpressung, Missbrauch von Ressourcen, illegaler Verkauf und Informationsgewinnung betrieben.

2.2 Datenschutz und Datensicherheit

Unter dem Aspekt Personen zu schützen vor Datendiebstahl und den daraus möglichen Konsequenzen hat sich die Notwendigkeit ergeben Daten nur unter rechtlich erlaubten Umständen verarbeiten zu dürfen. Mehrere Gesetze sind entwickelt worden, um die Verarbeitung und Nutzung von Personendaten aus verschiedenen Bereichen explizit zu definieren und damit einen Rechtsrahmen zu schaffen.

2.2.1 Rechtsgrundlage

Eine Vielzahl an Gesetzen sind in den vergangenen Jahren entwickelt worden, um den Ausbau der Digitalisierung im Gesundheitswesen zu beschleunigen und eine sichere Basis für den Datenverkehr von sensiblen Daten zu schaffen. Einige dieser Gesetze werden im Folgenden vorgestellt, um ein Verständnis zu schaffen für die rechtsgültigen Rahmenbedingungen, in denen digitale medizinische Anwendungen entwickelt und bereitgestellt werden.

Datenschutz

Der Begriff Datenschutz begegnet heutzutage vielen Menschen in Zusammenhang mit digitalen Vorgängen und persönlichen Daten. Die vom europäischen Parlament beschlossene Verordnung (EU) 2016/679 oder anders bekannt als „Datenschutz-Grundverordnung (DSGVO)“ gilt seit dem 25.05.2018 in Ländern der Europäischen Union, darunter auch Deutschland. Sie dient dem Schutz von natürlichen Personen hinsichtlich der Verarbeitung und dem Transfer ihrer personenbezogenen Daten. Hierzu werden Rahmenbedingungen geschaffen zum Umgang mit diesen sensiblen Daten, die das Einverständnis zur Nutzung, die Aufbewahrung und Weitergabe definieren. In Deutschland wird die DSGVO in einzelnen Bereichen durch das sogenannte Bundesdatenschutzgesetzt (BDSG) ergänzt, wodurch bezüglich der landesspezifischen Bedürfnisse konkretere Regelungen festgelegt werden können.

Damit auch Einrichtungen, Institutionen und andere Organisationen der EU sich datenschutzkonform verhalten, gibt es die Verordnung (EU) 2018/1725, welche sicherstellt, dass Datenschutzstandards eingehalten werden, wie es von Privatunternehmen verlangt wird.

Datensicherheit

Die Datensicherheit beschäftigt sich mit technischen und organisatorischen Maßnahmen zur Verarbeitung und Aufbewahrung von Daten, um sie vor Verlust, Manipulation und unberechtigtem Zugriff zu schützen. Das Ziel es, wie beim Datenschutz, den Missbrauch von sensiblen Daten zu verhindern und einen sicheren Datenaustausch zu ermöglichen. Unter den Aspekten der Vertraulichkeit, Integrität und Verfügbarkeit wird die Datensicherheit sichergestellt.

European Health Data Space (EHDS)

Als Mitglied der europäischen Union hat Deutschland seine Vorhaben für die Weiterentwicklung des Gesundheitswesens unter dem übergeordneten Plan der EU bestimmt. Die EU sieht vor einen gemeinsamen sicheren Datenraum zu schaffen und hat das EHDS ins Leben gerufen. Das EHDS steht wörtlich für den „europäischen Raum für Gesundheitsdaten“ und ist Teil der europäischen Gesundheitsunion, welche durch die Europäische Kommission entwickelt wurde zur Krisenbereitschaft und -bewältigung, für bezahlbare innovative medizinische Versorgung und für die Prävention, Therapie und Nachsorge bei schweren Erkrankungen (Europäische Union, 2025). Die EHDS, auch Verordnung (EU) 2025/327 genannt, ist eine am 11. Februar 2025 beschlossene europäische Verordnung und der erste gemeinsame EU-Datenraum in einem spezifischen Bereich, welcher Strategien verfolgt zum Austausch und Nutzen elektronischer Gesundheitsdaten. Patienten soll der Zugriff und die Verwaltung auf eigene Gesundheitsdaten ermöglicht werden und für das Gemeinwohl aller EU-Bürger soll aus den Daten Erkenntnisse für die Forschung gewonnen werden. In der Verordnung ist unter anderem auch geregelt, dass ausreichende Schutzmaßnahmen getroffen werden sollen für einen erhöhten Datenschutz, eine erhöhte Sicherheit, Vertraulichkeit und ethische Nutzung. Auf deutscher Seite ist die zuständige Schnittstelle das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM).

Dokumentationspflicht in einer Patientenakte

Es gibt verschiedene rechtliche Vorschriften zur Dokumentationspflicht. Dazu gehört das Selbstbestimmungsrecht, welches nach § 10 „Dokumentationspflicht der Musterberufsordnung-Ärzte (MBO-Ä)“ Ärzte dazu anhält eine Patientenakte anzulegen (Hensche, Medizinrecht von A bis Z: Patientenakte, 2012). Im Bürgerlichen Gesetzbuch (BGB) ist unter § 630f „Dokumentation der Behandlung“ festgehalten, dass Behandler in der Verpflichtung stehen eine Patientenakte zu führen und darin alle vorgenommenen Maßnahmen zeitlich nachvollziehbar und zeitnah zu dokumentieren. Die Informationen, die in eine Patientenakte aufzunehmen sind, bestehen aus: Anamnese, Diagnosen, Untersuchungen und die Ergebnisse dazu, Befunde, Therapiemaßnahmen und Eingriffe, sowie deren Wirkungsweise, Einwilligungen des Patienten und Aufklärungen, als auch Arztbriefe (Dokumentation der Behandlung, 2013). Zu den persönlichen Angaben gehören das Geschlecht, Alter, Körpergewicht und die Körpergröße. Hinsichtlich der Diagnosen werden sowohl vergangene als auch aktuelle Erkrankungen und Allergien festgehalten. Zur Therapie gehören medikamentöse und physiotherapeutische Maßnahmen. Und auch Befunde aus Labor und Bildgebungsverfahren, sowie

Impfungen und erteilte Arbeitsunfähigkeitsbescheinigungen werden dokumentiert. Der Arzt entscheidet in einigen Fällen nach Relevanz für seine Behandlung, ob er bestimmte Daten hinzufügt oder unterlässt. Sprachlich muss die Dokumentation objektiv, leserlich und fachlich nachvollziehbar sein, so dass ein anderer Arzt den Inhalt versteht. Außerdem müssen Ärzte dafür Sorge tragen, dass von diesen Dokumentationen täglich gesicherte Kopien erstellt werden und der Zugang von Dritten unbedingt unterbunden wird. Ab dem 1.10.2025 stehen Ärzte, Psychotherapeuten und Krankenhäuser in der Pflicht Daten in die ePA einzupflegen.

Patientendaten-Schutz-Gesetz (PDSG)

Das PDSG schützt die Gesundheitsdaten des Patienten und eröffnet ihm durch digitale Versorgungsmöglichkeiten den Zugang und die Souveränität über seine Daten. Das Gesetz ist im Sinne des Patienten am 19.10.2020 in Kraft getreten und verpflichtet Krankenkassen ihren Patienten die ePA anzubieten. Darüber hinaus ist genaustens geregelt, welche Inhalte, datenschutzrechtlichen und funktionalen Anforderungen an die Anwendungen der Telematik, wie die ePA (ePA), elektronische Gesundheitskarte (eGK) und andere Anwendungen, gestellt sind und wie die Zugriffsrechte auf Daten von Patienten, Leistungserbringern (Ärzte, Zahnärzte, Krankenhäuser, Apotheken, Physio- und Psychotherapeuten) und Forschenden aussehen. Jedoch ist die Umsetzung der Anforderungen den verantwortlichen Bereichen selbst überlassen.

Digital-Gesetz (DigiG)

Das DigiG ist ein Gesetz, welches ab dem 26.03.2024 in Kraft getreten ist, soll vor allem zur Beschleunigung der Digitalisierung des Gesundheitswesens beitragen. Ihr zentrales Element ist die ePA, deren landesweiter Einzug im „Opt-out“-Verfahren beschlossen worden ist. Zu den weiteren Beschlüssen gehören die verpflichtende Umstellung auf das E-Rezept, die Legitimation des Cloud-Einsatzes im Gesundheitswesen innerhalb der EU, der weitere Ausbau von digitalen Gesundheitsanwendungen in Versorgungsvorgänge, die Weiterentwicklung von Sprechstunden per Videoanruf und Behandlungsprogrammen, die Verbesserung der Interoperabilität und Erhöhung der Cybersicherheit.

Gesundheitsdatennutzungsgesetz (GDNG)

Gemeinsam mit dem DigiG ist auch das GDNG am 26.03.2024 in Kraft getreten und definiert die Regelung zur Nutzung von Gesundheitsdaten im Forschungssektor. Das Gesetz sorgt dafür, dass in Abstimmung mit Datenschutzaufsichtsbehörden Daten zugänglicher gemacht werden für die Forschung. Es reguliert die Art der Nutzung, so dass nur im gesetzlich erlaubten Rahmen Daten verwendet und weitergegeben werden dürfen. Des Weiteren sollen dezentral verortete Daten über eine zentrale Datenzugangs- und Koordinierungsstelle verknüpfbar gemacht werden, so dass gesamtheitliche Rückschlüsse gezogen werden können.

Opt-in- und Opt-out-Verfahren

Das sogenannte Opt-in-Verfahren ist ein Zustimmungsverfahren, bei dem Nutzer ihre Zustimmung aktiv erteilen müssen für einen bestimmten Zweck. Es ist noch zu unterscheiden zwischen dem Single Opt-in-Verfahren, bei dem eine einmalige Zustimmungserteilung ausreicht, und dem Double Opt-in-Verfahren, bei dem noch zusätzlich eine Bestätigung erteilt werden muss.

Das Opt-out-Verfahren, bei dem die Zustimmung des Nutzers automatisch gegeben ist, erfordert dass er aktiv werden muss, wenn er seine Zustimmung zurückziehen möchte.

Das bisher geltende Opt-in-Verfahren, welches bei der elektronischen Patientenakte Anwendung gefunden und die Einwilligung des Patienten benötigt hat, ist seit Januar 2025 abgelöst worden durch das Opt-out-Verfahren. Für jeden Patienten ist eine ePA angelegt worden, sofern er dem nicht aktiv widersprochen hat. Eine Ablehnung der Akte kann nur durch einen aktiven Widerspruch des Patienten bei seiner Krankenkasse wieder gelöscht werden. Wenn sich ein Patient nur gegen die Übermittlung seiner Daten für Forschungszwecke entscheidet, kann er dies über die mobile ePA-Anwendung oder durch Anfrage bei Ombudsstellen, das heißt unabhängigen Beschwerde- und Beratungsstellen, der Krankenkassen die Übermittlung ihrer Daten explizit mit einem Widerspruch tun. Die Verwendung der ePA-Anwendung bleibt trotz bestehender Akte eine freiwillige Entscheidung für den Patienten.

Exkurs zur Entstehung von Gesetzen im deutschen Gesundheitswesen

Die Veranschaulichung dieser Prozedur soll verdeutlichen, dass geltenden Gesetzen viele Hürden auferlegt werden bis zu ihrem Inkrafttreten, und mitunter auch ein Grund für die Verzögerung der Digitalisierung im Gesundheitswesen darstellen. Initiator für Gesetze im medizinischen Bereich ist das Bundesministerium für Gesundheit, das einen Gesetzesentwurf einreicht zur Evaluierung von Vertretern verschiedener Akteure aus den diversen Bereichen des Gesundheitswesens, darunter auch die Patientenvertretung. Die Vertreter reichen Verbesserungsvorschläge ein und das Ministerium überarbeitet seinen Entwurf, welchen er dann an den Bundestag weiterreicht. Dort wird über den Entwurf beraten, diskutiert, Änderungen beantragt und zum Schluss abgestimmt. Sollte der Entwurf den Bundestag passieren, wird er vom Bundeskanzler und Gesundheitsminister unterzeichnet und muss noch einer finalen Prüfung vom Bundespräsidenten unterzogen werden, ob ein Verstoß gegen das Grundgesetz vorliegt. Unterzeichnet der Bundespräsident den Gesetzesentwurf, wird dieser als geltendes Gesetz veröffentlicht.

2.2.2 Erhebung von Patientendaten

Forschungsdatenzentrum (FDZ) Gesundheit

Die Datenerhebung über die ePA berücksichtigt die Anonymität des Patienten, weshalb die Daten pseudonymisiert und dann an das Forschungsdatenzentrum (FDZ) Gesundheit im Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) übermittelt werden. Gemäß § 303b

„Datenzusammenführung und -übermittlung“ ist definiert, dass Krankenkassen und Pflegekassen bis spätestens nach 10 Wochen nach Quartalsende dazu verpflichtet sind für jeden Patienten Daten in Verbindung mit einem Pseudonym, die eine eindeutige Identifikation erlaubt, an eine zentrale Datensammelstelle, den Spitzenverband Bund der Krankenkassen, zu übermitteln. Die Daten enthalten folgende Informationen:

- Alter, Geschlecht, Wohnort
- Versicherungsverhältnis
- Kosten- und Leistungsdaten von Leistungserbringern
- Angaben zum Vitalstatus, Grad der Pflegebedürftigkeit, Sterbedatum
- Angaben zu abrechnenden Leistungserbringern

Daten zu Alter, Geschlecht und Wohnort, bei denen vorläufige Diagnosen gestellt, Informationen zu kognitiven Fähigkeiten im Rahmen eines Pflegegrads, Abrechnungsdaten und Leistungsnachweise für pflegerische Leistungen, Kosten- und Leistungsdaten zur Versorgung mit Heil- und Hilfs- und Transportmitteln beschrieben sind, sind von der Verpflichtung befreit übermittelt zu werden. Der Spitzenverband Bund der Krankenkassen prüft die erhaltenen Daten auf Plausibilität, Vollständigkeit und Konsistenz und wendet sich bei Auffälligkeiten an den Zulieferer der Daten.

Der Data Submission Service in der ePA erstellt Lieferpseudonyme, registriert Arbeitsnummern mit zugehörigem Lieferpseudonym und pseudonymisiert die medizinischen Daten. Anschließend werden diese medizinischen Daten mit einer Arbeitsnummer gekennzeichnet und ohne die Lieferpseudonym an das FDZ Gesundheit übermittelt. Die Datenübermittlung geschieht blockweise, so dass Daten inklusive ihrer Arbeitsnummern von verschiedenen ePA-Konten zusammengelegt werden. Ein weiteres Datenpaket mit einer Liste mit den Lieferpseudonymen und zugehörigen Arbeitsnummern erhält eine Vertrauensstelle, welche die Aufgabe hat, ein neues dauerhaftes Pseudonym zu erzeugen. Für die richtige Zuordnung haben beide Datenpakete dieselbe SubmissionID. Das neue dauerhafte Pseudonym wird in einem vom BSI abgesegneten, technisch aktuellen schlüsselabhängigen Verfahren festgelegt. Dieses Pseudonym für einen Patienten gilt auch bei neu übermittelten Datensätzen, darf aber keine Rückschlüsse auf das Lieferpseudonym oder die Identität des Patienten erlauben. Die Vertrauensstelle schickt die neuen Pseudonyme und Arbeitsnummern dem FDZ Gesundheit und löscht alle Daten zu alten und neuen Pseudonymen sowie Arbeitsnummern.

Erstmalig ist diese Datenübermittlung nach dem ersten Kalenderquartal 2025 erfolgt. Die übermittelten Daten werden vom FDZ Gesundheit für vier Quartale aufbewahrt und ein Quartal gelöscht, sobald für dieses Kalenderquartal neue Daten vorliegen. Nach der Löschung werden die neuen Daten eingelesen.

Jede natürliche Person und juristische Person, das heißt Einrichtung, Unternehmen, kann im Rahmen der dafür vorgesehenen Zwecke die Daten in anonymisierter und aggregierter Form erheben und verwenden. Erlaubte Zwecke sind:

- wissenschaftliche Forschungsfragen zu den Bereichen Gesundheit und Pflege
- Analyse zur Wirksamkeit von Versorgungsformen und Verträgen von Kranken- und Pflegekassen
- Verbesserung der Versorgungsqualität und Sicherheitsstandards der Prävention, Versorgung und Pflege
- Wahrnehmung von Aufgaben betreffend: Steuerung durch Kollektivvertragspartner (wie gesetzliche Krankenkassen u.a.), Gesundheitsberichterstattung, öffentliche Gesundheit und Epidemiologie
- Entwicklung, Weiterentwicklung und Sicherheitsüberwachung von Arzneimitteln, medizinischen Produkten, Untersuchungs- und Behandlungsverfahren, Heil- und Hilfsmitteln, digitale Gesundheitsanwendungen, Künstliche Intelligenz im Gesundheitswesen
- Bewertung zum Nutzen von Arzneimitteln, medizinischen Produkten, Untersuchungs- und Behandlungsverfahren, Hilfs- und Heilmitteln und digitalen Anwendungen

Um die Gesundheitsdaten nutzen zu können, muss die natürliche oder juristische Person beim FDZ Gesundheit einen Antrag stellen und anschließend eine Stellungnahme zur Plausibilität beziehen. Wird der Antrag bewilligt, werden dem Nutzungsberechtigten Daten im Rahmen seines Antrags in anonymisierter und aggregierter Form zur Verfügung gestellt. Das bedeutet, dass die Daten verallgemeinert werden zu Durchschnittswerten und somit nicht zurückzuführen sind auf einzelne Personendaten. Nutzungsberechtigte solcher Daten dürfen diese weiterhin im Rahmen ihres bewilligten Antrags verwenden, auch wenn das FDZ Gesundheit diese Daten bereits gelöscht hat.

Ein Antrag wird abgelehnt, wenn ein Risiko für die öffentliche Sicherheit und Ordnung oder für den Schutz personenbezogener Daten bestehen sollte, ein Verdacht auf Zweckentfremdung existiert oder zu viele Anträge gestellt worden sind seitens desselben Nutzungsberechtigten. Sollte die Datenschutzaufsichtsbehörde feststellen, dass ein Nutzungsberechtigter erhaltene Daten zu einem anderen Zweck verwendet als im Antrag angegeben und bewilligt, wird das FDZ Gesundheit diesen für bis zu zwei Jahre vom Datenzugang ausschließen (Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung, 2020). Jede absichtliche Wiederidentifikation von anonymisierten Daten zur eigentlichen Quelle, also Patienten oder Leistungserbringer, ist strafbar und kann zu einer Freiheitsstrafe führen.

Datenauskunft an Patienten

Patienten sind grundsätzlich im Recht die Daten ihrer eigenen Akte in einer Arztpraxis oder anderen medizinischen Einrichtung einsehen zu dürfen und gegen eine Entschädigung – beispielsweise bei ausgedruckten Informationen – auch aushändigen zu lassen. Auskünfte zu erbrachten Leistungen und Kosten einer Krankenkasse, können durch eine Antragsstellung seitens des Patienten erteilt werden. Krankenkassen dürfen diese Informationen nur an Dritte weitergeben, sofern der ausdrückliche Wunsch des Patienten besteht an eine bestimmte dritte Instanz diese Informationen zu übermitteln.

2.2.3 Datenaufbewahrung und Zugang

Laut Patientenrechtegesetz in § 630f BGB (Bürgerliches Gesetzbuch) sind Ärzte dazu angehalten medizinische Aufzeichnungen für die Dauer von 10 Jahren nach Behandlungsabschluss aufzubewahren, soweit sie kein anderes Gesetz zu anderen Aufbewahrungsfristen auffordert. Sinn und Zweck der Aufbewahrung dieser Daten ist es Ärzten eine nachvollziehbare Informationsstütze zu geben für eine sachgerechtere Behandlung von Patienten und dient ihnen auch als Beweis für vollzogene Behandlungen. Eine Unterlassung der Dokumentation gilt als Verstoß und macht den Arzt haftbar für eine mögliche nicht durchgeführte Maßnahme. Für Patienten ist die Dokumentation hilfreich, wenn sie in die Behandlung von einem anderen Arzt gehen (Dokumentation der Behandlung, 2013). Für Röntgenbilder und Strahldaten gilt nach § 85 Strahlenschutzgesetz eine Aufbewahrung von 10 bis 30 Jahren je nach Altersgruppe des Patienten. Krankenkassen dürfen ihre Abrechnungsdaten jedoch laut § 294 ff. SGB V (Sozialgesetzbuch Fünf) nur bis zu vier Jahre aufbewahren zu Prüfzwecken. Für die ePA gibt es eine andere Regelung, in der nach § 341 SGB V die Daten auf Wunsch des Patienten gelöscht werden, aber es sonst keine konkrete Speicherfrist gibt. Das heißt, ohne Eingreifen des Patienten können die Daten lebenslang erhalten bleiben. Es gibt bisher keine gesetzliche Regelung, die eine Löschung der Akte nach dem Versterben eines Patienten in Kraft tritt. Sofern keine Löschung von einem Angehörigen oder rechtlichen Vertreter beantragt wird, bleibt die Akte erhalten bis nach Ablauf der Aufbewahrungsfrist von 10 Jahren.

Die Zugangsberechtigung variiert je nach Anfrager: nur der Patient selbst hat die volle Einsicht in seine Patientenakte und kann zu dem jederzeit nachvollziehen, wer auf welche Dokumente zugegriffen hat. Ärzte und Pflegepersonal dürfen nur Daten, die sie zu ihrer Behandlung benötigen einsehen, Krankenkassen haben nur Einsicht auf Abrechnungsdaten, inklusive Diagnosen, aber keine ärztlichen Notizen. Therapeuten, Pflegeeinrichtungen oder Apotheken können die Akte nur mit der expliziten Einwilligung des Patienten einsehen. Aus technischen Gründen müssen IT-Dienstleister, wenn notwendig, ebenfalls Zugang zu den Akten erhalten, dürfen aber die Inhalte nicht nutzen und müssen sich strikt an die DSGVO-Regeln halten. Forschende können den Zugang zu Datensätzen nur innerhalb von sicheren, virtuellen Verarbeitungsräumen erhalten unter der Prämisse eines bewilligten Antrags beim FDZ Gesundheit, denn es werden grundsätzlich keine Daten freigegeben. Falls die Notwendigkeit besteht die Daten an Forschende verschicken zu müssen, dann nur in anonymisierter und aggregierter Form.

Künftig sollen alle Fragen zur Datenerhebung und -nutzung über eine zentrale Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten abgewickelt werden nach dem Prinzip des One-Stop-Shop, bei dem bürokratische Schritte über ein einziges Portal zusammengefasst werden können. Zunächst sind Daten der Krankenkassen und aus dem Krebsregister für die Nutzung vorgesehen. Die Verknüpfung von Daten aus medizinischen Registern mit den Daten des FDZ Gesundheit ist ein Ziel, für das noch Konzepte entwickelt werden sollen. Derzeit gibt es nur für das Krebsregister ein Konzept, bei dem der

Zugang nur in einer sicheren Verarbeitungsumgebung stattfindet. Den Daten aus den unterschiedlichen Quellen wird aber zuvor noch eine gemeinsame Forschungskennziffer zugeordnet und die Pseudonyme werden unter Verschluss gehalten.

2.3 Technische Definitionen

Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)

Das Bundesamt für Sicherheit in der Informationstechnik hat 2016 einen Kriterienkatalog definiert zum Cloud Computing für professionelle Cloud-Provider. Im Jahr 2019 wurde dieser Katalog überarbeitet und den neusten Entwicklungen angepasst. Die Kriterien schaffen eine Basis und Richtlinien für alle Aspekte eines sicheren Cloud-Computings. Die folgende Auflistung zeigt die Bereiche an, auf die der Katalog eingeht und worauf sich auch Regelungen und Entwicklungen von digitalen Gesundheitsanwendungen stützen.

Planung, Umsetzung, Aufrechterhaltung, Umgang, physischen Sicherheit, Autorisierung und Authentifizierung, Verschlüsselungsverfahren zum Schutz der Vertraulichkeit, Authentizität und Integrität von Informationen, Kommunikationssicherheit, Interoperabilität, Beschaffung oder Änderung von Informationssystemen, Steuerung und Überwachung von Dienstleistern und Lieferanten, Umgang mit Sicherheitsvorfällen, Notfallmanagement, Einhaltung von Regeln, Produktsicherheit, Umgang bei juristischen Ermittlungen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020).

Das BSI gibt seine Vorgaben und Empfehlungen zu Datensicherheitsvorkehrungen auf Basis der Gesetzesgrundlagen, wie die DSGVO. Zu den Qualitäts- und Sicherheitsanforderungen an die TI für ein funktionierendes und sicheres informationstechnisches System gehören die Interoperabilität, Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität (Patientendaten-Schutz-Gesetz – PDSG, 2020). Die Vertraulichkeit, Integrität und Verfügbarkeit sind Teil des IT-Sicherheitsstandards und gehören zum DIN EN ISO/IEC 27001, der deutschen Fassung des internationalen Standards für Informationssicherheitsmanagement.

Interoperabilität

Die Fähigkeit von informationstechnischen Systemen untereinander zu kommunizieren, Daten austauschen und korrekt verarbeiten zu können, beschreibt den Begriff Interoperabilität.

Verfügbarkeit

Die Verfügbarkeit von Daten, und damit der Zugang zu ihnen und ihre Nutzbarkeit, soll nur dann gegeben sein, wenn Personen mit Berechtigung sie benötigen. Dies setzt allerdings voraus, dass die Systeme, über die die Daten aufgerufen werden, hochverfügbar sind und damit auch bei technischen

Störungen oder einem Cyberangriff weiterhin hoher Anzahl funktionieren. Es sind mehrere Maßnahmen erforderlich, um der Verfügbarkeit gerecht zu werden:

- Redundante Systeme und Rechenzentren: Ausfälle können abgefangen werden
- Lastenverteilung und Skalierbarkeit von Diensten: Die Arbeitslast wird von mehreren Systemen getragen, so dass das Risiko eines Totalausfall reduziert wird. Systeme sind dazu in der Lage auf schwankende Arbeitslast zu reagieren bei gleichbleibender Effizienz.
- Monitoring und schnelle Fehlerbehebung: Eine gute Überwachung ermöglicht eine schnelle Reaktion, um entstandene Probleme zu beheben.
- Notfall- und Backup-Konzept: Das Konzept gibt einen konkreten Plan vor, welche Maßnahmen ergriffen werden sollen, um den Schaden so klein wie möglich zu halten.
- Schutz vor Angriffen und Störversuchen: Präventionsmaßnahmen, wie beispielsweise regelmäßige Verkehrs- und Dienstanalysen, können Angriffe verhindern oder erlauben zumindest eine höhere Reagibilität.

Eine 100%ige Verfügbarkeit ist ein nichtrealisierbares Ziel. Vielmehr wird versucht diesem Ziel so nah wie möglich zu kommen, indem die Ursachen zu Ausfällen ermittelt werden. Erstrebenswert ist eine Rate von 99% oder gar 99,9%, welche immerhin auf das Jahr berechnet einen Ausfall von etwa 3,5 Tagen bzw. im letzteren Fall 5,5 Stunden bedeuten würde (Bohne-Lang & Lang, 2019). Mit Hilfe von Risikoanalysen und den daraus gewonnenen Erkenntnissen wird versucht den bestmöglichen Rahmen zu schaffen für Kosten und Nutzen.

Mögliche Auslöser für Ausfälle werden im Folgenden herangeführt und können als Konsequenz die Verfügbarkeit von Daten beeinträchtigen:

- Personen: menschliches Versagen, unberechtigter Zutritt, Ausnutzen von Schwächen in Notfallsituationen, Social Engineering (Ausspionieren/Manipulieren von Personal), streikendes Personal, Nichteinhaltung von Leistungen
- Hardware: defekt, beschädigt, überhitzt, kontaminiert (Staub, Insekten, Schmutz), zerstört, veraltet
- Schäden durch Feuer, Wasser, Stromüberspannung oder Erdbeben
- Stromausfall
- Softwareprobleme: abgelaufene Dienste, Schadsoftware (Trojaner, Viren), gezielte Cyberangriffe

Für jeden dieser Auslöser gilt es nach entsprechenden Schutzmaßnahmen zu suchen, um diese zu verhindern, das Risiko zu reduzieren oder passend zu reagieren, um größere Schäden eindämmen zu können. Das Wissen um diese Auslöser allein verhilft bereits Lösungsansätze zu suchen. Die regelmäßige Sicherung von Daten ist ein zwingender Bestandteil des Datensicherheitsprozesses und wird in der Regel auf zwei verschiedene Arten gehandhabt. Die Archivsicherung, welche eine einmalige

Bestandsicherung der gesamten Datenlage ist und die Spiegelsicherung, welche eine regelmäßige Datensicherung in kurzen Zeitabständen ist und nur hilft, wenn schnell reagiert wird, um den letzten Datenstand retten zu wollen. Sonst wird dieser mit der nächsten automatischen Sicherung überschrieben mit dem bereits entstandenen Schaden. Als eine RAID (Redundant Array of Independent Disks) - Technologie ist die Spiegelsicherung die sogenannte RAID 1, welche Daten redundant auf mehrere ortsverschiedene Speichermedien ablegt, um so einem Ausfall entgegenzuwirken. RAID - Technologien werden meist kombiniert untereinander angewendet, um ein besseres Ergebnis bei Abruf, beim Speichern und für die Sicherheit zu erzielen.

Integrität

Die Integrität von Daten stellt sicher, dass sie vollständig und unverändert sind. Potenzielle Gefahren, die die Integrität in Frage stellen können, sind unter anderem eine physische Destruktion, eine Manipulation oder auch ein unbefugter Lesezugriff. Je nach Fall kann eine Gefährdung der Integrität leichte oder schwere Folgen haben. Auch muss berücksichtigt werden, dass Daten, welche dauerhaft an das Internetnetzwerk angeschlossen sind, häufiger Gefahren von außen ausgesetzt sind. Um die Integrität gewährleisten zu können, kommen folgende Maßnahmen zum Einsatz:

- Ende-zu-Ende-Verschlüsselung: hierbei werden Daten vom Absender verschlüsselt und vom Empfänger nach Erhalt entschlüsselt, so dass sie für andere unlesbar sind.
- Kryptografische Methoden: Manipulationen von Daten können erkannt werden durch Hashfunktionen, digitalen Signaturen und Prüfsummen, bei denen für beliebig große Daten eine einzigartige Zeichenfolge durch einen Algorithmus erzeugt wird. Jede Abweichung in dieser Zeichenfolge würde eine Veränderung der ursprünglichen Daten beweisen.
- Protokollführung: jeder Zugriff auf Daten und jede Änderung von Daten wird protokolliert, so dass Manipulationen schnell erkannt werden und gut überprüfbar sind.
- Transaktionskontrolle: jede Transaktion von Daten wird entweder vollständig oder gar nicht ausgeführt. Diese Methode gewährleistet, dass nur vollständige Daten in einem nicht fehlerhaften Zustand übermittelt werden und somit ihre Manipulation ausgeschlossen werden kann. Durch Monitoring werden verdächtige Aktivitäten erkannt und Kontrollmechanismen sichern die Datenintegrität.

Vertraulichkeit

Ziel der Vertraulichkeit ist es zu gewährleisten, dass nur autorisierte Personen und Gruppen Zugang zu bestimmten Daten haben und diese gegebenenfalls auch verwalten können. Hierzu kommen verschiedene Maßnahmen zum Einsatz:

- Verschlüsselung: Daten werden nur in verschlüsselter Form übertragen und gespeichert.
- Authentifizierung: der Zugang wird nur über sichere Zugangsverfahren ermöglicht.

- Zugriff: die Zugriffssteuerung wird über Rollen geregelt, so dass abhängig von der Rolle nur ein bedingter Zugriff erlaubt wird.
- DSGVO: Die Einhaltung von Datenschutzgesetzen und das verantwortungsbewusste Handeln autorisierter Personen spielen eine entscheidende Rolle, welche die Weitergabe sensibler Daten nur in einem entsprechenden erforderlichen Rahmen, unter Einverständnis und mit voller Transparenz handhaben.

Authentizität

Die Authentizität vermittelt die Gewissheit über die Echtheit und Vertrauenswürdigkeit der Datenquelle und des Zugriffs, so dass empfangene Daten auch wirklich vom erwarteten Absender stammen. Dies wird erreicht über:

- Authentifizierung: Mit Mechanismen zur Mehrfaktor-Authentifizierung wird sichergestellt, wer Zugang erhalten hat.
- Elektronische Signatur: die digitale Signatur garantiert die Urheberschaft und Echtheit von Dokumenten und Daten.
- Public-Key-Infrastruktur (PKI): die PKI stellt digitale Zertifikate über eine vertrauenswürdige Zertifizierungsstelle aus für die sichere Identifizierung einer Person, eines Gerätes oder Dienstes. Das Zertifikat enthält kryptografische Schlüssel, von denen der öffentliche Schlüssel zur Authentifizierung genutzt wird und der private vertraulich bleibt. Mittels Identitätsprüfung des Zertifikatbesitzers erkennt die Zertifizierungsstelle die Echtheit der Person, des Geräts oder Dienstes.

Risikoanalyse

Die Risikoanalyse ist ein Prozess des Informationssicherheitsmanagements und Teil der Datensicherheit zur Erkennung potenzieller Schwachstellen und Gefahren. Sie wertet diese hinsichtlich ihrer Gefährdung für die Vertraulichkeit, Integrität und Verfügbarkeit aus und entwickelt aus den Ergebnissen der Auswertung passende Sicherheitsmaßnahmen, um Risiken einzudämmen. Die endgültigen Ergebnisse der Analyse werden für Compliance-Zwecke dokumentiert und zur Verfügung gestellt. Nach den offiziellen Vorgaben des BSI zur Risikoanalyse gestaltet sich der Prozess grob beschrieben folgendermaßen:

- Erstellung einer Übersicht von Gefährdungen
- Einstufung der Risiken, die von den Gefährdungen ausgehen
- Behandlung von Risiken festlegen
- Überprüfung des Sicherheitskonzepts
- Sicherheitsprozess mit erneuertem Konzept fortsetzen

Compliance-Anforderungen

Die Compliance im Kontext der Datensicherheit ist zu Deutsch die Einhaltung von gesetzlichen Vorgaben zum Schutz von Daten und Reduzierung von Risiken, wie der DSGVO. Dies verpflichtet jedes Unternehmen dazu entsprechende Maßnahmen zu ergreifen, um die erforderlichen Sicherheitsstandards zu erfüllen. Eine Nichteinhaltung ist ein Verstoß gegen geltendes Recht und kann strafrechtlich verfolgt werden.

FAIR-Prinzip für Forschungsdaten

Der Anspruch an Forschungsdaten unterliegt dem FAIR-Prinzip, wobei die Daten auffindbar (Findable), zugänglich (Accessible), interoperabel (Interoperable) und wiederverwendbar (Reusable) sein müssen. Sinn und Zweck ist es Daten so aufzubereiten, dass sie wiederverwendbar und nachvollziehbar sind.

Konnektor

Ein Konnektor ist ein System aus Hard- und Software, das dafür sorgt, dass medizinische Einrichtungen sich über eine sichere und verschlüsselte Verbindung mit der TI verbinden und Daten übertragen können. Er ähnelt einem Router, ist aber wesentlich sicherer konzipiert. Er ist eine Schnittstelle für miteinander kommunizierende Dienste, bestehend aus einem Hardwareteil in physischer Form als Gerät oder virtuell in einer Cloud als „TI-Konnektor 2.0“. Der Softwareteil besteht aus einem VPN-Zugangsdienst und Softwaremodulen für Dienste wie die ePA, das eRezept oder KIM. Für die sichere Schlüsselverwaltung und digitale Signatur sorgt das Hardware-Sicherheits-Modul (HSM). Zur Verschlüsselung ist bisher das RSA-Verfahren verwendet worden. Dieses wird mit dem Beschluss der BSI und Bundesnetzagentur abgeschafft und ab dem 01.01.2026 unzulässig sein. Stattdessen wird für die kryptografischen Vorgänge der TI das ECC-Verfahren eingesetzt (gematik Fachportal, 2025c). Für eine Verbindung zu Kartenlesegeräten und zum PVS hat der Konnektor Schnittstellen. Der Konnektor ist für digitale Dienste im Gesundheitswesen ein obligatorisches Kernelement. Das sorgt aber auch für eine Abhängigkeit zu ihm, die in den vergangenen Jahren problematisch gewesen ist durch hohe Anschaffungskosten oder durch Ausfälle wegen Störungen. Aus diesen Gründen gewinnt die cloudbasierte, kostengünstigere und wartungseinfachere Version des Konnektors immer mehr an Popularität.

RSA-Zertifikat

Ein System mit RSA-Zertifikat ist in der Lage das asymmetrische RSA-Verschlüsselungsverfahren anzuwenden. Hierbei wird zum Ver- und Entschlüsseln nicht derselbe Schlüssel verwendet, sondern es wird über algorithmische Verfahren ein Schlüsselpaar aus öffentlichem und privatem Schlüssel erstellt. Der Sender erhält den öffentlichen Schlüssel des Empfängers, verschlüsselt damit das Datenpaket und nur der Empfänger kann mit seinem privaten Schlüssel die Entschlüsselung durchführen. Das RSA-Verfahren kann auch für digitale Signaturen eingesetzt werden. Hierbei wird mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüssel die Echtheit des Absenders geprüft. Die

Kompromittierung des privaten Schlüssels eliminiert die Sicherheit dieses Verfahrens. Da die Sicherheit des Schlüssels von seiner Länge abhängt, gilt ein sicherer Schlüssel mindestens 3000 Bit.

ECC (Elliptische Kurven Kryptografie)

Das ECC-Verfahren ist ein asymmetrisches Verschlüsselungsverfahren, wie RSA, arbeitet aber mit einem anderen algorithmischen Verfahren, so dass seine Schlüssel wesentlich kürzer sind, aber es trotzdem genauso sicher ist. Dies ist auch der entscheidende Grund dafür, dass ECC der neue Standard werden soll. Während bei RSA die Schlüssellänge beispielsweise 1024 Bit beträgt, würde ein gleichwertiger Schlüssel bei ECC nur 160 Bits ausmachen. Insbesondere für kleine Geräte oder auch zur Dateneinsparung ist dieser Unterschied von Bedeutung. Anwendungsbereiche wären die sichere Kommunikation, digitale Signaturen und die Kryptowährung (SSL-Support Team, 2024).

mTLS (mutual Transport Layer Security)

Die mTLS, ist eine asymmetrische Verschlüsselung mit Handshake, die zusätzlich noch eine gegenseitige Authentifizierung von Sender und Empfänger erfordert. Beim TLS-Handshake wird nach der ersten Kontaktaufnahme des Clients zum Server, dem Client das TLS-Zertifikat vorgelegt zur Verifikation. Der Client kennt nun den öffentlichen Schlüssel des Servers und übermittelt eine neue Nachricht zur Authentifikation, die der Server nur im Besitz des privaten Schlüssels entschlüsseln kann. Ein gemeinsamer Schlüssel für die Austauschsitzung wird generiert und der Handshake ist abgeschlossen. Beim mTLS wird der Handshake gegenseitig ausgeführt, so dass sowohl Client als auch Server ihre Zertifikate verifizieren müssen (Cloudfare, 2025a).

PVS (Praxisverwaltungssystem)

Das PVS ist eine spezielle Software für Arztpraxen und psychotherapeutische Praxen, um sich digital zu organisieren, zu dokumentieren und Abrechnungen durchzuführen. In ihm werden Patientendaten und -akten digital verwaltet, Termine koordiniert, Befunde und andere medizinische Dokumente gespeichert, Rechnungen an die Krankenkasse übermittelt und eine Anbindung an die TI ermöglicht. Heutzutage wird die Software browser-basiert als „Software as a Service“ - Modell angeboten, wodurch Updates automatisch und ohne Zusatzkosten laufen.

QES (Qualifizierte elektronische Signatur)

Über den explizit dafür konfigurierten Konnektor können QES-Dienste, wie SignatureService, EncryptionService, CertificateService, AuthSignatureService, Dokumente verschlüsseln und Signaturen erstellen (gematik, 2025c). Die QES basiert auf einem qualifizierten Zertifikat für elektronische Signaturen. Für ihre Nutzung ist ein Zugang zur TI, ein Konnektor, ein eHealth-Kartenterminal, ein elektronischer Heilberufsausweis und eine PIN erforderlich.

Komfortsignatur

Sie ist eine Funktion zum Signieren von digitalen Dokumenten ist die Komfortsignatur. Für einen Zeitraum von 24 Stunden nach erfolgreicher PIN-Eingabe, können bei eingesetztem Ausweis im Kartenleser bis zu 250 Dokumente signiert werden, ohne eine erneute PIN-Eingabe einzufordern. Um diese Funktion nutzen zu können, wird die aktuelle PVS-Version, die neueste Konnektorversion (PTV4+), Ausweise der Generation 2.0 und höher, sowie zusätzliche Kartenlesegeräte, da der Ausweis für einen längeren Zeitraum ein Gerät besetzt hält.

MIO (Medizinisches Informationsobjekt)

Ein Zusammenschluss von Informationen zu medizinischen, strukturellen oder administrativen Gegebenheiten heißen strukturierte Dokumente oder auch MIO genannt und werden nach klarer Vorgabe in Form einer XML-Datei in die elektronischen Patientenakte gespeichert. MIOs sind ein in Deutschland entwickelter Standard zur Wiederverwendbarkeit von Daten in anderen Anwendungen und Systemen, weil sie semantisch und syntaktisch interoperabel sind. Sie sind inhaltlich vollständige und nachvollziehbare Dokumente, die keine Ergänzung benötigen, um von einer anderen Person verstanden zu werden. Der Impfpass, Mutterpass oder das Zahnbonusheft sind jeweils Beispiele für ein MIO. Ein MIO kann auch aus mehreren MIOs bestehen, wie es beim Kinderuntersuchungsheft der Fall ist. MIOs werden in Ordnern, sogenannten Sammlungstypen, gespeichert, welche entweder statisch und damit fest vorgegeben und nicht-löschbar sind oder dynamisch und damit in der ePA anlegbar und löschbar sind und mehrfach vorkommen können. Die Interoperabilität eines MIO erhält es durch seine Ummantelung bzw. Schnittstelle mit einer FHIR-Schicht (gematik, 2021).

FHIR (Fast Healthcare Interoperability Resources)

Die FHIR ist eine internationale Technologie von „HL7 International“ und der Standard zum Datenaustausch im Gesundheitswesen und nutzt dazu standardisierte Protokolle und Datenformate. Ziel ist es einen reibungslosen und nahtlosen Austausch unterschiedlicher Systeme zu ermöglichen, also die Interoperabilität. FHIR ist ein plattformunabhängiger Webstandard und damit ideal für mobile und Desktop-Anwendungen (*MIO Allgemeines*, o. J.).

SNOMED CT (Systematized Nomenclature of Medicine and Clinical Term)

Es ist für eine unmissverständliche Kommunikation unverzichtbar, dass mit derselben Fachterminologie kommuniziert wird. SNOMED CT ist ein international angewendetes klinisches Terminologiesystem, welches für die ePA genutzt wird. Es werden einzelne klinische Befunde, Prozeduren, Substanzen und sozialer Kontext als Zahlencodes definiert. So können Leistungserbringer mit Hilfe von Codes unmissverständlich eintragen, welche Zustände vorliegen und welche Maßnahmen getroffen worden sind. Die Codes sind einer disjunkten Baumstruktur untergeordnet, so dass eine Diagnose beispielsweise einem übergeordneten Kapitel untersteht. In Deutschland ist dieses Terminologiesystem im März 2020 eingeführt worden in englischer Sprache und Teil der eHealth-Strategie der Bundesregierung geworden.

Seit 2023 ist sie die gesetzlich vorgegebene Terminologie für MIOs und die ePA (Sievers, 2024). In Abbildung 2-1 wird das Konzept veranschaulicht, mit dem SNOMED CT arbeitet. Die Diagnose Herzinfarkt, hat eine geltende Beschreibung, aber mehrere Synonyme, die je nach Präferenz ebenfalls genutzt werden. Letztendlich weisen aber alle Beschreibungen auf eine spezifische Diagnose hin, welche unmissverständlich wird durch den Zahlencode.

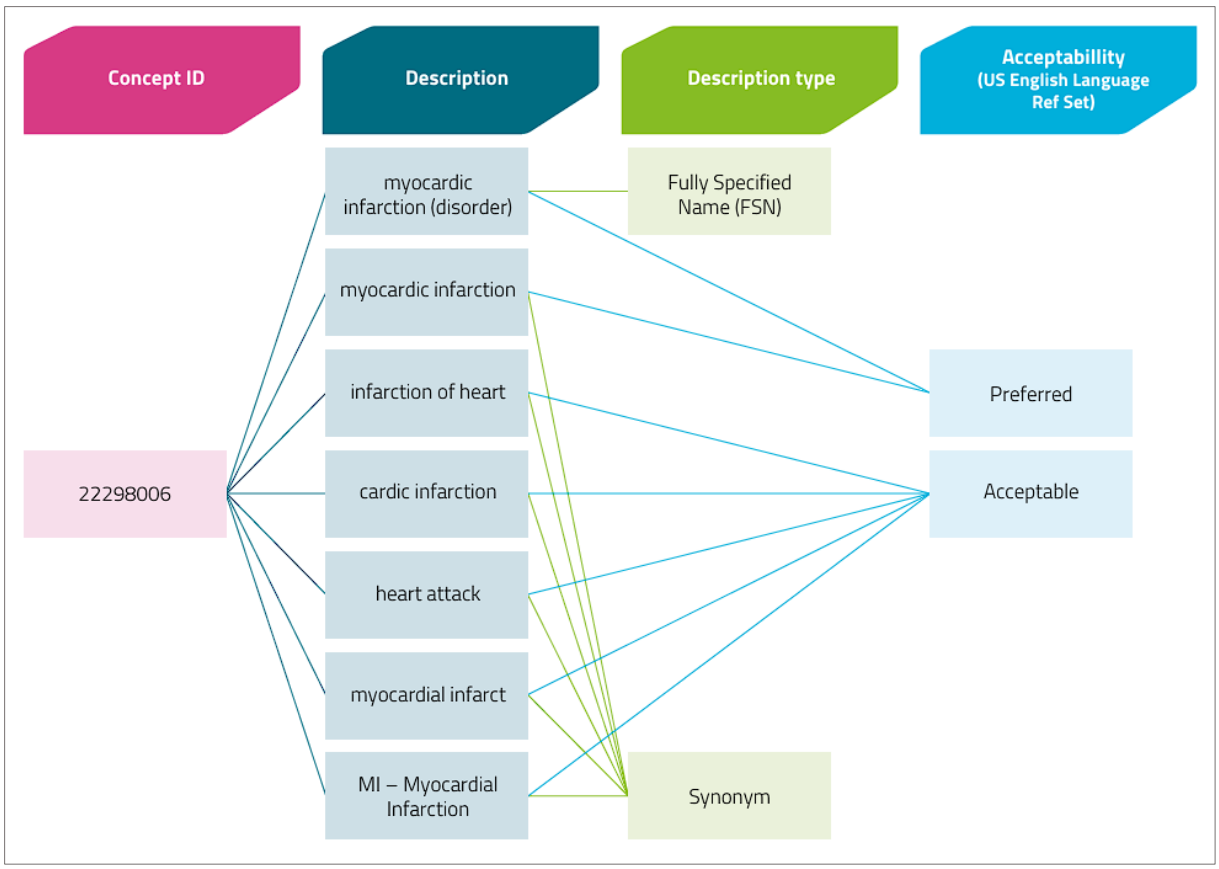


Abbildung 2-1 Veranschaulichung einer SNOMED CT Terminologie am Beispiel einer Herzinfarkt-Diagnose (Sievers, 2024)

KIM (Kommunikation im Medizinwesen)

Ein sicheres E-Mail-Verfahren innerhalb der TI, das üblicherweise mit Ende-zu-Ende-Verschlüsselung und digitaler Signatur zur Kommunikation medizinischer Unterlagen oder der elektronischen Arbeitsunfähigkeitsbescheinigung verwendet wird. Alle Nutzer sind in einem Verzeichnisdienst registriert, das einem typischen Lightweight Directory Access Protocol (LDAP)-Adressbuch entspricht. Eine versendete Nachricht wird mittels Konnektors verschlüsselt und digital signiert und landet dann auf dem KIM-Clientmodul, welches einem Simple Mail Transfer Protocol (SMTP) – Server ähnelt und das Versenden, Weiterleiten und Empfangen von E-Mails koordiniert. Der KIM-Fachdienst, ein Mailserver, versendet dann die Nachricht an den Empfänger, wo sie entschlüsselt wird und gelesen werden kann. Die aktuelle Version 1.5 erlaubt eine E-Mail-Kommunikation ohne Größenbeschränkungen. Die zukünftige Version 2.0 soll TI 2.0- und IMAP-fähig sein, wodurch E-Mails

auf einem Server liegen würden und von mehreren Geräten abrufbar wären (*KIM - Kommunikation im Medizinwesen*, 2025).

TI-Messenger

Der TI-Messenger ist eine bereits seit April 2024 verfügbare Nachrichtendienstanwendung, mit der Patienten und Leistungserbringer in Echtzeit korrespondieren können. Der Vorteil dieses Messengers ist, dass er das Matrix-Protokoll verwendet und dadurch unabhängig vom Messenger-Anbieter befähigt ist sektorenübergreifend in Echtzeit mit Ende-zu-Ende verschlüsselten Nachrichten zu kommunizieren. Der TI-Messenger ist damit eine Lösung mit hohem Sicherheitsniveau. Er ist ein zusätzliches Tool zu KIM und soll das Telefon irgendwann vollständig ersetzen, bei der Terminorganisation und dem Austausch innerhalb des Teams unterstützen sowie eine unkomplizierte Möglichkeit sein Rückfragen stellen zu können. Die ePa-Variante des Messengers ist in der elektronischen Patientenakte integriert und ermöglicht Patienten die Kommunikation mit Leistungserbringern und Krankenkassen (*TI-Messenger*, 2025).

2.4 Malware und Cyberangriffe

Es gibt eine Vielzahl an Malware und Cyberangriffstypen, von denen hier einige aufgeführt werden, die wahrscheinlicher sind, weil sie bereits aufgetreten sind.

DDoS-Angriff

DDoS steht für Distributed Denial-of-Service und ist im Prinzip ein Angriff auf die Verfügbarkeit. Bei diesem Angriffstyp wird das anzugreifende Ziel, ein Server, Dienst oder eine Website, mit Anfragen so stark überhäuft, dass das Ziel überlastet wird, weil es der Bearbeitung der Anfragen nicht mehr nachkommen kann. Die Konsequenz ist eine Verlangsamung oder gar ein Ausfall des Systems, so dass Nutzer keinen Zugriff mehr haben. Um diesem Angriffstyp entgegenzuwirken, gibt es Präventivmaßnahmen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018b):

- DDoS-Erkennung: mit Hilfe des Internet Service Providers (ISP) kann die Gefahr früh erkannt werden. Es müssen aber vorher schon Vereinbarungen mit dem ISP getroffen worden sein, damit auf seine Unterstützung gezählt werden kann.
- Checkliste: für eine angemessene Reagibilität mit Fahrplan ist eine Checkliste hilfreich. Hierzu bietet das BSI die Checkliste „Abwehr von DDoS-Angriffen“ (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018a) mit durchzuführenden Maßnahmen an.
- Anwendungen zur Verkehrs- und Dienstanalyse: Server sollten mit diesen Anwendungen ausgestattet sein, um Gefahren frühzeitig zu erkennen.
- Netzwerksegmentierung: mit mehreren Netzwerksegmenten, auf denen unterschiedliche Dienste bereitgestellt werden, wird verhindert, dass alle Dienste ausfallen, weil sie auf einem einzigen Netzwerk gelegen haben.

- Netzwerkinfrastruktur: das Netzwerk sollte fähig sein im Falle einer höheren Belastung nicht direkt zusammenzubrechen. Um dies zu erreichen, wird empfohlen Proxy-Server zur Abwehr und Loadbalancer zur Lastenverteilung zu verwenden und einzelne Netzsegmente durch Begrenzung des Datenverkehrs zu schützen.
- Überprüfung des eigenen Systems auf seine Leistungsgrenzen: um die Wahrscheinlichkeit und das Potenzial einer Gefahr einschätzen zu können und zu verstehen, wie die Gegenmaßnahmen aussehen müssen, muss eine richtige Einschätzung über die Überlastungsgrenzen und Schwachstellen existieren.
- Konfiguration: nach einer richtigen Einschätzung sollte das System entsprechend eingestellt werden, um Angriffe abzumildern. Dazu gehören Proxyserver, DoS-Schwachstellen erkennen, keine üblichen Voreinstellungen nutzen.
- DDoS-Abwehrsysteme: es gibt Softwarelösung für eine Abwehr oder Abschwächung eines Angriffs, die zusätzlich herangezogen werden können. Jedoch kann eine solche Software unter Umständen den normalen Betriebsverkehr beeinträchtigen.

Ransomware

Ein häufiger Angriff in Sachen Cyberkriminalität ist der Ransomware-Angriff, bei dem Daten nicht mehr zugreifbar gemacht werden, indem sie mit Hilfe einer Schadsoftware verschlüsselt werden oder der Zugriff zu ihnen blockiert wird. Über veraltete Software, Phishing-Mails oder Smishing gelangen Angreifer in das System. Mit Hilfe von Social Engineeing werden E-Mails und SMS derart abgestimmt auf das Opfer zusammengestellt, dass er nur schwer erkennen kann, dass es sich dabei um einen Hackerangriff handelt. Im System angekommen, gelangen sie bis in die zentralen Komponenten, eignen sich alle Rechte an und können das System vollständig ausspionieren. Wenn es sich um ein finanziell lohnendes Ziel handelt, betreten die Angreifer die nächste Phase und verschlüsseln Daten, so dass das Opfer nicht mehr handlungsfähig ist. Dann stellen sie Forderungen in einer Nachricht, in der die Freigabe der Daten nur dann erteilt wird, wenn das Opfer auf die Forderungen eingeht, wie beispielsweise Lösegeld. Zusätzlich kommt es vor, dass zur Druckerhöhung Daten gestohlen werden, um damit zu drohen diese zu veröffentlichen. Es wird vom BSI empfohlen nicht auf die Erpressungen einzugehen und stattdessen das System komplett neu aufzusetzen. Verlorene Daten sollen aus sicheren Backup-Quellen wiederhergestellt werden, sofern sie nicht ebenfalls Teil des Angriffs geworden sind. Ist dies der Fall, kann versucht werden mit den Angreifern zu verhandeln, um den Schlüssel für die Entschlüsselung zu erhalten. Es besteht jedoch stets die Gefahr, dass kein funktionierender Schlüssel übergeben wird oder nur eine fehlerhafte Entschlüsselung das Ergebnis ist. Es wird daher empfohlen stärkere Präventivmaßnahmen einzuläuten, um so einem Angriff gar nicht erst ausgesetzt zu sein. Zur Prävention sollten alle Systeme und jede Software auf dem aktuellen Stand sein, um die nötigen Sicherheitsupdates installiert zu haben. Das Netzwerk sollte segmentiert werden, um einer vollständigen

Übernahme entgegen wirken zu können, mit einem Application-Whitelisting dürfen nur ausgewählte Anwendungen im System installiert sein, Remote-Verbindungen über VPN sollten einer 2-Faktor-Authentifizierung unterliegen. Ein Datensicherungskonzept, mit dem Backups sinnvoll durchgeführt werden, retten Daten und schützen vor Erpressung. Der Nutzerverwaltungsbereich eines Systems sollte stärker geschützt werden, damit Angreifer nicht alles übernehmen können. Der Nutzer eines Systems müssen regelmäßig über Phishing und Smishing aufgeklärt werden (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021, 2022).

3 Die ePA in Deutschland

3.1 Struktur und Verantwortlichkeiten

3.1.1 Akteure und Verantwortlichkeiten

Mit der am 11. Januar 2005 gegründeten gematik GmbH hat die Bundesrepublik Deutschland ihrem Vorhaben einer Digitalisierung des Gesundheitswesens eine Steuereinheit gegeben, die ihre Wünsche in Ideen und Projekte umsetzen soll. Der Name gematik setzt sich aus den Worten: „Die Gesellschaft für Telematikanwendungen der Gesundheitskarte“ zusammen. Sie ist eine Unternehmensgesellschaft, deren Hauptgesellschafter das Bundesministeriums für Gesundheit ist. Die restlichen 49% bestehen aus sogenannten Kostenträger- und Leistungsbringer-Organisationen, zu denen der Spitzenverband der Gesetzlichen Krankenversicherungen (GKV-SV) (22,05%), die Kassenärztliche Bundesvereinigung (7,35%), die Deutsche Krankenhausgesellschaft (5,88%), der Deutsche Apothekenverband (3,92%) und zu jeweils 2,45% der Verband der Privaten Krankenversicherung, die Bundesärztekammer, die Kassenzahnärztliche Bundesvereinigung und die Bundeszahnärztekammer gehören. Mit etwa 93% ist die GKV-SV der Hauptfinanzier der gematik. (Gesellschafter und Gremien, 2025) Entscheidungen zur TI werden von einem Gremium aus den genannten neun Gesellschaftern mit einer Mehrheit aus 51% Zustimmungsanteil getroffen. Dem Gremium beratend fungiert der Beirat, welcher sich aus vertretenden Personen der Kategorien Länder, Patienten, Wissenschaft, Industrie und Berufsgruppen im Gesundheitswesen zusammensetzt. (Geschäftsordnung des Beirats, 2020) Die gematik selbst versteht sich als Kommunikationsstelle, um die verschiedenen Akteure an einen Tisch zu bringen und digitale Lösungen zu erarbeiten.

Die TI ist die Basis, auf der die digitale Medizin fußt, indem sie für Interoperabilität und Kompatibilität innerhalb von Informations-, Kommunikations- und Sicherheitsinfrastrukturen sorgt, die den verschiedenen Rollenträgern innerhalb des Gesundheitswesens ermöglichen miteinander sicher vernetzt zu sein und sich geschützt austauschen zu können. Die TI ist ein Vernetzungssystem, welches von der Bundesrepublik Deutschland in die Wege geleitet worden ist und über verschiedene Instanzen gesteuert, organisiert und umgesetzt wird. Dazu gehört das Bundesministerium für Gesundheit, der Spitzenverband Bund der Krankenkassen, die Kassenärztliche Bundesvereinigung, die Kassenzahnärztliche Bundesvereinigung, die Bundesärztekammer, die Bundeszahnärztekammer, die

Deutsche Krankenhausgesellschaft und die Spitzenorganisation der Apotheker auf Bundesebene (Anforderungen an die Telematikinfrastruktur, 2024).

Für die Realisierung der elektronischen Patientenakte haben mehrere Akteure des Gesundheitswesens unterschiedliche Verantwortungsbereiche und Aufgaben übernommen. Die folgende Auflistung zeigt eine Übersicht hierzu:

Akteur	Verantwortung
Bundesministerium für Gesundheit (BMG)	Gesetzgebung, Finanzierung, politische Steuerung, Eigentümer der Gematik GmbH
Gematik GmbH	Betreiber der TI Technische Entwicklung, Standards, Interoperabilität, Zertifizierung,
Gesetzliche Krankenkassen	Entwicklung und Betrieb eigener ePA, Aufklärungspflicht
Kassenärztliche Bundesvereinigung (KBV)	Vertretung für Ärzte, Integration in die Praxissoftware
Ärzte, Apotheken, Krankenhäuser	Umsetzung vor Ort, Anbindung an die TI, Datenpflege in der ePA
IT-Hersteller und Anbieter	Herstellung von Software für Praxen und Kliniken zur Anbindung an die ePA
Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI)	Datenschutz und Informationsfreiheit
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Sicherheit und Zertifizierung
Health Innovation Hub (hih)	Beratung und Kommunikation
Beirat Digitalstrategie, Kassenärztliche Bundesvereinigung, Bundesärztekammer	Begleitende Beratung, Integration
Gesetzliche Krankenversicherungen (GKV) Informatik	IT-Infrastruktur und Kartenverwaltung
Forschungsdatenzentrum Gesundheit	Forschungsunterstützung

Tabelle 3-1 Akteure zur Einführung der ePA (BMG)

3.1.2 Die Telematikinfrastruktur

Die TI ist ein digitales Netzwerk, besteht aus mehreren technischen Komponenten und ist die zentrale Schnittstelle für viele Anwendungen. Die TI arbeitet mit einem System aus technischen, organisatorischen und rechtlichen Maßnahmen, um den Datensicherheitsaspekten Verfügbarkeit, Integrität und Vertraulichkeit gerecht zu werden. Hierzu hat die TI ein „dreistufiges Sicherheitskonzept“, in dem die Dienste, Anwendungen und Komponenten konzipiert und anschließend einer Prüfung unterzogen werden, um die Zulassung zu erhalten. Zuletzt werden alle technischen Entwicklungen einer ständigen Beobachtung über das gematik „Computer Emergency Response Team (CERT)“ unterstellt, um Schwachstellen zu identifizieren und Bedrohungen abzuwehren. Außerdem kann jede Person, die eine Schwachstelle oder ein Problem entdeckt innerhalb der TI, diese dem „Coordinated Vulnerability Disclosure Program“ melden, damit sie sich dem Problem annehmen oder eine vorliegende Straftat an die entsprechenden Behörden weiterleiten können. Die Meldung bleibt diskret und wird beantwortet.

Zu den technischen Komponenten der TI gehören:

- der Konnektor: ist sicherheitszertifiziert und stellt Verbindung zur TI her
- das eHealth-Kartenterminal: zur Authentifizierung mittels Smartcard (Erfüllung der Vertraulichkeit) und Nutzung einiger Anwendungen
- die Smartcards zur Authentifizierung gegenüber der TI:
    - elektronischer Heilberuflerausweis (eHBA): Heilberufler, wie Ärzte etc.
    - elektronischer Berufsausweis (eBA): Gesundheitsberufe Handwerk, wie Optiker etc.
    - Security Module Card (SMC-B, physischer Ausweis) oder SM-B (digitaler Ausweis): Praxen, Einrichtungen
    - elektronische Gesundheitskarte (eGK): Patienten
- Anwendungen:
    - Versichertenstammdatenmanagement (VSDM)
    - Notfalldatenmanagement (NFDM)
    - elektronischer Medikationsplan (eMP)
    - elektronische Rezept (E-Rezept)
    - KIM
    - elektronische Arbeitsunfähigkeitsbescheinigung (eAU)
    - elektronischer Arztbrief (eArztbrief)
    - ePA

Ähnlich wie ein DSL-Router, aber mit einem hohen Sicherheitsniveau, ermöglicht ein Konnektor die Verbindung eines Leistungserbringers zur TI über VPN. Unter den Konnektoren gibt es mehrere

Versionen mit verschiedenen Funktionsmöglichkeiten, die unterschiedlich oft in Umlauf sind. Es gibt die Versionen „PTV1“, „PTV3, „PTV4“, „PTV4+“, „PTV5“, „PTV5+“, von denen die einfachste Version PTV1 die technischen Mindestanforderungen hat, um sich mit der TI zu verbinden, während jede weitere Version ein Upgrade zur vorherigen darstellt. Für die Verwendung der elektronischen Patientenakte müssen Leistungserbringer die neuesten Versionen verwenden. Ein Produktbeispiel von einem gängigen Anbieter ist die „KoCoBox MED+“ von der KoCo Connector GmbH (siehe Abbildung 3-1 und Abbildung 3-2). Sie fällt in die Kategorie PTV5+ und erfüllt die neusten technischen und sicherheitsspezifischen Anforderungen durch ihre ECC-Sicherheitstechnologie und Kompatibilität mit der elektronischen Patientenakte 2.5.

Abbildung 3-1 KoCoBox MED+ Konnektor, Frontansicht (KoCo Connector, 2025)

Abbildung 3-2 KoCoBox MED+ Konnektor, Rückansicht (KoCo Connector, 2025)

Smartcards ermöglichen erst das Auslesen von Notfalldaten und Signieren von Befunden und das Ausstellen von Rezepten und elektronischen Arbeitsunfähigkeitsbescheinigungen.

Die Art und Weise wie Leistungserbringer über die aktuelle TI als Netzwerk miteinander verbunden sind und sich austauschen können, zeigt die Grafik in Abbildung 3-3.

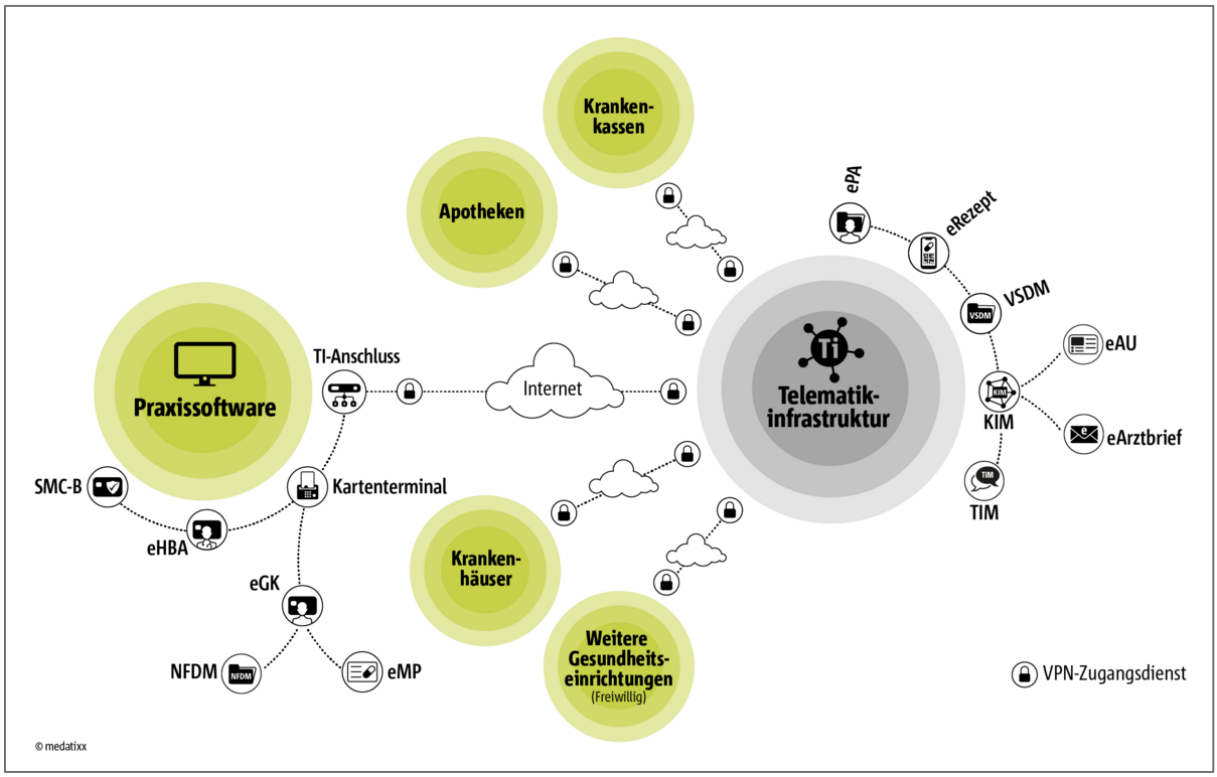


Abbildung 3-3 Vernetzung innerhalb der TI (mediatixx, 2025a)

Mit der Einführung von TI 2.0 plant die gematik eine Umstellung in die TIaaS (TI as a Service), welche eine fortschrittliche Anbindung an die TI mittels cloudbasierter Technologien ist, so dass physische Konnektoren bald nicht mehr benötigt werden sollen. Eine moderne Sicherheitsarchitektur, welche das Zero-Trust-Modell, die mTLS-Verschlüsselung und das TI-Gateway enthalten soll, sind die Wegbereiter für diesen Plan. Das Zero-Trust-Modell bedeutet als Sicherheitsstrategie, dass jeder nur notwendige Zugriff nach strengem Maß mittels Authentifikation kontrolliert, sicher Ende-zu-Ende verschlüsselt und dann autorisiert wird. Außerdem wird Anfragenden kein implizites Vertrauen zugewiesen, sondern unparteiisch jeder Zugriffsversuch geprüft. Damit wird die Anzahl der Zugriffe eingegrenzt und kann besser überwacht werden.

Die sogenannte TI-Gateway ist Teil der TI 2.0 und bietet die Möglichkeit sich über VPN und einem zertifizierten Dienstleistungsanbieter virtuell an einen Highspeed-Konnektor, der in einem Rechenzentrum steht, zu verbinden und darüber dann die Verbindung zur TI herzustellen. Der Vorteil ist, dass stets auf dem neusten Softwarestand inklusive aller Sicherheitsaspekte agiert wird. Mit digitalen Identitäten für Leistungserbringer, wie die GesundheitsID für Patienten, entfällt in Zukunft für Leistungserbringer die Authentifizierung und Identifizierung über Smartcards. Dieser Umstieg ist mit dem Ziel verbunden mehr Sicherheit und Mobilität und weniger Kosten in Verbindung mit Hardwareanschaffung, -wartung, -ausfall zu schaffen. Außerdem wird der Weg für vielseitige digitale medizinische Anwendungen eröffnet. Der Übergang zur TI 2.0 geschieht schrittweise, so dass bis zur vollständigen Umstellung die physischen Konnektoren ihre nur fünf Jahre gültigen Zertifikate

verlängern müssen und spätestens 2026 auf die aktuell vorgesehenen ECC-Zertifikate umsteigen müssen.

Die Abbildung 3-4 zeigt in einer Übersicht am Beispiel einer Arztpraxis, wie sich die Praxis über ihre Praxissoftware, dem Kartenterminal und einem VPN-Client mit dem Konnektor des TI-Gateway-Dienstanbieter verbindet. Über diesen Konnektor wird dann eine erfolgreiche Verbindung zur TI realisiert.

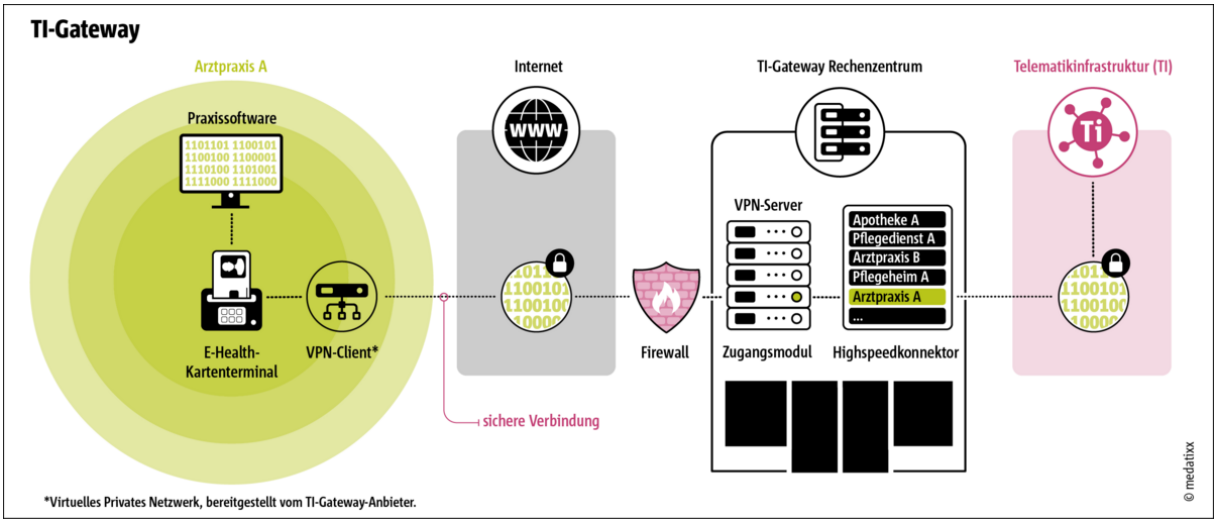


Abbildung 3-4 Die Verbindung von der Praxis zur TI über die TI-Gateway (mediatixx, 2025b)

Als offizielle Zulassungsstelle kann auf der Website „gematik Fachportal“ entnommen werden, dass zum Zeitpunkt der Verfassung dieser Arbeit 76 Institutionen zugelassen sind, um eine TI-Gateway anzubieten (gematik Fachportal, 2025d).

Es hat viele Jahre gedauert bis Arztpraxen und andere medizinische Einrichtungen gesetzlich verpflichtet worden sind sich über die TI zu verbinden. Für die entstehenden Anschaffungskosten wird ihnen eine monatliche Pauschale gezahlt. Sollte es an Diensten fehlen kann diese Pauschale gekürzt oder gar gestrichen werden. Wenn eine Praxis keine Anbindung zur TI hat, ist per Digital-Gesetz eine Honorarkürzung von bis zu 3,5% zur Strafe die Folge (Kassenärztlichen Vereinigung Hamburg, 2024).

Unter allen bisherigen Anwendungen der TI „ist die ePA die zentrale Anwendung der TI“ (Themen: Digitalisierung: Digitale Anwendungen: Telematikinfrastruktur: ePA, kein Datum), da sie Patienteninformationen aus verschiedenen medizinischen Einrichtungen bündelt und diese vernetzt und Dreh- und Angelpunkt in der digitalen Gesundheitsversorgung ist.

3.2 Die ePA – Anwendung

3.2.1 Technisches Konzept

Die Anforderungen des PDSG (Prof. Dr. Kuhlmann, 2020) an die Applikation sind unter anderem eine intuitive und einfache Bedienbarkeit, die den meisten Altersgruppen gerecht wird, ein geschützter

Zugriff, die rückwirkende Nachvollziehbarkeit von Änderungen an Daten und eine permanente Verfügbarkeit auf die medizinische Akte. In diesem Sinne sind mehrere zentrale Komponenten entwickelt worden:

- Zugang in die Akte über den Zugangsgateway
- Autorisierung von Zugriffsrechten und Verwaltung von Schlüsseln
- Dokumentenverwaltung
- Kontoverwaltung

Zu diesen Komponenten gehören verschiedene Funktionen und Sicherheitsstandards, die im Laufe der Zeit seit der erstmaligen Einführung der ePA im Jahr 2021 durch mehrere Versionen herausgegeben worden sind. Mit steigender Version ist das Spektrum an Funktionalitäten vergrößert und die Technologien und Maßnahmen zur Sicherheit verbessert und weiterentwickelt worden. Die Version 3.0.5 enthält folgende Features:

- Es können Dokumente mit einer maximalen Größe von 25MB hochgeladen werden. Dazu gehören ärztliche Befunde und Briefe, Medikationsliste, Laborergebnisse, medizinische Bildaufnahmen und ähnliches. Patienten haben die Möglichkeit die Dokumente einzusehen, zu verbergen oder zu löschen. Es ist jedoch nicht möglich ein Dokument nur für einzelne Personen/Einrichtungen sichtbar zu machen, sondern nur das Dokument für sich wird verborgen oder ist sichtbar für alle.
  ➔ In Zukunft soll es einen elektronischen Medikationsplan geben und eine Volltextsuche[1].
- Medikationsdaten werden in pseudonymisierter Form an das FDZ übermittelt.
  ➔ In Zukunft sollen weitere Daten an das FDZ gehen.
- Es können Vertreter für die ePA eingesetzt werden, wenn der Patient selbst nicht in Lage ist, die ePA zu verwalten. Vertreter können Angehörige oder nahestehende Personen sein, oder die Pflegeeinrichtung. Es können maximal fünf Vertreter ausgewählt werden, die nicht unbedingt dieselbe Krankenkasse haben müssen wie der Patient. Der Vertreter muss selbst registrierter Nutzer der ePA-Anwendung sein, mit der er Zugriff auf die Patientenakte des Patienten erlangt.
- Der TI-Messenger ist integriert worden für eine direktere Kommunikation in Echtzeit.

In Abbildung 3-5 wird die Funktionsweise der ePA innerhalb der TI dargestellt, wobei die Zusammenhänge der einzelnen Rollen und Schritte veranschaulicht sind. Gezeigt wird, wie sowohl über die Software von Leistungserbringern medizinische Dokumente als auch über die ePA-Anwendung von

[1] Die derzeitige Suchfunktion basiert auf einer Metadatensuche. Das heißt, dass der Ersteller eines Dokuments eigenständig Schlagworte zu diesem Dokument einpflegen muss, so dass das Dokument bei der Suche nach einem dieser Worte in den Suchergebnissen auftaucht. Es ist bereits ein Update auf die Volltextsuche geplant. Im Moment können nur Begriffe aus dem Medikationsplan, wie bei einer Volltextsuche, gesucht und gefunden werden.

einem privaten Gerät auf das ePA-Aktensystem zugegriffen wird. Außerdem übermitteln die Krankenkassen ihre Abrechnungsdaten und der E-Rezept-Server die Daten der E-Rezepte. Der XDS Document Service verwaltet die Dokumente im Aktensystem, bietet eine Metadatensuchfunktion an und ruft die Dokumente ab. Der FHIR Medication Service legt alle verordneten Medikamente aus den E-Rezepten in die elektronische Medikationsliste ab.

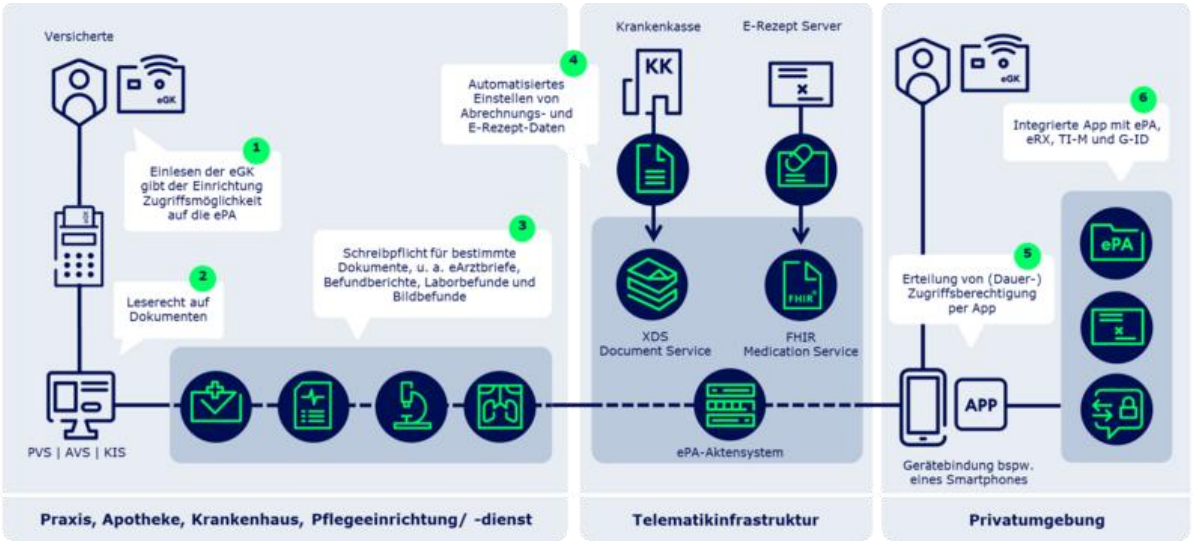
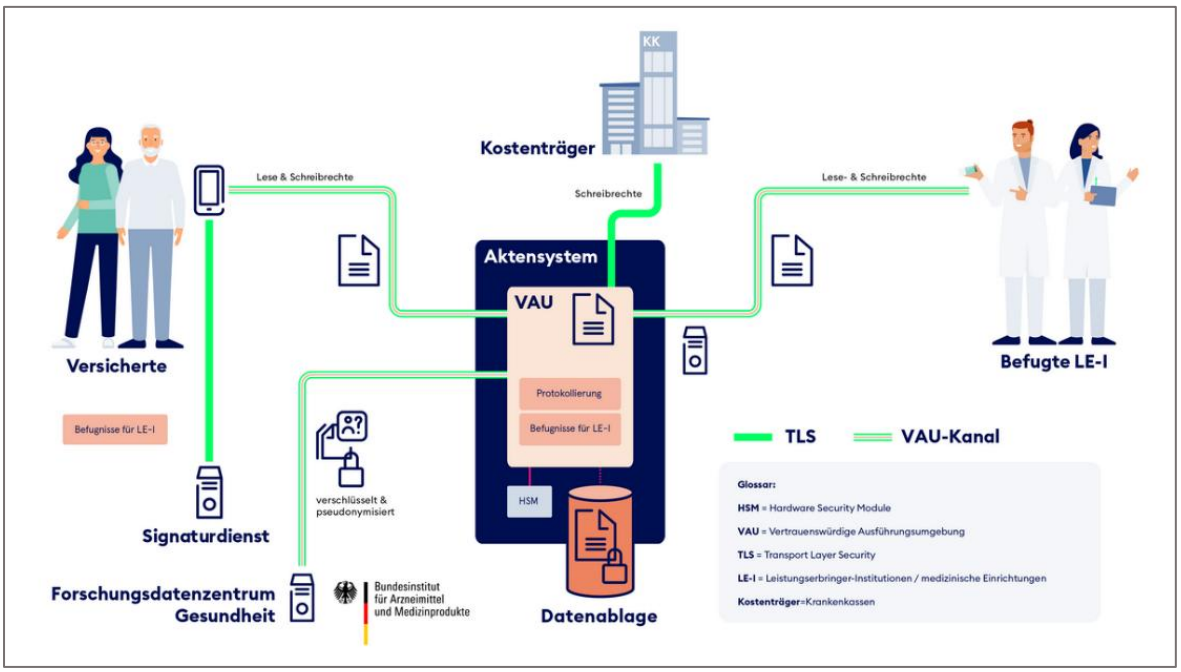


Abbildung 3-5 Die grundlegende Architektur der ePA (gematik Fachportal, 2025a)

3.2.2 Sicherheitsstruktur

Die

Abbildung 3-6 zeigt die Sicherheitsarchitektur der ePA, in der Patienten und Leistungserbringer, wie



Ärzte, in einer VAU die Inhalte der ePA lesen und selbst Eintragungen vornehmen können.

Abbildung 3-6 Schaubild zur Sicherheitsarchitektur der ePA (gematik, 2025b)

Die VAU ist ein isolierter TLS-verschlüsselter Bereich zur Datenübertragung, der vor unbefugtem Zugriff schützt. Während des Transports über die VAU-Verbindung sind die medizinischen Daten zusätzlich verschlüsselt. Bevor die Daten im VAU des Aktensystems ankommen, passieren sie das Access Gateway, welches über Paketfilter den Zugriff von außen nochmal absichert. Im VAU des Aktensystems angekommen, werden die Daten mit einem individuellen komplexen Datenablageschlüssel verschlüsselt, der sicher und unzugänglich im Hardware Security Module (HSM) liegt. Jeder Zugriff auf die Daten und Dokumente im Aktensystem wird protokolliert und ist nur mit erteilter Erlaubnis des Patienten möglich. Zur Authentifizierung des Absenders werden die Daten mittels TLS-Verbindung digital signiert über einen zertifizierten Signaturdienstleister. Die Daten, die an das FDZ übermittelt werden, laufen verschlüsselt und pseudonymisiert über eine eigene VAU-Verbindung. Die Kostenträger haben nur Schreibrechte über eine TLS-Verbindung und dürfen die Dokumente im Aktensystem nicht lesen.

Die ePA hat keinen eigenen Virenschutz, da ein solches Schutzprogramm nicht in der Lage ist alle existierenden Viren zu kennen und zu erkennen. Denn täglich kommen neue Viren hinzu und es ist einfacher und sicherer, wenn der Fokus auf die Daten und Dokumente gelegt wird, die in der Akte verarbeitet werden sollen. Computer, auf denen die ePA genutzt wird, sollten trotzdem ein Virenschutzprogramm haben.

Für das Hochladen von Dokumenten ist der XDS Document Service der ePA verantwortlich. Der Service akzeptiert nur Dokumente mit den Dateiendungen pdf (nur PDF/A-1 und 2), txt, xml, p7 und json entsprechen. Die einfache PDF kann ausführbaren Code enthalten und wird aus Sicherheitsgründen abgelehnt. Außerdem müssen die Formate txt, xml und json UTF-8 zeichenkodiert sein (gematik, 2025d).

Zugriff

Die Krankenkassen haben jeweils einen Schlüsselgenerierungsdienst 1 (SGD1), welcher der eGK einen Schlüssel generiert. Ein zweiter Schlüsselgenerierungsdienst, D-Trust, ist die SGD2 der gematik, welcher einen zweiten Schlüssel generiert. Erst wenn beide Schlüsselpaare zusammenkommen, ist ein Zugriff auf die ePA technisch möglich. Dies soll verhindern, dass Betreiber der ePA auf Patientendaten zugreifen können. Zusätzlich werden beide SGD-Schlüssel mit AES-256 verschlüsselt. Wenn der Patient mit seiner eGK den Zugriff auf die ePA einem Leistungserbringer oder einer Einrichtung im Rahmen einer Behandlung vergibt, besteht eine Gültigkeit von 90 Tagen und verlängert sich mit jedem erneuten Einstecken der eGK ins Kartenlesegerät um 90 Tage. Apotheken erhalten einen Zugriff für drei Tage.

Ein vom Patienten erlaubter Zugriff in die ePA setzt voraus, dass der Patient tatsächlich gerade anwesend ist und diese Erlaubnis erteilt hat. Andernfalls wäre das Potenzial für Missbrauch von Daten und Leistungen sehr hoch. Damit also eine Person berechtigterweise, weil sie versichert und anwesend ist, behandelt werden kann von einem Leistungserbringer, muss sie sicher authentifiziert werden.

Diesem Grundsatz unterliegt die Proof of Patient Presense (PoPP). Die Authentifizierung kann über eine GesundheitsID oder mit der eGK durchgeführt werden, wodurch die Anwesenheit auch mobil sein kann. Eine berechtigte Behandlung wird über den PoPP-Service mit einem „kryptografisch gesicherten PoPP-Nachweis“ festgehalten, dem PoPP-Token, welche Informationen zur Versicherten-ID, Krankenkassennummer, Institutions-ID, Leistungsempfänger-ID, zum Zeitstempel und eine Signatur inklusive Zertifikat zur Verifikation enthält. Der Token wird erst nach erfolgreich verifizierter beidseitiger Authentifizierung erzeugt. Für ein Szenario, bei der eine mobile Behandlung, das heißt ohne physische Anwesenheit des Patienten, stattfinden soll, müssen technische Voraussetzungen gegeben sein. Die eGK und mobiles Kartenlesegerät oder Smartphone müssen NFC-fähig sein. In die Datenbank des PoPP-Service wird dann die Authentifizierung über Authentifizierungszertifikate einmalig gespeichert, so dass eine weitere physische Anwesenheit zur Bestätigung der Identität nicht mehr notwendig ist. Im Zusammenhang mit der TI 2.0, die zeitnah wahrscheinlich der neue Standard sein wird, ist der PoPP-Token auch für Leistungserbringer ein notwendiges Mittel für die kontaktfreie Authentifizierung (gematik, 2024a).

Gemäß dem Prinzip „Vertrauen ist gut, Kontrolle ist besser“ werden für einen strengkontrollierten und deshalb noch sichereren Zugriff die Anwendungen der TI stückweise ab 2026 auf den Zero-Trust-Sicherheitsstandard umgestellt. Die ePA ist noch nicht komplett im Zero-Trust-Sicherheitsstandard umgesetzt worden. So gilt, entgegen dem Zero-Trust-Prinzip, die TI als „trusted zone“ und alle Personen in ihr werden als vertrauenswürdig eingestuft, ein gewährter Zugriff ist ohne erneute Prüfung für 90 Tage gültig und Dienste zur Bereitstellung von zentralen Komponenten werden als vertrauenswürdig eingestuft, ohne einer vorherigen Prüfung mit einer Trust-Domain.

Lese- und Schreibrechte

Solange der Patient die initial vorgegebenen Berechtigungen zum Lesen und Schreiben für alle Nutzergruppen nicht selbst entzieht, gelten diese. Die Berechtigungen betreffen das Erstellen, Anlegen, Hochladen, Herunterladen, Lesen, Schreiben, Aktualisieren und Löschen von Daten bzw. Dokumenten.

Diese initialen Vorgaben sehen für die Nutzergruppen folgendermaßen aus:

Ärzte/Zahnärzte/Psychotherapeuten:

- haben alle Berechtigungen für fast alle Daten und Dokumente
- haben nur Lese- und Löschberechtigung bei Daten vom Patienten selbst kommend, zur Abrechnung von der Krankenkasse oder aus einer Digitalen Gesundheitsanwendung kommend
- mit Patienteneinwilligung: alle Berechtigungen für Patientenverfügung und Vorsorgevollmacht, Organ- und Gewebespende (nur Ärzte/Zahnärzte)

Apotheker:

- haben alle Berechtigungen für den Medikationsplan, Mutterpass, Impfdokumentation, Verordnungen

- haben nur Leseberechtigung auf fast alle Daten und Dokumente, außer Zahnbonusheft, eAU, Rehadaten, Patientenkurzakte, sonstige Daten

Pflegekräfte:

- haben alle Berechtigungen für Daten der pflegerischen Versorgung betreffend
- haben nur Leseberechtigung auf fast alle Daten und Dokumente, außer Abrechnungsdaten der Krankenkassen, eAU, Rehadaten, sonstige Daten
- mit Patienteneinwilligung: nur Leseberechtigung für Patientenverfügung und Vorsorgevollmacht

Heilmittelerbringer (Physiotherapeut und ähnliche Berufsgruppen):

- haben alle Berechtigungen für Befunde, Diagnosen
- haben nur Leseberechtigung auf fast alle Daten und Dokumente, außer Zahnbonusheft, Impfdokumentation, eAU, Rehaten, Vorsorgevollmacht, Patientenverfügung, Organ- und Gewebespende, sonstige Daten

Für den Patienten selbst gelten folgende Berechtigungsvorgaben:

- Alle Berechtigungen für den Medikationsplan, Mutterpass, selbst bereitgestellte Daten, die Patientenverfügung, Versorgungsvollmacht, Organ- und Gewebespende
- Nur Lese- und Löschberechtigung für alle Daten und Dokumente

(gematik, 2025a)

Datenspeicher und Einblick in Quellcode

Die Daten, die in die ePA abgelegt werden, landen über die TI in Rechenzentren mit hohem Sicherheitsstandard. Diese Rechenzentren stehen in Frankfurt am Main, Nürnberg und München und werden von dem Unternehmen IBM vertrieben, das sie über deren „IBM Cloud Satellite“ Technologie miteinander vernetzt. IBM nutzt die Technologien der Plattform Red Hat OpenShift, welche sich auf Hybrid Clouds spezialisiert hat, die für Anwendungen wie die ePA benötigt werden (Silicon Saxony, 2025).

Um das Vertrauen in die Sicherheitskonzepte der gematik zu vergrößern, hat die gematik ihre Vorgehensweise inklusiver Quellcodes öffentlich zur Verfügung gestellt. Die Quellcodes stellen keine abgeschlossene Anwendung dar, geben jedoch einen Einblick in die grundlegende Struktur.

- ePA-Basic inklusiver Vorgängerversionen auf GitHub als open source: https://github.com/gematik/ePA-Basic/tree/ePA-3.0.5
- Mock-Up der ePA zu Test- und Entwicklungszwecke:

Interessierte können in einer lokalen Dockerumgebung die ePA ausführen und zu Testzwecken Daten im VAU-Kanal versenden, einen Medikationsplan einsehen, Kontakt aufnehmen mit dem Informationsservice, ein Dokument anlegen.
https://github.com/gematik/epa-deployment

ePA-App: Anmeldung, Berechtigungen, Dokumente

Die nachfolgenden Erklärungen und Darstellungen werden mit der mobilen ePA-App der DAK-Krankenkasse für Android veranschaulicht. Nach einer erfolgreich abgeschlossenen Registrierung kann die Anmeldung in der ePA durchgeführt werden. Hierzu wird zunächst eine erste Authentifizierung mittels Logins mit Versichertennummer und selbst vergebenem Passwort durchgeführt und anschließend eine zweite Anmeldung mit der eGK und PIN oder mit dem Personalausweis und PIN oder über den vorher eingerichteten App-Code. Die Nutzung des App-Codes ist eine Vereinfachung der Anmeldung und setzt voraus, dass eine Identitätsbestätigung mit eGK und PIN oder Personalausweis und PIN oder in einem DAK Servicezentrum oder über Post-Ident-Verfahren in einer Post-Filiale erfolgt ist. Diese Identitätsbestätigung muss alle sechs Monate erneuert werden. Nach erfolgreicher Anmeldung wird eine Übersicht gezeigt, in der zur Kontoverwaltung, Patientenakte, E-Rezepte-Bereich und zum TI-Messenger navigiert werden kann (siehe Abbildung 3-7).

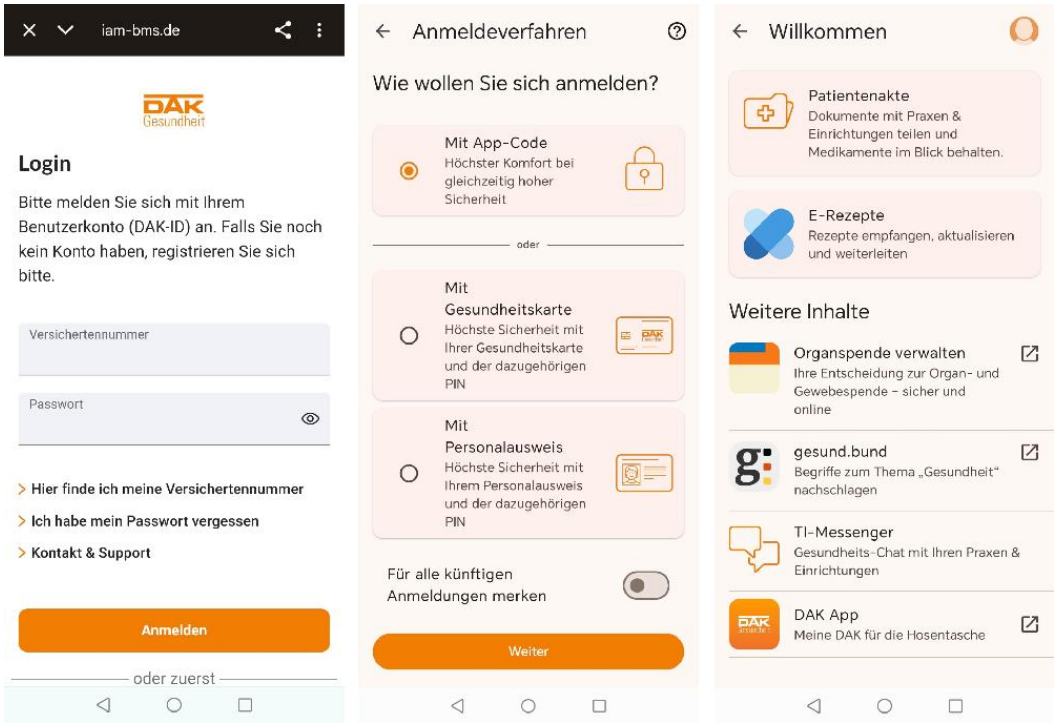


Abbildung 3-7 Anmeldeschritte in der mobile ePA (eigen Darstellung)

Das Benutzerkonto erlaubt die eigene Verwaltung des Kontos mit den aufgezeigten Funktionen (siehe Abbildung 3-8). Im Untermenü der Patientenakte kann diese ebenfalls verwaltet werden, darunter auch die Konfiguration der erteilten Berechtigungen (siehe Abbildung 3-8).

Abbildung 3-8Abbildung 3-8 Verwaltung in der mobilen ePA (eigene Darstellung)

In der App ist es möglich eine Zugangsberechtigung zur Akte für einzelne Leistungserbringer zu vergeben, zeitlich einzugrenzen oder zu entziehen. Außerdem kann bestimmt werden, ob Daten zur Medikation geteilt werden sollen mit einem Leistungserbringer und welche Schreib- und Leseberechtigungen bei welcher Kategorie an Dokumenten vergeben werden sollen (siehe Abbildung 3-9 und Abbildung 3-10).

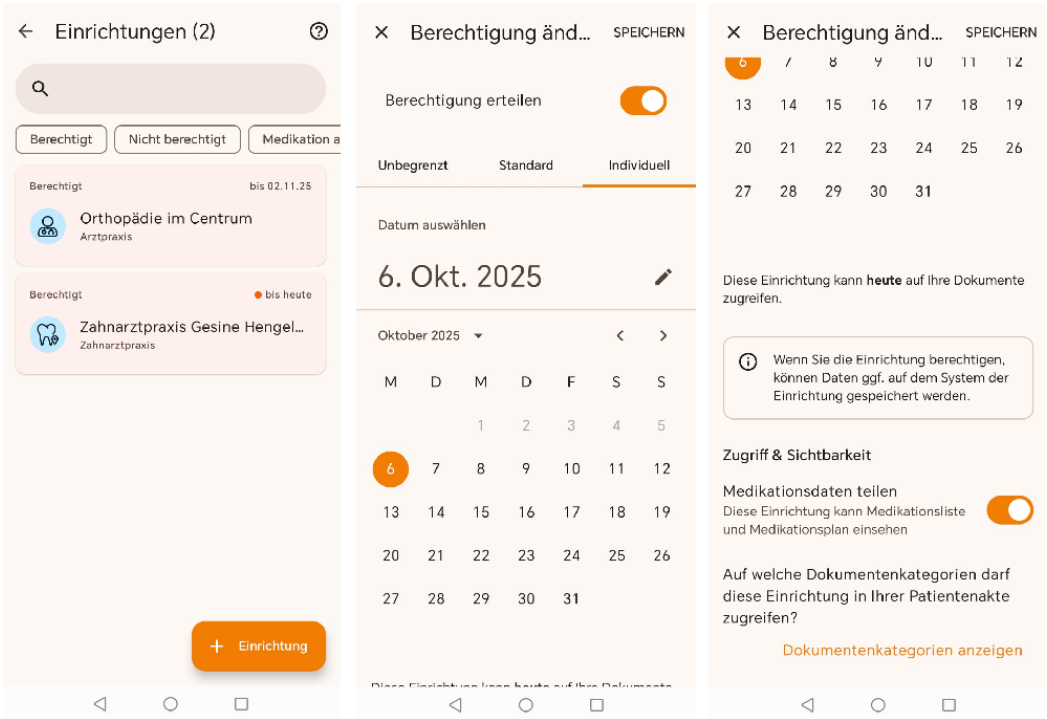


Abbildung 3-9 Erteilung von Berechtigungen, Teil 1 (eigene Darstellung)

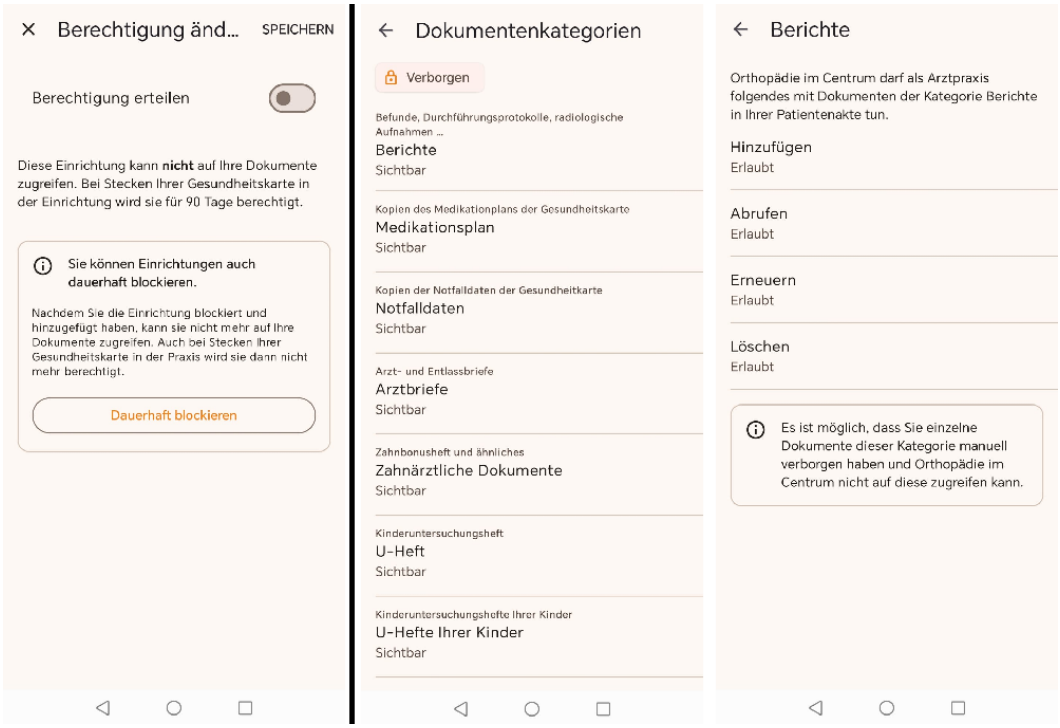


Abbildung 3-10 Erteilung von Berechtigungen, Teil 2 (eigene Darstellung)

Jede vorgenommene Aktivität von allen Zugangsberechtigten kann über das Aktivitätsprotokoll verfolgt werden. Innerhalb der ePA besteht die Möglichkeit einen Widerspruch einzulegen, um die Akte löschen zu lassen, keine E-Rezepte mehr zu beziehen oder keine Abrechnungsdaten der Krankenkasse mehr zu erhalten (siehe Abbildung 3-11).

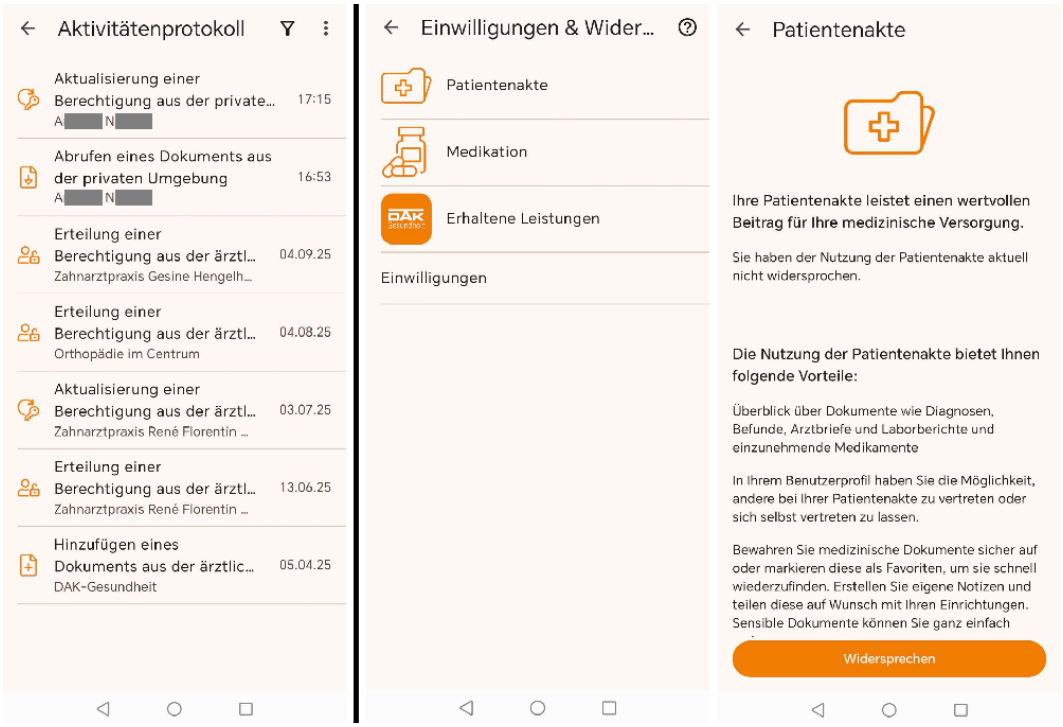


Abbildung 3-11 Aktivitätsprotokoll und Widerspruchsfunktion (eigene Darstellung)

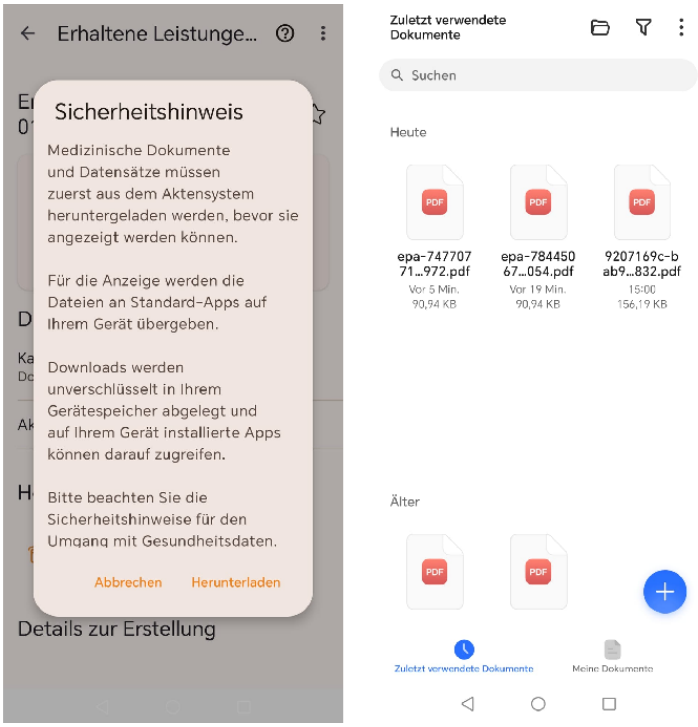


Abbildung 3-12 Dokumentendownload aus der mobilen ePA der DAK (eigene Darstellung)

Dokumente sind nur einsehbar, nachdem sie heruntergeladen worden sind. Die heruntergeladenen Dokumente liegen unverschlüsselt im Gerätespeicher (siehe Abbildung 3-12). Der Patient ist somit selbst dafür verantwortlich seine Daten zu schützen, indem er ein ausreichend sicheres mobiles Endgerät nutzt und dafür sorgt, dass die Daten vor Zugriff anderer Personen geschützt sind.

3.2.3 Kritik und Sicherheitslücken

In Deutschland hat die ePA ihren Einzug im Jahr 2021 auf freiwillige Basis erhalten und erst im Jahr 2025 ist sie verpflichtend für alle gesetzlich versicherten Patienten eingeführt worden. Bisher hat es keinen offiziell bestätigten Sicherheitsvorfall in direktem Zusammenhang gegeben, bei dem Angreifer Daten von Patienten gestohlen oder das System kompromittiert haben sollen. Es sind aber immer wieder Bedenken und Kritik geäußert worden über das Konzept, die Umsetzung und technische Sicherheit der ePA und über die ihr angebundene Strukturen oder Institutionen. Die herausgefundenen und publizierten Schwachstellen und Kritiken zum Konzept werden nachfolgend dargelegt.

Falsch installierte Konnektoren (Jasmin Klofta et al., 2019)

Die Installation von Konnektoren innerhalb von Arztpraxen zur Anbindung an die TI ist zwar von der gematik vorgegeben, jedoch wie im Jahr 2019 festgestellt, von den IT-Dienstleistern in über 90% der Fälle nicht korrekt ausgeführt worden. Die Praxen sind ohne ausreichenden Sicherheitsschutz angeschlossen worden, da die Firewall nicht mehr gegriffen hat und kein zusätzlicher Schutz installiert worden ist, so dass es für Angreifer leicht gewesen ist Patientendaten zu stehlen. Mit der Einführung des Digitalen-Versorgungs-Gesetzes (DVG) Ende 2019 sind IT-Richtlinien für die Installation von Systemen gesetzlich vorgegeben worden, damit nach einem vorgegebenen Standard gearbeitet wird.

Der bisher am häufigsten erwähnte Kritiker der elektronischen Patientenakte ist der Chaos Computer Club (CCC). Die Hacker haben sich mit der Digitalisierung im Gesundheitswesen beschäftigt und umfangreich recherchiert zu den Plänen und Vorgehensweisen zur Gestaltung ePA und äußern sich bedenklich hinsichtlich ihrer Datensicherheit.

Vortrag aus dem Chaos Communication Congress, Dezember 2019 (Tschirsich et al., 2019)

Der CCC kritisiert, dass zwar die rechtlichen und theoretischen Grundvoraussetzungen für Sicherheits- und Datenschutz-anforderungen gegeben seien, aber eine angemessene Identifikation der Leistungserbringer und Patienten fehlen würden. Hierzu sind zwei konkrete Beispiel herangeführt worden:

1. Da Leistungserbringer über das Authentifizierungsverfahren SGD ebenfalls Zugriff zum Aktenschlüssel und damit zur Akte erhalten, würde dies ein Verlust der Zugriffskontrolle für den Patienten bedeuten.
2. Es sei leicht an Smartcard Ersatzkarten heranzukommen zur Authentifizierung, um in die TI Zugang zu finden. In der Kritik steht der Kartenanbieter und Trust Service Provider „medisign".
    a. SMC-B: Benötigt werden die Angaben Betriebsstättennummer, Geburtsdatum, Arztnummer, Nachname und Profession, um einen Ausweis bei medisign zu beantragen. Ein Arztstempel enthalte alle Angaben bis auf das Geburtsdatum, welches unter Umständen schon im Partnerschaftsregister einer Praxis aufzufinden sei. Nach der Prüfung und Genehmigung des Kassenärztlichen Vereinigung, ob ein solcher Arzt existiere, würde der Ausweis und später auch die PIN an die angegebene Lieferadresse, welche eine beliebige Adresse sein kann, geschickt werden. Ab dann bestehe der Zugang zur TI und damit auch die Gelegenheit Ressourcen zu missbrauchen oder Daten zu stehlen.
    b. eHBA: Bei einer Bank ist ein Arzt bereits mit Personalausweis identifiziert. Die Bank bestätigt über das BankIdent-Verfahren dem Kartenanbieter die Identität des Arztes. Die Ärztekammer bestätigt ebenfalls die Identität des Arztes und schon könne der Angreifer wieder in den Besitz des eHBA und der PIN über eine andere angegebene Lieferadresse kommen.
    c. eGK: Es reiche aus bei mehreren Krankenkassen bei angeblichem Verlust und Adressänderung der Karte telefonisch oder per E-Mail um eine neue eGK zu bitten. Eine präzise Identitätsprüfung würde gar nicht erst durchgeführt werden und die neue eGK an die gewünschte neue Adresse zugeschickt werden.
3. Zuletzt heißt es noch, dass zwar die benötigten Anforderungen definiert seien, aber die Umsetzung denen nicht gerecht werde und Ärzte nicht ausreichend aufgeklärt seien zum Thema Datensicherheit.

Deutschlandfunk Interview mit Andreas Meißner, Oktober 2024

Der Psychiater Andreas Meißner äußert sich in einem Interview vom Oktober 2024 dem Deutschlandfunk gegenüber, dass er eine Verletzung der Schweigepflicht in der Handhabung der ePA sehe, da die sensiblen Daten, die von Ärzten dokumentiert werden, auch von beispielsweise Apothekern einsehbar seien (Tobias Armbrüster, 2024).

Vortrag aus dem Chaos Communication Congress 38C3, Dezember 2024 (Tschirsich & Kastl, 2024)

Zum Jahresende 2024 und kurz vor der Einführung der ePA meldete sich der CCC erneut mit Bedenken zur ePA in einem Vortrag auf ihrem Chaos Communication Congress.

1. Das Herankommen an die eGK, SMC-B und eHBA ist bereits in einem vergangenen Vortrag aus 2019 veranschaulicht worden. Mit Hilfe einer SMC-B oder eHBA und einem gekauften Konnektor ist es bereits möglich einen Zugriff auf eine bzw. alle ePA zu erhalten, die dem Leistungserbringer freigegeben und unter dessen Namen die elektronischen Ausweise erstellt worden sind.
2. Glück im Unglück: im Jahr 2019 ist ein Fehler entdeckt worden, bei dem viele Konnektoren falsch installiert worden sind, weil der LAN-Anschluss für das Netz der Praxis an das öffentliche Netz angeschlossen gewesen ist. Damit wäre eine ePA von außen lesbar gewesen, wenn sie bereits eingeführt worden gewesen wäre.
3. Im August 2022 ist es dem CCC gelungen das bis dahin noch eingesetzte Video-Ident-Verfahren zur Identifikation einer Person zu überwinden, indem das Video mit Videotechnik angepasst worden ist und das Hologramm als Sicherheitsmerkmal auf dem Personalausweis gefälscht werden konnte. Mit einer KI und Deepfake-Technik ist das Video-Ident-Verfahren keine Hürde mehr und absolut unsicher. Einem Angreifer wäre es möglich gewesen eine ePA anlegen zu lassen (bis dahin noch freiwillig) und Gesundheitsdaten anzufordern.
4. Mit einem SQL-Injection-Angriff ist es möglich gewesen in den Eingabefeldern von Portalen von Kartenherausgebern Schadcode einzufügen und die Datenbank zu manipulieren, eigene Daten einzuschleusen und eine SMC-B-Karte erschließen.
5. Beim Einstecken der eGK in das Kartenlesegerät wird der medizinischen Einrichtung der Zugang zur ePA ermöglicht. Hierbei wird die Kartennummer ICCSN (Integrated Circuit Card Serial Number) von der eGK elektronisch eingelesen und an den Versichertenstammdatendienst (VSDD) übermittelt, der wiederum einen Prüfungsnachweis herausgibt, welcher an das Versichertenstammdatenmanagement (VSDM+) übermittelt wird und anschließend die Daten der ePA herausgegeben werden. Die ICCSN liegt auf der eGK einmal als einfache Datei und einmal als eine verschlüsselte signierte Datei vor, die die Authentizität der Karte nachweist, vor. Bei der Übermittlung an den VSDD wird aber die unverschlüsselte Datei genutzt. Es bedarf nur die Firewall und andere Schutzmechanismen zu umgehen, um letztendlich zum Zugang in die VSDM+ zu erhalten und Patientendaten einzuholen.

6. Die Zugangsdaten von Praxisverwaltungssystemen sind leicht zugänglich, da medizinische Einrichtungen nicht ausreichend geschützt sind. Die Strukturen innerhalb der Einrichtung können bei so einem Zugriff remote mitgenutzt werden und Zugang zu Daten gewähren.
7. Die Ausgabe von eGK ist noch zu einfach und die Identität des Antragstellers für eine eGK wird nicht ausreichend nachgeprüft. Bereits im Jahr 2023 hat der Bundesbeauftragte für Datenschutz und Informationsfreiheit Ulrich Kelber kritisiert, dass die eGK nur persönlich zugestellt werden solle oder ein Identitätsnachweis muss sichergestellt werden, bevor die eGK aktiviert und angebunden wird an die TI.
8. Geräte und SMC-B-Karten sind auf „Kleinanzeigen“ ohne Hindernisse zu kaufen gewesen, sogar mit PIN. Ebenfalls ist es möglich gewesen sich auf Kleinanzeigen als Dienstleister auszugeben und Hilfe anzubieten zur Installation von Konnektoren und ähnlichem und so auf Wunsch von medizinischen Einrichtungen remote Zugriff zu erhalten.

Die gematik äußert sich zu den Kritiken vom CCC mit Dank und bezieht Stellung zu ihrem weiteren Vorgehen. So heißt es in ihrer Stellungnahme (gematik, 2024b):

„Die zusätzlichen Sicherungsmaßnahmen sind bereits in Erarbeitung und haben folgenden Fokus:

- Verhinderung, dass Ausweise der Telematikinfrastruktur missbräuchlich verwendet werden können.
- Schließung der Sicherheitslücke durch eine zusätzliche Verschlüsselung der Kranken-versichertennummer.
- Sensibilisierung der Nutzerinnen und Nutzer der Telematikinfrastruktur im Umgang und Schutz der technischen Infrastruktur, Ausweisen und Karten.
- Ausweitung der Überwachungsmaßnahmen wie Monitoring und Anomalie-Erkennung.“

Datenleck bei D-Trust, Januar 2025 (dpa/APOTHEKE ADHOC, 2025; Marcel Roth et al., 2025)

Im Antragsportal von „D-Trust“, ein Tochterunternehmen der Bundesdruckerei, welches die Ausweise für Ärzte und Einrichtungen herstellt, hat es ein Datenleck im Januar 2025 gegeben. Die Eingabedaten sind auslesbar und abrufbar gewesen. Das Datenleck hat dazu geführt, dass die personenbezogenen Daten von mindestens 10.000 Ärzten online öffentlich zugänglich gewesen sind. Öffentlich einzusehen gewesen sind Name, E-Mail-Adresse, Geburtsdatum, teilweise Adressen und Ausweisdaten. Die Ursache ist ein Software-Fehler gewesen, der zu einer ungenügenden Zugriffskontrolle geführt hat. Ein Hacker hat diesen Angriff verübt, um auf die Sicherheitslücke hinzuweisen.

CCC entdeckt neuen Sicherheitsmangel (Daniel Leisegang, 2025)

Die gematik hat zur Kritik vom CCC weitere Maßnahmen ergriffen, um den Nachweis eines Behandlungskontextes besser abzusichern. Zuletzt im Dezember 2024 hat der CCC aufgezeigt, dass mit

einfachen Mitteln an die eGK und SMC-B heranzukommen ist und damit ein Zugriff in die ePA. Zu den ergriffenen Maßnahmen hat gehört weitere Merkmale aus der eGK abzufragen, die nur durch ein Einlesen der Karte möglich wären. Hierzu gehören die Versichertennummer, die Kartennummer und ein hash check value (hcv), der sich aus der Wohnadresse und dem Versicherungsbeginn des Patienten errechnet. CCC ist es möglich gewesen diese Hürde zu umgehen, da einige Krankenkassen elektronische Ersatzbescheinigungen (eEB) ausgehändigt haben, auf denen diese Daten verfügbar gewesen sind. Sinn und Zweck der eEB sollte bei Nicht-Einlesbarkeit oder nicht vor Ort sein der eGK ein alternativer Versicherungsnachweis des Patienten sein. Über diese Schnittstelle ist es dem CCC möglich gewesen mit einem schnell selbst gecodeten Programm Daten einzelner Patienten abzurufen und zu manipulieren. Die gematik hat die Schnittstelle sofort geschlossen und nach einer Behebung der Schwachstelle die eEB ab dem 1. Juli 2025 verpflichtend für alle Arztpraxen eingeführt (Dr. Christine von Reibnitz, 2025).

Für einen gesicherten Behandlungskontext ist die bereits entwickelte Lösung das PoPP-Prinzip der TI, welches auf dem Konzept zur Zero-Trust-Architektur basiert. Das Prinzip setzt den Rahmen, dass ein Zugriff in die Patientenakte nur unter der Voraussetzung eines Behandlungskontextes unter Anwesenheit des Patienten technisch erlaubt sein darf.
Die gematik plant die Zero-Trust-Architektur als Teil der TI 2.0 in einem Stufenplan einzuführen, der eine schrittweise Umstellung von Technik und Abläufen bedeutet und die Einführung von PoPP erst für 2026 oder 2027 wahrscheinlich macht. Eine sofortige Umstellung ist deshalb nicht möglich, weil die Theorie zwar da ist, aber die technische und organisatorische Umsetzung nur stufenweise möglich ist. Bis dahin ist angeraten die Patienten darüber aufzuklären die Berechtigungen für die ePA innerhalb der App angemessen zu verwalten und Zugriffe für Leistungserbringer auf ein nötiges Minimum zu gewähren und wieder zu entziehen.

Vortrag aus einer Veranstaltung des CCC, Juni 2025 (Streit, 2025)

Der Arzt und Kritiker der ePA bezieht Stellung mit folgenden Kritikpunkten:

1. Die aggregierten und anonymisierten Daten, die an das FDZ verschickt werden, sind nicht so sicher, wie die gematik behauptet. Mehrere Studien haben gezeigt, dass mit einigen wenigen Attributen Rückschlüsse auf Personen geschlossen werden können. Je mehr Attribute, desto höher die Wahrscheinlichkeit die Person korrekt zu identifizieren. Die Metadaten, die ins Spiel kommen, wenn die ePA auf dem Smartphone genutzt wird, liefern weitere Attribute. Als Rückschlussmittel kommt beispielsweise das E-Rezept in Frage, welches die Angaben vollständiger Name, Geburtstag, Postleitzahl und Datum der Rezeptausstellung enthält.
2. Die Verwendung von künstlicher Intelligenz (KI) erhöhe die Rückschlussquote immens. Wenn eine höhere Datensicherheit priorisiert werde, müssen Daten stärker verändert und reduziert werden, damit die KI nicht mehr in der Lage sei einen korrekten Rückschluss zu ziehen auf eine Person. Jedoch reduziere dies die Nutzbarkeit der KI unter Umständen.

Deutschlandfunk berichtet zur ePA, Juli 2025 (Deutschlandfunk, 2025)

In einem weiteren Bericht vom Deutschlandfunk vom Juli 2025 spricht Thomas Moormann von der Verbraucherzentrale Bundesverband über seine Bedenken.

1. So heißt es darin, dass jede Krankenkasse ihre eigene ePA-App entwickelt habe und Patienten nur über die Vorzüge der ePA informiert seien.
2. Des Weiteren sei nicht genau genug definiert worden, was die „gemeinwohlorientierte" Weitergabe der Daten zu Forschungszwecken bedeuten soll.

Moormann empfiehlt, dass Patienten die Dokumente in der ePA verwalten sollten, um sensible Daten zu Erkrankungen zu schützen und gegebenenfalls zu löschen, auch wenn die Bedienung der ePA herausfordernd sein könne. Welche Daten einsehbar sein sollten, muss der Patient gut überdacht entscheiden, empfiehlt Jürgen Windeler vom Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG).

Die Angriffsszenarien des CCC haben das Potenzial für einen Ransomeware-Angriff und werden für den analytischen Vergleich für Deutschland herangezogen. Es ist gibt aber darüber hinaus immer wieder einzelne Fälle, in denen vor allem Krankenhäuser oder Kliniken ein Datenleckvorfall und ein kompromittiertes System erleben. Zuletzt ist dies im Juli 2025 auf die Ameos Kliniken zugetroffen, wobei durch Zugriff auf lokale administrative Systeme Daten von Patienten und Mitarbeitern gestohlen worden sind und der Betrieb für mehrere Wochen gestört gewesen ist. Es ist noch immer unklar, wem die Daten in die Hände gefallen sind (MDR SACHEN-ANHALT, 2025).

4 Sicherheitsrelevante Vorfälle: Großbritannien

Direkter Angriff auf das NHS-System

Der britische Gesundheitsdienst National Health Service (NHS) ist für die medizinische Versorgung im Land verantwortlich und besteht aus verschiedenen Organisationen, die unterschiedliche Bereiche steuern und organisieren. Im Mai 2017 ist der NHS, wie auch viele Großunternehmen weltweit, Opfer eines Ransomware-Wurm-Angriffs namens „WannaCry" geworden. Eine Schwachstelle, das Dateifreigabeprotokoll SMBv1 (Server Message Block Version 1), im Betriebssystem von Windows ist mit Hilfe des Exploits „EternalBlue" ausgenutzt worden, um sich über sämtliche Netzwerke zu verbreiten. Der Wurm sucht über ein Netzwerk nach Geräten, die ebenfalls diese Schwachstelle vorweisen und installiert und führt sich eigenständig aus, ohne weiteres Zutun. Die Schwachstelle wird bei Microsoft unter der Bezeichnung MS17-010 geführt und ein entsprechender Sicherheitspatch zu ihrer Behebung ist von Microsoft herausgegeben worden. Leider haben sehr viele Windows-Nutzer keine Kenntnis von dem Patch gehabt, so dass ihre Computer dem Angriff ausgesetzt gewesen sind. Die

Angreifer haben etliche Computer lahmgelegt, weltweit mehr als 200.000, und vor die Wahl gestellt innerhalb eines vorgegebenen Zeitraums von drei Tagen 300$ in Bitcoins zu zahlen, um wieder Zugriff zu ihren Daten zu erhalten. Nach drei Tagen ist die Forderung verdoppelt worden. Etwa ein Drittel der NHS Trusts, eigenständige Bereiche, sind betroffen gewesen mit Einschränkungen in Abläufen.

Dies hat zur Folge gehabt, dass es einen Zugangsverlust zu den Patientenakten, die Umleitung von Rettungswagen in andere Einrichtungen, die Verspätung von nicht-dringlichen Operationen und Absagen von mehreren Tausend Patiententerminen gegeben hat. Durch die Schließung des Netzwerkzugriffs ist es zu Ausfällen und Umstellungen gekommen (Collier, 2017; *NHS England business continuity management toolkit case study: WannaCry attack*, 2023):

- Rettungswagen-Zentrale: Übergabe und Bildschirme funktionsuntüchtig, digitale Transportbuchungsübersicht nicht zugänglich
- Keine Übersendung von CT/MRT-Bildern und Chemotherapie-Anordnungen
- Keine automatische Übersendung von Laborergebnissen
- Kein Zugang zu Daten bei einem Teil der Hausärzte

Dies hat dazu geführt, dass viele digitale Strukturen und Abläufe gezwungenermaßen in analoge Prozesse umgewandelt worden sind und dadurch wesentlich langsamer abgewickelt werden konnten.

- Rettungswagen-Zentrale: Kommunikation und Absprachen auf dem Landweg, Ankunft von Rettungswagen unangekündigt, telefonische Umstellung von neuen Buchungen
- Übersendung von CT/MRT-Bildern auf DVDs mit Taxi
- Chemotherapie-Anordnungen per Papier und Fax
- Laborergebnisse per Papier
- Einige Hausärzte sind in der Lage gewesen klinische Patientenakten aufzurufen

Laut NHS England und der National Crime Agency hat die NHS nicht gezahlt und ist damit nicht auf die Erpressungen eingegangen. Jedoch haben die entstandenen Störungen der NHS einen finanziellen Schaden von etwa 92 Millionen Pfund verursacht (NHS Counter Fraud Authority, o. J.).

Es ist gelungen den Angriff mit Hilfe eines „Kill Switch“ einzudämmen, indem ein junger Cyber-Experte entdeckt hat, dass WannaCry vor seiner Ausführung versucht auf eine bestimmte Domain zuzugreifen, die jedoch nicht existiert. Es wird vermutet, dass diese Abfrage dazu gedient hat, festzustellen, ob sich die Ransomware in einer Sandbox befindet. Die Sandbox würde so reagieren, als würde es die Domain tatsächlich geben und die Ransomware veranlassen sich abzuschalten. Die gefälschte Domain im Code ist registriert worden und hat der Ransomware vorgetäuscht in einer Sandbox zu sein. Dieser Umstand ist entweder unbeabsichtigt codiert worden oder eine unfertige Version ist eingesetzt worden, wodurch jedoch weitere Infektionen verhindert werden konnten (Cloudfare, 2025b).

Ransomeware-Angriff auf IT-Unternehmen Advanced Computer Software Group (Advanced)

Advanced hat IT-Dienstleistungen und Software für die NHS angeboten und deshalb auch personenbezogene Daten verarbeitet. Im August 2022 haben es Hacker geschafft sich Zugang in ein Kundenkonto zu verschaffen, das nicht ausreichend geschützt gewesen ist, weil die Multi-Faktor-Authentifizierung nicht vorhanden gewesen ist. Über das Kundenkonto haben sie Zugriff auf Gesundheits- und Pflegesysteme gehabt und dabei Daten von 79.404 Personen gestohlen und NHS-Dienste kompromittiert. Unter diesen personenbezogenen Daten sind auch Telefonnummern, Patientenakten und Informationen zum Reinkommen in Wohnungen von 890 betreuten Personen enthalten. Die Daten sind bisher nicht veröffentlicht worden und Informationen zu einer Lösegeldforderung und Zahlung sind nicht aufzufinden. Advanced ist wegen dieses Fehlers finanziell belangt worden in Höhe von 3 Millionen Pfund. Für den NHS sind durch diesen Vorfall Einbußen in der medizinischen Versorgung entstanden, die durch Mehraufwand und Umstrukturierungen getragen werden mussten. Hinzu kommt der Verlust von zahlreichen Patientendaten und einen indirekten Vertrauensverlust in die Sicherheit der IT-Systeme bei NHS (Anna Lamche, 2025).

Angriff auf externen Dienstleister Synnovis

Ein zweiter Fall hat sich im Juni 2024 ereignet, bei dem der NHS Pathologiedienstleister Synnovis betroffen gewesen ist. Synnovis ist ein großes Pathologiedienstleistungsunternehmen, das für den NHS unter anderem Routineuntersuchungen ausführt. Seit dem Ransomeware-Angriff im Jahr 2017 habe die NHS ihre Sicherheitsbedingungen erhöht, jedoch ist in diesem Fall ein Dienstleister angegriffen worden, der in direkter Zusammenarbeit mit dem NHS gestanden hat. Durch eine ungepatchte Schwachstelle im System sind die Angreifer in der Lage gewesen sich mit einem Exploit Zugriff ins System zu verschaffen. Eine russische Hackergruppe namens Qilin hat die Tat zugegeben und ein Lösegeld in Höhe von 50 Millionen Dollar verlangt, um den Ransomeware-Angriff zu beenden und die verschlüsselten Daten freizugeben. Erneut sind zahlreiche Patiententermine erzwungenermaßen abgesagt, viele Abläufe analog abgewickelt worden und zusätzlich haben Behandlungen mit fatalen Verspätungen erfolgen können. Synnovis hat der Erpressung nicht nachgegeben und neben dem finanziellen Schaden von 32 Millionen Pfund, hat es auch einen Patiententod gegeben, da dringende Laborwerte zu spät angekommen sind. Außerdem sind knapp 400 Gigabyte an sensiblen Daten, wie Patientennamen, NHS Nummern (ähnlich wie eine Versichertennummer), Geburtsdaten und Blutuntersuchungsergebnisse im Dark Web veröffentlicht worden (~goody, 2025; Craig Pepper, 2025).

5 Vergleichende Analyse

5.1 Kriterienwahl

Die Wahl der ausgewählten Kriterien zur Gegenüberstellung hat sich durch die Recherche zum Thema ergeben und den daraus gewonnenen Erkenntnissen welche Faktoren in der Datensicherheit des Gesundheitswesens eine Rolle spielen. Alle Faktoren einzubeziehen wäre nicht mehr dem Rahmen dieser Arbeit gerecht geworden, weshalb folgende Kriterien gewählt worden sind.

Infrastruktur

Die Infrastruktur eines Gesundheitssystems spielt eine gewichtende Rolle in ihrer Gestaltungsform und -freiheit und Gewährleistung von Ressourcen für eine angemessene Datensicherheit.

Technische Infrastruktur

Die technische Infrastruktur zielt darauf ab einen groben Überblick über die technischen Elemente und wie sie zueinanderstehen aufzuzeigen. Das System, das diese Infrastruktur bildet, hat auch Einfluss in der Handhabung von Vorgängen und getroffenen Sicherheitsmaßnahmen.

Technische Sicherheit

Eine Gegenüberstellung von verwendeten technischen Methoden zur Verschlüsselung und Authentifizierung und die Handhabung der Zugriffskontrolle verdeutlichen Unterschiede im Sicherheitsniveau.

Zugriff auf die Patientenakte

Der Zugriff und die Kontrolle über die Daten müssen geregelt sein, damit Unbefugte sich nicht Zutritt zu Systemen und Daten verschaffen können. Diese Parameter sind Kernelemente der Datensicherheit.

Weiterverwendung von Daten

Aus digital gespeicherten Daten wird meistens ein weiterer Nutzen gezogen, indem die Daten an entsprechende Personen oder Institutionen weitergegeben werden. Wohin, für welche Art der Verwendung und wie sicher dies ist, ist nicht überall gleich geregelt und zeigt den Umgang mit diesen sensiblen Daten.

Sicherheitsrelevante Schwachstellen

Die Schwachstellen der IT-Infrastruktur eines Gesundheitssystems sind die Ursache für Cyberangriffe. Diese anhand von Vorfällen oder Sicherheitslücken zu ermitteln, erlaubt ein besseres Bild Maßnahmen zu ergreifen für höhere Sicherheitsstandards.

5.2 Gegenüberstellung und Bewertung

Nachfolgend werden die Gesundheitssysteme in Deutschland und Großbritannien über die vorher genannten Kriterien analysiert und verglichen.

Tabelle 5-1 Die Infrastruktur der verschiedenen Gesundheitssysteme (eigen Darstellung)

	Infrastruktur
Deutschland	Versicherungssystem: gesetzlich und privat
Großbritannien	Steuerfinanziertes System

Das deutsche Gesundheitssystem ist staatlich reguliert und basierend auf dem Bismarck-Modell, welches ein Sozialversicherungssystem gefördert aus Beiträgen von Arbeitgebern und Arbeitnehmern ist, wobei die Beitragshöhe sich an der Höhe des Einkommens orientiert. Dies ermöglicht eine Sicherung des Lebensstandards, da durch soziale Solidarität letztendlich alle Versicherten mit medizinischen Leistungen versorgt werden können. Weitere Finanzierungsmittel sind Steuergelder und private Zuzahlungen. Aber auch die gematik und TI werden aus den Einnahmen der Krankenkassen finanziert. Das britische Gesundheitssystem nennt sich National Health Service (NHS), ist staatlich reguliert und wird für die größte Region von der NHS England geleitet. Der NHS basiert auf dem Beveridge-Modell, welches eine aus hauptsächlich Steuergeldern und zu geringem Anteil Sozialversicherungsbeiträgen finanzierte, medizinische Universalversorgung aller Bürger gewährt. Dieses vor Armut schützendes Modell hat aber den Nachteil, dass nur die Sicherung eines Existenzminimums für medizinische Versorgung geschaffen wird und das begrenzte Budget in manchen Regionen ein Grund für lange Wartezeiten für Termine und Behandlungen ist. Trotz der besseren Umverteilung der Kosten im Beveridge-Modell, da diese nicht vom Lohn abhängig sind, überwiegen die Vorteile für den Patienten im Bismarck-Modell aufgrund des Anspruchs dem Patienten höhere Leistungen anzubieten. Denn Patienten genießen das Privileg sich frei entscheiden zu dürfen zwischen krankenkassen- oder privatfinanzierter medizinischer Versorgung und bei welchem Arzt sie behandelt werden möchten. Die heutige medizinische Versorgung der gesetzlichen Krankenkassen erlaubt es noch auszukommen, entwickelt sich aber tendenziell zu immer mehr Privatzahlungen für Untersuchen oder Behandlungen. In Großbritannien ist für Patienten die Versorgung grundsätzlich kostenlos, jedoch genießt der Hausarzt zum potenziellen Nachteil für den Patienten ein hohes Entscheidungsprivileg ihm eine Weiterbehandlung zu ermöglichen. Patienten sind daran gebunden als erstes den Hausarzt aufsuchen zu müssen, der dann darüber entscheidet, ob eine fachärztliche Weiterbehandlung überhaupt notwendig ist. Alternativ gibt es Privatversicherungen oder die Option als Direktzahler privatärztliche Einrichtungen aufzusuchen, wo Termine schneller vergeben werden, die Behandlungsmöglichkeiten breiter gefächert sind und die Ärzteauswahl und Auswahl an Kliniken größer und freier gestaltet ist. Privatversicherungen

sind allerdings teuer und medizinische Rezepte müssen unabhängig vom Medikament ebenfalls vom Patienten gezahlt werden (Woodgrange Medical Practice, 2025), was dazu führt, dass nur sozial besser gestellte Personen sich eine bessere medizinische Versorgung leisten können. Aus den Finanzhaushalten beider Länder wird jeweils das Budget für das Gesundheitssystem getragen. Dies schließt sowohl die medizinische Versorgung als auch die digitale Umstrukturierung und Versorgung mit ein.

In Deutschland ist die Digitalisierung des Gesundheitssystems ein sehr langsam wachsendes Projekt und noch im Aufbau, wenn berücksichtigt wird, dass die Einführung der ePA seit über 20 Jahren auf dem Plan steht (Bundesministerium für Gesundheit (BMG), 2025b). Verantwortliche Strukturen für die Digitalisierung gibt es erst seit 2005 mit der Gründung der gematik und ihrem Bestreben Prozesse stückweise im Gesundheitswesen zu digitalisieren. Es nehmen allerdings sehr viele Akteure an diesen Prozessen teil, die zwar die Beteiligten aller Parteien im Gesundheitswesen berücksichtigen, aber Entscheidungen, Beschlüsse und Konzepte verzögern. Insgesamt herrscht somit ein Tauziehen zwischen finanziellen, rechtlichen, technisch durchführbaren und im Alltag nutzbaren Aspekten, die den Fortschritt auf sich warten lassen. Nicht zuletzt deshalb ist die ePA, obwohl die sie umgebenden Strukturen noch nicht vollständig bereit und auf sie ausgelegt sind, gemäß der geplanten Agenda der deutschen Politik eingeführt worden. Der Druck als Land mit einem hohen akademischen Hintergrund nicht abgehängt zu werden im Fortschritt ist einer der Gründe dafür. Als Mitgliedsstaat der EU und mit den europäischen Plänen einen gemeinsamen Gesundheitsdatenraum zu schaffen, bewegt sich auch Deutschland in diesen Rahmen und muss bei ihrer Umsetzung als rechtliche Grundlage für die Verarbeitung und Aufbewahrung von Daten die DSGVO und das Bundesdatenschutzgesetz (BDSG) berücksichtigen. Die digitalen Strukturen des NHS sind ausgebauter, da schon erste IT-Strategien in den 1990er Jahren entwickelt worden sind und bereits im Jahr 2005 ein Programm gestartet worden ist, um eine zentralisierte elektronische Patientenakte zu entwickeln (Rainer Thiel et al., 2018). Vielleicht etwas voreilig gehandelt, ist das Programm an der Komplexität dieses Unterfangens gescheitert. Auch Deutschland muss viel umstrukturieren für das Gelingen dieses Vorhabens. Die Digitalisierung des NHS wird größtenteils aus Steuereinnahmen finanziert und von der NHS Digital umgesetzt. Sie unterliegt den rechtlichen Grundlagen für die Verarbeitung und Aufbewahrung von Daten nach The General Data Protection Regulation (GDPR), die der DSGVO entspricht und damit denselben Anspruch stellt wie in Deutschland, und wird von dem Data Protection Act 2018 und neuerdings New UK Data Protection and Digital Information Act ergänzt. Jedoch bleibt weiterhin ein Defizit vorhanden: das Recht auf Löschung von eigenen Patientendaten wird trotz Gesetzgebung nur begrenzt ermöglicht.

Ein vorteilhafter Schachzug ist der Zusammenschluss im Jahr 2023 der NHS Digital als technischer Umsetzer mit der NHS England als Stratege und Konzeptvorgeber. Statt getrennt zu arbeiten, hat sich das Team zusammengetan vergrößert bei gleichbleibender Verantwortung, aber weniger Komplexität durch Separation. Darüber hinaus werden auch Softwarelösungen von externen Anbietern beansprucht, die aber durch die nun existenten technischen Experten am selben Tisch, besser kommuniziert und verstanden werden. NHS Digital, heute NHS England, hat die technologischen Systeme aufgebaut und

verwaltet für das Gesundheitssystem, darunter die Spine, der Summary Care Record (SCR) und die Infrastruktur, die die NHS-App nutzt. Außerdem gibt NSH England die technischen Richtlinien vor und ist verantwortlich für den sicheren Datenaustausch und die Cybersicherheit (Silicon Practice, 2025).

Die gematik als Konzeptgeber bezieht das Wissen für IT-Systeme in enger Zusammenarbeit mit Experten wie dem BSI und gibt die Umsetzung an externe IT-Dienstleister weiter. Die Vorteile hierbei sind, dass eine weitere Perspektive auf Pläne und Konzepte entstehen und so auch durch die Erfahrungen der externen Parteien neuartige Ideen eingebracht werden können. Außerdem können Kosten eingespart werden, da die Experten nur für den Rahmen eines Auftrags benötigt werden. Die Nachteile entstehen aus der Abhängigkeit zu den Experten und ein ständiger Kommunikations- und Koordinationsaufwand, um die Ziele der gematik richtig realisieren zu können. Unter Umständen kann der Kostenvorteil auch in einen Nachteil umschlagen, wenn die Experten mehr Geld verlangen oder sich ihre Tätigkeit über einen längeren Zeitraum hinzieht. Insgesamt überwiegen die Vorteile für eine bessere Qualität im Ergebnis, sind aber behaftet mit dem Risiko Fortschritte langsamer zu erreichen, da viele Akteure einbezogen werden müssen in die Entscheidungen.

Derzeit bewahrheitet sich in Deutschland aus den Pressemitteilungen die Sorge, dass das Gesundheitssystem trotz steigender Beiträge an ihre monetären Grenzen gestoßen ist. Zum Aufatmen für den Patienten als finanzieller Hauptträger des Systems sollen die Krankenkassen aus den Ersparnissen an anderen Stellen entlastet werden und nicht durch weiter steigende Beiträge für den Patienten, so die Politik (MDR Deutschland, 2025).

Grundsätzlich ist zu sagen, dass die NHS ein zentralisiertes System ist, das mit wenigen Akteuren die Bereiche Finanzierung, Steuerung, die IT-Infrastruktur und Forschung und Datenstrategie vorangetrieben wird. Einige wenige dezentrale Akteure kümmern sich um regionale Bereiche, wie dem Integrated Care System (ICS), die Leistungserbringung (Krankenhäuser, Hausärzte) und die Qualitätskontrolle. Im Vergleich dazu ist Deutschland dezentral aufgebaut, da es viele Akteure gibt für dieselben Bereiche. So läuft die Finanzierung über Beiträge, die Steuerung über die vielen Krankenkassen, Kammern und Kassenvereinigungen, die IT-Infrastruktur über viele Anbieter und einer dezentral konzipierten Telematik und die Leistungserbringung über viele private medizinische Einrichtungen.

Tabelle 5-2 Die Systemkonzept zum Datenaustausch (eigene Darstellung)

	Systemkonzept zum Datenaustausch
Deutschland	TI
Großbritannien	NHS Spine

In Deutschland wird für den sicheren Austausch von medizinischen Daten die TI als Netzwerk eingesetzt. Zu ihrem Aufbau und Funktionen ist in den Grundlagen unter „Die Telematikinfrastruktur“Die Telematikinfrastruktur genaueres erklärt. Digitale Anwendungen mit entsprechenden Schnittstellen und sogenannte TI-Anwendungen ermöglichen diesen Datenaustausch in einem geschlossenen Netzwerk, das vom öffentlichen Netz abgekapselt ist und über eine gesicherte VPN-Verbindung mit entsprechender Befugnis zu erreichen ist und damit sehr sicher erscheint im Konzept. Die NHS verwendet die Plattform NHS Spine, über welche angebundene IT-Systeme Patientendaten mit anderen Einrichtungen austauschen können. Mehr als 44.000 IT-Systeme aus 26.000 Einrichtungen werden über die NHS Spine verbunden (this, 2025). Während für eine Verbindung zur TI 1.0 zurzeit noch ein Konnektor benötigt wird, ist die NHS Spine mittlerweile eine fortschrittliche cloudbasierte Netzwerkplattform (NHS England, 2023a), auf die verschiedenen NHS-Dienste laufen. Mit der TI 2.0 soll ebenfalls ein cloudbasiertes Netzwerk Einzug finden im deutschen Gesundheitswesen und die physischen Konnektoren durch die TI-Gateway ersetzen; die Implementierung läuft bereits und erfolgt stückweise. Die technologischen Entwicklungen in Richtung Cloud-Systeme finden aus Gründen der Vereinheitlichung, Effizienz und Wartung in beiden Gesundheitssystemen ihren Platz.

Diese erwähnenswerten Dienste sind einige unter den zahlreichen Komponenten der NHS Spine Plattform (NHS England, 2025a):

Nationale Komponenten:

- Summary Care Record (SCR): Patientenkurzakte mit wichtigsten Patientendaten
- Personal Demographics Service (PDS): Datenbank mit demografischen Daten zur Identifizierung und Kontaktaufnahme von Patienten
- Electronic Prescription Service (EPS): Übermittlung von E-Rezepten an Apotheken
- e-Referral Service (e-RS): Übermittlung von elektronischen Überweisungen an Fachärzte

Komponenten zur Verwaltung und zum Zugriff:

- Spine Directory Service (SDS): nationales Verzeichnis mit Informationen zu Standorten, Abteilungen und Gesundheitspersonal von NHS-Organisationen
- Care Identity Service: Authentifizierung und Autorisierung für nationale NHS-Dienste über die Smartcard
- Spine Secure Proxy (SSP): Datenverkehr-Schnittstelle zwischen externen Systemen und zentralen NHS-Diensten

Zusätzliche Komponenten:

- GP Connect: erlaubt den Zugriff auf die Patientenakte beim Hausarzt (GP Records) von autorisiertem medizinischem Personal

Die sichere Verbindung zwischen den NHS-Diensten in der Spine gelingt über das Netzwerk Health and Social Care Network (HSCN), das aus Sicht des OSI-Modells eine Transportschicht ist und ähnlich wie eine VPN fungiert. So wie eine medizinische Einrichtung in Deutschland über Konnektoren und TI-Gateways auf die TI zugreift, greifen diese Einrichtungen in Großbritannien über die HSCN auf die NHS Spine zu. In Zukunft soll die HSCN gänzlich wegfallen und auf einen Zugriff übers Internet umgestellt werden (NHS England, 2025b), um die Einbindung von Internet-basierten Systemen zu erleichtern und einen hardwareunabhängigeren Zugang zu ermöglichen. Die NHS Spine ist weniger flexibel für andere Dienste und Innovationen, so wie es die TI 1.0 ist, aber die TI 2.0 nicht mehr sein wird. Die TI 2.0 erlaubt umfangreichere Dienstangebote, erzeugt aber Bedenken aufgrund seiner Cloud-Funktion und möglichen Zugriffen von Drittanbietern bei Datenpannen beispielsweise.

Eines der digitalen Dienste des NHS ist der GP Connect, da er für eine sichere Weitergabe von Patientendaten zwischen Hausarztpraxen (GP-Praxen) und anderen medizinischen Einrichtungen sorgt. Diese Art des Datenbezugs ist aktuell im deutschen Gesundheitswesen nicht möglich, da nur im Fall der ePA unter Einwilligung des Patienten ein Zugriff auf sie den Zugriff auf die Daten ermöglicht und darüber hinaus Datenanfragen technisch nur über KIM gezielt versendet werden. In Großbritannien ist dies nicht so streng geregelt, um die Verfügbarkeit der Daten zu erhöhen. Am Beispiel des NHS-Dienstes GP Connect wird nachfolgend veranschaulicht, wie eine Datenabfrage einer medizinischen Einrichtung über GP Connect abläuft in drei Schritten (siehe Abbildung 5-1):

1. Zunächst muss der Anfragende über den Personal Demographics Service (PDS) prüfen, ob ein Patient oder eine bestimmte NHS-Nummer existieren.
2. Dann muss der Anfragende mit dem Spine Directory Service (SDS) herausfinden, welcher Endpoint (ASID oder MHS)[2] zuständig ist.
3. Über die API (FHIR / REST) stellt der Anfragende dann seine Anfrage, die der Spine Security Proxy (SSP) bereitgestellt hat.

[2] MHS steht für den Message Handling Server und ist für die Behandlung, Weiterleitung und Verarbeitung von Nachrichten zuständig. Systeme, die sich mit der Spine verbinden, müssen sich identifizieren über einen Accredited System Identifier (ASID), den sie vom Spine Directory Service erhalten.

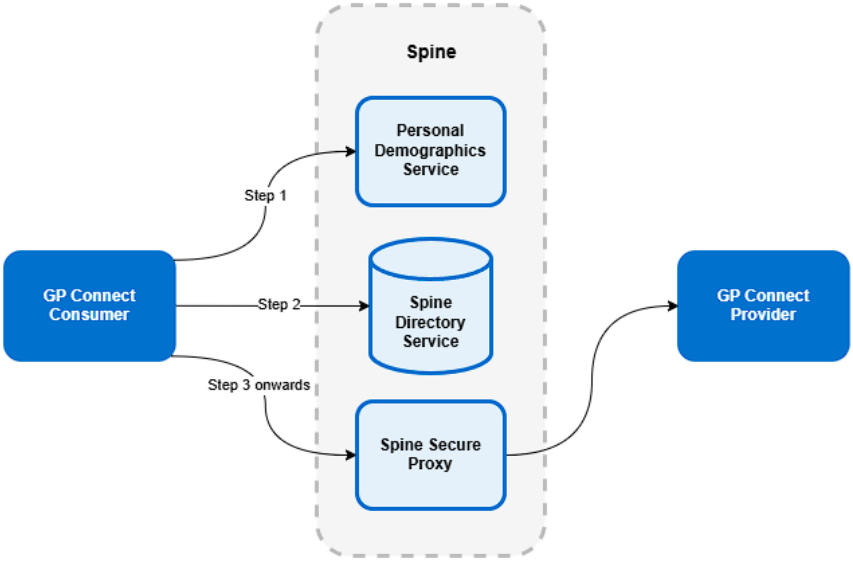


Abbildung 5-1 Datenabfrage über Spine (NHS England, 2025e)

Wenn die anfragende medizinische Einrichtung über NHS Smartcards korrekt authentifiziert ist und sie hinsichtlich ihrer Rolle befugt ist, erhält sie auf TLS verschlüsseltem Weg eine Antwort. Die Interaktionen werden protokolliert und geben zumindest die Möglichkeit zur Überwachung von Zugriffen.

Tabelle 5-3 Verwendete Mittel zur technischen Sicherheit von Patientenakten (eigene Darstellung)

	Technische Sicherheit
Deutschland	Verschlüsselung: E2EE, TLS 1.2 oder 1.3, RSA/später ECC Authentifizierung: Leistungserbringer: SMC-B + PIN, eHBA + PIN Patienten: Einmaliger Identitätsnachweis bei Registrierung (ePA App) Zugangsdaten + 2FA (ePA App)
Großbritannien	Verschlüsselung: teilweise E2EE im NHS Spine, TLS 1.2 oder 1.3, AES-256 Authentifizierung: Leistungserbringer: NHS CIS2 Authentication oder, NHS Smartcard + PIN Patienten: Einmaliger Identitätsnachweis bei Registrierung (NHS Login), Zugangsdaten + 2FA (NHS App)

ECC ist für eine asymmetrische Verschlüsselung besser geeignet, da es genauso sicher, aber weniger datenlastig ist. Allerdings ist die Implementierung komplexer und könnte unter Umständen zu Fehlern führen, die die Sicherheit gefährden.

Beide Gesundheitssysteme nutzen für den Transport der Daten die E2EE und TLS. Die E2EE erlaubt eine Unlesbarkeit der Daten während des gesamten Transports, während die TLS zusätzlichen Schutz gibt durch seine Authentifizierung. Beide zusammen geben ein hohes Maß an Integrität für die Daten. Großbritannien nutzt außerdem noch AES-256 zur symmetrischen Verschlüsselung und setzt damit ein unknackbares Sicherheitsniveau gegen Brute-Force-Angriffe.

Insgesamt sind die Verschlüsselungstechniken auf einem sicheren und leistungsfähigen Niveau.

Die Authentifizierung im deutschen Raum mit Ausweisen und PIN ist ein Verfahren, das bald schon durch digitale Identitäten ersetzt werden wird. Genauere Angaben zur Authentifizierung mit den Ausweisen können in Kapitel 3 unter „Die Telematikinfrastruktur“ und „Sicherheitsstruktur“ Sicherheitsstrukturnachgelesen werden. Die Karten für sich sind ausreichend gesichert, nachdem die Sicherheitslücke zur Kartennummer behoben werden konnte. Das Problem mit ihrer Sicherheit besteht eher durch die vielen Möglichkeiten an die Ausweise und Zugangsdaten heranzukommen. Vergleichsweise ist die Regulierung und Abwicklung zur Erlangung von Smartcards in Großbritannien sicherer konzipiert und durchgeführt. Die Authentifizierung für Leistungserbringer im NHS erfordert die Nutzung von zertifizierten NHS-Smartcards mit PIN, die von örtlichen „Registration Agents (RA)“ vergeben werden. Hierzu muss eine Person ein persönliches Treffen mit einem RA abhalten und von ihm ihre Identität mit einer Photo-ID und Nachweis ihrer Adresse bestätigen lassen. Darüber hinaus muss der Anfrageprozess eingeleitet und zu Ende geführt werden. Bei der Authentifizierung von Leistungserbringern wird ihre Rolle erkannt und falls sie nicht autorisiert ist, wird der Zugriff blockiert. Jede Rolle ist verbunden mit die ihr zugewiesenen Aktivitäten, wonach das Prüfsystem einen Zugriff autorisiert (NHS England, 2023b, 2025c). Moderne Authentifizierungsverfahren sind das Authentifizierungsframework Care Identity Service (CIS) bzw. CIS2 mit verschiedenen Methoden (siehe (NHS England, 2025g)) und Smartcard Connect (NHS England, 2025d) zur Authentifikation der Smartcard übers Internet.

Für einen Zugang zu den eigenen medizinischen Daten müssen Patienten sich bei NHS registrieren und benötigen dafür eine E-Mail-Adresse mit mindestens sechs Zeichen, eine Mobilfunk- oder Festnetznummer, die persönliche NHS-Nummer oder den vollständigen Namen, das Geburtsdatum und die Postleitzahl. Jeder Patient hat eine eindeutige 10-stellige Identifikationsnummer, die NHS-Nummer, mit der er eindeutig identifiziert und seine Patientenakten abgerufen werden kann. Außerdem muss die Identität bestätigt werden, wofür folgende Möglichkeiten zur Verfügung gestellt werden:

1. Falls die angegebene Rufnummer mit der hinterlegten Rufnummer beim Hausarzt übereinstimmt, kann der Hausarzt die Identität bestätigen.
2. Ein Gesichts-Scan, der mit eingesendeten offiziellen Ausweisdokumente mit Foto verglichen wird, beispielsweise: Reisepass, nationaler Führerschein, eVisa als Aufenthaltsbeweismittel, EU-Führerschein, EU-Personalausweis.

Anstelle des Gesicht-Scans kann auch ein Video eingesendet werden, in welchem der Patient vier Nummern nennen muss durch Sprache, britische Gebärdensprache oder Schreiben und Zeigen.

3. Der Patient kann die Registrierungsdaten beim Hausarzt anfragen und zu verwenden, die aus einer Linkage Key, einem Organisation Code/Surgery ID und einer Konto-ID. Die Linkage Key dient als Verknüpfungsschlüssel bzw. Passphrase, um ein Nutzerkonto mit einer Anwendung, wie der NHS-App, zu verbinden.

Nach erfolgreicher Registrierung ist es dem Patienten möglich sich sowohl in die NHS-App als auch auf diversen Websites und einigen Apps zur Gesundheitsversorgung anzumelden (NHS England, 2021), für letztere beide wird gegebenenfalls eine weitere Identitätsbestätigung benötigt wird. Für die Anmeldung muss die angegebene E-Mail-Adresse eingegeben und ein Passwort erstellt werden. NHS schickt dann einen einmaligen Sicherheitscode an die E-Mail-Adresse, die ebenfalls bei der ersten Anmeldung angegeben werden muss. Für eine zusätzliche Absicherung mit 2FA wird bei jeder weiteren Anmeldung ein sechsstelliger Sicherheitscode an die angegebene Rufnummer geschickt, die angegeben werden muss. Als Zugangsdaten werden also die E-Mail-Adresse, das Passwort und der 2FA-Code benötigt, um sich in die NHS App anzumelden.

Für einen Zugang zur eigenen ePA wird die Installation der mobilen ePA App benötigt. Nach dem Starten der ePA, wird der Nutzer aufgefordert sich mit seiner Versichertennummer und Passwort anzumelden oder zu registrieren. Bei der Registrierung wird ein Benutzerkonto angelegt, indem die Versichertennummer, Kennnummer der Karte und eine E-Mail-Adresse angegeben werden und ein Passwort vergeben wird. Als nächstes folgt die Verifizierung der E-Mail-Adresse über einen Link in einer E-Mail, der bestätigt werden muss (Double-Opt-in-Verfahren). Für einen einfacheren und sicheren Zugang zur App wird nun ein eigener Code vergeben und optional zusätzlich der Login über die Face-ID konfiguriert. Dies soll einerseits den Zugriff vor anderen Personen in die Akte schützen und andererseits den eigenen Zugriff erleichtern, da ein umständlicher Login wegfallen würde. Im letzten Schritt erfolgt die Identitätsbestätigung als 2FA. Hierfür werden vier Möglichkeiten angeboten:

- Online: Personalausweis und PIN, sofern der Ausweis die Onlinefunktion hat
- POSTIDENT-Verfahren: mit Personalausweis und Coupon aus der ePA-App in einer Filiale der Deutschen Post
- Krankenkasse: Personalausweis und Versichertenkarte
- eGK: NFC-fähige eGK und PIN

Einige Krankenkassen bieten auch das neue Video-Ident-Verfahren von Nect an.

Damit ist die Identitätsbestätigung abgeschlossen und es kann auf die eigene ePA zugegriffen werden. Für eine Anmeldung in die App muss jedes Mal zunächst die Anmeldung mit der Versichertennummer und Passwort und als 2FA mit dem App Code oder alternativ mit eGK und PIN oder Personalausweis

und PIN die Authentizität sichergestellt werden. Bei der Verwendung des App-Codes muss eine regelmäßige Bestätigung der Identität über die oben genannten Verfahren durchgeführt werden.

Für die Registrierung verlangt der NHS mehr Angaben, aber in der Bestätigung der Identität ist der Aufwand gleichermaßen bemessen für die NHS App und ePA. Auch verwenden beide die 2FA für einen besseren Schutz vor dem Zugang mit gestohlenen Daten.

Tabelle 5-4 Datenzugriff und -kontrolle (eigene Darstellung)

	Zugriff auf die Patientenakte
Deutschland	Zugriffskontrolle: rollenbasiert und protokolliert Kontrolle über Daten: vollständig beim Patienten
Großbritannien	Zugriffskontrolle: rollenbasiert und protokolliert Kontrolle über Daten: Patient darf die Daten einsehen und teilweise den Zugriff festlegen

Die Patientendaten liegen in beiden Gesundheitssystemen dezentral vor, da sie in verschiedenen Praxis- oder Krankenhaussoftware ebenfalls eingetragen werden. Diese dezentrale Handhabung bietet aus der Perspektive des Datenschutzes eine bessere Sicherheit für die Daten, da sie verteilt sind und bei einem Cyberangriff nicht alle Daten gefährdet werden. Im NHS Gesundheitssystem hat jedoch die Patientenakte beim Hausarzt (GP Record) eine zentrale Rolle, da er die erste Anlaufstelle ist für Patienten und Fachärzte an ihn zurückberichten. Zurzeit müssen für die Füllung der ePA der Arzt oder sein medizinisches Fachpersonal Daten und Dokumente in die ePA hinzufügen, da es an passenden Schnittstellen fehlt, die die verschiedenen Systeme verknüpfbar machen und eine automatische Übertragung ermöglichen könnten. Es obliegt dem Leistungserbringer, welche Daten er in die ePA aufnehmen wird und ob der Patient damit einverstanden ist. Es steht in Diskussion, ob in Zukunft eine zentrale Patientenakte realisiert werden soll, wobei Kritiker die Selbstbestimmung und den Datenschutz verletzt sehen. Sofern keine feingranulare Steuerung von Zugriffsberechtigungen möglich ist, ist die Selbstbestimmung gefährdet. Die britische Digitalstrategie sieht vor weiterhin die Interoperabilität und Zugänglichkeit von Daten durch eine einheitliche Sprache, SNOMED CT, die Verwendung von technischen Mitteln mit standardisiertem Konzept und auch eine gemeinsame Patientenakte zu ermöglichen. NHS England strebt bereits seit längerer Zeit schon an unter verschiedenen Projekten eine zentrale gemeinsame Patientenakte zu entwickeln und zu implementieren. Das „Shared Care Records“ Programm hat bereits im Jahr 2023 einen Austausch von grundlegenden medizinischen Daten als eine Übersicht bewerkstelligt, damit Patienten ihre Krankengeschichte nicht immer wieder aufs Neue vortragen müssen. Es gibt derzeit ein Konzept für eine gemeinsame Patientenakte unter dem Programm

„Connecting Care Records“ (ConCR), dessen Umsetzung und vollständige Implementierung noch nicht abgeschlossen ist, aber einen vollständigen landesweiten Rollout bis März 2026 zum Ziel hat (NHS England, 2025f).

Leistungserbringer können nach einer Authentifizierung und Autorisierung gemäß den Vorgaben der DSGVO durch die Einwilligung des Patienten in einem Behandlungskontext den Zugriff auf die ePA erhalten. Entsprechend ihrer Rolle ist vorgegeben, ob sie Daten einsehen, eintragen, bearbeiten oder löschen können (genaueres in Kapitel 3 unter „Sicherheitsstruktur“: Lese- und Schreibrechte). Der 90-tägige Zugriff nach Gewährung mit der eGK ist allerdings ein zu langer Zeitraum für einen Zugriff und sollte kürzer ausfallen. An dieser Stelle ist die Empfehlung, dass Patienten die Funktion der Zugriffseingrenzung oder -entziehung nutzen, um unnötige Einsichten in die Akte zu unterbinden. Es ist im Sinne der Datenkonsistenz, Fälschungssicherheit und Revisionssicherheit, dass eingestellte Dokumente oder Daten von Leistungserbringern nicht von anderen Leistungserbringern manipuliert werden dürfen. Durch digitale Signaturen und Protokollführung wird jeder Zugriff nachvollziehbar festgehalten und für den Patienten transparent gehandhabt im Sinne der Patientensouveränität. Auch für diesen Zweck bestimmt der Patient über die ePA-App, ob und auf welche Dokumentenkategorie er Lese- und Schreibrechte vergibt oder entzieht. Einzig die nichtvorhandene Möglichkeit zur Bestimmung, welches Dokument für welchen Leistungserbringer zugänglich sein dürfen, dürfte auf Unzufriedenheit beim Patienten stoßen. Gerade diese Funktion stellt ein Kernelement im Nutzungspotenzial der ePA dar und ist nicht mehr vorhanden mit der neusten ePA 3.0 Version. Bei der Recherche zu dieser Arbeit sind keine Aussagen von der gematik gefunden worden zu dem Aussetzen dieser Funktion. Es besteht die Befürchtung, dass Patienten alle Dokumente verbergen, um sich und ihre sensiblen Daten zu schützen.

Der Zugriff auf die NHS-Patientenakten ist rollenbasiert und folgt dem Prinzip „nur, wenn benötigt“ und in einem Behandlungskontext. Jeder Zugriff wird protokolliert und kann je nach NHS-Anwendung vom Patienten nachverfolgt werden. Diese Aspekte teilen die NHS-Patientenakten mit der ePA, unterscheiden sich jedoch technisch im Punkt der rollenbasierten Umsetzung. Die NHS hat detaillierte technische Abfragemechanismen mit vorgegebenen Zugriffgewährungen je nach Rolle des Anfragenden. So haben Ärzte nicht automatisch einen Zugang zu allen medizinischen Daten, sondern nur im Rahmen ihrer genauen Tätigkeit und des Behandlungskontextes (NHS England, 2023b), was ungewollte Einsichten technisch eingrenzt und den Datenschutz erhöht. Eine grobe Einteilung für ein grundlegendes Verständnis über Zugriffe gibt auch die NHS vor, wenn auch mit dieser Übersicht allein ein falscher Eindruck entstehen könnte:

- Ärzte haben einen Vollzugriff auf Diagnosen, Medikation, Allergien, Laborergebnisse, Arztbriefe und Krankenhausbefunde von Patienten in ihrer Behandlung für die Dauer der Behandlung.
- Pflegepersonal hat einen eingeschränkten Zugriff und kann Pflegepläne, Medikationspläne und Vitalzeichen einsehen.

- Diagnostikpersonal kann nur ihren Untersuchungsauftrag und die Ergebnisse einsehen.
- Notfallpersonal kann auf die Summary Care Record (SCR)[3] zugreifen, welche eine Patientenkurzakte ist mit grundlegenden medizinischen Informationen wie Medikation, Allergien und Notfalldaten.

In dieser Auflistung fehlen die konkreten Regelungen für Psychotherapeuten und Physiotherapeuten oder Personen ähnlicher Berufe, da diese Regelungen nicht zu finden gewesen sind, sondern nur eine mit Vorsicht zu genießende Information, dass sie Zugriff hätten. Apotheker wird richtigerweise der Lesezugriff auf Patientendaten gewährt.

Die Zugangsberechtigungen für Leistungserbringer sind von der NHS in klar definierten Regeln festgehalten, was ein hohes Maß an Datensicherheit gewährleistet. Die Möglichkeit für Patienten über die NHS-App ihre Daten einzusehen, bestimmte Daten sperren oder ihren Zugriff beschränken zu können, verleiht ihnen eine größere Kontrolle darüber, welche Informationen sie teilen möchten. Allerdings kann es zu Spannungen kommen, da sie keine Berechtigungen haben Daten eigenständig zu löschen oder zu bearbeiten, falls diese fehlerhaft sein sollten oder sie diese in ihrer Akte nicht haben wollen. Sie können aber der Nutzung der Daten für Forschungszwecke widersprechen, welches ihnen das Recht auf die Verwendung ihrer Daten ausschließlich im Behandlungskontext wieder einräumt. Die Zugriffsdauer ist jedoch nicht allgemein festgelegt worden, aber richtet sich nach dem Prinzip des Behandlungskontextes, der Notwendigkeit und überraschenderweise auch nach der Rolle des Zugreifenden. So hat ein Hausarzt einen Dauerzugriff auf die Patientenakte, Fachärzte und Krankenhäuser im Rahmen der Behandlungsdauer und Apotheken für die Versorgungsdauer. Auf den Shared Care Record kann für die Dauer der Versorgungsbeziehung zum Patienten zugegriffen werden. Im Vergleich zum deutschen System ist die Zugriffsdauer eingeschränkter, verdeutlicht aber durch den bestehenden Dauerzugriff erneut die zentrale Rolle des Hausarztes als Hauptverantwortlicher in der Versorgung im britischen Gesundheitssystem. Dies verdeutlicht nochmals, dass der Patient nicht die vollständige Kontrolle über seine Daten hat, da er den Zugriff nur bei einem datenschutzverletzenden Verhalten entziehen kann.

Ähnlich wie die Authentifizierung einer medizinischen Einrichtung in Deutschland mittels SMC-B Karte, identifiziert sich eine medizinische Einrichtung in Großbritannien eindeutig über den Organisation Code. Dieser fünfstellige, eindeutige Code wird benötigt, um NHS-Dienste nutzen zu können, für den Datenaustausch, Zugriff auf gemeinsame Patientenakten und Verschreibung von Medikamenten. Die Einfachheit an diesen Code zu gelangen über eine gewollte Suchfunktion auf der ODS Data Search and Export Website, lässt Warnsignale aufleuchten. Zwar genügt der alleinige Code nicht für einen Zugang in Systeme, da weitere Authentifizierungsmittel benötigt werden, ermöglicht aber gezieltere Phishing- oder Spoofing-Angriffe, genaueres Social-Engineering, Angriffe über

[3] Ein Patient kann die SCR verweigern, indem er ein dafür vorgesehenes Formular ausfüllt und beim Hausarzt einreicht.

Drittanbieter mit Schwachstellen (Digital Care Hub, 2024). Er erlaubt außerdem eine Zugriffseinschränkung auf Dokumente, so dass nur bestimmte Organisationen diese abrufen können. Allerdings ist zu beachten, dass Organisationen auch miteinander kooperieren und ihnen deshalb der Zugriff auf Dokumente untereinander erlaubt ist. Dies wird über den Organisation Code Service geregelt (NHS England, 2024).

Tabelle 5-5 Wie und wohin werden Patientendaten weitergegeben (eigen Darstellung)

	Weiterverwendung von Daten
Deutschland	Forschung und Statistik, KI
Großbritannien	Statistik, Planung und Gesundheitsmanagement Überwachung für die öffentliche Gesundheit Forschung

In Deutschland sollen die gesammelten Daten der Patientenakte in anonymisierter und aggregierter Form an das Forschungsdatenzentrum Gesundheit weitergeleitet werden, von wo aus künftig über eine zentrale Anlaufstelle Anträge auf Daten evaluiert, angenommen oder abgelehnt werden sollen. Die Bestimmungen für die Verwendung von Daten soll strengen Regeln unterliegen, zeitlich begrenzt sein und bei Missbrauch strafrechtlich geahndet werden. Genauere Angaben sind in Kapitel 2 unter „Erhebung von Patientendaten“ zu finden. All dies klingt zunächst sicher, ist aber nicht so einfach, wie dargestellt wird, da Daten mit wenigen Attributen zurückführbar sein können auf die Identität der zugehörigen Person. Zu diesen Attributen kann schon die Postleitzahl gehören, die den Personenkreis auf einen Ort beschränkt, was bei kleinen Orten ein sehr kleiner Personenkreis bedeutet. Es fehlen dann nur noch wenige Attribute, wie Angaben zum Geburtsdatum oder das Geschlecht, um die Person eindeutig zu identifizieren. Welche Merkmale konkret weggelassen werden bei der Anonymisierung kommuniziert keine offizielle Stelle, so dass dies eine Unsicherheit hinterlässt. Die Anonymisierung würde also nicht unbedingt vor Diebstahl und den Konsequenzen schützen. Das BfArM hat sich bereits vor drei Jahren zur künftigen Verwendung von künstlicher Intelligenz zur Erzeugung neuer synthetischer Daten. Hier stellt sich aber die Frage, ob eine KI nicht trotzdem eine Rückführbarkeit durch Erkennung von Mustern durchführen kann, zu dem der Mensch nicht imstande wäre und auch die Frage, ob diese künstlich erzeugten Daten ein realistisches Bild der Tatsachen wiedergeben. Es gibt bereits mehrere Projekte, die die Idee der Datengewinnung aus einer KI auf Basis von echten Gesundheitsdaten, versuchen oder versucht haben umzusetzen, wie das „KI-AIM“-Projekt oder das „KI-FDZ“-Projekt, aus dem ein erfolgreicher Ansatz entwickelt werden konnte (Prasser et al., 2024). Es besteht also Hoffnung auf eine sicherere Weiterverwendung von Gesundheitsdaten für Forschungs- und kommerzielle Zwecke, aber noch in der Entwicklung ist.

Gesundheitsdaten verbergen sich auch dort, wo sie heutzutage wie selbstverständlich nicht sofort gesehen werden. Die App „Doctolib“ bietet vor allem den Service der Online-Terminvergabe und -verwaltung an, sofern sich eine medizinische Einrichtung registriert hat bei Doctolib. Um den Service nutzen zu können, müssen auch Patienten sich mit vollem Namen, Geburtsdatum, E-Mail-Adresse und gegebenenfalls weiteren Angaben registrieren. Darüber hinaus bietet Doctolib auch an ein Gesundheitsprofil anzulegen, die der Patient selbstständig füllen kann mit Daten und Dokumenten, was einer Patientenakte gleichkommt, und die Möglichkeit sich mit medizinischen Einrichtungen per Nachricht auszutauschen. Doctolib kann also bei vollständiger Nutzung eine Menge Daten sammeln, die sie nicht vorhat zu verkaufen, aber angekündigt hat Daten bewusst zu sammeln, um KI-Modelle zu trainieren zur Entwicklung von KI-Produkten, wie einen Sprechstunden-Assistenten (WDR, 2025). Hierzu holt sich die App die Einwilligung der Nutzer über die App ein, was gerade bei älteren Menschen zu versehentlichen Einwilligungen führen kann. An diesem Beispiel ist zu erkennen, dass Gesundheitsdaten auch von privaten Unternehmen genutzt werden können und eine besondere Sorgfalt und Aufmerksamkeit bei der Nutzung ihrer Dienste erfordern.

Die NHS sammelt ebenfalls Patientendaten unter der Prämisse „zum Nutzen der Gesellschaft“ seit ihrer Gründung im Jahr 1948, was die britische Bevölkerung mit dem Thema vertraut macht. Heutzutage sammelt die NHS diese Daten aus allen NHS-Organisationen, Trusts, lokalen Behörden und Hausarztpraxen, sowie privaten medizinischen Einrichtungen oder direkt über den Patienten selbst. Die gesammelten Daten sind aus drei Kategorien:

- Demografisch:
  Name, Geschlecht, NHS-Nummer, ethnische Zugehörigkeit, Adresse, Beschäftigung etc.
- Gesundheit:
  körperlich, mental, Symptome, Diagnosen, Risikofaktoren (Gewicht, Größe, Raucher etc.) etc.
- Behandlung:
  Krankenhauseinweisungen, Kontrolltermine, Laborergebnisse, Anordnungen, Impfungen etc.

In Deutschland ist die Lage recht ähnlich hinsichtlich der Informationen, die gesammelt werden. Auch hier werden Daten für die Nachvollziehbarkeit, Überwachung, Schutz und Kostenplanung gesammelt von verschiedenen Akteuren: Krankenkassen, Ärzten, Labore, Apotheken, ePA-Anbieter, öffentliche Gesundheitsdienste, Behörden.

Diese Daten werden vom NHS weitergegeben für folgende Zwecke (GOV UK, 2021):

- Forschung und Analysen der öffentlichen Gesundheit
  z.B. Studien, epidemiologische Entwicklungen
- Planung und Steuerung des Gesundheitssystems
  z.B. Serviceoptimierung, materieller Verbrauch
- Statistik

z.B. Vorkommen von Krankheiten, Servicenutzung

- Maßnahmen für die öffentliche Gesundheit
  z.B. Seuchenkontrolle, Impfraten

Zum Schutz der Personen werden die Daten ebenfalls pseudonymisiert und aggregiert weitergegeben. Die folgenden Forschungseinrichtungen haben die Möglichkeit den Zugriff auf diese Daten zu beantragen: Universitäten, Krankenhäuser, Medizinische Royal Colleges und Pharmaunternehmen zur Erforschung neuer Behandlungsmethoden. Wie beim FDZ Gesundheit wird der Zugang zu den Daten nur nach einem streng geprüften Antrag auf Forschungsgrund und Einsatz der Daten gewährt.

Ein Unterschied liegt aber in der Dauer der Aufbewahrung der Daten. Während in Deutschland medizinische Unterlagen in der Regel nur 10 Jahre aufbewahrt werden, handhabt der NHS die Aufbewahrung der Daten je nach Kontext und richtig sich dabei nach dem „The NHS Records Management Code of Practice“. So werden unter anderem Daten bei Hausärzten lebenslang und 10 Jahre nach dem Tod aufbewahrt, Daten von Kindern und Jugendlichen bis zum 25. Geburtstag und 8 Jahre nach frühzeitigem Tod, Daten über die mentale Gesundheit für 20 Jahre und Daten zu Krebspatienten für 30 Jahre (Somerset LMC, 2024). Die einzige Gemeinsamkeit zum deutschen System besteht in der Aufbewahrung der Patientendaten in der ePA, für die es ebenfalls keine automatische Löschung nach einer abgelaufenen Frist gibt, außer nach 10 Jahren, wenn der Patient stirbt.

Patienten haben das Recht der Weitergabe ihrer Daten für Forschungs- oder Planungszwecke zu online oder telefonisch widersprechen. Außerdem können sie ihre erforderliche Einwilligung für eine Weitergabe an beispielsweise Drittanbietern verweigern. Sie sind jedoch nicht berechtigt die Weitergabe von Daten für eine direkte medizinische Versorgung zu verweigern und ihre Einwilligung wird auch nicht explizit eingeholt. Dies ist ein Kontrast zum deutschen Gesundheitssystem, wo Patienten schriftlich bestätigen müssen, dass die Weitergabe ihrer Daten an den von ihnen angegeben Arzt erlaubt ist. Des Weiteren dürfen Patienten vom NHS gesammelte Daten für eine Weitergabe nicht löschen oder gänzlich einschränken lassen, die dem öffentlichem Wohl dienlich sind, zur Aufklärung in der Forensik genutzt oder für Abrechnungsnachweise und eine Qualitätssicherung verwendet werden. Dies überschneidet sich mit dem deutschen System nicht immer Widerspruch einlegen zu können und obwohl nach dem Datenschutzrecht der DSGVO vorgegangen wird, schränkt es den Patienten in seiner Selbstbestimmung über seine Daten ein.

Tabelle 5-6 Gemeinsamkeiten und Unterschiede von Schwachstellen (eigene Darstellung)

	Sicherheitsrelevante Schwachstellen
Deutschland	Unsichere IT-Strukturen Mangelnder Schutz von Zugangsmitteln
Großbritannien	Veraltete Geräte und Software IT-Struktur nicht auf angemessenem Sicherheitsstandard Mangelnde Sensibilisierung für Cyberangriffe

Gesundheitssysteme werden zunehmend zum Ziel von Cyberangriffen, da in ihnen ein hohes Zahlungspotenzial gesehen wird durch die gestohlenen Daten oder Kompromittierung des IT-Systems. So passieren regelmäßig Cyberangriffe, von denen einige immensen Schaden anrichten und andere ein unbehagliches Gefühl hinterlassen. Bisher hat es noch keine direkten Angriffe auf ePA gegeben, schon aber auf Dienstleister, die mit der TI kooperieren. Der D-Trust-Fall Anfang des Jahres 2025 hat nochmal verdeutlicht, dass sogar einem IT-Dienstleister mit Spezialisierung auf Sicherheitsstandards durch die Unaufmerksamkeit über einen Software-Fehler ein verheerender Fehler unterlaufen kann. Derartige Vorfälle von Dienstleistern bringen auch das Vertrauen in die Sicherheit der TI ins Schwanken. Auch in Großbritannien ist mit dem Synnovis-Fall ein Dienstleister die Sicherheitslücke für einen Angriff geworden. Eine ungepatchte Schwachstelle im System bedeutet entweder die Nutzung von veralteten Geräten oder veralteter Software, für die es keine Sicherheitspatches mehr gibt oder die nicht explizit installiert worden sind. Auch hier ist unaufmerksames Fehlverhalten ein Grund für die entstandene Sicherheitslücke.

Eine fehlende Multi-Faktor-Authentifizierung hat dem IT-Dienstleister Advanced Ansehen und sehr viel Geld gekostet und die NHS Einrichtungen in eine Lage gebracht, in der sie die medizinische Versorgung zum Teil nicht mehr in vollem Umfang gewährleisten konnten und zu vielen zusätzlichen Maßnahmen greifen mussten. Die Authentifizierung ist ein grundlegendes Merkmal der IT-Sicherheit und erlaubt keine Fehler, da die Konsequenzen weitreichend sind.

Dass es immer noch mit wenig Aufwand möglich ist an offizielle Ausweise, wie die eGK, SMC-B und eHBA zu kommen, ist gleichermaßen überraschend und erschreckend, da diese Schwachstelle den Krankenkassen und Kartenherausgebern bereits vor mehreren Jahren aufgezeigt worden ist. Die Vorgänge zur Bereitstellung von diesen Ausweiskarten unterliegt nicht ausreichend schützenden Maßnahmen, die auf eine mangelnde Sensibilität für Datensicherheit hinweisen. Die Unwissenheit der Ärzte oder anderer Akteure über den verantwortungsbewussten Umgang mit diesen Ausweisen macht sich besonders deutlich durch den Verkauf von solchen Ausweiskarten und auch Geräten, wie Konnektoren und Kartenlesegeräte, auf Plattformen wie Kleinanzeigen. Diese Handlungen erleichtern Angreifern ihren Aufwand und erhöhen das Sicherheitsrisiko. Zu Smartcards in Großbritannien sind der

Missbrauch der Karten unter den Mitarbeitern bekannt, aber keine Vorfälle zu Diebstählen mit Datenverlust oder Systemkompromittierung.

Viele aufgezeigte Schwachstellen zeigen, dass vor allem externe Anbieter von Dienstleistungen Schwachstellen erzeugen, wie auch der Service des Video-Ident-Verfahren, bei dem es mit etwas mehr Aufwand möglich gewesen ist, die Identität zu fälschen und einen Zugang zu erlangen. Identifikationsverfahren sollten genau beleuchtet werden, damit sie nicht zu leichten Zugängen für Hacker werden. Die gematik hat das Verfahren bis zu einer technischen Verbesserung als unzulässig eingestuft. Seit dem 01.08.2025 hat die gematik das Video-Ident-Verfahren wieder zugelassen, unter der Voraussetzung, dass nur das Identifikationsverfahren der Nect GmbH ausschließlich mit der Nect App und keiner Drittanbieteranwendung ausgeführt werden darf (Deutsches Ärzteblatt, 2025). Es stellt sich die Frage, inwieweit solche Systeme getestet werden, bevor sie in Umlauf gebracht werden.

Aber auch interne IT-Schwachstellen durch falsche Konfigurationen oder nicht ausreichend gesicherte Mittel zum Prüfungsnachweis, wie der ICCSN, führen zu unauffälligen Einfallstoren, die erst bei oder nach einem Cyberangriff bemerkbar würden.

Im Vergleich ähneln sich die Schwachstellen der IT in den Gesundheitssystemen, da sie oftmals auf menschliches Versagen durch Unaufmerksamkeiten entstehen. Es fehlt aber auch an Maßnahmen, die diese natürlichen Ursachen auffangen könnten, wie eine mehrfache Testung auf Schwächen von Softwaresystemen und IT-Strukturen wie die Authentifizierung. So könnten auch unsichere Schnittstellen entdeckt werden und Vorkommnisse wie den Fall des Zugangs über Ersatz-bescheinigungen, den der CCC aufgedeckt hat, unwahrscheinlich machen.

6 Diskussion

6.1 Einordnung der deutschen ePA-Sicherheit im internationalen Kontext

Die deutsche ePA macht insgesamt einen guten Schnitt im Vergleich zu den Systemen, die es in anderen Ländern gibt. Sie erfüllt zwar noch nicht die wünschenswerten Funktionalitäten, damit sie einen besseren Nutzen erreicht, fußt aber auf IT-Strukturen, die hohe Sicherheitsstandards anstreben. Es ist nicht vorgesehen, dass die ePA zu einer Primärakte und damit eine zentrale Patientenakte wird. Die ePA soll vor allem für den Patienten zur Verwaltung ihrer Patientendaten fungieren und bleibt daher eine Sekundärakte. Das bedeutet für die Datensicherheit, dass Daten weiterhin dezentral verteilt sein werden und damit eine sicherere Basis liefern. Das Konzept der dezentralen Akte verfolgt bislang auch Großbritannien und viele andere Länder[4]. Seit ihrer Einführung Anfang des Jahres hat es keine kompromittierenden Vorfälle gegeben, die die ePA oder ePA App direkt betroffen haben. Jedoch hat es Sicherheitslücken gegeben, die auch von Kritikern scharf benannt und von der gematik zügig behoben worden sind. Ein Bedarf für Verbesserungen gibt es dennoch, aber die gibt es in jedem System und in jedem Land. Mit den Plänen und Konzepten zur Zero-Trust-Architektur der TI 2.0 wird das Sicherheitsniveau nochmal steigen, da Zugriffe noch strenger kontrolliert werden sollen und ein umfangreicheres Monitoring jeden Vorgang festhält und bei Auffälligkeiten anschlägt.

Das deutsche Gesundheitssystem hat viele Akteure und IT-Lösungen in hoher Anzahl, die miteinander agieren. Dies macht das System so komplex, dass sich ein Erfassen und Durchdringen davon herausfordernd sein kann und damit auch unentdeckte Sicherheitslücken unter Umständen zulässt. In dem Sicherheitsgutachten zur ePA des Frauenhofer Instituts (Frauenhofer SIT, 2024) wird versucht die sehr vielen technischen und regulatorischen Spezifikationen, die die gematik konzipiert und veröffentlicht hat, mit Hilfe einer KI durchdringbarer zu machen. Dies sollte helfen in der Masse und dem Chaos aus Informationen gewinnbringende Erkenntnisse zur Sicherheitsstruktur zu erlangen. Die Dokumente mit den Spezifikationen sind in die KI eingespeist worden, so dass gezielt Fragen gestellt werden sollten, deren Antworten die KI aus dem Dokumentenberg herausfiltern sollte. Dies hat auch die KI nicht zufriedenstellend bewältigen können und zeigt, dass die gematik weniger auf Komplexität und mehr auf Klarheit und Eindeutigkeit setzen sollte. Es ist anzunehmen, dass die Umsetzung dieser Spezifikationen, die Konzepte sind, vor Hürden stellen und sich eben auch dann Fehler einschleichen, wenn das Konzept richtig gestellt sein sollte.

[4] Ein interessantes und sehr sicheres Gegenstück zur dezentralen Akte ist die finnische My Kanta, welche eine zentrale Patientenakte ist, in die jeder Leistungserbringer Daten einträgt. Ob Deutschland seinen Kurs jemals ändert und sich an dem finnischen Konzept orientiert, wird die Zeit zeigen.

6.2 Potenzielle Risiken und Optimierungsmöglichkeiten

Zu den Risiken gehören vor allem auch Systeme, die eine Anbindung haben zur ePA oder zur TI und müssen daher ebenfalls betrachtet werden.

Der App Code stellt nicht zwangsläufig eine sichere Variante für die 2FA dar, denn die erste Anmeldung mit Versichertennummer läuft über ein selbstvergebenes Passwort und auch der App Code ist selbstvergeben. Sollte eine Person die Passwörter sichtbar für jemand anderen eingeben oder irgendwo notieren, nützt auch die 2FA nicht, um einen unbefugten Zugriff zu verhindern. Je nach Anbieter der ePA braucht es dann vielleicht nur noch das Gerät, mit dem die Registrierung stattgefunden hat. Bei manchen Anbietern, wie der Techniker Krankenkasse, ist die Authentifikation für ein neues Gerät etwas einfacher gehalten, so dass das Gerät des Opfers nicht zwingend benötigt wird. Für die 2FA sollten für den hochsicheren, aber auch nutzerfreundlichen Aspekt der Nachweis über Biometrie, über Apps, wie die Authenticator von Google oder Microsoft, oder Apps mit TAN-Funktion genutzt werden.

Die Unwissenheit über Datensicherheit von Nutzern der ePA kann zu ungewolltem fehlerhaftem Verhalten führen und Datenlecks oder Sicherheitslücken auslösen. Eine Nachlässigkeit bei den Zugangsdaten und -mitteln, eine geöffnete Phishing-Mail, ein unbedachter Download sind unbeabsichtigte Fehler mit potenziell schweren Folgen. Eine klare Kommunikation und Aufklärung aller Beteiligten über die Risiken, die durch Fehlverhalten entstehen können, und die möglicherweise weitereichenden Konsequenzen dazu sollte als Teil der Nutzbarkeit ePA integriert werden. Mit regelmäßigen Erklärvideos müssen alle Nutzer sensibilisiert werden für das Thema Datensicherheit. Eventuell würde eine Erklärung zur Haftbarmachung bei böswilligem oder fahrlässigem Verhalten, da eine Aufklärung stattgefunden hat, das Bewusstsein für dieses Thema stärken. Es müssen darüber hinaus bessere Anlaufstellen für Fragen und Probleme geben als die derzeitigen Krankenkassen, Ombudsstellen und gematik selbst. Diese Anlaufstellen sollten gut erreichbar für jeden und ausreichend technisch geschult sein, um auch Fragen zum Datenschutz und zur Datensicherheit souverän beantworten können.

Eines der größten Unsicherheitsfaktoren stellen veraltete Systeme dar. Noch immer werden in vielen Einrichtungen Geräte verwendet, die nicht auf dem neuesten Sicherheitsstandard sind und Schwachstellen aufweisen. Insbesondere Krankenhäuser sind davon betroffen. Die Umstellung der Konnektoren auf eine cloudbasierte Lösung kann die Schwachstelle „hardwarebasierter Konnektor“ aushebeln, aber nicht die Unsicherheit, die durch andere Geräte bestehen. Veraltete Geräte sind welche mit alter Software, die keine Sicherheitsupdates mehr erhält und inkompatibel ist mit modernen Protokollen, die die Cloud verwendet. Außerdem verwenden sie unsichere Netzwerkprotokolle, wie SMBv1 oder alte TLS-Versionen. Darüber hinaus kann andere Software auf solchen Geräten veraltet sein und eine Sicherheitslücke schaffen oder sie unterstützen keine modernen Authentifizierungs-verfahren und haben oft eine schwache Endgerätesicherheit. Es ist ein teures Ziel alle Systeme zu modernisieren, sollte aber nicht vernachlässigt werden.

Genauso sind schlecht installierte oder konfigurierte IT-Strukturen ein potenzielles Risiko für Angriffe, wie beispielsweise ein offener Server oder schlecht gesicherte APIs oder Formularfelder und unsichere Schnittstellen. Eine genaue und wiederholte Prüfung von IT-Strukturen reduziert das Risiko diese Schwachstellen zu einer Bedrohung werden zu lassen. Es sollten genaue Konzepte herausgearbeitet werden, nach denen Software konzipiert, entwickelt und bereitgestellt wird. Mitarbeiter müssen auf Feinheiten in der Datensicherheit besser geschult sein. Bei einem Softwarefehler als Schwachstelle sollte der Quellcode mehrfach geprüft und Penetrations-Tests durchgeführt werden.

Unentdeckte Veränderungen im Betrieb können ein Risiko für einen Angriff darstellen. Vielleicht auch zu Transparenzzwecken hat die gematik das Monitoring über die aktuellen betrieblichen Ereignisse der TI auf der Website gematik Fachportal (gematik Fachportal, 2025b) veröffentlicht, worin sowohl geplante als auch nicht-geplante Ereignisse und Störungen aufgezeigt und erklärt werden. Außerdem wird die Möglichkeit geboten aktuelle Störungen in der TI über einen WhatsApp Channel als Live-Ticker direkt zu erfahren und weitere Informationen zu Maßnahmen oder Einschränkungen zu verfolgen.

Ein unsicheres Gefühl vermittelt die fehlende Funktion in der aktuellen ePA Version 3.0 Dokumente feingranular einzustellen, so dass bestimmten Ärzten oder medizinischen Einrichtungen der Zugriff gewährt wird und anderen nicht. Ein Dokument ist entweder für alle sichtbar oder für niemanden, außer dem Patienten selbst. Dies ist noch mit der ePA 2.0 möglich gewesen und sollte künftig wieder implementiert werden.

Für alle drei Ausweiskarten ist zu empfehlen, dass ihre Herausgeber

- erst nach einem authentisierten Antrag Karten erstellen. Dies kann persönlich vor Ort mittels Personalausweises oder online über Video-Ident- bzw. Post-Ident-Verfahren sein.
- die Karten und den PIN nur vertraulich übermitteln. Das heißt, dass die Karten nur persönlich unter Authentisierung mittels Personalausweises in einer Dienststelle übergeben werden sollten.

Diese Vorgehensweise würde zumindest sicherstellen, dass die ausgehändigte Ausweiskarte nicht in falsche Hände gerät.

7 Fazit

7.1 Beantwortung der Forschungsfrage

Die aufgezeigten Mängel in Betracht gezogen ist es vermutlich sogar gut, dass die ePA zuerst als Opt-in-Verfahren eingeführt worden ist, so dass sich nicht viele Patienten für eine digitale Akte entschieden haben, zum Teil auch aus mangelnder Informiertheit. So hat die ePA noch etwas mehr Zeit gehabt sich weiterzuentwickeln und an ihr erhobene Kritik umsetzen zu können. Nach aktuellem Stand bietet technisch betrachtet ein hohes Sicherheitsniveau, da sie auf einem dezentralen System basiert, Verschlüsselungstechniken und Authentifizierungsmechanismen verwendet und Daten in

vertrauenswürdigen Umgebungen (VAU) verarbeitet, die voneinander getrennt sind. Im direkten Vergleich zum Gesundheitssystem und Patientenaktensystem in Großbritannien, schneidet die deutsche ePA gleichermaßen oder sogar besser ab. Denn die Kontrolle über die Daten in der ePA bleibt beim Patienten, was für die NHS App nicht gilt. Der Patient kann in der NHS App nur seine Daten einsehen und entscheiden, ob Apps von Drittanbietern Zugriff haben dürfen auf die Daten. Bezüglich Cybervorfällen kann über die ePA nach beinahe 10 Monaten der flächendeckenden Einführung noch kein Fall festgestellt werden. Ob dies so bleibt, wird die Zukunft zeigen. Jedoch sind beteiligten Akteure an der Konzeption und Entwicklung der ePA bemüht ihre Sicherheitsstrategien zu überdenken, um noch bessere Lösungen anbieten zu können. Da die Bevölkerung etwas empfindlich auf das Thema Daten, Datenschutz und Datensicherheit reagiert, hat jede öffentlich diskutierte Schwachstelle zum Misstrauen in die ePA geschürt.

Noch immer schauen zu viele Menschen weg und nutzen die ePA nicht aktiv, so dass sie damit einen Kontrollverlust billigen, da ihre Akte weiterhin existiert, gefüllt wird und Daten aus ihr erhoben werden. Die aktive Selbstverwaltung der Dokumente und Daten und die Zugriffsverwaltung in der ePA sind sehr wichtig, wenn Daten nicht ungewollt eingesehen werden sollen. Dies hat aber nicht grundsätzlich mit der Datensicherheit zu tun, sondern ist höchstens ein Datenschutzproblem, welches durch die aktive Beteiligung eines Patienten leicht lösen lässt.

Die verpflichtende Einführung der ePA hätte noch etwas warten sollen, damit bereits konzipierte Sicherheitspläne, wie die Zero-Trust-Architektur, umgesetzt werden und letzte Sicherheitslücken geschlossen werden können. Eine absolute Sicherheit gibt es nie und nirgends, aber eine forcierte Einführung, die noch Unsicherheiten hat und welche auslöst bei Patienten, erfüllt nicht das Ziel eines modernen, funktionierenden und sicheren Gesundheitswesens.

7.2 Handlungsempfehlungen

Um Sicherheitslücken und Schwachstellen besser zu identifizieren, sollte sich eine unabhängige Institution mit IT-Sicherheits- und Datenschutz-Expertise der Evaluierung von technischen Entwicklungen und Implementierungen annehmen und diese erst für die Öffentlichkeit zugänglich machen, wenn ein ausreichendes Sicherheitsniveau erreicht worden ist. Denn jede Schwachstelle kann zu Vorfällen führen, die vor allem die Unsicherheit der Menschen in ein digitales Gesundheitssystem verstärken und als Konsequenz eine Ablehnung dieser eigentlich hilfreichen Systeme herbeiführen.

Die Compliance von Leistungserbringern und Patienten ist essenziell, um wichtige Sicherheitsupdates auf ihren Geräten installiert zu haben, die Weitergabe und Zugänglichkeit zu Daten an unberechtigte Personen zu unterbinden und sich damit datenschutzkonform zu verhalten. Das aufmerksame Mitdenken von Personen reduziert die Risiken erheblich, erfordert aber auch eine positive Gesinnung und ausreichende Aufgeklärtheit in der Datensicherheit.

Technische Vorgehensweisen sollten bis zu einem gewissen Grad transparent kommuniziert werden, um das Vertrauen in die ePA zu stärken.

Die ePA ist ein fester Teil der Agenda für das Gesundheitswesen und es wäre falsch ihr Potenzial aufgrund von ersten schlechten Berichten oder Erfahrungen zu verschmähen. Patienten sollten anfangen ein aktiver Bestandteil ihrer weiteren Entwicklung und Gestaltung zu sein, indem sie sie aktiv nutzen und ihre Vor- und Nachteile verstehen lernen. Dabei sollten hohe Erwartungen etwas zurückgeschraubt werden, denn obwohl die ePA ein lang gehegtes und konzipiertes Projekt ist, überwindet sie nicht alle Hürden sofort, die in den Weg fallen seit ihrer Einführung. Geduld und eine aktive Nutzung sind hilfreicher als bloße Kritik. Falls jemand absolut nicht überzeugt ist von der Idee der ePA, sollte er ebenfalls aktiv werden, um ihr zu widersprechen und seine Daten zu schützen.

7.3 Ausblick für die Zukunft

Das Potenzial, welches die Einführung der ePA eröffnet, ist auf der bürokratischen Ebene, sowie in der Forschungsmedizin enorm. Ein unkomplizierter Zugang zu allen Gesundheitsdaten für die Patientenseite und dem medizinischen Personal, welches alle erforderlichen Daten sofort auf Abruf bereitgestellt bekommt. Aber auch für die Mediziner in der Forschung, welche aus der Masse der gesammelten Daten die Möglichkeit haben bedeutsame Thesen herzuleiten zu Erkrankungen, ihren Ursachen sowie Ansätzen für Therapieformen.

Es besteht die Möglichkeit, dass die Selbstverwaltung der Patienten dazu führt, dass Ärzte kein vollständiges Bild zum Gesundheitszustand des Patienten haben, aber derzeit dennoch ein Mehraufwand existiert für Ärzte, weil sie die ePA pflegen müssen. Mit der Entwicklung von strukturierten Daten und einer einheitlichen Sprache, die maschinell verstanden wird, könnte letzteres Problem über Schnittstellen gelöst werden. Das unvollständige Bild könnte in Zukunft vollständiger werden, wenn Patienten sich sicher fühlen mit der Digitalisierung ihrer Daten. Dies gelingt allen voran über eine Gewissheit, dass Datensicherheit und Datenschutz gewährleistet sind und eine Gewöhnung an das „Neue“.

Welche Risiken auch existieren, die Vorteile sind insbesondere die medizinische Forschung betreffend sehr groß. Deshalb werden schon Wege bereitet die Nutzung von Daten sicher und effizient zu ermöglichen, wie die Datenzugangs- und Koordinierungsstelle, die Anonymisierung von Daten auf klassischem Weg mit Pseudonymen oder sogar die Nutzung von KI-erzeugten Daten. Inspirationen für Ideen und Technologien liegen nicht weit in Ländern, die bereits Vorreiter auf diesem Gebiet sind, wie beispielsweise Finnland.

Die Digitalisierung des Gesundheitswesens wird ein fortschreitendes Projekt bleiben und damit auch der Erhalt der ePA als Teil von ihr. Die ePA wird vermutlich noch mehrere Entwicklungen durchmachen, um funktionaler und sicherer zu werden, aber sie wird der medizinische Alltagsbegleiter für Patienten und Gesundheitspersonal sein.

Literaturverzeichnis

~goody. (2025, Februar 28). Understanding the Synnovis Ransomware Attack: Key Insights, Vulnerabilities, and Defence Strategies [Medium]. *Medium*. https://medium.com/@goodycyb/understanding-the-synnovis-ransomware-attack-key-insights-vulnerabilities-and-defence-strategies-7e9fcd464140

Al-Awqati, Q. (2006). How to write a case report: Lessons from 1600 B.C. *Kidney International*, *69*(12), 2113–2114. https://doi.org/10.1038/sj.ki.5001592

Anforderungen an die Telematikinfrastruktur, Pub. L. No. § 306 (2024). https://www.gesetze-im-internet.de/sgb_5/BJNR024820988.html#BJNR024820988BJNG008700308

Anna Lamche. (2025, März 27). *NHS software provider fined £3m over data breach after ransomware attack* [News]. BBC. https://www.bbc.com/news/articles/cp3yv1zxn94o

Bohne-Lang, A., & Lang, E. (2019). *Praxishandbuch IT: Grundlagen für Bibliothekare*. De Gruyter Saur.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018a, Juli 11). *Abwehr von DDoS-Angriffen*. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_002.pdf?__blob=publicationFile&v=1

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2018b, Juli 11). *Prävention von DDoS-Angriffen*.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020, Oktober). *Cloud Computing Compliance Criteria Catalogue – C5:2020 – Kriterienkatalog Cloud Computing*.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2021, März 16). *Ransomware: Managementabstract Fortschrittliche Angriffe*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2022, Oktober 7). *Erste Hilfe bei einem schweren ITSicherheitsvorfall*.

Bundesinstitut für Arzneimittel und Medizinprodukte (Hrsg.). (2023, Dezember 28). *Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V*. www.bfarm.de/diga

Bundesministerium für Gesundheit (BMG). (2025a). *Geschichte der gesetzlichen Krankenversicherung*. https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/grundprinzipien/geschichte.html

Bundesministerium für Gesundheit (BMG). (2025b, April 28). *ePA für alle startet morgen* [Presse]. Bundesministerium für Gesundheit (BMG). https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/epa-fuer-alle-startet-morgen.html

Cloudfare. (2025a). *Was ist mutual TLS (mTLS)?* [Was ist mutual TLS (mTLS)?]. Cloudfare. https://www.cloudflare.com/de-de/learning/access-management/what-is-mutual-tls/

Cloudfare. (2025b). *Was war der WannaCry-Ransomware-Angriff?* [Ransomware]. Cloudfare. https://www.cloudflare.com/de-de/learning/security/ransomware/wannacry-ransomware/

Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, *189*(22), E786–E787. https://doi.org/10.1503/cmaj.1095434

Craig Pepper. (2025, Juli 2). Ransomware Attack Contributed to Patient's Death: A Wake-Up Call for Health-Tech and Healthcare [Periculo]. *Cyber Security Blog*. https://www.periculo.co.uk/cyber-security-blog/ransomware-attack-contributed-to-patients-death-a-wake-up-call-for-health-tech-and-healthcare

Daniel Leisegang. (2025, Mai 6). *Elektronische Patientenakte: Keine Verantwortung, nirgends*. Netzpolitik.org. https://netzpolitik.org/2025/elektronische-patientenakte-keine-verantwortung-nirgends/

Deutsches Ärzteblatt. (2025, August 14). *Elektronische Patientenakte: Gematik lässt Video-Ident-Verfahren zu* [News - Vermischtes]. Deutsches Ärzteblatt.

https://www.aerzteblatt.de/news/elektronische-patientenakte-gematik-lasst-video-ident-verfahren-zu-c5331add-894f-456f-adda-b587cc993890

Deutschlandfunk. (2025). *Darum warnen Verbraucherschützer vor der ePA*. https://www.deutschlandfunk.de/elektronische-patientenakte-vorteile-nachteile-kritik-widerspruch-100.html

Digital Care Hub. (2024, Januar 25). *How to find an ODS code*. Digital Care Hub. https://www.digitalcarehub.co.uk/resource/how-to-find-an-ods-code/

Dokumentation der Behandlung, Pub. L. No. § 630f (2013). https://www.gesetze-im-internet.de/bgb/__630f.html

dpa/APOTHEKE ADHOC. (2025, Januar 31). *D-Trust-Datenlücke: Mindestens 10.000 Ärzte betroffen* [Nachrichten - Politik]. apotheke adhoc. https://www.apotheke-adhoc.de/nachrichten/detail/politik/d-trust-datenluecke-mindestens-10000-aerzte-betroffen

Dr. Christine von Reibnitz. (2025, Juli 24). *Annahme der elektronischen Ersatzbescheinigung ist ab sofort Pflicht* [Neuigkeiten]. DRACO. https://www.draco.de/news/detail/annahme-der-elektronischen-ersatzbescheinigung-ist-ab-sofort-pflicht/#:~:text=Nutzen%20Sie%20diesen%20Weg%20zum,Ihnen%20als%20MFA%20akzeptiert%20werden.&text=Halten%20Sie%20die%20KIM%2DAdresse,diesem%20sp%C3%A4teren%20Termin%20nachgeholt%20werden.

Europäische Union. (2025). *Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847 (Text von Bedeutung für den EWR)*. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ%3AL_202500327

Frauenhofer SIT. (2024, August 9). *Sicherheitsanalyse des Gesamtsystems ePA für alle*.

gematik. (2021, Juli 1). *MIO-Baukasten*. https://fachportal.gematik.de/fileadmin/Fachportal/Anwendungen/MIO/gemInfo_MIO-Baukasten_V1.0.0.pdf

gematik. (2024a, August 20). *Technisches Konzept Proof of Patient Presence (PoPP)*.

gematik. (2024b, Dezember 27). *Aktuelles | Stellungnahme zum CCC-Vortrag zur ePA für alle* [Newsroom]. gematik. https://www.gematik.de/newsroom/news-detail/aktuelles-stellungnahme-zum-ccc-vortrag-zur-epa-fuer-alle

gematik. (2025a). *Berechtigungen in der ePA für alle* [ePA für alle: Übersicht Berechtigungen]. gematik. https://www.gematik.de/anwendungen/epa-fuer-alle/epa-fuer-alle-uebersicht-berechtigungen

gematik. (2025b). *Die Sicherheitsarchitektur der ePa für alle* [ePA für alle]. gematik. https://www.gematik.de/anwendungen/epa-fuer-alle

gematik. (2025c, August 8). *Implementierungsleitfaden Primärsysteme—Telematikinfrastruktur (TI) (V2.26.0)*. https://gemspec.gematik.de/docs/gemILF/gemILF_PS/latest/

gematik. (2025d, September 12). *Implementierungsleitfaden Primärsysteme ePA für alle Version 3.6.0*.

gematik Fachportal. (2025a). *DiGA* [DiGA-Hersteller]. gematik Fachportal. https://fachportal.gematik.de/informationen-fuer/diga-hersteller

gematik Fachportal. (2025b). *TI-Status* [TI-Status]. gematik Fachportal. https://fachportal.gematik.de/ti-status

gematik Fachportal. (2025c, September 19). *Umstellung des Verschlüsselungsalgorithmus für TI-Komponenten—Abschaltung RSA-Unterstützung zum 31.12.2025* [Wartung & Sonstige Informationen]. gematik Fachportal. https://fachportal.gematik.de/ti-status/wartungen-sonstige-informationen

gematik Fachportal. (2025d, September 21). *Zulassungen und Bestätigungen* [Zulassungs- und Bestätigungsübersichten]. gematik Fachportal. https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten

Gillum, R. F. (2013). From Papyrus to the Electronic Tablet: A Brief History of the Clinical Medical Record with Lessons for the Digital Age. *The American Journal of Medicine*, *126*(10), 853–857. https://doi.org/10.1016/j.amjmed.2013.03.024

GOV UK. (2021, September 30). *Privacy information* [PHE privacy information]. GOV UK. https://www.gov.uk/government/publications/phe-privacy-information/privacy-information

Iris an der Heiden, Luisa Grundmann, Jannis Bernhard, & Marcus Otten. (2024). *Wissenschaftliche Evaluation des Produktivbetriebs der Anwendungen der Telematikinfrastruktur 2024* (S. 111) [Studienbericht]. IGES Institut GmbH. https://www.gematik.de/media/gematik/Medien/Telematikinfrastruktur/TI-Atlas/Studienbericht_IGES_2024.pdf

Jasmin Klofta, Katrin Kampling, & Anne Ruprecht. (2019, November 12). *Sensible Patientendaten in Gefahr*. NDR. https://www.ndr.de/fernsehen/sendungen/panorama3/Sensible-Patientendaten-in-Gefahr,patientendaten110.html

Kassenärztlichen Vereinigung Hamburg. (2024). eRezept-Pflicht: Honorarkürzung und TI-Pauschalenkürzung vermeiden. *Rundschreiben des Vorstands der Kassenärztlichen Vereinigung Hamburg*, *8*. https://telegramm.kvhh.net/nr-08-22-mai-2024/erezept-pflicht-honorarkurzung-und-ti-pauschalenkurzung-vermeiden#:~:text=Das%20sieht%20das%20Digital%2DGesetz,eine%20K%C3%BCrzung%20der%20TI%2DPauschale.

KIM - Kommunikation im Medizinwesen. (2025). [KIM]. gematik Fachportal. https://fachportal.gematik.de/anwendungen/kommunikation-im-medizinwesen

KoCo Connector. (2025, September 20). *Starke Leistung, kompakt-neuer Look: Die KoCoBox MED+* [Startseite]. KoCo Connector E-Health Company. https://www.kococonnector.com/deu_de

Marcel Roth, Norma Düsekow, & Mario Köhne. (2025, Januar 29). *1.200 Ärzte in Mitteldeutschland von Datenleck betroffen* [Nachrichten - Deutschland - Gesellschaft]. MDR SACHSEN ANHALT. https://www.mdr.de/nachrichten/deutschland/gesellschaft/datenleck-aerzte-epa-trust-patienten-daten-100.html

MDR Deutschland. (2025, Oktober 11). *Warken plant Millionen-Sparpaket gegen höhere Krankenkassenbeiträge* [Politik]. MDR. https://www.mdr.de/nachrichten/deutschland/politik/krankenkasse-beitraege-steigerung-sparpaket-nina-warken-100.html

MDR SACHEN-ANHALT. (2025, Oktober 8). *Nach Hackerangriff bei Ameos: Ausmaß des Schadens für Betroffene noch unklar* [Nachrichten]. MDR SACHSEN ANHALT.

https://www.mdr.de/nachrichten/sachsen-anhalt/magdeburg/salzland/ameos-ermittlungen-hackerangriff-dauern-100.html

mediatixx. (2025a). *Der Aufbau der TI* [Der Aufbau der TI]. dip - Digitalisierung in der Praxis. https://dip.medatixx.de/mediathek/detail/ti-sicher-vernetzt-so-ist-die-ti-aufgebaut

mediatixx. (2025b). *TI Gateway* [TI Gateway]. dip - Digitalisierung in der Praxis.

MIO Allgemeines. (o. J.). [MIO Allgemeines]. MIO. https://mio.kbv.de/display/MIOATT/MIO+Allgemeines

NHS Counter Fraud Authority. (o. J.). *Maleware* [Cyber Threats - Malware]. NHS Counter Fraud Authority. Abgerufen 4. Oktober 2025, von https://cfa.nhs.uk/fraud-prevention/reference-guide/cyber-enabled-fraud/cyber-threats/malware

NHS England. (2021, August 2). *Websites and apps you can access with NHS login*. NHS England. https://www.nhs.uk/nhs-services/online-services/nhs-login/websites-and-apps-you-can-access-with-nhs-login/

NHS England. (2023a, Oktober 6). *Spine Futures* [Spine futures]. NHS England. https://digital.nhs.uk/services/spine/spine-futures

NHS England. (2023b, Dezember 15). *National role-based access control (RBAC) for developers*. NHS England. https://digital.nhs.uk/developer/guides-and-documentation/security-and-authorisation/national-rbac-for-developers

NHS England. (2024, Juli 2). *Access and authorisation*. nh. https://digital.nhs.uk/services/secondary-uses-service-sus/sus-portal-user-guide/access-and-authorisation#registration-agents

NHS England. (2025a). *Service catalogue* [Service Catalogue]. NHS England. https://digital.nhs.uk/services/service-catalogue

NHS England. (2025b). *Spine*. NHS England. https://digital.nhs.uk/services/spine?preview-token=c304777e-7baf-463a-b1c8-7c47d6faf700&__cf_chl_tk=BD5E45VjKsrbhzhBbzGU6.FebkTwZQnPYSPI9XgmZDk-1760281605-1.0.1.1-CtJYB.STQvnKAR3oxiErvL0hmDd_fIUnXd0NwDrfAL8

NHS England. (2025c, April 9). *Smartcards and access controls*. NHS England. https://www.england.nhs.uk/long-read/smartcards-and-access-controls/

NHS England. (2025d, Juli 3). *Smartcard software for authentication via the internet*. NHS England. https://production-like.nhsd.io/services/care-identity-service/applications-and-services/cis2-authentication/smartcards-via-internet

NHS England. (2025e, Juli 25). *Integrate with Spine*. NHS England. https://digital.nhs.uk/services/gp-connect/develop-gp-connect-services/integrate-with-spine

NHS England. (2025f, September 16). *Connecting Care Records programme*. NHS England. https://digital.nhs.uk/services/connecting-care-records

NHS England. (2025g, Oktober 6). *NHS CIS2 Authentication*. NHS England. https://digital.nhs.uk/services/care-identity-service/applications-and-services/cis2-authentication

NHS England business continuity management toolkit case study: WannaCry attack. (2023, April 21). [Publication]. NHS England. https://www.england.nhs.uk/long-read/case-study-wannacry-attack/

Patientendaten-Schutz-Gesetz – PDSG (2020). https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/P/PDSG_bgbl.pdf

Prasser, F., Riedel, N., Wolter, S., Corr, D., & Ludwig, M. (2024). Künstliche Intelligenz und sichere Gesundheitsdatennutzung im Projekt KI-FDZ: Anonymisierung, Synthetisierung und sichere Verarbeitung für Real-World-Daten. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, *67*(2), 171–179. https://doi.org/10.1007/s00103-023-03823-z

Prof. Dr. Kuhlmann. (2020, April 27). *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)* (Bundestag, Hrsg.). Bundesanzeiger Verlag GmbH.

Rainer Thiel, Lucas Deimel, Klaus Piesche, Daniel Schmidtmann, Tobias Hüsing, Jonas Rennoch, Veli Stroetmann, Karl Stroetmann, & Dr. Thomas Kostera. (2018, November 29). *Der elektronische englische Patient*. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/de/unsere-projekte/der-digitale-patient/projektthemen/smarthealthsystems/england

Rashid, A., Choukair, D., Bauer, C., Ullrich, M., & Maisch, T. (2022). Praxiseinsatz Elektronischer Patientenakten: Erkenntnisse aus 2 Versorgungsprojekten in Zentren für Seltene Erkrankungen. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, *65*(11), 1143–1150. https://doi.org/10.1007/s00103-022-03599-8

Sievers, C. (2024). *SNOMED CT – brauchen wir noch mehr Code-Systeme?* BARMER. https://doi.org/10.30433/ePSTRA.2024.006

Silicon Practice. (2025, Juni 23). *Everything you've wanted to know about NHS Digital and Digital Healthcare (but didn't want to Google)*. Silicon Practice. https://siliconpractice.co.uk/2025/06/23/nhs-digital-and-digital-healthcare/

Silicon Saxony. (2025, März 13). *IBM: Die elektronische Patientenakte für die größten gesetzlichen Krankenkassen* [Aktuelles - News]. Silicon Saxony - The hightech network. https://silicon-saxony.de/ibm-die-elektronische-patientenakte-fuer-die-groessten-gesetzlichen-krankenkassen/#:~:text=Die%20IBM%20Cloud%20Satellite%20Technologie,Knappschaft%20Bahn%20See%20(KBS).

Somerset LMC. (2024). *Retention of Medical Records*. Somerset LMC. https://somersetlmc.co.uk/guidance/retention-of-medical-records/

Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung, Pub. L. No. § 303a bis §303f (2020). http://www.gesetze-im-internet.de/sgb_5/BJNR024820988.html#BJNR024820988BJNG008700308

SPD, Bündnis 90 / Die Grünen, & FDP. (2021). *Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit*. 65–65.

SSL-Support Team. (2024, Oktober 8). *Was ist Elliptic Curve Cryptography (ECC)?* [Artikel]. SSL.com. https://www.ssl.com/de/Artikel/Was-ist-elliptische-Kurve-Kryptographie-ecc/

Streit, S. (2025, Juni 21). *elektronische Patientenakte (ePA)—Whatever it takes!* Gulaschprogrammiernacht 23, ZKM Medientheater. https://media.ccc.de/v/gpn23-298-elektronische-patientenakte-epa-whatever-it-takes-digitalisierung-in-der-medizin-2025#t=234

Struktur | gematik. (2025, Juli 7). gematik. https://www.gematik.de/ueber-uns/struktur

this. (2025). *Registration Authority—NHS Spine & Healthcare IT Integration* [Our Services]. this. https://www.this.nhs.uk/our-services/it-operational-support-services/registration-authority

TI-Messenger. (2025). [TI-Messenger]. gematik Fachportal. https://fachportal.gematik.de/anwendungen/ti-messenger

Tobias Armbrüster. (2024, Oktober 24). *Was spricht für und gegen die elektronische Patientenakte?* Deutschlandfunk. https://www.deutschlandfunk.de/epa-pro-und-contra-dr-andreas-meissner-und-martina-stamm-fibich-spd-dlf-b84631fb-100.html

Tschirsich, M., & Kastl, B. (2024, Dezember 27). *„Konnte bisher noch nie gehackt werden“: Die elektronische Patientenakte kommt—Jetzt für alle!* 38C3: Illegal Instructions. https://media.ccc.de/v/38c3-konnte-bisher-noch-nie-gehackt-werden-die-elektronische-patientenakte-kommt-jetzt-fr-alle#t=0

Tschirsich, M., Zilch, A., & Brodowski, C. (2019, Dezember 27). *„Hacker hin oder her“: Die elektronische Patientenakte kommt!* 36C3: Resource Exhaustion, London. https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt#t=604

WDR. (2025, Februar 24). *Diese Daten nutzt die Patientenplattform Doctolib für KI-Modelle* [Nachrichten]. WDR. https://www1.wdr.de/nachrichten/doctolib-arzttermine-praxen-patientendaten-ki-100.html

Woodgrange Medical Practice. (2025). *Private healthcare professionals/clinicians, including private GPs are not allowed to issue NHS prescriptions.* Woodgrange Medical Practice. https://www.woodgrangemedicalpractice.co.uk/prescriptions-following-private-consult#:~:text=Private%20healthcare%20professionals/clinicians%2C%20including,private%20prescription%20following%20a%20consultation.

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit mit dem Titel:

Die elektronische Patientenakte in Deutschland:
Eine Analyse zur Datensicherheitslage im internationalen Vergleich

selbständig und nur mit den angegebenen Hilfsmitteln verfasst habe. Alle Passagen, die ich wörtlich aus der Literatur oder aus anderen Quellen wie z. B. Internetseiten übernommen habe, habe ich deutlich als Zitat mit Angabe der Quelle kenntlich gemacht.

Datum	Unterschrift