

# Patienten – Datenschutz – Gesetz <sup>1</sup>

## PDSG oder eHealth

(Stand: 01/2022)

### Inhaltsverzeichnis

1. Der Ruf nach digitaler Transformation im Gesundheitswesen.....1	3. Die Telematikinfrastruktur (SGB V §306ff).....2
2. Die elektronische Gesundheitskarte (SGB V Kp.10 §291ff).....1	4. Die elektronische Patientenakte i. w. S. (ePA, SGB V §334ff).....2
	5. Exkurs: Videosprechstunde (SGB V §365ff).....3

## 1. Der Ruf nach digitaler Transformation im Gesundheitswesen

Das Ärzte, Labore und Kliniken bereits einen hohen (mehrheitlich internen) Digitalisierungsgrad aufweisen, haben leider die Cyberangriffe der letzten Jahre gezeigt. Auf der anderen Seite besteht ein erheblicher Mangel in der digitalen Kommunikation mit Dritten, z. B. mit den Patienten. Daraus folgt die Forderung nach: „**Transformation, aber mit Sicherheit!**“, zumal Datenschutz-Grundverordnung (DS-GVO) und Bundesdatenschutzgesetz (BDSG) medizinische Daten unter besonderen Schutz gestellt wissen wollen. Zur Vereinheitlichung der Regelung wurde das PDSG beschlossen und festgehalten im Sozialgesetzbuch, fünftes Buch, zehntes Kapitel (§§284-305b Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz) und elftes Kapitel (§§306-383 Telematikinfrastruktur) oder SGB V Kp10<sup>2</sup> und SGB V Kp.11<sup>3</sup>

## 2. Die elektronische Gesundheitskarte (SGB V Kp.10 §291ff)

Für Ausstellung, Sicherheit und Authentifizierung ist die jeweilige Krankenkasse verantwortlich und die Karte muss neben einem Foto und der Unterschrift, über eine kontaktlose Schnittstelle verfügen. Bei Versendung ist der Versicherte „umfassend und in allgemein verständlicher, barrierefreier Form zu informieren über die Funktionsweise der elektronischen Gesundheitskarte und die Art der personenbezogenen Daten, die nach §291a auf der elektronischen Gesundheitskarte oder durch sie zu verarbeiten sind.“ (Zitat: SGB V Kp.10 §291 Abs.5). Nach den Abs.7&8 ist ab 01.01.2022 ein technisches Verfahren zum Zugriff des Versicherten und ab 01.01.2023 eine digitale Identität (Online-Legitimation) für den Versicherten auf Verlangen zur Verfügung zu stellen.

Von der(n) **behandelnden Arztpraxis / Klinik / Leistungserbringer** müssen die Daten zum Status der Krankenversicherung elektronisch lesbar und in Abrechnungsvorlagen übertragbar sein. Auf dem Abrechnungsschein hat der Versicherte dem Arzt die Mitgliedschaft in der Krankenkasse durch Unterschrift in ¼ jährlichem Rhythmus zu bestätigen. Ab 01.01.2024 auch durch seine digitale Identität, was Online über die Krankenkasse aktualisierbar und prüfbar ist. Eine Befreiung besteht für „kontaktlose“ Behandlungen. Es besteht eine Pflicht zum Anschluss an die „Telematik – Infrastruktur“ seit 30.06.2020 (SGB V §291b Abs.4)

Das **Forschungsdatenzentrum**, als Zentralstelle für die Steuerung der Prüfungen zur Wirtschaftlichkeit, Qualität, Bundesbezuschussung, Wahrnehmung von Patienteninteressen, Gesundheitsvorsorge- und Gesundheitsforschung, erhält Auswertungsdaten von der Vertrauensstelle, mit einem vom BSI\* genehmigten Pseudonymisierungsverfahren für die von den Krankenkassen mit Lieferpseudonym an die Vertrauensstelle übermittelten Patientendaten (SGB V §303ff).

Für diese **reinen Abrechnungsdaten** (Wirtschaftlichkeit, Statistik & Forschung) gelten gleichgelagerte Regelungen zur DS-GVO für die Aufbewahrungs- bzw. Löschpflichten, d. h. 10 Jahre für rechtliche und wirtschaftliche Nachweispflichten sowie nach gesetzlichen Vorgaben für

1 Quelle: <https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html>

2 LINK: [https://dejure.org/gesetze/SGB\\_V/284.html](https://dejure.org/gesetze/SGB_V/284.html)

3 LINK: [https://dejure.org/gesetze/SGB\\_V/306.html](https://dejure.org/gesetze/SGB_V/306.html)

\*) BSI Bundesamt für Sicherheit in der Informationstechnik

## Für den eiligen Leser kurz zusammengetragen (2/3)

den Gesundheits- und den Strukturausgleichsfonds. Statistik und Forschungsdaten sind anonymisiert ([SGB V §304](#)).

Es besteht eine **Auskunftspflicht** gegenüber dem Versicherten. Eine **Übermittlung an Dritte** ist nur mit ausdrücklicher Einwilligung (Berechtigungsregelung siehe ePA) des Versicherten erlaubt.

### 3. Die Telematikinfrastruktur<sup>4</sup> ([SGB V §306ff](#))

Ziel ist die Schaffung einer **sicheren**, wie **kompatiblen** Information und **Kommunikation** zwischen allen Beteiligten des Gesundheitswesens, einschließlich Rehabilitation, Pflege und Versicherten / Patienten und für Zwecke der Gesundheits- und pflegerischen Forschung. Wegen der besonderen Kategorie der medizinischen Daten nach der DS-GVO, gilt es ein entsprechend hohes Schutzniveau für die technische – organisatorischen Maßnahmen einzuhalten (Authentifizierung, eSignatur, Ver- und Entschlüsselung, Berechtigungsmanagement).

**Verantwortlich(e) i. S. d. Datenschutzes** ist zunächst die Gesellschaft für Telematik (gematik GmbH) als Entscheider, Zulassungsstelle und Auftraggeber für den gesicherten Netzbetrieb, die Anbieter / Betreiber (Netz, Komponenten, Geräte, Software) für die vorgegebene, operative Durchführung und die Nutzer (Leistungserbringer, Versicherte, Patienten) für die Einhaltung der ihnen vorgegebenen Regelungen gemäß Anleitung (z.B. Gerätestandort, Anschluss usw.). Vorgaben der DS-GVO zu Transparenz, Information nach [Art.12](#) und Profiling nach [Art.22](#) sind ausgeschlossen, soweit diese nicht, oder nur unter Umgehung von Schutzmaßnahmen erfüllbar sind ([SGB V §308](#)). Zur Datenschutzkontrolle ist eine 3-jährige Protokollierung erforderlich.

Nach der Datenschutz-Grundverordnung ist für besondere Kategorien von Daten (hier: medizinische Daten) eine Datenschutz- Folgenabschätzung (DS-FA) zwingend. Diese hat der Gesetzgeber im Bundesanzeiger mit dem Gesetz verbindlich veröffentlicht.<sup>5</sup>

PS: Gesellschafter der Telematik (gematik GmbH) mit 51% = BRD durch das Bundesministerium für Gesundheit, 24,5% = Spitzenverband der Krankenkassen, 24,5% die Spitzenorganisationen der Leistungsträger im Gesundheitswesen (nach SGB V §306 Abs.1).

### 4. Die elektronische Patientenakte i. w. S. (ePA, [SGB V §334ff](#))

Nach Authentifizierung (2.) und sicher gestalteten, technischen Infrastruktur (3.), werden die Anwendungsmöglichkeiten aufgezeigt bzw. behandelt.

#### (a) **Anwendungsinhalte**

2. Erklärungen zu Organ- und Gewebespenden
3. Vorsorgevollmachten und Patientenverfügungen
4. Medikationspläne & Prüfungen der Arzneimitteltherapiesicherheit
5. Elektronische Notfalldaten (ausschließlich für die medizinische Notfallversorgung)
6. elektronische Verordnungen
7. & 1. die elektronische Patientenakte i. e. S. und ePatientenkurzakte

Vollständige, einheitliche Funktionsfähigkeit wohl ab 01.07.2023. Eine Erweiterung der Funktionen, z. B. zum Austausch von Befunden, Diagnosen, Therapieempfehlungen, Erklärungen, Formulare, Unterlagen u. ä. nach Freigabe von Anwendungen &/o Komponenten durch die gematik GmbH als Verantwortliche für die Infrastruktur. Verbot der Bevorzugung / Benachteiligung / Diskriminierung aus Nutzung, nicht Nutzung, Verweigerung von Zugriffen oder der Freigabe an Dritte.

#### (b) **Rechte des Versicherten / Patienten**

Nach Authentifizierung mit der Gesundheitskarte oder der eID mit geeignetem Endgerät, besteht die Berechtigung auf barrierefreien Zugriff, abhängig von der Speicherung (Offline = mit Karte/PIN bei einem Leistungserbringer, Online = verschlüsselt auf Krankassenportal). Eigene (nicht abrechnungserforderliche) Daten dürfen ausgelesen, übermittelt, bearbeitet, gelöscht und müssen

<sup>4</sup> Quelle: gematik GmbH: [Atlas zur Telematik – Infrastruktur PDF](#); [Informationspflichten der gematik GmbH PDF](#)

<sup>5</sup> Quelle: [Bundesgesetzblatt Nr. 28, 8.6.2021: Datenschutz – Folgenabschätzung \(DSFA\) zum PDSG, PDF ab Seite 42](#)



[Auf einen Blick \(Link zum PDF der KBV im Bild\)](#)



## Für den eiligen Leser kurz zusammengetragen (3/3)

für Leistungserbringer freigegeben werden. Diese müssen sich ebenfalls durch einen Heilberufs- und Berufsausweis für den Zugriff authentifizieren.

Nach einer Einwilligung durch den Versicherten/Patienten mittels eindeutiger, bestätigender Handlung zur Teil- oder Gesamtfreigabe ([SGB V §353](#)) dürfen ausschließlich in Medizin, Heil- und Pflegeberufen ausgebildete Fach- & Hilfskräfte, mit einem entsprechenden Ausweis, auf die Daten Zugriff nehmen. ([SGB V §252](#)).

### (c) Die elektronische Patientenakte i. e. S. (ePA, [SGB V §341ff](#))

Die ePA ist freiwillig und wird von der Krankenversicherung geführt und zur Verfügung gestellt. Ein Automatismus besteht nicht, deshalb muss die ePA bei der Krankenversicherung beantragt werden und diese ist seit 01.01.2021 dazu verpflichtet.

Zu den Anwendungsinhalten unter 4 (a) 2-6 können zusätzlich in der ePA eingestellt werden:

- ✓ (elektronische) Arztbriefe zur übergreifenden Versorgung und aus sonstigen Leistungserbringungen (z. B. Behandlungsprogramme bei chronischen Krankheiten)
- ✓ Untersuchungsergebnisse zu „Nachweisheften“ (Zahnärztliches Bonusheft, Kinder- und Schwangerschaftsvorsorgeuntersuchungen) sowie generelle Impfnachweise
- ✓ Leistungsdaten der Krankenversicherung, einschließlich Unterstützung und Datenübermittlung für bzw. an dritte Leistungserbringer (z. B. eigen-finanzierte Leistungen).
- ✓ Eigene Gesundheitsdaten sowie Daten aus digitalen Gesundheitsanwendungen
- ✓ Arbeitsunfähigkeitsbescheinigungen

Die Leistungserbringer (z. B. Arztpraxen, Krankenhäuser u.s.w.) haben zur Teilnahme und bis spätestens 30.06.2021 den Nachweise über die entsprechende Infrastruktur / Komponenten zu erbringen und sind verpflichtet, den Patienten im Kontext der Behandlung bei der Pflege in der ePA zu unterstützen ([SGB V §346](#)), sowie die Verpflichtung auf Übertragung in die ePA ([SGB V §347ff](#)).

## 5. Exkurs: Videosprechstunde ([SGB V §365ff](#))

Die Anforderungen an die Telematik - Infrastruktur für Videokonferenzen wird von der gematik GmbH (Gesellschaft für Telematik) im Benehmen mit der Kassenärztlichen Bundesvereinigung und dem Spitzenverband Bund der Krankenkassen festgelegt / genehmigt, wie auch die Authentifizierung. Die Empfehlung eines Videokonferenzsystem zur Patientensprechstunde, eingebunden in die Telematik – Infrastruktur, durch die gematik GmbH habe ich noch nicht finden können.

Die Kassenärztliche Bundesvereinigung KBV spricht auf ihrer Website „Videosprechstunde“<sup>6</sup> Empfehlung für Anbieter mit Zertifizierung durch die **datenschutz cert GmbH** aus<sup>7</sup> und gibt Handlungsempfehlungen bei Nutzung (z. B. Einwilligungs- und Informationspflichten u.ä.)

Bleibt noch die Frage nach der **Datenschutz – Folgenabschätzung** (DS-FA) nach [Art.35 DS-GVO](#), aufgrund besondere Kategorien von Daten nach [Art.9 DS-GVO](#). Hierzu verweist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf die Positivliste der Datenschutzkonferenz (DSK)<sup>8</sup>. **Nein, nur wenn** der Einsatz von *Telemedizin - Lösungen zur detaillierten Bearbeitung von Krankheitsdaten* erfolgt. Beispiel: *Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.*

### Bei Bedarf, einfach einmal sprechen!

*Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.*

6 Quelle: <https://www.kbv.de/html/videosprechstunde.php>

7 LINK: [https://www.kbv.de/media/sp/liste\\_zertifizierte-Videodienstanbieter.pdf](https://www.kbv.de/media/sp/liste_zertifizierte-Videodienstanbieter.pdf)

8 Quelle: *BfDI: DS-GF - Liste von Verarbeitungsvorgängen der DSK für den nicht-öffentlichen Bereich.*

