Leben mit der DSGVO und Erwartungen an die Umsetzung des E-Health-Gesetzes

Dominik Neumaier

Rechtsanwalt

kwm - Kanzlei für Wirtschaft und Medizin

Münster · Berlin

0251 - 5359939

030 - 2061433

www.kwm-rechtsanwaelte.de

Gliederung

I. Welche (neuen) Anforderungen gibt es?

II. Wie setze ich die Anforderungen um?

III. Ausblick auf das E-Health-Gesetz

Welche (neuen) Anforderungen gibt es?

Zusammengefasste Prinzipien der DS-GVO (Art. 5):

1. **Zweckbindung**
2. **Transparenz**
3. Datenminimierung
4. Richtigkeit
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit
7. **Rechenschaftspflicht**

Welche (neuen) Anforderungen gibt es?

Art. 5 Abs. 1 DSGVO: Enge **Zweckbindung!**

- Personenbezogene Daten dürfen nur für vorher festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden.
- Nutzungsänderung nur zulässig, wenn vom ursprünglichen Zweck umfasst, zB Rechnungslegung nach Behandlung

- Beispiel: Wissenschaftliche **Forschung** / Studien?
- Beispiel: **Factoring?**
- Beispiel: **Labor?**

Welche (neuen) Anforderungen gibt es?

Art. 12 DSGVO stellt hohe Anforderungen an **Transparenz**:

- **Informationspflichten**
- **„leicht zugängliche Form“**
- **„klare und einfache Sprache“**
- **Dokumentationspflichten**

Welche (neuen) Anforderungen gibt es?

Art. 5 Abs. 2 DSGVO: umfassende **Rechenschaftspflicht!**

Der Verantwortliche ist für die Einhaltung der Prinzipien der DSGVO verantwortlich und muss dessen Einhaltung nachweisen können.

→ Umkehr der Beweislast! Die Aufsichtsbehörde muss nicht mehr den Verstoß nachweisen. Der Verantwortliche muss die Erfüllung der Anforderungen nachweisen.

Welche (neuen) Anforderungen gibt es?

Umsetzung der Prinzipien durch:

- **„technisch organisatorische Maßnahmen (TOMs)**
- **Pflichtmethoden**

Welche (neuen) Anforderungen gibt es?

TOMs - Art. 32 DS-GVO:

*„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten.“*

Welche (neuen) Anforderungen gibt es?

Der nötige **Dreischritt** bei TOMs:

1. Risiken **identifizieren**

2. Nötige Maßnahmen **implementieren**

3. Alle Maßnahmen **dokumentieren**

Wie setze ich die Anforderungen um?

Pflichtmethoden

→ nicht direkt abhängig von eigener Risikoeinschätzung, sondern dann zu tun, wenn gesetzliche Voraussetzungen vorliegen

- **Bestellung eines Datenschutzbeauftragten**
- Datenschutz-Folgenabschätzung
- Datenschutzerklärung auf Homepage
- **Datenschutzerklärung an Patienten (Infoblatt)**
- Datenschutzerklärung an Angestellte (Infoblatt)
- Datenschutzverpflichtung der Angestellten
- **Erstellung eines Verarbeitungsverzeichnisses**
- **Nutzung von Auftrags(daten)verarbeitungsverträgen**

Gliederung

I. Welche (neuen) Anforderungen gibt es?

II. Wie setze ich die Anforderungen um?

III. Ausblick auf das E-Health-Gesetz

Wie setze ich die Anforderungen um?

TOMs - was folgt nun daraus?

Als „Grundschutz“ haben sich 8 Säulen etabliert:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Ihr IT-Beauftragter hilft!

Wie setze ich die Anforderungen um?

kwm

• Zutrittskontrolle	**= Türschloss Außentür, Fenstersicherungen**
• Zugangskontrolle	**= Türschlösser innen, Serverraum abgeschlossen, Standorte PCs**
• Zugriffskontrolle	**= Passworthygiene (sichere Passwörter, Wechsel), Firewall**
• Weitergabekontrolle	**= Verschlüsselung, auch von mobilen Geräten, keine USB-Sticks, sichere Entsorgung**
• Eingabekontrolle	**= Protokoll über Zugriffe, Löschungen, etc**
• Auftragskontrolle	**= Ordnungsgemäßer Abschluss v. ADV-Verträgen**
• Verfügbarkeitskontrolle	**= Backups, Notstromaggregate**
• Trennungsgebot	**= Ordnungsgemäße Karteiführung, Personal- und Patientendaten getrennt führen**

Braucht die Praxis einen DSB?

Datenschutzkonferenz, 26.04.2018:

„Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufs-unternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).“

Zusammenfassung:

- Arztpraxen mit **10 oder mehr Personen** müssen einen Datenschutzbeauftragten benennen.
- **Einzelärzte** mit weniger als 10 Personen können davon absehen, einen Datenschutzbeauftragten zu benennen.

Braucht die Praxis einen DSB?

kleine Mehrbehandlerpraxen (< 10 Personen)

hierzu die **Datenschutzkonferenz, 26.04.2018:**

> „Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.“

→ also auch hier **Entwarnung, falls nicht besonderes Risiko**, zB aufgrund der Verarbeitung genetischer Daten, besteht

Verband für Datenschutz in der Medizin

Datenschutzerklärung an Patient

Art. 13 DS-GVO:

„(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit: (…)

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung (…)“

→ **Jede Praxis muss allen Patienten künftig ein Datenschutz-Infoblatt aushändigen**

- Name und Kontaktdaten des/der Praxisinhaber
- Datenschutzbeauftragter der Praxis
- Zwecke und Rechtsgrundlagen der Datenverarbeitung
- Speicherung und Löschung der Daten
- Weitergabe von Daten an Dritte
- Rechte der Patienten zum Datenschutz
- Information über Landesdatenschutzbeauftragten

→ kann um Einwilligungen ergänzt werden; Infoblatt an sich ist aber nicht unterschriftsbedürftig

Das Verarbeitungsverzeichnis

Art. 30 DSGVO:

„Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (…);
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (…);
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1…“

→ **Jede Praxis muss künftig ein Verarbeitungsverzeichnis erstellen und führen**

Das Verarbeitungsverzeichnis

Verarbeitungsverzeichnis für Praxen nach Art. 30 DS-GVO

Praxis: [Bezeichnung der Praxis]

Aktueller Stand: xx.xx.2018

Inhaber: [Name und Adresse]

Datenschutzbeauftragte: [falls nötig/vorhanden]

Verarbeitungstätigkeit	Verantwortlicher	Zweck der Verarbeitung	Kategorien Betroffener	Kategorie von personenbezogenen Daten	Kategorien externer Empfänger	Löschfristen
Lohnabrechnung	[Name] Tel.: Mail:	- Auszahlung der Gehälter - Abgabe Steuern und Sozialabgaben	Angestellte	- Name, Geburtsdatum, Adresse, Bankverbindungsdaten - Entgeltdaten - ggf. Religionszugehörigkeit, Sozialversicherungsdaten, Steuerdaten, Berufsgenossenschaftsangaben	- Finanzamt - Steuerberater	10 Jahre (gesetzliche Aufbewahrungsfrist)
Personalaktenführung	[Name] Tel.: Mail:	Verwaltung der Arbeitnehmer	Angestellte	Personalaktendaten, die in den Personalunterlagen enthalten sind, z.B. Zeugnisse, Stammdaten (vgl. Lohnabrechnung), diagnosefreie Arbeitsunfähigkeitsbescheinigungen	Grundsätzlich keine; nach gesonderter Einwilligung eventuell nachfolgende Arbeitgeber	3 Jahre, beginnend mit dem Ende des Kalenderjahres, indem das Beschäftigungsverhältnis beendet wurde
Arbeitszeiterfassung	[Name] Tel.: Mail:	Erfassung der Arbeitszeit und Pflege der Zeitkonten der Arbeitnehmer	Angestellte	- Name - Arbeitszeiten	Keine	Unverzüglich nach Auswertung des Zeitkontos. Zwei Jahre bei Überschreitung des Zeitkontos

Kommentar [A1]: Bitte kontinuierlich pflegen und sodann stets ein neues Datum eintragen.

Kommentar [A3]: Hier sollten jeweils der oder die Hauptverantwortlichen in der Praxis für den jeweiligen Verarbeitungsvorgang benannt werden.

Es kann sich hierbei auch um einen qualifizierten Mitarbeiter handeln.

Kommentar [A2]: Es handelt sich bei den im Folgenden aufgeführten Verarbeitungstätigkeiten um typische Beispiele. Diese können und sollten Sie für Ihre Praxis individualisieren.

Ergänzend sind zum Beispiel darüber hinaus denkbar Newsletterversand, sonstige Werbeaktionen, regelmäßige Studien, etc.

Auftrags(daten)verarbeitung

→ man verarbeitet die Daten nicht selber, sondern bedient sich hierzu **externer Dritter**, die dies **nach Weisung** des Praxisinhabers als Verantwortlichem übernehmen

→ zur Sicherstellung der datenschutzrechtlichen Vorgaben braucht es hierzu eines **AV-Vertrags** nach Art. 28 Abs. 3 DSGVO:

→ **Jede Praxis muss mit Auftragsverarbeitern ergänzende Verträge schließen**

Beispiele:

ADV: IT-(Fern)-Wartung, PVS ohne Factoring, Daten in der Cloud, Lohnbüro, Datenentsorgung durch Dienstleister, Terminvergabe-Tools, Online-Kontakt-Formular

Keine ADV: Labor, PVS mit Factoring, Telekommunikationsdienstleister (Post, E-Mail-Provider, etc.), Insolvenzverwalter, Rechtsanwälte

Auftrags(daten)verarbeitung

Braucht es bei einer Auftrags(daten)verarbeitung einer Einwilligung des Patienten?

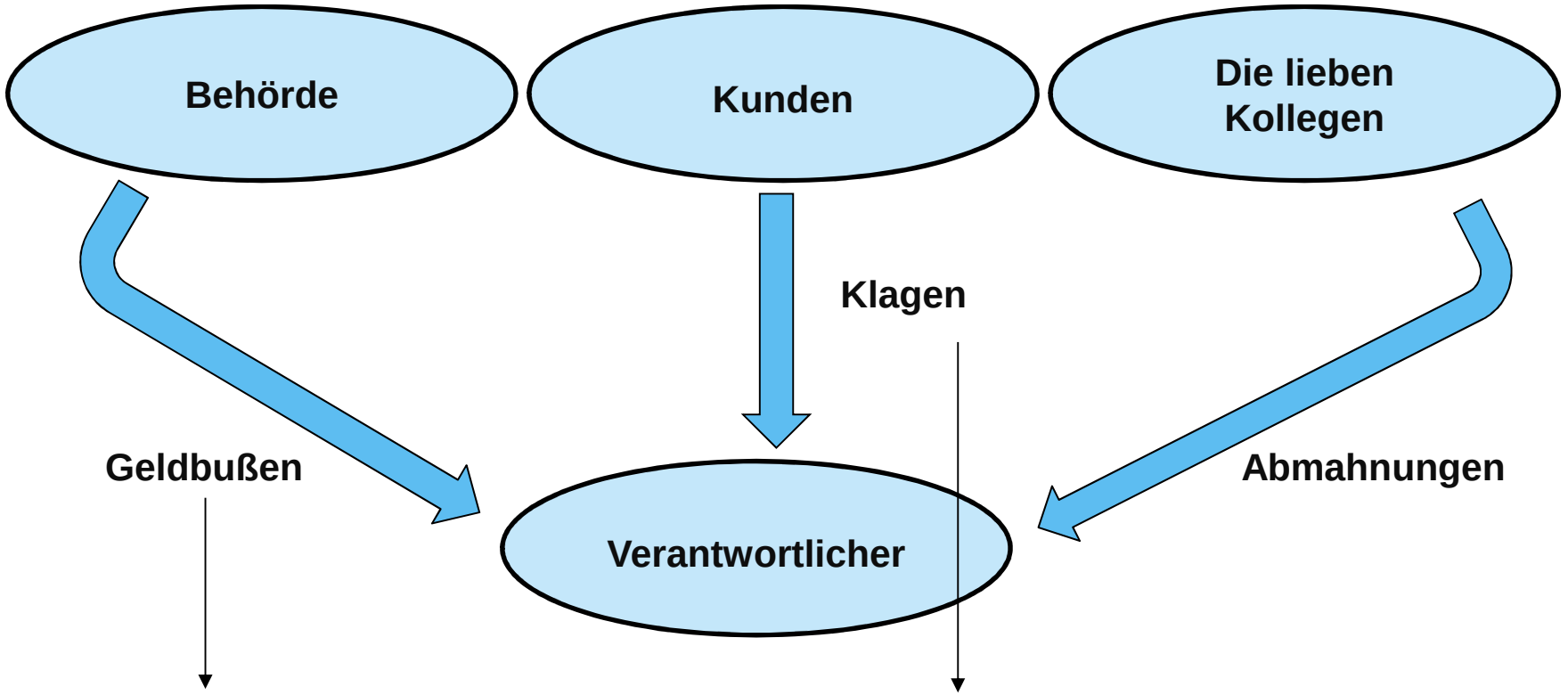
→ Datenschutzkonferenz:

„Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es regelmäßig keiner weiteren Rechtsgrundlage im Sinne von Art. 6 bis 10 DS-GVO als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt.“

→ Also laut Datenschutzkonferenz: Nein! Es bestünde insoweit eine Privilegierung.

Dimensionen eines Verstoßes

Konsequenzen von Datenschutzverstößen – 3 Dimensionen:



Gliederung

I. Welche (neuen) Anforderungen gibt es?

II. Wie setze ich die Anforderungen um?

III. Ausblick auf das E-Health-Gesetz

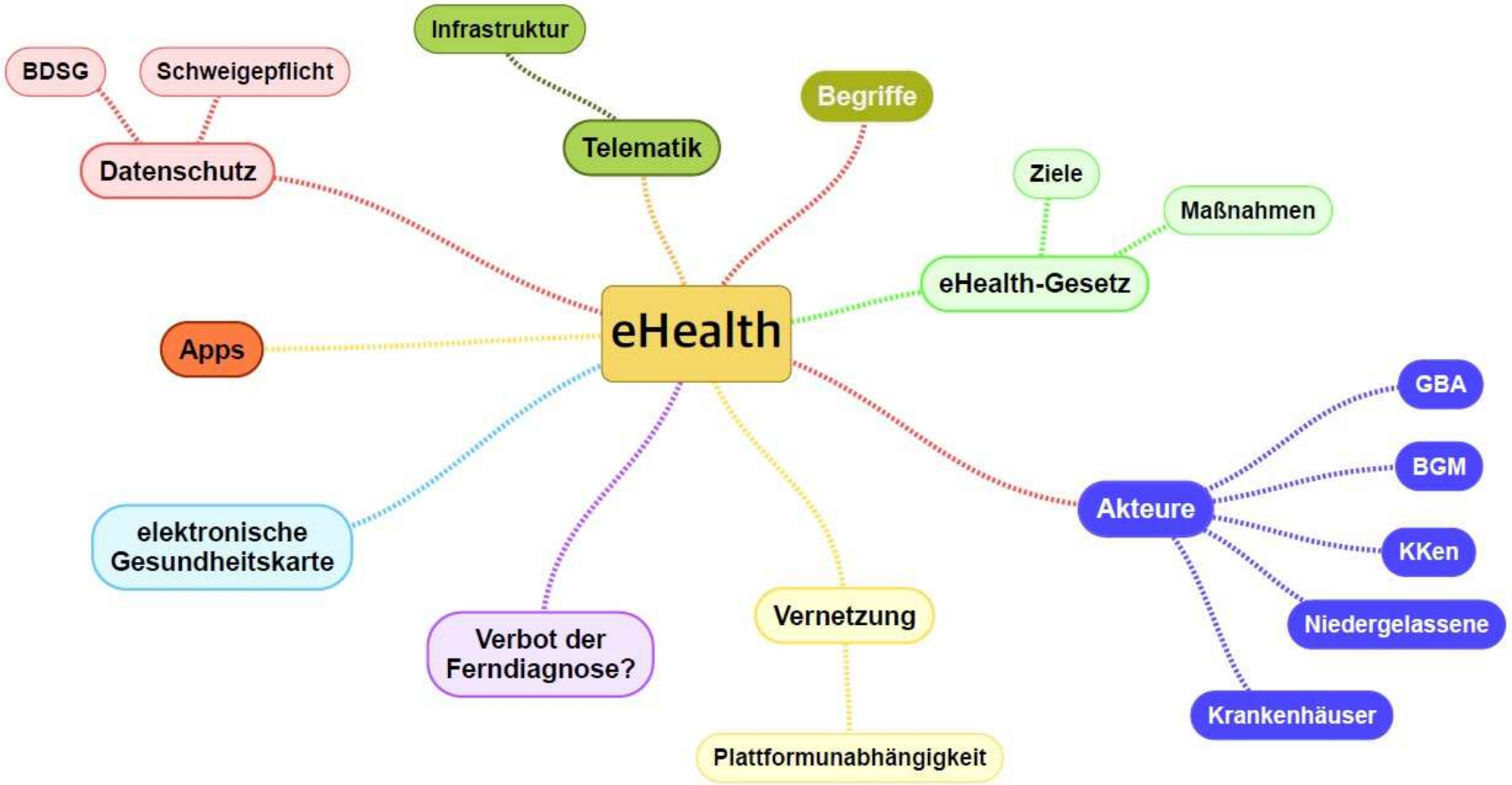
Orientierung

- **eHealth** ist Stichwort und Sammelbegriff für Vernetzung im Gesundheitswesen
- Begriff ist mitunter wenig trennscharf aber sehr eingängig

- **eHealth-Gesetz** soll diverse Aspekte der Digitalisierung im Gesundheitswesen für gesetzlich Krankenversicherte regeln

- Thema ist **komplex**, da Technik, Medizin, verschiedene Sektoren und Akteure, juristische Aspekte wie Datensicherheit und Datenhoheit als auch Fragen der bundesweiten Vereinheitlichung ineinander greifen

Digitalisierung nimmt zu!



E-Health-Gesetz: Überblick

- Telematikinfrastruktur
- Medikationsplan
- elektronischer Arztbrief
- Telemedizin
- Versichertenstammdaten
- Notfalldatenmanagement
- elektronische Patientenakte

Telematikinfrastruktur

- Datenautobahn des GKV-Gesundheitswesens
- weltweit größtes IT-Projekt (70 Mio. Menschen in einem Netz)
- Vernetzung von Ärzten, Zahnärzten, Krankenhäusern, Apotheken, KVen, Krankenkassen und Patienten

→ für **Patienten** ist die elektronische Gesundheitskarte (eGK) der persönliche Schlüssel zur TI

- eGK ist Mikroprozessorkarte
- speichert Daten und schützt diese vor unbefugtem Zugriff
- der Versicherte entscheidet, wem er Zugriff gewährt

Telematikinfrastruktur

→ **Praxen** benötigen

- ein Zugangsgerät zur TI, den sog. **Konnektor** (VPN-Router zur TI)
- **Kartenterminals** für die eGK der Patienten
- **Praxisausweis** (ähnelt einer SIM-Karte für den Konnektor)
- zuletzt ist das **Praxisverwaltungssystem anzupassen**, um eine Verbindung zur TI zu ermöglichen

! mittels des **elektronischen Heilberufsausweis kann** ein Zugriff auf die vom Patienten freigegebenen Daten erfolgen;
ist ebenso wie die eGK eine Mikroprozessorkarte

! daneben existiert das **Sichere Netz der KVen** (SNK), das man über die TI auch erreichen kann, aber nicht mit dieser identisch ist

→ ist derzeit das größte Netz zur Online-Kommunikation für Ärzte

Fernbehandlungsvebot?

- 121. Deutschen Ärztetag in Erfurt hebt bisheriges strenges Fernbehandlungsverbot auf
- der geänderte § 7 Absatz 4 der (Muster-)Berufsordnung lautet:

„Ärztinnen und Ärzte beraten und behandeln Patientinnen und Patienten im persönlichen Kontakt.

Sie können dabei Kommunikationsmedien unterstützend einsetzen.

*Eine **ausschließliche** Beratung oder Behandlung über Kommunikationsmedien ist im Einzelfall erlaubt, **wenn** dies ärztlich vertretbar ist und die erforderliche ärztliche Sorgfalt insbesondere durch die Art und Weise der Befunderhebung, Beratung, Behandlung sowie Dokumentation gewahrt wird und die Patientin oder der Patient auch über die Besonderheiten der ausschließlichen Beratung und Behandlung über Kommunikationsmedien aufgeklärt wird.“*

elektronische Patientenakte

Start ~~**ab 2019**~~ geplant: sektorenübergreifende elektronische Patientenakte

sektor- und fallübergreifende Zusammenführung bereits vorhandener Informationen von gesetzlich Krankenversicherten

- Anamnese
- Behandlungsdaten
- Medikamente
- Allergien
- weitere Gesundheitsdaten

→ Ärzte, Zahnärzte, Apotheken, etc. sollen hierauf ohne Zeitverlust zugreifen können, zB per elektronischem Heilberufsausweis

elektronische Patientenakte

- Patient soll selbst über den Umfang und die Dauer der Speicherung entscheiden
- behält alleinige Verfügungsgewalt über seine Akte

Umfrage März 2017: **60%** der Patienten würden die ePA nutzen

Patient erhält daneben ein **Patientenfach**

→so kann er selbst Daten abspeichern und einsehen

zentrales Problem: Umsetzung → viele Modelle, Akteure und Systeme

BMG: angestrebter Zeitplan ist nicht zu halten

neues Ziel laut TSVG: **01.01.2021**

… und jetzt?!?

Fazit und Hausaufgaben

Der neue Datenschutz: Zusammenfassendes Fazit

- Ruhe bewahren! Aber Handeln!
- Setzen Sie die TOMs soweit wie möglich um. Ihr IT-Beauftragter hilft.
- Setzen Sie die Pflichtmethoden um, soweit für Sie nötig.
- Der Umsetzungsaufwand ist nur am Anfang hoch!
- Nutzen Sie, falls vorhanden, Leitlinien von Verbänden, Kammern, etc.

- Holen Sie sich ggf. externe Hilfe:

  kwm-Datenschutzpaket / VDM-Mitgliedschaft

➡ Die Digitalisierung kommt! **Mitgestaltung statt Resignation!**

➡ Telefonische **Erstberatung** zu Datenschutz und Digitalisierung ist für Sie als heutige Teilnehmer **kostenlos**. Rufen Sie gerne an!

Vielen Dank für Ihre Aufmerksamkeit!

Offenlegung finanzieller Interessen

Offenlegung finanzieller Interessen des Autors, für den o. g. Vortrag

☐	P- Produkt:	Finanzielles Interesse bei der Ausrüstung, dem beschriebenen Verfahren und/oder dem beschriebenen Produkt (z. B. Forschungsunterstützungen, **Referentenhonorare**, Reisekostenunterstützungen, Stipendien etc.)
☐	I – Investor:	Finanzielles Interesse an Firmen, die eine beschriebene Ausrüstung, ein Verfahren oder Produkte liefern (z. B. Aktienbesitz, Anteilseigner etc.)
☐	B - Berater:	Kommerzielle Vergütung oder Unterstützung des Autors in den letzten drei Jahren in Form von Beratungsverträgen (Mitgliedschaft in Gremien, Beiräten, Aufsichtsräten etc.)
X	K - Keine:	Keine Interessenskonflikte; keine kommerzielle Unterstützung der vorgelegten Arbeit in irgendeiner Form