

Datenschutz im Gesundheitswesen: Nutzen, Risiken und Mythen

Autor: Wolfram Klatt

Veröffentlicht am: 10.08.2026

Dokument generiert über Gesundheitsmythen.de

ZUSAMMENFASSUNG (ABSTRACT)

Falsch verstandener Datenschutz und veraltete IT-Strukturen beeinträchtigen im deutschen Gesundheitswesen den lebensrettenden Informationsfluss. Das dadurch entstehende Vakuum wird von Akteuren der Pseudomedizin für Panikmache und Geschäftsmodelle genutzt. Eine sichere Digitalisierung mit Opt-out-Verfahren und modernen Sicherheitsstandards ist nötig.

Gefangen im Papier-Labyrinth: Wie fehlgeleiteter Datenschutz die Patientenversorgung bremst – und wie echte IT-Sicherheit Leben rettet

Stellen Sie sich vor, Sie werden nach einem schweren Verkehrsunfall oder einem plötzlichen Kreislaufkollaps bewusstlos in eine Notaufnahme eingeliefert. Jede Minute zählt, und das Notfallteam muss augenblicklich Entscheidungen über Leben und Tod treffen. Die behandelnden Ärztinnen und Ärzte müssen unverzüglich wissen: Nehmen Sie gerinnungshemmende Medikamente ein? Liegt eine schwere Allergie gegen ein Standardantibiotikum vor? Besteht eine bisher unerkannte Niereninsuffizienz, die eine veränderten Dosierung von Narkosemitteln erfordert?

In vielen digital fortgeschrittenen Gesundheitssystemen – etwa in Estland, Dänemark oder Israel – genügt ein autorisierter Klick auf die elektronische Notfallakte, um innerhalb von Sekunden eine verlässliche, lebensrettende Übersicht zu erhalten. In Deutschland hingegen greift das medizinische Personal in einer solchen akuten Gefahrensituation häufig noch zum Festnetztelefon, durchsucht die Geldbörse des Betroffenen nach einem zerknitterten Papier-Medikationsplan oder wartet vergeblich auf die Übermittlung eines Lesefaxes aus der Hausarztpraxis – sofern diese außerhalb der Sprechzeiten überhaupt erreichbar ist.

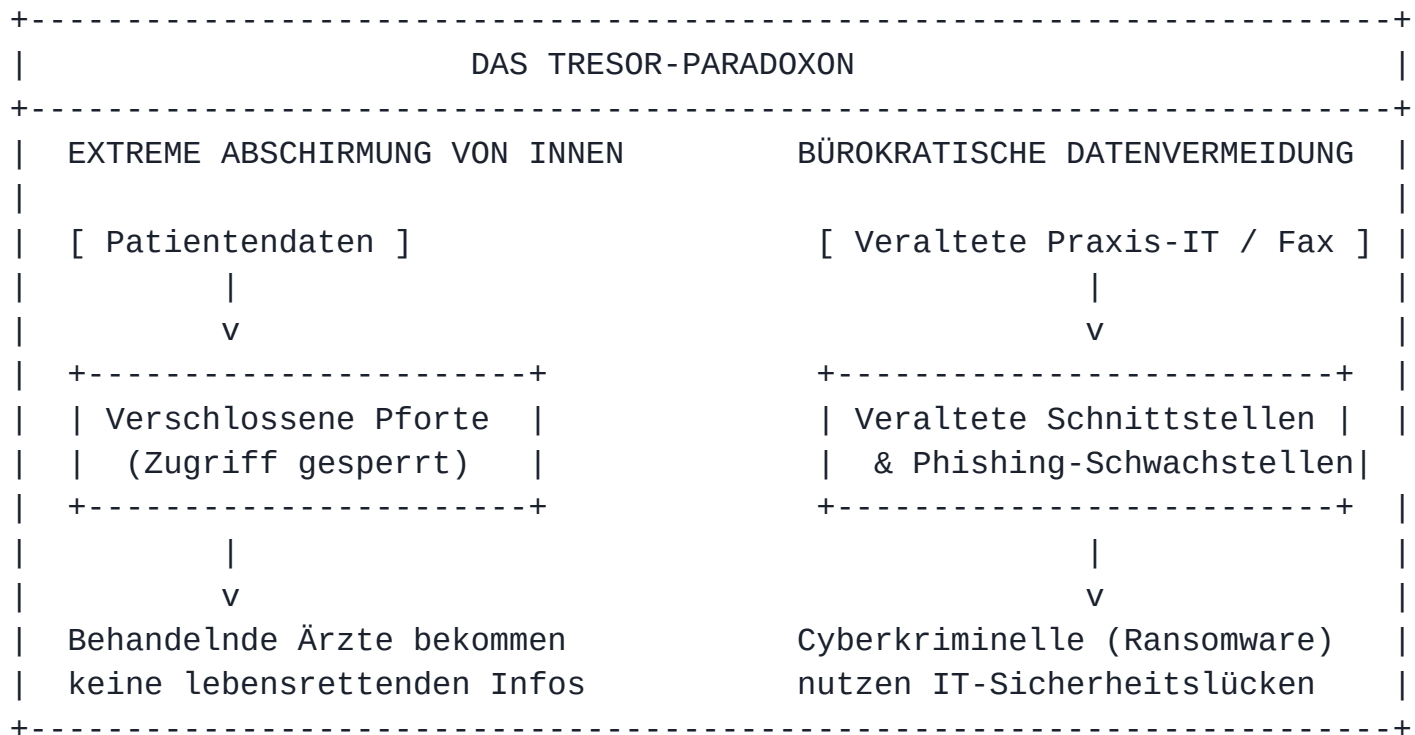
Dieses Szenario schildert keinen extremen Ausnahmezustand, sondern die tägliche Realität in einem der teuersten Gesundheitssysteme der Welt. Im Spannungsfeld zwischen einem oft bürokratisch verengten Verständnis von Datenschutz und veralteten IT-Strukturen entsteht ein gravierender Versorgungsengpass.

Gleichzeitig verunsichert diese Situation viele Bürgerinnen und Bürger verständlicherweise zutiefst: Sie befürchten einerseits den Verlust ihrer Intimsphäre, werden andererseits im Behandlungsalltag aber mit den konkreten Gefahren einer verzögerten medizinischen Versorgung konfrontiert. Dieses Vakuum aus begründeter Unsicherheit und systemischem Reformstau wird vereinzelt von Akteuren der Pseudomedizin instrumentalisiert. Durch das Schüren von Panik vor dem vermeintlich „gläsernen Patienten“ versuchen sie, das Vertrauen in die evidenzbasierte Medizin zu erschüttern und eigene Behandlungsangebote als vermeintlich sichere Zuflucht darzustellen.

Eine sachliche, didaktisch aufbereitete und streng evidenzbasierte Betrachtung zeigt jedoch: Wer Datenschutz und Patientensicherheit gegeneinander ausspielt, schadet der Gesundheit der Menschen. Echter Datenschutz im 21. Jahrhundert bedeutet nicht das Verstecken von Informationen vor lebensrettenden Helfern, sondern die Kombination aus hoher Datenverfügbarkeit im Notfall und modernster cybertechnischer Sicherheitsarchitektur.

1. Problemdefinition: Das Tresor-Paradoxon aus Datenvermeidung und IT-Sicherheitslücken

Das zentrale Dilemma der Digitalisierung im deutschen Gesundheitswesen lässt sich veranschaulichen anhand der didaktischen Metapher des "**Panzerschanks auf baufälligem Fundament**" (dem sogenannten Tresor-Paradoxon):



Über zwei Jahrzehnte hinweg wurde der medizinische Datenschutz in Deutschland vorrangig im Sinne der traditionellen **passiven Datenvermeidung** interpretiert. Nach diesem Verständnis gilt ein sensibles Datum genau dann als ideal geschützt, wenn es gar nicht erst digital erhoben, nicht gespeichert und keinesfalls einrichtungsübergreifend ausgetauscht wird. Diese Sichtweise führt zu einem gefährlichen Paradoxon:

- **Innere Blockade für die Heilkunde:** Die Pforten des Informationssystems werden gegenüber genau denjenigen Personen verschlossen, die den Schlüssel zur Diagnose und Heilung benötigen – den behandelnden Notärztinnen, Fachärzten und Pflegekräften.
- **Äußere Verwundbarkeit durch veraltete IT:** Während der rechtmäßige Datenaustausch im Klinikalltag durch bürokratische Hürden blockiert wird, basiert die dahinterliegende IT-Infrastruktur in vielen Einrichtungen auf veralteten Betriebssystemen und schutzlosen lokalen Praxisservern.

Rechtlich verankert die europäische Datenschutz-Grundverordnung (DSGVO) in Artikel 9 Absatz 1 zwar einen besonders strengen Schutz für Gesundheitsdaten. Gleichzeitig sieht die DSGVO in Artikel 9 Absatz 2 lit. h ausdrücklich vor, dass die Verarbeitung dieser Daten rechtmäßig ist, wenn sie für Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik oder der Versorgung erforderlich ist. In der deutschen Praxis führte die föderale Struktur mit 16 eigenständigen Landesdatenschutzbeauftragten jedoch lange Zeit zu zersplitterten

Interpretationen. Das Ergebnis war das Entstehen isolierter „Datensilos“: Das Krankenhaus erfuhr nichts von den relevanten Vorerkrankungen der Facharztpraxis, und die Spitzenforschung blieb von anonymisierten Versorgungsdaten weitgehend abgeschnitten.

2. Die wissenschaftliche Faktenlage: Versorgungsrisiken, Polypharmazie und internationale Evidenz

Die Konsequenzen des digitalen Entwicklungsrückstands sind keine hypothetischen Befürchtungen, sondern durch wissenschaftliche Berichte und Studien umfassend empirisch belegt.

A. Das Puzzlespiel der Arzneimitteltherapiesicherheit (AMTS)

Eine der gravierendsten Folgen fehlender digitaler Vernetzung ist das Phänomen der **Polypharmazie** (die gleichzeitige Einnahme mehrerer Medikamente), insbesondere bei älteren und chronisch kranken Menschen. Wenn Patientinnen und Patienten von unterschiedlichen Fachärzten behandelt werden, ohne dass ein zentral einsehbarer Medikationsplan vorliegt, gleicht die Verordnung neuer Arzneien einem Puzzlespiel ohne Vorlage:

[STUMME POST DER MEDIKATION (Analoges Papier-System)]

Facharzt A (Kardiologie)	---> Verschreibt Blutverdünner (z.B. Marcumar/DO)
Facharzt B (Orthopädie)	---> Verschreibt Schmerzmittel (z.B. Ibuprofen/N
Hausarzt	---> Weiß nichts von Orthopädie-Rezept
Resultat	---> Exponentielles Risiko für schwere Magenblut

[INTEGRIERTE ePA-MEDIKATIONS-PRÜFUNG (Digitales System)]

Facharzt B gibt Rezept ein	---> Automatische Interaktionswarnung in Echtze
	---> Dosierungsanpassung / Alternativpräparat

Empirische Analysen des Zentralinstituts für die kassenärztliche Versorgung (Zi) und des Sachverständigenrates zur Begutachtung der Entwicklung im Gesundheitswesen (SVR) zeigen das Ausmaß dieser Informationslücke:

1. **Unerwünschte Arzneimittelwirkungen (UAW):** Unerkannte Wechselwirkungen zwischen Medikamenten führen in Deutschland jährlich zu schätzungsweise 250.000 bis 400.000 vermeidbaren Krankenhauseinweisungen.

2. **Kritische Interaktionsbeispiele:** Die Kombination aus blutdrucksenkenden ACE-Hemmern, Aldosteronantagonisten und Kaliumpräparaten kann unbemerkt zu lebensbedrohlichen Hyperkaliämien führen. Ohne einheitliche digitale Medikationskontrolle bleiben solche Risiken im Alltag häufig unentdeckt.

B. Redundanz und Belastung durch Doppeluntersuchungen

Ein weiteres Problem ist die mangelnde Interoperabilität. Wenn Vorbefunde, MRT- oder CT-Bilder und Laborwerte nicht digital übertragen werden können, müssen diagnostische Eingriffe wiederholt werden:

- **Strahlenbelastung:** Unnötige Doppel-Röntgen- oder CT-Aufnahmen bedeuten eine vermeidbare kumulative Strahlenbelastung für die Patienten.
- **Ressourcenverschwendung:** Die finanzielle Belastung des Gesundheitssystems durch redundante Diagnostik beläuft sich nach Schätzungen des SVR auf Beträge in Milliardenhöhe – Geld, das an anderer Stelle in der Pflege fehlt.

C. Internationaler Vergleich: Der Bertelsmann Digital-Health-Index

Die Bertelsmann Stiftung verglich im Rahmen ihrer Studie *Smarthealthsystems* den Digitalisierungsgrad von 17 Gesundheitssystemen. Während Länder wie Estland, Dänemark oder Israel Spitzenplätze belegen, rangiert Deutschland im unteren Drittel.

+-----+ DIGITAL-HEALTH-INDEX (BERTELSMANN STIFTUNG) +-----+	
Top-Performer (z.B. Estland, Dänemark):	
- Zentrale, verschlüsselte Notfall- & Patientenakte seit >10 Jahren	
- Transparenz: Patienten sehen jeden Zugriff im Logbuch	
- Erhebliche Reduktion von Behandlungsfehlern & UAW	
Schlusslichter (z.B. Deutschland in Vorerhebungen):	
- Fragmentierte Datensilos, Papierakten, Faxgeräte	
- Hohe Rate an Doppeluntersuchungen & Medikationskonflikten	
+-----+	

In Estland existiert seit über 15 Jahren die nationale e-Health-Plattform. Notärzte können im Einsatz sofort auf allergologische Daten zugreifen. Die empirische Evidenz belegt: Eine hohe

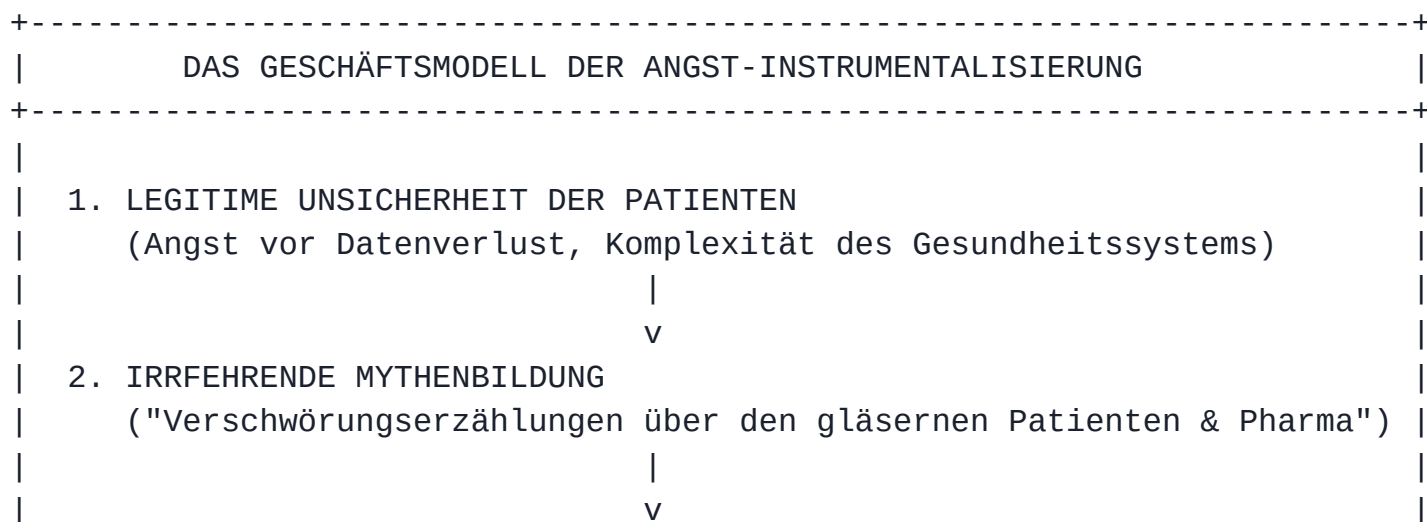
Digitalisierungsquote korreliert direkt mit einer höheren Patientensicherheit, ohne dass es zu systematischen Datenschutzverletzungen gekommen ist.

D. Echte IT-Bedrohungen laut BSI: Cyberkriminalität vs. Telematikinfrastruktur

Dass analoge Arbeitsweisen keineswegs vor Cyberkriminalität schützen, belegt der jährliche Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Krankenhäuser gehören zu den primären Zielen von Ransomware-Angriffen. Hacker verschlüsseln Kliniknetzwerke, sodass Notaufnahmen abgemeldet werden müssen. Die Ursache für diese Angriffe liegt jedoch **nicht** an zentralen, verschlüsselten Plattformen wie der elektronischen Patientenakte (ePA), sondern an veralteten Betriebssystemen auf lokalen Praxisservern und fehlender Netztrennung. Die sichere Digitalisierung über die nationale Telematikinfrastruktur (TI) ersetzt diese veralteten Infrastrukturen durch moderne, kryptographisch abgesicherte Verbindungen.

3. Psychologische Dynamik: Wie Pseudomedizin die Sorgen der Patienten ausnutzt

Die Diskussion um Gesundheitsdaten berührt zutiefst intime Lebensbereiche. Die Sorge vor Datenmissbrauch ist keine unberechtigte Paranoia, sondern ein verständlicher Ausdruck des menschlichen Bedürfnisses nach Selbstbestimmung und Sicherheit. Diese psychologische Vulnerabilität bildet jedoch den Nährboden für gezielte Fehlinformationen, die vereinzelt von Akteuren der Pseudomedizin genutzt werden.



	3. VERMEINTLICHE ALTRUISTISCHE ALTERNATIVE	
	("Bei uns bleiben Sie anonym – Zahlen Sie bar, meiden Sie ePA & TI")	
	v	
	4. REALER SCHADEN FÜR DEN PATIENTEN	
	(Verzicht auf Wechselwirkungsprüfungen, verzögerte Schulmedizin)	
+-----+		

Die Mechanik der Desinformation

In einschlägigen Medien wird die Einführung digitaler Notfallakten und E-Rezepte bisweilen systematisch entstellt. Es wird fälschlicherweise behauptet, dass Krankenakten ungefragt an Konzerne verkauft oder Bürger lückenlos überwacht würden.

Die kommerzielle und weltanschauliche Funktion

Diese Schreckensszenarien erfüllen häufig einen konkreten Zweck:

- **Aufbau eines exklusiven Vertrauensverhältnisses:** Indem das wissenschaftlich fundierte Gesundheitssystem als übergriffig dargestellt wird, positionieren sich pseudomedizinische Anbieter als Beschützer der Patientensouveränität.
- **Vermeidung von Leistungskontrollen:** Nicht-evidenzbasierte Therapieverfahren halten einer wissenschaftlichen Überprüfung oft nicht stand. Eine Verweigerung digitaler Dokumentation schützt solche Angebote vor Transparenz.
- **Kommerzielles Angebot:** Den Hilfesuchenden wird empfohlen, Behandlungen privat bar zu bezahlen und den Kontakt zum digitalen Versorgungsnetz abubrechen.

Die Gefahren für die Patienten

Patienten, die diesen Narrativen vertrauen und sich vollständig abkoppeln, erleiden erhebliche Nachteile: Sie verzichten auf automatische Sicherheitskontrollen bei Medikamentenverordnungen. Im akuten Notfall fehlen den Ärzten lebensrettende Informationen. Schwere Erkrankungen werden durch die Inanspruchnahme unbelegter Alternativmethoden oft erst spät diagnostiziert.

4. Medizinischer Alltag: Die konkreten Folgen für chronisch Kranke

Für Patientinnen und Patienten mit chronischen Erkrankungen – wie Typ-2-Diabetes, chronischer Niereninsuffizienz oder koronarer Herzkrankheit – entscheidet der nahtlose Informationsfluss maßgeblich über Behandlungsqualität und Lebenserwartung.

Das Szenario der Behandlungso dyssee

Ein multimorbider Patient konsultiert im Laufe eines Jahres typischerweise ein Dutzend unterschiedlicher Leistungserbringer: Hausarzt, Kardiologe, Diabetologe, Nephrologe, Augenarzt, Radiologe und Notfallambulanzen.

[MULTIMORBIDER PATIENT IM FRAGMENTIERTEN SYSTEM]

```
|
+---> Hausarzt (Papierakte A & lokale EDV)
|
+---> Kardiologe (Fachpraxis-Software B)
|
+---> Diabetologe (Papierbefund C)
|
+---> Notaufnahme (Kein Zugriff auf A, B, C)
|
v
```

Faktor Mensch / Notfallsituation ---> Informationsverlust

---> Behandlungsverzögerung & Fehldosierung

Ohne eine zentrale elektronische Patientenakte liegt die Verantwortung für die Vollständigkeit der Akte allein beim Patienten. In Notfällen oder im Alter ist der Mensch damit oft überfordert. Das Versäumnis, ein einziges Dokument vorzulegen, kann dazu führen, dass ein nierenschädigendes Kontrastmittel für ein CT verabreicht wird – mit potenziell irreversiblen Folgen.

5. Evidenzbasierte Reformansätze: Wie moderne IT-Architektur Datenschutz und Nutzen verbindet

Die Lösung für die Defizite liegt weder im Festhalten an Papierstrukturen noch im Verzicht auf Bürgerrechte. Erforderlich ist ein Ansatz, der **Datenschutz als aktiven Patientenschutz** versteht. Der Gesetzgeber hat mit dem Digitalgesetz (DigiG) und dem Gesundheitsdatennutzungsgesetz (GDNG) wichtige Schritte eingeleitet.

SÄULEN EINES MODERNEN DATENSCHUTZES IM GESUNDHEITSWESEN	
1. OPT-OUT & SOUVERÄNITÄT	2. HOCHSICHERE INFRASTRUKTUR
- Automatischer Nutzen für alle	- Zero Trust & E2E-Verschlüsselung
- Feingranulare Widerspruchsrechte	- Zertifizierte BSI-Standards
3. FORSCHUNGS-PSEUDONYMISIERUNG	4. TRANSPARENZ & DOKUMENTATION
- Sichere Datennutzung im FDZ	- Patient sieht jeden Zugriff
- Schutz vor Re-Identifikation	- Vollständige Nachvollziehbarkeit

A. Das Opt-out-Prinzip bei der elektronischen Patientenakte (ePA)

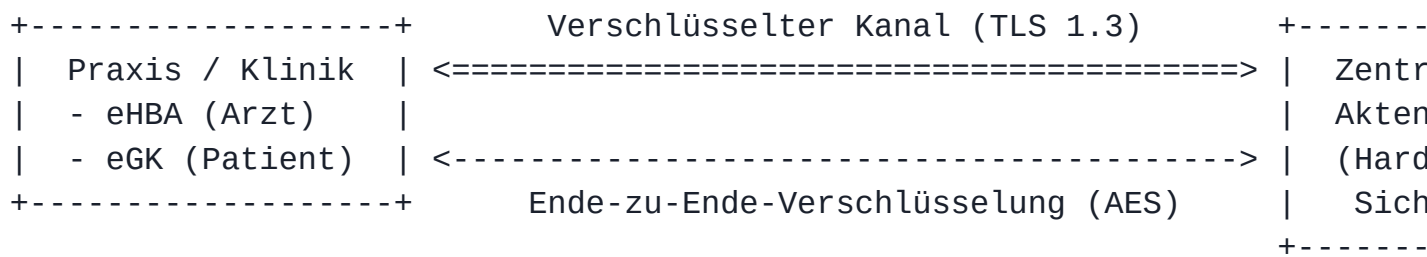
Das mit dem DigiG flächendeckend eingeführte **Opt-out-Verfahren** kehrte die bisherige Logik im Sinne der öffentlichen Gesundheit um: Jede versicherte Person erhält automatisch eine ePA. Bürgerinnen und Bürger können der Einrichtung der Akte jederzeit widersprechen oder den Zugriff für bestimmte Praxen oder einzelne Dokumente feingranular sperren. Dies kombiniert Nutzen für die Allgemeinheit mit Schutz der individuellen Wahlfreiheit.

B. Das Gesundheitsdatennutzungsgesetz (GDNG) und die Forschung

Wissenschaftlicher Fortschritt benötigt Daten. Das GDNG regelt die Nutzung pseudonymisierter Versorgungsdaten über das zentrale **Forschungsdatenzentrum Gesundheit (FDZ)**. Identifizierende Merkmale werden vor der Verarbeitung unwiderruflich durch mathematische Schlüssel ersetzt. Forscher arbeiten in abgesicherten Serverumgebungen, sodass eine Re-Identifizierung ausgeschlossen ist.

C. Das Baugerüst der Cyber-Resilienz: Technische Sicherheitsarchitektur

Moderne IT-Sicherheit im Gesundheitswesen beruht auf international erprobten kryptographischen Standards, die vom BSI geprüft werden:



1. **Ende-zu-Ende-Verschlüsselung (E2EE):** Daten werden auf dem Gerät des Absenders verschlüsselt und können erst auf dem Autorisierungsgerät des Empfängers wieder entschlüsselt werden.
2. **Zwei-Faktor-Authentifizierung:** Der Zugriff erfordert stets die Kombination aus elektronischer Gesundheitskarte (eGK) und elektronischem Heilberufsausweis (eHBA).
3. **Zero-Trust-Architektur:** Jedes Dokument und jede Abfrage wird einzeln kryptographisch verifiziert.
4. **Unveränderbare Zugriffsprotokolle:** Jede Einsichtnahme in die ePA wird fälschungssicher protokolliert. Versicherte können in ihrer ePA-App jederzeit nachvollziehen, wer wann welche Datei geöffnet hat.

6. Empathischer Dialog und Patientensouveränität: Sorgen ernst nehmen

Ein zukunftsfähiges Medizinsystem darf Bedenken von Bürgerinnen und Bürgern niemals spöttisch entgegentreten. Wenn Menschen zögern, ihre Krankengeschichte digital zu teilen, basiert dies oft auf verständlichen Erfahrungen mit Datenlecks im Internet oder unzureichender Transparenz.

Für das medizinische Fachpersonal ergibt sich daraus die Verpflichtung zu einem empathischen Dialog:

1. **Transparente Kommunikation:** Patientinnen und Patienten müssen verständlich über den konkreten Nutzen der ePA sowie über ihre Kontrollrechte informiert werden.
2. **Wahrung der Scham- und Intimsphäre:** Es muss als selbstverständlich respektiert werden, wenn Personen sensible Diagnosen (etwa psychiatrische Vorbehandlungen)

nicht im allgemeinen Teil der Akte sichtbar machen möchten. Die ePA bietet hierfür Verbergungsfunktionen.

3. **Stärkung der Patientensouveränität:** Die Digitalisierung ist ein Werkzeug, das den Menschen befähigt, als mündiger Partner an seiner Genesung mitzuwirken.
-

7. Fazit: Digitale Vernunft im Dienste der Heilkunst

Der mangelhafte Informationsfluss und veraltete IT-Strukturen im deutschen Gesundheitssystem stellen reale Versorgungsrisiken dar. Die Überwindung dieser Defizite erfordert weder den Rückzug in analoge Zettelwirtschaft noch das Errichten unüberwindbarer bürokratischer Hürden.

Vielmehr benötigt eine moderne Heilkunde eine digitale Infrastruktur, die dem Menschen dient. Wenn Datenschutz nicht als Datenvermeidung, sondern als **aktive Datensicherheit und Patientenschutz** verstanden wird, schützt er die Privatsphäre und befähigt Ärztinnen, Pflegende und Wissenschaftler dazu, Leben zu retten. Bürgerinnen und Bürger sind eingeladen, sich sachlich über ihre Rechte und Schutzmechanismen zu informieren – um die Chancen einer evidenzbasierten, digital unterstützten Medizin vollumfänglich und sicher zu nutzen.
