Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens
(Digital-Gesetz – DigiG)
&
Gesetz zur verbesserten Nutzung von Gesundheitsdaten
(Gesundheitsdatennutzungsgesetz – GDNG)

1. Evolution der elektronischen Patientenakte (ePA)

Anwendungen der elektronischen Gesundheitskarte (anfangs)

Anwendungen der Telematikinfrastruktur nach § 334 (aktuell):

1. ePA nach § 341
2. Hinweise auf Erklärungen zur Organ- und Gewebespende
3. Hinweise auf Vorsorgevollmachten, Patientenverfügungen
4. elektronischer Medikationsplan
5. elektronische Notfalldaten
6. elektronische Verordnungen
7. elektronische Patientenkurzakte

Elektronische Patientenakte nach § 341 (geplant):

1. medizinische Informationen über den Versicherten, insbesondere
    a) Befunde, Diagnosen, durchgeführte und geplante Therapiemaßnahmen, Vorsorgeuntersuchungen, Behandlungsberichte usw.
    b) elektronischer Medikationsplan
    c) elektronische Notfalldaten / Patientenkurzakte
    d) elektronische Arztbriefe,
2. elektronisches Zahn-Bonusheft,
3. elektronisches Untersuchungsheft für Kinder,
4. elektronischer Mutterpass,
5. elektronische Impfdokumentation,
6. durch den Versicherten zur Verfügung gestellte Gesundheitsdaten,
7. Daten aus einer Krankenkassen-eGA,
8. Daten von den Krankenkassen über in Anspruch genommene Leistungen,
9. Daten aus Digitalen Gesundheitsanwendungen (DiGA),
10. Daten zur pflegerischen Versorgung aus Digitalen Pflegeanwendungen (DiPA),
11. Verordnungsdaten u. Dispensierinformationen elektronischer Verordnungen n. § 360,
12. Elektronische AUB,
13. sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, z.B. aus DMP

2. Opt-Out / (Vorab-)Widerspruch gegen ePA (§ 353)

- schriftlich oder elektronisch, Details noch nicht bekannt

3. Zugriffsverfahren für Versicherte

vorab einmalige Identitätsfeststellung, danach für jeden Zugriff Authentisierung (§ 336)

Möglichkeiten der Authentisierung:

- per eGK + PIN
- ab 2026 auch per digitale Identität,
- für ePA- und eRezept-App Authentisierung künftig auch ohne eGK möglich,
  nach schriftlicher oder elektronischer Erklärung, dieses Verfahren nutzen zu wollen

4. Was können Versicherte in ihrer ePA tun? (geplant)

Mittels „Benutzeroberfläche eines geeigneten Endgeräts“ (ePA-App):

- Opt-out (in der ePA der ePA widersprechen)
- Inhalte einfügen, ändern, löschen, beschränken (d.h. für andere unsichtbar machen),
- Zugriff durch Leistungserbringer widersprechen oder erlauben, dokumentengenau
- eigene Zugriffsberechtigungen vergeben, von beliebiger Dauer, auch unbefristet
- aus der eRezept-App heraus eGK + PIN oder digitale Identität beantragen

Ohne ePA-App:

- In „Leistungserbringerumgebung“ dem Zugriff durch Leistungserbringer widersprechen, auf Kategorien von Dokumenten und Datensätzen (medizinische Fachgebietskategorien)

5. Was passiert, wenn man nicht widerspricht (Teil 1):

Die ePA wird befüllt:

- Man bekommt eine ePA (Krankenkassen sind gesetzlich verpflichtet, sie einem zur Verfügung zu stellen, sofern man nicht widerspricht)
- Daten auf eGK werden in entsprechen-de ePA-Anwendungen übertragen und alles (außer Notfalldaten) von eGK gelöscht
- Krankenkassen übermitteln Daten über in Anspruch genommen Leistungen via ePA-Anbieter in die ePA, sofern man nicht widerspricht
- eRezeptdaten und Dispensierinformationen werden automatisiert in die ePA übermittelt (§ 360 Abs. 14)
- Leistungserbringer übermitteln Daten in ePA (§§ 346 bis 349):
- Ärzte, Zahnärzte und Psychotherapeuten *müssen* Daten zu aktuellen Behandlungen des Versicherten in ePA zu übermitteln, Krankenhäuser die Entlassbriefe
- Ärzte *dürfen* weitere Daten (Laborbefunde, Röntgenbilder usw.), eArztbriefe und AUBs in der ePA speichern, nach Rücksprache mit dem Versicherten
- weitere Leistungserbringer dürfen Daten in ePA speichern, sofern kein Widerspruch

5. Was passiert, wenn man nicht widerspricht (Teil 2):

Die ePA-Daten werden genutzt:

- Leistungserbringer aller Art dürfen "im zeitlichen Zusammenhang mit der Behandlung" auf ePA-Anwendungen zugreifen
- Ärzte sind zur Erstellung des Medikationsplans verpflichtet, sofern man mindestens 3 Medikamente nimmt.
- Daten aus der ePA werden zu Forschungszwecken weitergegeben (§ 363), sofern man nicht widerspricht
- und künftig noch vieles mehr (Nutzung für Telemedizin, Datenaustausch mit DiGAs…)

6. eRezept (§ 360 SGB V, DigiG):

- ab 2024
- eRezepte dürfen nur über die TI übermittelt werden:

  - das eigentliche Rezept liegt im eRezept-Fachdienst der TI

  - die Zugangsdaten erhält der Versicherte auf Papier oder elektronisch

  - und kann sie über den im Gesundheitswesen "als sicheres Übermittlungsverfahren nach § 311 Absatz 6 genutzten Sofortnachrichtendienst" weiterleiten
- erlaubt sind aber Systeme, über die Ärzte das Token zum Zugang zum eRezept außerhalb der TI an die Versicherten übermitteln, damit diese sie an eine Apotheke ihrer Wahl weiterleiten
- kein opt-out aus eRezept-Fachdienst der TI möglich

7. Telemedizin (DigiG):

- Aufhebung der bisherigen Begrenzung der Videosprechstunden auf 30%
- Apotheken dürfen „assistierte Telemedizin“ anbieten (§ 129 Abs. 5h)
- Für Videosprechstunden sollen "ergänzend zu von Dritten angebotenen technischen Verfahren zu Videosprechstunden auch Dienste der Telematikinfrastruktur genutzt werden müssen, sobald diese zur Verfügung stehen" (§ 365)
- KBV betreibt (ab Juli 2024) elektronisches System (Schnittstelle) zur Vermittlung und Unterstützung telemedizinischer Leistungen (§ 370aI

8. Digitale Gesundheitsanwendungen (DigiG):

- Verschreibungsfähige Apps
- DiGA müssen ab 2024 digitale Identitäten unterstützen
- DiGA-Daten sollen in ePA übermittelt und gespeichert werden können, DiGA sollen therapierelevante Daten aus der ePA auslesen können (mit Zustimmung des Versicherten)

9. Digitalisierte DMP (§ 137f Abs. 9 SGB V, DigiG)

- Strukturierte Behandlungsprogramme mit digitalisierten Versorgungsprozessen
- Pilotprojekt: digitalisierte DMP für Diabetes Typ 1 und 2,
- Der Gemeinsame Bundesausschuss soll dabei in Richtlinien insbesondere regeln: die Nutzung
  1. der ePA
  2. des eMedikationsplans
  3. der sicheren Übermittlungsverfahren nach § 311 Abs. 6
  4. ambulanter telemedizinischer Leistungen
  5. von DiGAs
  6. von Gesundheitsdaten zum Zweck der **Personalisierung der Behandlung**

10. Interoperabilität (DigiG)

Kompetenzzentrum für Interoperabilität im Gesundheitswesen bei der gematik, das überall zu beteiligen ist, wo Schnittstellen / Anwendungen spezifiziert oder geändert werden

Medizinische Informationsobjekte:

- geben einheitliche Daten-Strukturierung vor, damit Daten in allen Systemen gleich dargestellt und verarbeitet werden können
- der Medikationsplan muss sektorübergreifend interoperabel sein
- die Patientenkurzakte (neue Version, inkl. Notfalldaten und Willenserklärungen) muss auch grenzüberschreitenden Datenaustausch ermöglichen, da sie die Behandlung EU-weit unterstützen soll (§ 358 Abs. 7)

11. Datensicherheit und Datenschutz (DigiG)

Bedeutungsverlust BSI, BfDI:

- überall nur noch Benehmen mit BSI, BfDI, aber Einvernehmen mit "Kompetenzzentrum für Interoperabilität im Gesundheitswesen“
- Einrichtung eines "Digitalbeirats“ der gematik
  (nach 1 Jahr Evaluation, ob Belange der Datensicherheit und des Datenschutzes ausreichend berücksichtigt wurden)

Änderungen IT-Sicherheits-Richtlinie der KBV (§ 75b), z.B.:

- Festlegungen im Einvernehmen mit dem BSI, in Benehmen mit BfDI, Bundesärztekammer, Bundeszahnärztekammer, Deutsche Krankenhausgesellschaft, IT-Industrie-Verbände
- Verpflichtende "Security Awareness"-Schulungen für Praxis-/Krankenhaus-Mitarbeiter
- Auch Anforderungen an sichere Installation / Wartung von TI-Komponenten und –Diensten in Praxen,
  Mitarbeiter von IT-Dienstleistern müssen dafür von KBVen zertifiziert werden

12. Datensicherheit und Datenschutz (DigiG)

Cloud-Nutzung:

Leistungserbringer, Krankenkassen und deren Auftragsdatenverarbeiter dürfen Sozialdaten auch per Cloud-Computing verarbeiten, und zwar

1. im Inland

2. in einem EU-Mitgliedsstaat

3. in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat *oder*,

sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat

und sofern die beauftragte, datenverarbeitende Stelle eine Niederlassung im Inland hat

13. Datenzugangs-und Koordinierungsstelle (§ 1 GDNG)

(beim Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM)

zentraler Ansprechpartner für sekundäre Datennutzer,

hat (bisher) koordinierende Aufgaben:

1. führt Metadaten-Katalog über vorhandene Gesundheitsdaten und deren Halter
2. berät bei Identifizierung und Lokalisierung der benötigten Daten
3. berät beim Stellen von Anträgen bei den Datenhaltern
4. nimmt Anträge entgegen und leitet an die eigentlichen Adressaten weiter
5. unterstützt Kommunikation zw. Antragsteller und Adressaten
6. informiert Öffentlichkeit über ihre Tätigkeit
7. unterstützt Bundesregierung bei Steigerung der Verfügbarkeit vor Gesundheitsdaten und Aufbau einer vernetzten Gesundheitsdateninfrastruktur (in BRD und EU)
8. erstellt Konzepte
   a) für sichere Verarbeitungsumgebungen für Sekundärnutzung
   b) zu ihrer Weiterentwicklung zur EHDS-Datenzugangsstelle
9. nimmt Aufgaben im Antragsverfahren bei Datenverknüpfung zwischen Krebsregistern und FDZ wahr

14. Datenverknüpfung FDZ - Krebsregister (§ 2 GDNG)

genehmigt die Datenzugangsstelle

- Daten werden in sicherer Verarbeitungsumgebung einer öffentlich-rechtlichen Stelle über eine "Forschungskennziffer" verknüpft, pseudonymisiert, zur Verfügung gestellt
- die sichere Umgebung muss gewährleisten, dass Datenverarbeitung auf den genehmigten Zweck beschränkt ist und keine Daten kopiert werden können
- Nutzungsberechtigte dürfen Daten

  1. nur für die Zwecke nutzen, für die sie zugänglich gemacht wurden

  2. nicht an Dritte weitergeben
- Re-Identifizierung von Personen / Leistungserbringern / Leistungsträgern ist verboten, ebenso Betriebs- und Geschäftsgeheimnisse ausspionieren.
  versehentliche Re-Identifizierung ist der Zugangsstelle zu melden

15. Publikationspflicht bei Verarbeitung im öffentlichen Interesse (§ 5 GDNG)

- Forschungsergebnisse aus Datenverarbeitung auf Grundlage gesetzlicher Vorschriften
  - ohne Einwilligung der Betroffenen oder
  - mit öffentlichen Mitteln geförderten Vorhaben

  sind binnen 12 Monaten nach Abschluss anonymisiert zu veröffentlichen (open data, Fachzeitschrift oder Internetseite des Verantwortlichen).
- In begründeten Ausnahmefällen kann die Zentrale Datenzugangs- und Koordinierungsstelle vorsehen, dass nicht oder erst später veröffentlicht werden muss.

16. KK/KV-Forschung: Anonymisierung optional (GDNG)

§ 287 SGB V:

- Sozialdaten sind nicht mehr unbedingt zu anonymisieren, sondern nur "sobald dies nach dem Forschungszweck möglich ist“

und zwar

- wenn KK oder KVen mit Datenbestände Arzt- oder Patienten-beziehbar auswerten für
  - epidemiologischer Erkenntnisse
  - Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen
  - örtliche Krankheitsschwerpunkte
- oder über die eigentliche Frist hinaus aufbewahren.

17. Versichertendaten-Auswertung durch KK (GDNG)

§ 287a SGB V:

- KK und Pflegekassen werten Gesundheitsdaten ihrer Versicherten automatisiert aus, um gesundheitliche Risiken zu erkennen und die Versicherten daraufhin anzusprechen
- Widerspruch ist möglich
- Zulässige Verarbeitungszwecke:

  1. Früherkennung von seltenen Krankheiten
  2. Überprüfung der Arzneimitteltherapiesicherheit
  3. "risikoadaptierten Früherkennung von Krebsrisiken"
  4. vergleichbare Maßnahmen zur Erkennung akuter und schwerwiegender Gesundheitsgefährdungen
- erkannte konkrete Gefährdungen sind dem Betroffenen umgehend mitzuteilen - in Form der Empfehlung, ärztliche Unterstützung in Anspruch zu nehmen

18. Forschungsdatenzentrum (GDNG)

§ 303a-e SGB V:

- Aufbewahrungsfrist für Daten im FDZ von 30 Jahren gestrichen, künftig unbegrenzt
- (abschließende) Liste der Nutzungsberechtigten wird gestrichen - nutzungsberechtigt sind künftig natürliche und juristische Personen im Anwendungsbereich der DSGVO, die bestimmte Zwecke verfolgen (analog zum EHDS)
- Zulässige Zwecke werden erweitert um Entwicklung, Nutzenbewertung, Überwachung der Sicherheit von Arzneimitteln, Medizinprodukten, Hilfs- und Heilmitteln, DiGAs, DiPAs, „einschließlich Testen und Trainieren von Anwendungen der Künstlichen Intelligenz im Gesundheitswesen„
- Verbotene Zwecke (analog zum EHDS):

  1. Entscheidung über Abschluss / Ausgestaltung von Versicherungsverträgen
  2. "Treffen von Entscheidungen zum Schaden einer natürlichen Person"
  3. Entwicklung von Produkten/ Dienstleistungen, die Einzelpersonen / Gesellschaft schaden können (Drogen Alkohol, ...)
  4. Marktforschung, Werbung, Vertriebstätigkeiten für Arzneimittel, Medizinprodukte…

- bei begründetem Verdacht auf Datenmissbrauch kann das FDZ den Übeltäter vom Datenzugang ausschließen, auch unbefristet
  FDZ informiert außerdem Datenschutzaufsichtsbehörden (zwecks weiterer Sanktionen nach DSGVO)

19. (unfreiwillige) Datenspende (GDNG)

§ 363 SGB V:

- „Datenspende“ aus der ePA passiert automatisch, sofern man nicht widerspricht, automatisierte Übermittlung an das FDZ und zwar ausschließlich Daten, die "zuverlässig automatisiert pseudonymisierbar sind." (Informationsobjekte),
- Widerspruch nur über ePA-App,

  kann auf bestimmte Zwecke / bestimmte Gruppen von Akteuren beschränkt werden, ist zu dokumentieren
- Versicherte werden bei erster Benutzung einer ePA-App über die Datenverarbeitung zwecks Datenspende und die Widerspruchsmöglichkeiten informiert

20. Forschungsgeheimnis (GDNG)

§ 203 StGB:

- Offenbaren personenbezogener Gesundheitsdaten, die einem zu Forschungszwecken anvertraut wurden, wird mit Freiheitsstrafe von max. 3-4 Jahren / Geldstrafe bestraft
- Daten dürfen nicht zur Re-Identifizierung von Personen oder zum Ausspionieren von Betriebs-/Geschäftsgeheimnissen missbraucht werden

§ 53 StPO:

- Zeugnisverweigerungsrecht künftig auch für „Personen, die zu Forschungszwecken berechtigt personenbezogene Gesundheitsdaten speichern oder verarbeiten“

§ 97 StPO:

- Beschlagnahme von Forschungsdaten / daraus abgeleiteten Erkenntnissen ist unzulässig