

25.082 Elektronisches Gesundheitsdossier. Bundesgesetz

Faktenblatt: Grundlagen technische Infrastruktur

1. Auftrag

Die Verwaltung wurde beauftragt, aufzuzeigen:

- » Welche Modelle bei der zentral vs. dezentral organisierten technischen Infrastruktur zur Diskussion stehen.
- » Wie das Verhältnis zwischen E-GD und DigiSanté/Gesundheitsdatenraum aussieht. Hintergrund: Beim E-GD ist eine zentralisierte technische Infrastruktur vorgesehen, beim Gesundheitsdatenraum Schweiz (DigiSanté) sollen die Gesundheitsdaten jedoch dezentral zugänglich gemacht werden.
- » Wie sich das Projekt «Justitia 4.0» zum E-GD verhält und welche Lehren daraus gezogen werden können.

2. Ausgangslage

Gesundheitsdaten sind heute in der Schweiz dezentral gespeichert – auf zahllosen Systemen bei Leistungserbringern und Gesundheitseinrichtungen wie Praxen, Spitälern, Apotheken und Laboren. Die Leistungserbringer und Gesundheitseinrichtungen sind selbst für die sichere und datenschutzkonforme Datenhaltung verantwortlich.

Auch in Zukunft bleiben Gesundheitsdaten grundsätzlich dezentral gespeichert, zumal die individuelle Dokumentationspflicht auf Seiten der Leistungserbringer unverändert fortbesteht.

Im Rahmen des Programms DigiSanté wird der Gesundheitsdatenraum Schweiz (SwissHDS) zur Etablierung einheitlicher Standards für den nahtlosen Datenaustausch und eine systemübergreifende interoperable Kommunikation geschaffen. So können Daten ohne manuelle Zwischenschritte und automatisch zwischen Leistungserbringern untereinander oder zwischen ihnen und dem Bund effizient ausgetauscht werden.

Die Service-Infrastrukturen und -Dienste des SwissHDS bilden das notwendige Rückgrat zur Gewährleistung der Governance, der Interoperabilität und der Nachvollziehbarkeit. Das elektronische Gesundheitsdossier (E-GD) ist ein integraler Bestandteil des SwissHDS und dient als Langzeitspeicher für Gesundheitsdaten, da Leistungserbringer Daten aus rechtlichen Gründen nicht unbegrenzt aufbewahren dürfen. Im Vergleich zu gängigen Informationssystemen in Arztpraxen und Spitälern wird das E-GD als Schutzobjekt des Bundes restriktivere Sicherheitsmassnahmen ausweisen.

3. Datenhaltung im E-GD

Das Informationssystem E-GD ist und bleibt ein Sekundärsystem. Das bedeutet, dass sämtliche medizinischen Informationen weiterhin dezentral bei den Leistungserbringern bleiben. Hingegen bleiben Gesundheitsdaten, welche für das ganze Leben relevant sind, im E-GD langfristig erhalten. Beispielsweise sind so Impfungen und Allergien auch nach Ablauf der Aufbewahrungspflicht oder nach der Schliessung einer Praxis verfügbar.

Ein zentrales Informationssystem bedeutet nicht ein einziger Datentopf, sondern vielmehr, dass einheitliche Regeln und gemeinsame Standards gelten, während die Daten nach dem Stand der Technik segmentiert, auf mehreren Instanzen verteilt und verschlüsselt gespeichert werden. Eine Kombination von technischer Isolation, kryptografischer Verfahren und prozessualer Restriktionen stärkt die Sicherheit. Eine dezentrale Lösung, die auf Primärsysteme abstellt, wurde geprüft, erweist sich jedoch mittelfristig als nicht realisierbar. Sie setzt voraus, dass sämtliche Leistungserbringer über hochverfügbare, sicherheitskonforme Systeme verfügen und ihre Daten dauerhaft, standardkonform und rund um die Uhr zugänglich halten. Diese Vision wird als langfristiges Ziel im Rahmen des SwissHDS verfolgt; eine schweizweite Umsetzung ist jedoch realistisch erst nach 2034 zu erwarten. Das E-GD übernimmt in diesem Kontext eine zentrale Brückenfunktion: Es schafft frühzeitig die notwendigen Grundlagen für eine strukturierte, standardisierte und qualitätsgesicherte Datenaufbereitung an der Quelle – in den Primärsystemen der Leistungserbringer – und wirkt damit als entscheidender Katalysator auf dem Weg zum SwissHDS. Zudem wird das Informationssystem E-GD auch in Zukunft den einzigen Langzeitspeicher für die persönlichen Gesundheitsdaten darstellen.

4. Verschlüsselung

Eine konsequente, endpunktgebundene Verschlüsselung mit ausschliesslich patientenseitig kontrollierten Schlüsseln würde ein Mass an digitaler Kompetenz und Eigenverantwortung bedeuten, das realistischlicherweise nicht von der ganzen Bevölkerung vorausgesetzt werden kann. Dies würde die Alltagstauglichkeit entsprechender Lösungen einschränken. Für die effektive informationelle Selbstbestimmung hingegen ist ein niederschwelliger, verlässlicher und rechtssicherer Zugang für alle entscheidend. Aus diesem Grund setzt die Architektur des E-GD auf eine starke Verschlüsselung auf Dossierebene, verzichtet jedoch bewusst auf eine ausschliessliche Schlüsselverwaltung durch die Patientinnen und Patienten. Gleichzeitig ist sowohl technisch als auch regulatorisch sichergestellt, dass weder die Betreiber der Infrastruktur noch die Behörden Zugriff auf die Inhalte der Gesundheitsdaten erhalten.

5. Datensicherheit und Datenschutz

Mit dem neuen Gesetz bleiben die Sicherheitsanforderungen für sensible Gesundheitsdaten unverändert hoch. Das E-GD wird mit moderner Sicherheitsarchitektur nach den Prinzipien «Zero-Trust», «Security by Design» und «Security by Default» entwickelt und unterliegt den strengen Anforderungen des Bundesgesetzes über die Informationssicherheit (ISG), des Datenschutzgesetzes (DSG) und des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG). Die Daten müssen nach Schweizer Recht und ausschliesslich in der Schweiz gespeichert werden. Ein Security Operations Center, durchgehende Systemüberwachung sowie ein strukturiertes Bug-Bounty-Programm bieten zusätzlichen Schutz. Entscheidend wird die vollständige und unveränderbare Protokollierung sämtlicher Zugriffe sein, welche für Patientinnen und Patienten jederzeit einsehbar und ex post überprüfbar ist. Anomalie- und Missbrauchserkennung identifizieren zudem verdächtige Muster und lösen automatische Alarmer aus.

6. Vergleich zum Projekt Justitia 4.0

Das BAG steht im Austausch mit dem Projektteam von Justitia 4.0. Die beiden Systeme – das E-GD und Justitia 4.0 – sind bei näherer Betrachtung nur eingeschränkt vergleichbar: Die Justitia-Plattform ist auf den sicheren Dokumententransfer ausgerichtet, also auf die Übermittlung von Dokumenten zwischen einzelnen Stellen. Sie nutzt derzeit keine Ende-zu-Ende-Verschlüsselung. Beim E-GD handelt es sich hingegen um ein wesentlich komplexeres Vorhaben, bei dem besonders schützenswerte Daten langfristig gespeichert sowie situationsabhängig und kontrolliert für eine Vielzahl unterschiedlich berechtigter Stellen bereitgestellt werden. Der Fokus liegt damit nicht auf der Dokumentenübermittlung, sondern auf der dauerhaften Datenhaltung und der differenzierten Zugriffssteuerung über lange Zeiträume hinweg, auch im Notfall. Diese Unterschiede haben erhebliche Auswirkungen sowohl auf die jeweilige Systemarchitektur als auch auf die zugrunde liegenden Sicherheitskonzepte.

7. Fazit und weitere Arbeiten

Für die Umsetzung des Datenschutzes sind hohe Datensicherheitsstandards entscheidend, da sie die notwendige Vertrauensbasis für die Akzeptanz und den Erfolg des E-GD schaffen. Das BAG prüft verschiedene Varianten – vorgesehen ist ein mehrstufiges Sicherheitsmodell mit starker Verschlüsselung und klaren Zugriffskontrollen. Analysiert wird auch, ob eine Integration der Vertrauensinfrastruktur der elektronischen Identität (e-ID) sowie der SwissGovernmentCloud möglich ist. Die konkrete Ausgestaltung des kryptografischen Schutzes bildet Gegenstand laufender Abklärungen eines Fachgremiums, wobei sämtliche Massnahmen in enger Koordination mit bundesinternen Fachstellen und externen Sicherheitsexperten konkretisiert werden. Es gilt dabei, das optimale Gleichgewicht zwischen Sicherheit, Benutzerfreundlichkeit und Kosten zu finden. Die technischen Details werden im Ausführungsrecht festgelegt. So wird sichergestellt, dass die Regelungen laufend dem technologischen Wandel angepasst werden können und stets dem Stand der Technik entsprechen. Interessierte Kreise sind in verschiedenen Gremien eingebunden und können sich im Rahmen der Vernehmlassung zum Ausführungsrecht einbringen.