Folie 1

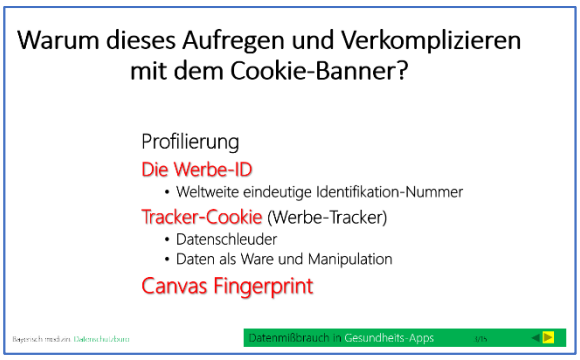
Folie 2

Agenda:

*** Unsere Agenda heute:**

- Auf Grund des EuGH-Urteils Oktober 2019 müssen Cookie-Banner völlig neu konzipiert werden. Hierbei wird noch viel verkehrt gemacht und deshalb Bußgeld riskiert. Und auch beim Newsletter gibt es Tücken. Daher das Thema heute, wie dies richtig rechtskonform gestaltet werden muss.
- Das PVS-System, das den Arzt sehr umfangreich mit Umsatz-Optimierungs-Algorithmen unterstützt, kann aber auch in der Umsatz-Minderung durch Bußgeldvermeidung bei einer falschen Abwicklung von DSGVO-Patientenrechte seinen Beitrag leisten. Wie, möchte ich heute darstellen.
- Aufgrund eines aktuellen Falles möchte ein gravierendes Problem bei Praxis Ende, oder Übergabe mit PVS-Systemen aufzeigen.
- Als 4. Thema, das immer aktueller zu werden scheint ist, die Datensicherung oder das ganze Arzt-Programm in der Cloud. Worauf man achten muss in diesem Beitrag
- Zu Letzt die DIGA, das sind Digitale Applikationen, die jetzt Schwung aufnehmen, nicht nur wegen der Corona-App, sondern weil sie wie Medikamente auf den Markt kommen.

Folie3



Warum dieses Aufregen und Verkomplizieren mit dem Cookie-Banner?

Dem liegt zu Grunde, dass Daten in unvorstellbaren Mengen aus dem Besuch einer Internet-Seite gewonnen werden können, frei nach dem Motto, „Sag mir, welche Website du besuchst und ich sag dir wer du bist“.

Wie kommt das? „…ich habe nichts zu verbergen, ich gebe auch keine Daten ein…“ erzeugt aber eine ungehemmte Weitergabe von Daten.

Aber aus jedem Internetkontakt wird ein spezifisches Benutzer-Profil erstellt. Je öfter desto granularer, z.B. durch:

- Wie oft wird die Webseite besucht, von welcher Seite kommt er, zu welcher wechselt er, zu welcher Zeit, in welchen Perioden -> Interessen-Profilierung

- Wie intensiv beschäftigt man sich mit dem Inhalt -> Lebens-Prioritäten
- Woher kommt der Nutzer geografisch -> Bewegungsprofil
- Welche IT-Technik wird verwendet -> Aufgeschlossenheit gegenüber Neuerungen
- Wurde „gelikt“ -> soziales Engagement

Fazit: Daraus werden Rückschlüsse gezogen, über politischen Affinitäten, Charakter, Ängste, Alter, Geschlecht, Konfession, Ethnie, Beruf, besondere Vorlieben, usw.

Wie wird der Benutzer im Internet jedes Mal identifiziert?

Das passiert über die Werbe-ID.
Sie ist die Erkennungsnummer, die bei jeder Internet-Berührung mitgesendet wie eine Anmeldung. Sie ist für jedes Gerät einzigartig. Sie ist in jedem PC, in jedem Smart-Phone im Betriebssystem verankert. Nicht zu verwechseln mit der IP-Adresse (Internet-Punkt-Adresse), die typischer Weise vom Provider in bestimmten Abständen dem Benutzer zugewiesen wird. Diese Nummer ist nur dem Provider bekannt. Die Werbe-ID kann in jedem Gerät zurückgesetzt oder abgeschalten werden. Sie ist in den Datenschutzeinstellungen zu finden. Über Google findet man zu seinem Gerät mehr darüber, bzw. die passende Anleitung.

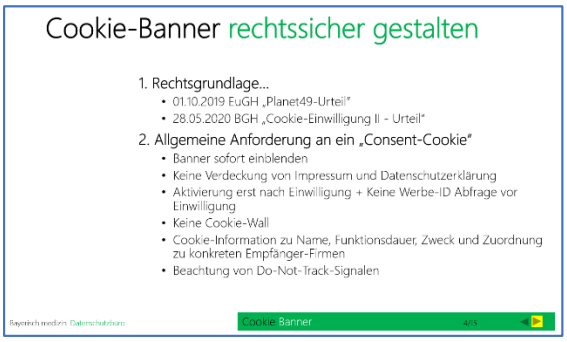
Wer ist der Verräter?

Das sind die Tracker-Cookies. Sie sind die Agenten, die die Daten an die meistbietenden weiterreichen. Es sind kleine Programme, die in die Webseite vom Programmierer eingebaut werden. Sie haben nichts mit dem Seitenaufbau zu tun, sondern dienen alleine der Übersendung der Werbe-ID mit den aktuellen Clicks und URLs. Marketing-Firmen, bezahlen für diese Datensätze viel Geld und machten den Erfinder Google damit zum Milliarden-Unternehmen.
Seit Juli 2019 hat der EUGH und seit Mai 2020 der BGH per Urteil, dem einen Riegel vorgeschoben, um damit den Benutzer vor Ausspähung zu schützen insoweit, dass für jedes **einzelne** Tracker-Cookie, **vor Aktivierung** des Cookies, vom Anwender seine Einwilligung eingeholt und **umfassend** über den Zweck des Cookies informiert werden muss.
Die Industrie argumentiert damit, dass dem Benutzer angeblich eine individuellere Werbung oder Benachrichtigung angeboten werden soll. Ganz nebenbei entstehen aber dadurch sehr genaue Persönlichkeits-Profile von beträchtlichem und monetären Wert für Industrie und Politik mancher Staaten.
Diese Einschränkungen zum Cookie-Banner, die nun sehr viel Zeit des Anwenders zu Einwilligungs-Prozess abverlangt, führt meist mit dazu, dass das mit einer gänzlichen Ablehnung quittiert wird. Das ist natürlich nicht im Sinne von der Industrie.

Der nächste Trick, die Canvas Fingerprint Technologie: (Canvas engl. Leinwand)

Diese neue Technologie ersetzt in Zukunft die herkömmlich Werbe-Tracker-Technik und ist zurzeit nicht blockierbar. Bei dieser Technik ist es nicht nötig einen „Agenten“ auf der Webseite einzuschleusen. Sondern der Benutzer wird jetzt aus der Ferne fotografiert und das als Erkennungs-Merkmal verwendet und Clicks und URLs damit verknüpft.
Das „Erkennungsfoto“ ist die Summe aller Hardware und Software-Daten des PCs oder Smartphones des Anwenders, das tatsächlich zu einer einzigartigen Bild (Image) konvertiert wird.
Aber mit Hilfe der Browser-Erweiterung „Canvas-Fingerprint-Defender“ werden bei jedem Kontakt andere, falsche, technische Daten zurück übermittelt. Dadurch entsteht jedes Mal eine andere Webe-ID und kann nicht für eine sinnvolle Profilierung verwendet werden. Auch diese Technik ist ohne Einwilligung rechtswidrig.

Folie 4



Cookie-Banner rechtssicher gestalten

1. Rechts-Grundlage:

- EuGH: 01.10.2019 Urteil C-673/17 „Planet49"
- BGH: 28.05.2020 Urteil I ZR 7/16 „Cookie Einwilligung II"

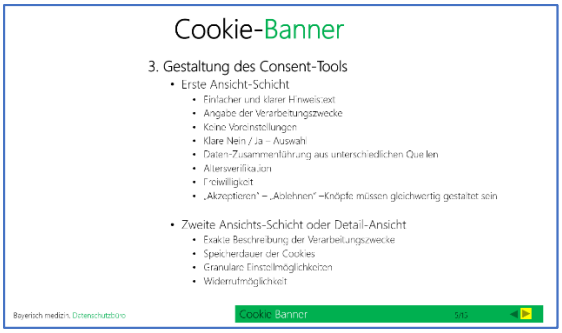
Die Urteile gehen gegen solche Cookies vor, die das Surfverhalten der Nutzer analysieren und protokollieren und mit der Werbe-ID des Benutzers an unbekannte Dritte rücklinks weitergeben.
Beispiel: Google Analytics, - Maps, - Fonts, Werbetracker, Soziale-Dienste wie Facebook, Twitter usw.,

Nicht gemeint sind Cookies, die zwingend zum Seitenaufbau notwendig sind, oder Fonts, wenn sie lokal zur Verfügung gestellt werden oder, Verhaltensanalyse mit eigenen lokalen Programmen und ohne Verwendung externer Dienste. In diesen Fällen können Cookie-Banner in Gänze entfallen.
Kern-Aussage der Urteile: Sobald Daten an Dritte übermittelt werden, ist grundsätzlich eine Einwilligung notwendig. Dadurch ist eine neue Art von Einwilligungs-Banner nötig (Consent-Banner, consent engl. Zustimmung).

2. Allgemeine Anforderungen an Consent-Banner

- Einblendung des Consent-Banners sofort bei Besuch der Startseite oder jeder anderen Unterseite bzw. beim Start einer App (§ 5 TMG, § 305 Abs. 2, § 312i, 312j BGB; Art. 12 Abs. 1 DSGVO)
- Das Consent-Banners darf die gesetzlichen Pflichtinformationen nicht Überdecken, wie Impressum, AGBs oder Datenschutzhinweise (§ 5 TMG, § 305 Abs. 2, § 312i, 312j BGB; Art. 12 Abs. 1 DSGVO) Das Consent-Banner darf nicht in den AGBs eingebettet sein (Art. 7 Abs. 2, Art. 7 Abs. 4 DSGVO)
- Tracker-Cookies oder Werbe-IDs dürfen erst aktiviert werden, wenn die Zustimmung des Nutzers aktiv erfolgt ist. Eine Zustimmung durch passive Verhaltensweisen wie z.B. durch Navigieren auf der Website, automatisiertes Schließen nach einer Zeitspanne oder Wegklicken des Consent-Banners ist nicht zulässig (Erwägungsgrund 32 DSGVO, vgl. auch EuGH, Urt. v. 1.10.2019 – C-673/17 – „Planet49").
- Der Besuch der Website/App muss auch möglich sein, wenn der Nutzer Cookies oder Werbe-IDs etc. ablehnt, also keine Cookie-Wall errichten, der Zugang zu einer Website/App darf nicht von einer Einwilligung abhängig gemacht werden. (Art. 7 Abs. 4 DSGVO, Erwägungsgrund 42, 43 DSGVO, laut Aufsichtsbehörden: DSK, CNIL, ICO, Dutch DPA)
- Die Beschreibung der einwilligungspflichtigen Cookies, die auf der Webseite verwendet werden, wie Name, Funktionsdauer, Zweck und Zuordnung zu konkreten Empfänger-Firmen muss beschrieben werden. (Art. 4 Nr. 11 DSGVO „informierte Einwilligung", vgl. EuGH, Urt. v. 1.10.2019 – C-673/17 – „Planet49"; ebenso Aufsichtsbehörden: DSK, CNIL, ICO)
- Der Beachtung von Do-Not-Track-Signalen vom Browser der Nutzer, ggf. die Blockierung von Drittanbietern, muss nachgekommen werden. (Art. 21 Abs. 5 DSGVO)

Folie 5



3. Gestaltung des Consent-Tools

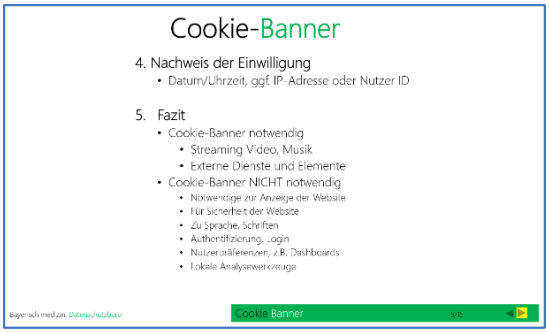
Erste Ansicht / 1st Layer

- Er beinhaltet einen Hinweistext in einfacher, klarer und verständlicher Sprache, dass u.a. · Endgeräteinformationen z.B. IP-Adresse, Browserinformationen und · personenbezogene Daten durch Tracking-Technologien und · Cookies verarbeitet werden (Art der Daten, Art. 4 Nr. 11 DSGVO).
- Es müssen hinreichende bestimmte Angaben zu den Verarbeitungszwecken gegeben werden, wie Analyse, Reichweitenmessung, verhaltens- und standortbezogene Werbung, Anzeige von Diensten Dritter wie z.B. Videocontent oder Maps, oder E-Mail-Marketing, etc. (eigene Festlegung der Zwecke oder Zwecke nach IAB TCF v2; Art. 4 Nr. 11, 5 Abs. 1 lit. b, 6 Abs. 1 lit. a DSGVO).
- Es dürfen keine Voreinstellungen wie bereits aktivierte Häkchen oder Schaltflächen gemacht werden (EuGH, Urt. v. 1.10.2019 – C-673/17 – „Planet49", ErwGr. 32 DSGVO).
- Es muss ein klares Ja oder Nein-Auswahl für den Nutzer ersichtlich sein (ErwGr. 42, 43 DSGVO, so z.B. ICO).
- Es muss der Hinweis gegeben werden, dass Dritte ebenfalls Cookies auf Endgeräten platzieren und Nutzerdaten verarbeiten (Art. 4 Nr. 11 DSGVO) oder, ob Daten aus unterschiedlichen Quellen zusammengeführt werden (Art. 7 Abs. 4 DSGVO, ErwGr. 42, 43 DSGVO).
- Eine Altersverifikation bei Angeboten, die sich direkt an unter 16jährige richten muss vorhanden sein (Art. 8 Abs. 2 DSGVO).
- Es muss der Hinweis gegeben werden, dass die Einwilligungen freiwillig erteilt werden, nicht für die Nutzung der Website/App erforderlich sind und jederzeit widerrufen werden können (Art. 7 Abs. 3, Abs. 4 DSGVO).
- Die Aufsichtsbehörde Baden-Württemberg empfiehlt zur Gestaltung der 3 Zustimmungs-Knöpfe:
  1. Knopf, „Alle Anbieter akzeptieren",
  2. Knopf, „Alle Anbieter ablehnen", wobei die ersten beiden Knöpfe gleichwertig gestaltet sein müssen und
  3. Knopf, „Erweiterte Einstellungen" wobei dieser Button nicht gleichwertig gestaltet sein muss.

Zweite Ansicht oder Detailansicht oder „Erweiterte Einstellungen" / 2nd Layer

- Es müssen alle Drittanbieter die Empfänger der Daten sind, mit Unternehmensbezeichnung und Anschrift genannt werden (Art. 4 Nr. 11 DSGVO, Art. 13 Abs. 1 DSGVO). Nur die Nennung der Cookie-Domain z.B. ist nicht ausreichend (EuGH, Urt. v. 1.10.2019 – C-673/17 – „Planet49" Angabe der Empfänger erforderlich).
- Die Speicherdauer der Cookies muss angegeben werden, ggf. auch Beispielwert, Name, Ablaufdatum und Empfängername (EuGH, Urt. v. 1.10.2019 – C-673/17 – „Planet49").
- Die Einstellmöglichkeiten, aktivieren oder deaktivieren, müssen mit separaten, unterschiedlichen, granularen Optionen ausgestattet werden, um das Einverständnis für verschiedene Zwecke und Arten der Verarbeitung gesondert erteilen zu können (ErwGr. 42, 43 DSGVO). Jeder einzelnen Drittanbieter sollte so einstellbar sein (Art. 7 Abs. 4, ErwGr. 42, 43 DSGVO).
- Abschließend muss die Möglichkeit des jederzeitigen Widerrufs gegeben werden, ohne Angaben von Gründen, z.B. per Button „alle deaktivieren" (Art. 7 Abs. 3 S. 4 DSGVO).

Folie 6



4. Dokumentation/Nachweis der Einwilligung

- Die Dokumentation zum Nachweis der Einwilligung können Dienstleister-Tools erledigen, wie z.B. das Tool „ConsentManager.de.“
  Dieses protokolliert automatisch, wann zu welchem Datum/Uhrzeit, welche IP-Adresse oder Nutzer ID und wie die Einwilligung erteilt wurde (Art. 7 Abs. 1 DSGVO).

5. Zusammenfassung, wann notwendig wann nicht

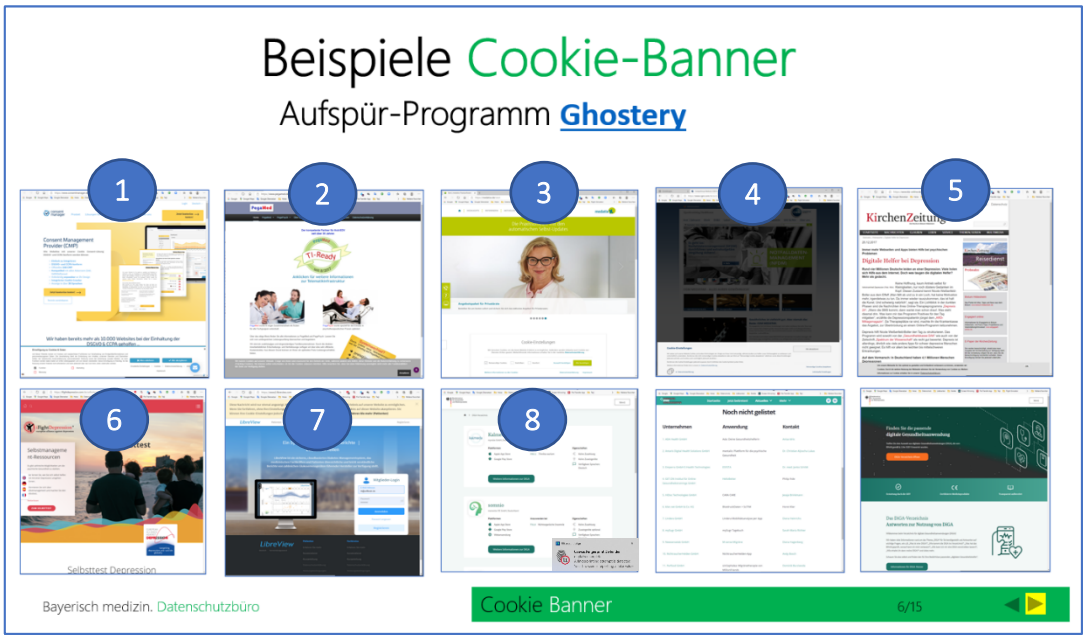
Notwendigkeit eines Einwilligungs-Banners ist dann, wenn

- Einbindung von Streaming Content (z.B. Video/Musik), der bei Dritten gehostet wird (laut ICO)
- Einbindung sonstiger externer Dienste und Elemente Dritter z.B.:
  - Kartendienste (laut LfDI BaWü)
  - Statistische Analyse und Reichweitenmessung
  - Verhaltensbezogene/ standortbezogene Werbung
  - Sozial Plugins
  - Externe Fonts

Keine Notwendigkeit einer Einwilligung und damit KEIN Cookie-Banner.
(Art. 5 Abs. 3 S. 2 RL 2002/58/EG (ePrivacy-RL) bzw. nach Art. 6 Abs. 1 S. 1 lit. f)

- Clientseitige Endgeräteinformationen (z.B. IP-Adressen, Bildschirmauflösung, Betriebssystem) für IT-Security-Maßnahmen, Sicherheit der Website/App
- Technisch notwendige Cookies für Einstellungen zur Sprache und zu Schriften, Cookie- Einstellungen, etc.
- Technisch notwendige Cookies für Nutzer-Authentifizierung beim Log-In (Session-Cookies) sowie für Nutzereinstellungen (Session-Cookies)
- Technisch notwendige Cookies für Warenkorb-Funktion (Session-Cookies) oder Bereitstellung von Online-Formularen (Session-Cookies)
- Speicherung von Nutzerpräferenzen, wenn der Nutzer dies ausdrücklich wünscht (laut ICO), z.B. Dashboards
- Einbindung von Diensten zur Verbesserung der Darstellung und Optimierung der Website (z.B. Auslieferung von Content mittels CDN, Web Fonts, etc., Verkürzung von Ladezeiten, laut ICO)
- ggf. für Firstparty-Logfile-Analyse oder lokal implementierte (on premises) Analysewerkzeuge (laut deutscher Aufsichtsbehörden, neue Stellungnahme hierzu angekündigt)
- Analyse Programm „Matomo“ bei lokaler Installation von „Matomo On-Premise“ (kostenlos)

Folie 7



(1) Consent Management Provider (CMP)Consent Manager Deutschland
Korrekter Cookie-Banner, Consent-Banner Musterbeispiel.

(2) PegaMed - das Praxisprogramm für clevere Ärzte"> PegaMed - das Praxisprogramm für clevere Ärzte
Rechtskonform: Aber Cookie-Banner nicht nötig. Es werden keine Dritt-Anbieter Dienste oder Elemente verwendet.

(3) Start | medatixx Praxissoftware
Kritik würdig. Knöpfe „Auswahl bestätigen“ und „Alle bestätigen“ werden nicht gleichwertig dargestellt.

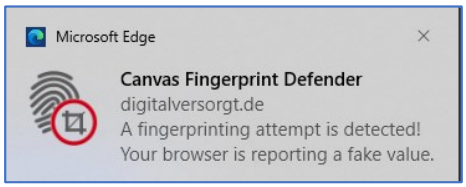
(4) CompuGroup Medical | CGM MEDISTAR - einfach Arzt sein!
Rechtswidrig: Gesetzlich vorgeschriebener Zugriff auf Impressum wird durch Cookie-Banner überdeckt. Knöpfe „Alle akzeptieren“ und „Notwendige Cookies akzeptieren“ werden nicht gleichwertig dargestellt.

(5) Digitale Helfer bei Depression | KirchenZeitung (kiz-online.de)
Rechtswidrig. Drittanbieter-Werbetracker wird sofort gestartet ohne Einwilligung.

(6) Selbsttest - iFightDepression [DE]
Hochgradig rechtswidrig: Komplett fehlender Cookie-Banner, trotz Werbetracker, und Übertragung von Gesundheitsdaten.

(7) LibreView
Hochgradig rechtwidrig: Falscher Cookie-Banner, Werbetracker werden gestartet ohne Einwilligung, selbst bei Übertragung von Patienten-Diabetes-Daten. Daten-Übertragung in die USA ohne Rechtsgrundlage.

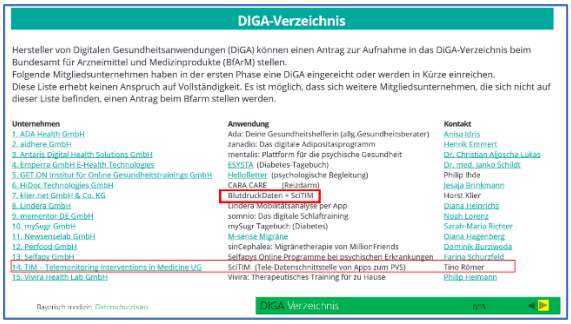
(8) DiGA-Verzeichnis - Spitzenverband Digitale Gesundheitsversorgung e.V. (digitalversorgt.de)
Rechtswidrig. Verwendung von Canvas-Technik. Diese Technik erzeugt aus der Rückantwort der technischen Daten von Browser und Computer einen Fingerabdruck und benutzt diese als Identifikations-Marker bei der Wiedererkennung. Die Daten werden damit an Dritte gesendet.



Canvas Fingerprint Technologie:
Diese neue Technologie ersetzt in Zukunft die herkömmlich Werbe-Tracker-Technik und ist zurzeit nicht blockierbar. Aber mit Hilfe der Browser-Erweiterung „Canvas-Fingerprint-Defender“ werden bei jedem Kontakt andere, falsche, technische Daten zurück übermittelt. Dadurch

entsteht jedes Mal eine andere Webe-ID und kann nicht für eine sinnvolle Profilierung verwendet werden. Auch diese Technik ist ohne Einwilligung rechtswidrig.

Folie 8



DIGA (digitale Gesundheitsanwendung)

Digitale Gesundheitsanwendungen eröffnen vielfältige Möglichkeiten, um bei der Erkennung und Behandlung von Krankheiten sowie auf dem Weg zu einer selbstbestimmten gesundheitsförderlichen Lebensführung zu unterstützen. DiGA sind damit „digitale Helfer“ in der Hand der Patienten.
Eine DiGA ist ein CE-gekennzeichnetes Medizinprodukt, das folgende Eigenschaften hat:

- Medizinprodukt der Risikoklasse I oder IIa nach MDR oder, im Rahmen der Übergangsvorschriften, nach MDD (Hinweise zur Frage „wann ist eine App ein Medizinprodukt?“).
- Die Hauptfunktion der DiGA beruht auf digitalen Technologien.
- Der medizinische Zweck wird wesentlich durch die digitale Hauptfunktion erreicht.
- Die DiGA unterstützt die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen.
- Die DiGA wird vom Patienten oder von Leistungserbringer und Patient gemeinsam genutzt.

Die Anforderungen sind in § 33a Fünftes Buch Sozialgesetzbuch (SGB V) definiert.

Rechtliche Grundlagen:

Digitale-Versorgung-Gesetz (DVG) und Digitale Gesundheitsanwendungen-Verordnung (DiGAV).
Mit dem Inkrafttreten des Digitale-Versorgung-Gesetzes (DVG) am 19. Dezember 2019 wurde die „App auf Rezept“ für Patientinnen und Patienten in die Gesundheitsversorgung eingeführt (§§ 33a und 139e Fünftes Buch Sozialgesetzbuch). Damit haben ca. 73 Millionen Versicherte in der gesetzlichen Krankenversicherung einen Anspruch auf eine Versorgung mit DiGA, die von Ärzten und Psychotherapeuten verordnet werden können und durch die Krankenkasse erstattet werden.
Voraussetzung hierfür ist, dass die DiGA ein Prüfverfahren beim BfArM erfolgreich durchlaufen haben und in einem neu zu schaffendem Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen (DiGA-Verzeichnis) gelistet sind. In diesem Verzeichnis werden für Ärzte, Psychotherapeuten und Nutzer wesentliche Informationen zur DiGA zusammenfassend dargestellt. Dies sorgt für umfangreiche Transparenz, damit gut informierte Entscheidungen getroffen werden können und eine vertrauensvolle Nutzung möglich wird.
Details zu diesem Verfahren regelt eine ergänzende Rechtsverordnung des Bundesministeriums für Gesundheit (BMG), die Digitale Gesundheitsanwendungen-Verordnung (DiGAV).

Bereitstellung und verordnungsrelevante Daten

Wesentliches identifizierendes Merkmal einer DiGA für die Verordnung ist die Pharmazentralnummer, die auf Basis unterschiedlicher Verordnungseinheiten der DiGA vom BfArM zugewiesen wird:
Verordnungseinheit einer DiGA
Zu einer DiGA kann es unterschiedliche Verordnungseinheiten geben, analog z.B. verschiedenen Dosierungen und Packungsgrößen bei Arzneimitteln, die der Arzt oder Psychotherapeut dem Patienten verordnen kann. Jede Verordnungseinheit wird mit einer eigenen Kennnummer versehen und kann entsprechend spezifisch verordnet werden. Die einzelnen Verordnungseinheiten können je nach Ausgestaltung der DiGA variieren und sich z.B. hinsichtlich der folgenden Merkmale unterscheiden:

- Ist in der Verordnung Hardware (z.B. Pulsmesser, EKG-Sensorik) eingeschlossen?
- Handelt es sich um ein Startpaket mit einmaligem zusätzlichem Aufwand (z.B. einmalige besondere Datenerhebung zu Beginn oder einmalige Installation besonderer Hardware) oder um eine Fortführung einer bereits begonnenen Anwendung (z.B. Anwendung für weitere 30 Tage)?

- Für welche Anwendungsdauer (z.B. 30, 60, 90 Tage) wird die DiGA verordnet?
- Sofern eine DiGA unterschiedliche Module umfasst: Welches Modul soll verordnet werden (z.B. „Gelenkfit - Modul Knie“, „Gelenkfit - Modul Schulter“)?

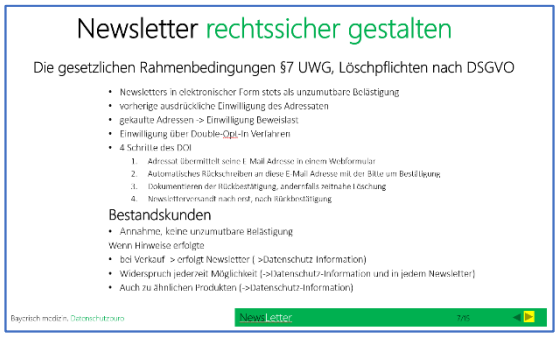
DiGA-ID und DiGA-Verordnungseinheit-ID im Verzeichnis

Gemäß § 20 Abs. 1 der Digitale Gesundheitsanwendungen-Verordnung (DiGAV) vergibt das BfArM für jede ins Verzeichnis nach § 139e SGB V aufgenommene DiGA eine eineindeutige Verzeichnisnummer, die diese innerhalb des Verzeichnisses identifiziert und damit die Referenz zum Verzeichniseintrag darstellt.
Entsprechend wird jeder DiGA (z.B. DiGA „Gelenkfit“) bei Aufnahme in das Verzeichnis eine 5-stellige numerische DiGA-ID zugeordnet (z.B. 12345).
Zur eineindeutigen Kennzeichnung unterschiedlicher Verordnungseinheiten derselben DiGA im Verzeichnis erhält jede Verordnungseinheit eine 8-stellige numerische DiGA-Verordnungseinheit-ID (DiGA-VE-ID), die sich aus der 5-stelligen DiGA-ID und einer sich unmittelbar anschließenden fortlaufenden 3-stelligen Verordnungseinheit-Nummerierung zusammensetzt (z.B. „Gelenkfit - Modul Knie - Verordnung für 30 Tage“: 12345001, „Gelenkfit - Modul Knie - Verordnung für 60 Tage“: 12345002“, „Gelenkfit - Modul Schulter - Verordnung für 30 Tage“: 12345003).
Damit ist aus der DiGA-VE-ID erkennbar, dass es sich um eine bestimmte Verordnungseinheit (letzte drei Stellen) einer bestimmten, im Verzeichnis gelisteten DiGA (erste fünf Stellen) handelt.

Pharmazentralnummer (PZN)

Zur Verordnung der DiGA und ihrer spezifischen Verordnungseinheiten durch Arzt oder Psychotherapeut wird jeder DiGA-Verordnungseinheit bei der Aufnahme ins Verzeichnis zusätzlich eine eineindeutige 8-stellige numerische Pharmazentralnummer (PZN) zugeordnet, eine Nummer, die den etablierten Standard zur Identifizierung z.B. unterschiedlicher Dosierungen und Packungsgrößen bei Arzneimitteln darstellt und dementsprechend bereits in allen Praxisverwaltungssystemen (PVS) implementiert ist.
Die PZN wird zentral von der Informationsstelle für Arzneimittelspezialitäten - IFA GmbH vergeben, die dem BfArM die benötigten PZN zur Zuordnung zu den DiGA-Verordnungseinheiten zur Verfügung stellt, sodass diese zusätzlich zur DiGA-VE-ID im Verzeichnis nach §139e SGB V gelistet werden.
Unabhängig vom Verfahren der Datenübertragung in die Praxisverwaltungssysteme (PVS) stellt die PZN damit die für die Verordnung von DiGA relevante Kennnummer dar und DiGA bzw. ihre einzelnen Verordnungseinheiten können unter Nutzung der im Verzeichnis nach § 139e SGB V gelisteten und sukzessive in den PVS angezeigten PZN verordnet werden, indem sie auf dem entsprechenden Rezeptvordruck (Muster 16) eingedruckt oder manuell vermerkt werden.

Folie 9



Newsletter rechtssicher erstellen

Für Marketingabteilungen sind Newsletter per E-Mail ein wichtiger Kanal, um Kunden und Interessenten über Angebote, Gewinnspiele, Produktneuheiten oder Unternehmensnews zu informieren. Damit fallen Newsletter in den Bereich der Werbung und es gibt einige gesetzliche Regelungen rund um die Datenerhebung und den Newsletter Versand. Auf dieser Folie erkläre ich, wie Sie Ihren Newsletter rechtssicher erstellen.

Die gesetzlichen Rahmenbedingungen

Das Gesetz gegen den unlauteren Wettbewerb (UWG) schützt in Deutschland den Verbraucher zum Beispiel vor irreführender Werbung. Daraus ergeben sich für die Online-Marketeers einige Vorgaben.

So regelt § 7 UWG, wie Sie die Kommunikationsdaten rechtssicher erheben können und vor allem, was es bei der Nutzung dieser Daten beim Newsletter Versand zu beachten gilt:

- Nach § 7 Abs. 2 Nr. 3 UWG ist der Empfang eines Newsletters in elektronischer Form stets als unzumutbare Belästigung anzusehen, wenn keine vorherige ausdrückliche Einwilligung des Adressaten vorliegt.
- Verwendet der Versender gekaufte Adressen ist er für das Vorliegen der Einwilligung darlegungs- und beweispflichtig. Das heißt, Sie sollten zumindest in Stichproben prüfen und sich überzeugen, dass die Einwilligungen auch tatsächlich vorliegen (LG Dresden, Urteil vom 30.10.2009, Az.: 42 HKO 36/09).
- Da in der Regel ein persönlicher Kontakt und eine schriftliche Einverständniserklärung nicht existieren, müssen Sie eine elektronische Form wählen. Achten Sie darauf, dass mit einer ausreichreichenden Sicherheit die Authentizität der Einwilligung beziehungsweise der betreffenden Person sichergestellt ist. Eine Einwilligung ist nur dann wirksam, wenn Sie den künftigen Newsletter Empfänger vollständig über den Gegenstand und den Umfang informieren. Außerdem muss er das Einverständnis aktiv selbst zum Beispiel per Double-Opt-In vornehmen.

Überblick Double-Opt-In-Verfahren (DOI)

Ein von den Gerichten anerkanntes Verfahren ist das sog. Double-Opt-In-Verfahren. Bei diesem Verfahren erhält der Interessent, der einen Newsletter angefordert hat, an die angegebene E-Mail-Adresse und den dortigen Namen eine nochmalige Aufforderung, die Newsletter Bestellung zu bestätigen.
Wichtig ist, dass diese Bestätigungs-E-Mail frei von Werbung sein muss (siehe OLG München, Urteil vom 27.09.2012, Az.: 29 U 1682/1232), weil zum Zeitpunkt der Übersendung der Bestätigungs-Email noch keine wirksame Einwilligung vorliegt. Die Einwilligung bezieht sich immer nur auf die in der Einwilligung konkret angegebene Adresse. Hat der Empfänger mehrere E-Mail-Adressen eingerichtet und soll der Newsletter an mehrere Adressen des Empfängers versandt werden, muss für jede Adresse eine Einwilligung eingeholt werden (OLG Celle, Urteil vom 15.05.2014, Az.: 13 U 15/14).
Für den Nachweis der Einwilligung mittels Double-Opt-In wird eine korrekte und vollständige Dokumentation der Einverständniserklärung verlangt (AG Düsseldorf, Urteil vom 09.04.2014, Az.: 23 C 3876/13). Die Wirksamkeit der Einwilligung setzt auch die jederzeitige Möglichkeit eines Ausdrucks voraus (BGH, Urteil vom 10.02.2011 – I ZR 164/09).
Welche Daten Sie protokollieren müssen, ist nicht konkret festgelegt. Um aber eine vollständige Dokumentation sicherzustellen, sollte die konkrete Einwilligung, Adresse sowie die Daten der Anforderung des Newsletters und der Bestätigung gespeichert werden. Neben diesem Verfahren sind die allgemeinen Informationspflichten des Telemediengesetzes zu beachten. Das gilt insbesondere dann, wenn vom Nutzer Daten über sein Nutzungsverhalten gespeichert und analysiert werden.

Vier Schritte des DOI-Verfahrens:

1. Ein Verbraucher trägt seine E-Mail-Adresse in das Anmeldeformular auf der Webseite ein und sendet dieses ab.
2. In einem nächsten Schritt generiert der Webserver eine automatische E-Mail an die angegebene E-Mail-Adresse und informiert den Empfänger, dass eine Anmeldung für den Newsletter des Unternehmens für die eingegebene E-Mail-Adresse vorliegt. Diese initiale E-Mail enthält einen automatisch generierten Bestätigungslink, auf den der Verbraucher, sofern er mit der Newsletter Anmeldung einverstanden ist, klickt. Webserverseitig sollte das Klicken des Bestätigungslinks mit Uhrzeit, Datum, IP-Adresse und gegebenenfalls Angaben zu dem Newsletter, für den die Anmeldung vorgenommen wurde, protokolliert werden. **Die Protokollierung dieser Angaben ist essenziell, da im Fall von Streitigkeiten das Unternehmen den Nachweis führen können muss, dass eine Anmeldung zum Newsletter vorlag.**
3. Systemseitig sollte sichergestellt werden, dass E-Mail-Adressen, für die kein Klick auf einen Bestätigungslink protokolliert wurde, nach einer definierten Zeit wieder aus dem System gelöscht werden (24 Stunden).
4. Die Newsletter Beschickung darf erst gestartet werden, wenn das Anklicken des Bestätigungslinks in der initialen E-Mail des Webserversystems protokolliert wurde.

Newsletter bei Bestandskunden

- Ausnahmen bestehen für Bestandskunden und es wird von keiner unzumutbaren Belästigung bei elektronischer Post ausgegangen, wenn vier Voraussetzungen erfüllt sind. (Art. 6 Abs. 1 lit. (a) DSGVO, § 7 UWG, Abs. 3)
    - Das Unternehmer hat im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten,
    - Und hat bereits die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
    - der Kunde hat der Verwendung nie widersprochen und
    - - der Kunde wurde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.“

  Fehlt bereits eine der in § 7 Abs. 3 UWG genannten Voraussetzungen, ist ein Versand von Newslettern an Bestandskunden nicht zulässig.

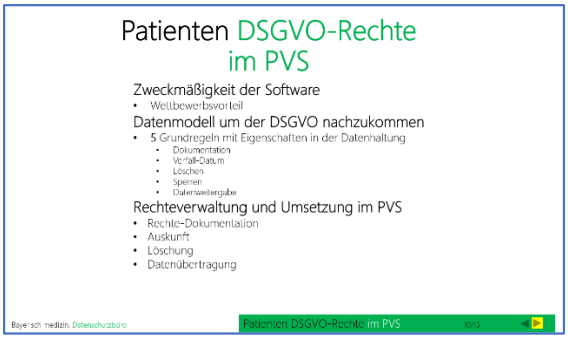
Umsetzung der gesetzlichen Vorgaben:

- Der Kunde muss zum Zeitpunkt des Verkaufs eines Produkts oder einer Dienstleistung darauf hingewiesen worden sein, dass der Unternehmer ihn künftig mittels Newsletter über ähnliche Produkte oder Dienstleistungen informieren wird.
- Der Kunde ist auf sein jederzeitiges Widerrufsrecht hinzuweisen.
- Bei der Bewerbung von Produkten oder Dienstleistungen müssen sich diese auf ähnliche wie das gekaufte Produkt bzw. die Dienstleistung, beziehen.
- Der Kunde ist in jedem Newsletter auf sein Widerspruchsrecht hinzuweisen.
- Seitens des Unternehmens muss sichergestellt sein, dass ein früherer Widerspruch gegen die werbliche Ansprache berücksichtigt werden muss.

Newslettern in der Datenschutzerklärung

Wie bei allen Erhebungen von personenbezogenen Daten ist auch bei Newslettern eine entsprechende Information nach Art. 13 DSGVO zu erteilen. Diese Information sollte in der allgemeinen Datenschutzerklärung der Webseite enthalten sein, auf die bei allen Erhebungen (z. B. bei Anmeldeformularen oder im Kaufprozess) mittels Verlinkung hingewiesen werden sollte.

Folie 10



Das PVS-System unterstützt den Arzt in seiner Erfüllung der Patienten DSGVO-Rechte

Zweckmäßigkeit

Software ist dann zweckmäßig, wenn sie den Anwender bei seiner täglichen Arbeit hilfreich unterstützt. Zeitintensive Arbeitsschritte werden möglichst automatisch abgenommen (Automatisation). Er wird durch komplizierte Prozesse intuitiv geleitet (Intelligente Nutzerführung). Er wird vor Fehlern gewarnt und es werden Lösungsvorschlägen angeboten (Error-Handling). Die Darstellung und Menueführung beschränkt sich auf das Wesentliche, gewährleistet aber trotzdem den Gesamt-Überblick (Ergonomie).

Software-Qualität und –Aktualität sind Voraussetzung für die Wettbewerbsfähigkeit.
Der Datenschutz verlangt den Praxen verantwortungsvollen Umgang mit den Patientendaten ab. Leider sind aber viele Praxis-Mitarbeiter in dieser Verantwortlichkeit sehr verunsichert. Die

Datenschutzgesetze haben klare Regeln mit vielen Eventualitäten, die sich aber besonders gut in der EDV abbilden lassen. Deswegen können Anwender auch im Datenschutz umfassend von der Software unterstützt werden.

Datenmodell als Grundregeln zur DSGVO

Definition: Mit dem Begriff Gesundheitsdaten sind nur Anamnese-, Diagnose-, Befund-, Therapie-, soziale Beschreibungs- und Abrechnungs-Ziffern gemeint, nicht Stammdaten wie Adresse und Versicherungsart. Damit das PVS-System die Patientenrechte unterstützen kann, müssen diesen Daten zusätzliche Informationen mitgegeben werden. Dies wird in 5 Grundregeln definiert.

5 Grundregeln mit Eigenschaften in der Datenhaltung

- Grundregel-1: **Dokumentation**. Alle Datenveränderungen müssen mit Zeitstempel und Verursacher dokumentiert werden.

- Grundregel 2: **Verfall-Datum.** Alle Gesundheitsdaten haben ein Verfall-Datum. Folglich muss diese Eigenschaft diesen Daten mitgegeben und mit abgespeichert werden. Das Verfall-Datum von Gesundheitsdaten wird durch 3 Kriterien festgelegt gemäß,
  - der KV-Aufbewahrungsfristen Tabelle
  - eine mögliche Speicher-Verlängerungs-Einwilligungen des Patienten, z.B. zwecks Familienanamnese
  - zum Schutz des Arztes vor BGB-Schadensersatz-Klagen (30 Jahre)

- Grundregel-3: **Löschen**. Unterschiedliche Verfall-Datums werden entsprechend unterschiedlich gezielt gelöscht. Haben alle Daten einer Patienten-Akte das Verfall-Datum erreicht, wird die gesamte Patienten-Akte automatisch mit entsprechendem Hinweis und mit Grundregel-1 gelöscht.

- Grundregel-4: **Sperren**. Die Patientenakte kann aus bestimmten Gründen gesperrt werden. Sperren heißt, die Patientenakte wird z.B. in eine andere Datenbank (Sperr-Datenbank) ausgelagert, verschoben, sie existiert dadurch nicht mehr in der ursprünglichen Datenbank. Zur Sperr-Datenbank haben nur besonders befugte Personen Zugriff. Die Verschiebe-Termine werden in der Regel zum Quartalsende vollzogen werden.
  Der Zugriffs-Grund muss dokumentiert werden.
  Gültige Gründe sind:
  - öffnen der Patientenakte zur eigenen Rechtsverteidigung gegenüber Gerichten oder Abrechnungsträgern (Nicht wegen „... ich muss mal eine Diagnose nachschauen…“ oder ähnlich).
  - Freischaltung einer einzelnen Patientenakte
    - bei Praxisübergabe (siehe Folie „Praxis Ende-Übergabe im PVS“),
    - versehentliche Sperrung
    - Patienten Einwilligung

  Hinweis:
  Die Löschpflicht nach Ablauf des Verfall-Datums muss auch in der Sperr-Datenbank beachtet werden.

- Grundregel-5: **Datenweitergabe**. Gesundheitsdaten können an Dritte, oder andere Stelle übermittelt werden. Diese Daten erhalten die Eigenschaft
  - Weitergabe-Datum,
  - Ziel-Adresse
  - gesetzliche-Grundlage (Überweisung, Patienten-Einwilligungs-Datum, BG-Anforderungs-Datum, Notfall-Datum)

Rechte-Verwaltung und Umsetzung im PVS (Pflichtdokumentation gemäß DSGVO)

- Die Vorfälle auf Rechtsansprüche werden in einer DSGVO-Rechte-Tabelle gesammelt und dokumentiert:
    - Lfde. Nummer
    - ID, Patienten-Name, -Adresse.
    - Art des Rechtes,
    - Beantragt-Datum,
    - Ausgeführt-Datum,

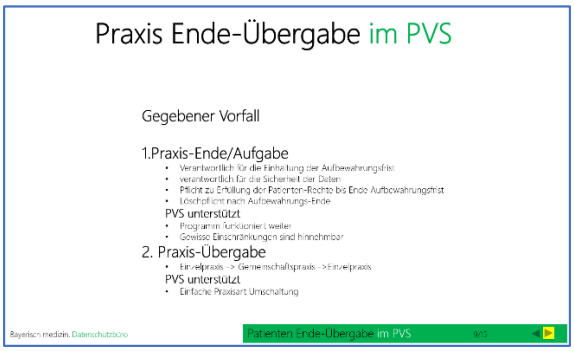
  Bei drohender Überschreitung von 4 Wochen zwischen Beantragt-Datum und Ausgeführt-Datum sollte die Software rechtzeitig vor einem möglichen DSGVO-Bußgeld warnen.
  Das voraussichtliche Bußgeld könnte nach einer mir vorliegenden Tabelle zusätzlich angegeben werden, das nach Praxisumsatz berechnet wird. Beispiel bis 700.000,-€ Umsatz erzeugt ein Bußgeld zwischen 972,-€ bis 7.582, - € je nach Länge der Fristüberschreitung in den 4 Stufen leicht - mittel - schwer – sehr_schwer, wobei die Stufenbewertung willkürlich von der Aufsichtsbehörde festgelegt wird.

- Patienten-Recht auf Auskunft:
  Nimmt der Patient sein Recht auf Auskunft wahr, so muss die gesamte Patienten-Akte auf Wunsch als Papier-Ausdruck oder Datenträger ausgehändigt werden. Häufig wird die Meinung vertreten, dass bestimmte Einträge nicht ausgegeben werden müssen. Dies betrifft aber nur persönliche Ansichten des Arztes z. B. zur Wirksamkeit von medizinischen Produkten. Nicht aber, wenn der Patient sozial beschrieben wird z.B. durch sein unangenehmes Auftreten usw., dies wäre Bestandteil seiner persönlichen sozialen Daten. Es gilt daher der Grundsatz, gesundheitliche oder soziale Daten, die der Patient auslöst, sind Patienten-Gesundheitsdaten. Der Patient erhält ein Anschreiben das seinem Recht zur Auskunft nachgekommen wurde. Aus der Datenauflistung muss auch die Datenübertragung an Dritte mit Adresse und Grund ersichtlich sein. (Ausgeführt-Datum -> DSGVO-Rechte-Tabelle)

- Patienten-Recht auf Löschen:
  Nimmt der Patient sein Recht auf Löschen wahr, so muss die gesamte Patienten-Akte auf Wunsch des Patienten nur dann gelöscht werden, wenn alle Gesundheitsdaten die Aufbewahrungsfrist erfüllt haben. Dieser Fall sollte aber nie eintreten, da die Akte bereits automatisch gelöscht sein sollte.
  Typischer Fall ist aber, dass die Patientenakte noch innerhalb der Aufbewahrungsfrist liegt. Die Patientenakte muss gemäß Grundregel-4 gesperrt werden. Der Patient erhält ein Anschreiben, dass seinem Recht zum Löschen erst nach Ablauf der Aufbewahrungsfrist nachgekommen werden kann und daher bis zu diesem Zeitpunkt die Daten gesperrt werden. Sperren heißt, Daten sind versiegelt und dürfen nur zur eigenen Rechtsverteidigung des Arztes geöffnet werden. (Ausgeführt-Datum -> DSGVO-Rechte-Tabelle)

- Patienten-Recht auf Datenübertragung:
  Der Patient hat das Recht von der Arztpraxis zu verlangen, dass seine komplette Patientenakte, ohne sein dazu tun, an eine andere Praxis übersendet wird. Dies betrifft nur elektronische Daten. Die Daten müssen dann in einer strukturierten Form übertragen werden. Es bietet sich deswegen das XML-Format an, das von der KV benutzt wird, zur Übertragung von Daten an die Software-Entwicklung.
  Da 2022 die ePatientenakte im Telematik System eingeführt werden soll, ist eine Eigenentwicklung dazu nicht mehr zu empfehlen, sondern der anfragende Arzt/Patient sollte auf diesen Zeitpunkt verwiesen werden.

Folie 11



Was bedeutet Praxis-Ende oder –Übergabe aus dem Blickwinkel des Datenschutzes.
Wie kann das PVS den Arzt dabei unterstützen?

In meiner Datenschutztätigkeit ergab sich ein Vorfall bei dem ein Arzt durch einen PVS-Hersteller in eine datenschutzrechtliche Sackgasse geführt wurde, die nur mit intensiver Intervention beim Hersteller zwar nicht gelöst, aber letztlich provisorisch überbrückt werden konnte.

Der Fall:

Ein Arzt beendet seine Praxistätigkeit und kündigt alle Versicherungen und Dienstleistungen. Später merkt er, dass er auf die Patientendaten in seinem Computer nicht mehr zugreifen kann.

Folgen:

Macht jetzt ein Patient sein Recht auf Auskunft, Datenübertragung oder Löschen geltend, kann er dem nicht nachkommen. Dies ist ein Datenschutzverstoß. Datenschutzverstoß - > Bußgeld.
Will er seine Privatrechnungs-Außenstände bearbeiten geht das auch nicht –> Umsatzverlust.

Ursache:

Der Hersteller des PVS-Systems kontrollierte automatisch über das Internet die Aktualität der Software. Die PVS-Software wurde nicht als Ein-Preis plus Wartungsgebühr, sondern als nur-Abbo-Nutzungsgebühr verkauft. Endet die Nutzung und damit das Abbo, wurde das Programm aus der Ferne deaktiviert. Das Starten des Programmes war nicht mehr möglich. Damit war auch kein Patientenaufruf, keine Nachverfolgung von offenen Rechnungen und kein nachkommen von DSGVO-Verpflichtungen mehr möglich.

Bewertung:

Diese Handlungsweise ist nicht nur Hersteller-Image schädigend, sondern ist eine Sinnverletzung des DSGVO Art 25 mit Erwägungsgründe 78, es heißt dort, die Hersteller sollen zur korrekten DSGVO konformen Entwicklung beitragen, sie sollen dazu „ermutigt werden“, usw. aber leider ohne Repressalien. Da dieses Undenken doch öfters vorkommt, haben verschiedene Behördenstellen bereits angekündigt hier nachschärfen zu wollen. Deswegen ist dies eine Chance, durch DSGVO korrekte Entwicklung einen Wettbewerbsvorteil zu erlangen.

1. Fall, die Praxis-Aufgabe

Die Praxis wird aufgelöst, geschlossen, nicht mehr weitergeführt.
Neben der Abwicklung bei Ärzte-Kammer, KV, Versicherung, Dienstleister und Personal, besteht für den Arzt jedoch weiterhin die Treuhandverpflichtung für die Patientendaten. Verstirbt er, geht die Verpflichtung auf die Erben über, oder auf einen von der Behörde eingesetzten Treuhänder.

Die Treuhandverpflichtung besteht bis zum Aufbewahrungs-Ende

- Er bleibt für die Sicherheit der Daten verantwortlich
  - Regelmäßiges Sichern und überprüfen der Datenträger-Qualität
  - Schutz vor unberechtigten Internet- und physischen Angriffen und Zugriffen
- Er bleibt in der Pflicht den DSGVO-Patientenrechten nach zu kommen
  - Löschung, Auskunft, Datenübertragbarkeit
- Er bleibt in der Pflicht die Daten nach Aufbewahrungsende endgültig zu löschen

Welche Unterstützung kann das PVS-System geben

- Das Programm funktioniert nach Wartungsende durch den Hersteller mit bestimmten Einschränkungen weiter (Wettbewerbsvorteil)
- Keine Aktualisierung ist nicht mehr nötig oder nicht mehr möglich, der Stand der Software ist eingefroren (Fehlerbehebung? Minuten-Support per Fall? Kosten?)

2. Fall, die Praxis-Übergabe

Der Arzt übergibt seine Praxis einem Nachfolger, der die Geschäfte weiterführt. Dazu gibt es 2 Möglichkeiten.

- Modell, Einzelpraxis.

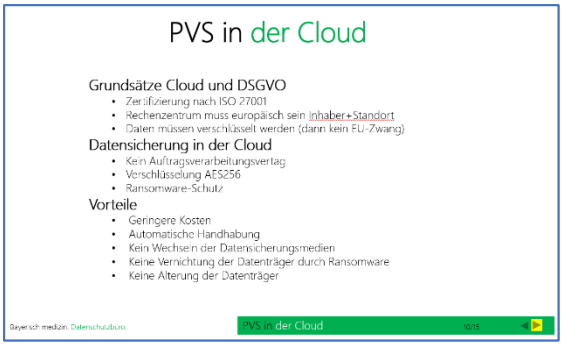
  Der Arzt übergibt an seinen Nachfolger und hört selber auf. Die Praxis bleibt Einzelpraxis.
  Die Patientendaten können aber nicht als Paket mitübergeben, oder wie das Inventar mit verkauft werden. Für eine Datenweitergabe an Dritte (neuer Arzt) ist datenschutzrechtlich die Einwilligung des Patienten nötig. Es muss also bei jedem einzelnen Patientenbesuch aus dem Paket die Patientenakte in die Datenbank des neuen Arztes übertragen oder freigeschalten werden. Da der vorhergehende Arzt aber in der Praxis nicht mehr tätig ist, muss eine andere ständig anwesende Person im Namen des vorigen Arztes die Treuhänderschaft vertraglich übernehmen und für die Überführung in die neue Inhaberschaft sorgen. Der neue Arzt ist wegen Interessen-Konflikt dazu nicht geeignet. Typisch übernimmt daher eine Arzthelferin diese Aufgabe.
  Welche Unterstützung kann das PVS-System geben:
  Vorstellbar wäre eine Konstruktion wie bei der Sperr-Datenbank, in der sich nun alle Daten befinden und von dort rückübertragen werden. Als Grund zur Öffnung der Patient-Akte steht jetzt nicht „Rechtsverteidigung“, sondern „Patientenübertragung“. Dies ist ein Wettbewerbs-Vorteil! Weiter dient es zur Kundenbindung, da ein Systemwechsel bei Arztwechsel immer im Raum steht.

- Modell, Vorübergehende Gemeinschaftspraxis

  Die Einzel-Praxis wird als Gemeinschafts-Praxis umgemeldet Beide Ärzte arbeiten über einen Zeitraum zusammen, was Vorteile für den neuen Arzt bringt, da er sanft in das Patienten-Klientel eingeführt wird.
  In einer Gemeinschaftspraxis kann jeder darin tätige Arzt jeden Patienten behandeln, ohne dessen Einwilligung zu benötigen. Der Begriff „Gemeinschaftspraxis“ kündigt dem Patienten an, dass hier mehrere Ärzte tätig sind. Durch Betreten der Praxis gibt er seine „stillschweigende Einwilligung“ ab, durch einen beliebigen oder wechselnden Arzt behandelt zu werden, es sei denn er benennt explizit einen speziellen Arzt. Nach einem angemessenen Zeitraum, in dem man annimmt, dass alle (meisten) Patienten in der Praxis waren, scheidet der alte Arzt aus und die Gemeinschaftspraxis wird wieder zur Einzelpraxis umgemeldet. Dieser angemessene Zeitraum wird mit 2 Quartalen angenommen.
  Welche Unterstützung kann das PVS-System geben:
  Das PVS-System sollte mühelos von Einzel- nach Gemeinschafts- und wieder auf Einzel-Praxis umschalten können. Die Kosten gehen mit der Umschaltung mit. (Wettbewerbsvorteil!)

Eine Praxissoftware, die den ganzen Praxislebenszyklus im Auge hat, wie das Arbeitsende eines Arztes berücksichtigen und eine strukturierten Praxisnachfolge regeln kann, trägt sicherlich auch zum Praxisverkaufswert bei.

Folie 12



Grundsätze für Cloud Nutzung

Werden Daten in der Cloud **verarbeitet**,

- muss das Unternehmen in der EU als Hauptniederlassung gemeldet sein. Es sind nach dem Urteil vom 16.07.2020 des EuGH Schrems II Urteil keine US-Firmen mehr möglich.
- Das Rechenzentrum bzw. der Provider muss ISO 27001 zertifiziert sein.
- Ein Auftragsverarbeitungsvertrag ist notwendig

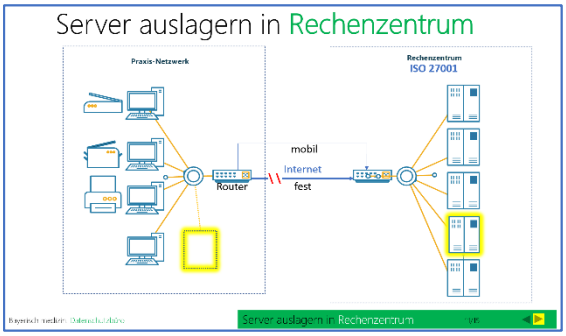
Werden Daten lediglich **gespeichert**,

- so können sie verschlüsselt mit AES256 an beliebigen Stellen abgelegt werden, es besteht dann kein EU-Zwang.
- Und kein AVV

Datensicherung in der Cloud, die Vorteile

- Die Kosten für eine Datensicherung mit Ransomware-Schutz, Verschlüsselung, Hybridfähigkeit und mit Cloudspeicher von 1 TB sind bereits ab 100,-€/Jahr möglich (Acronis). Das ist günstiger als mehrere lokale 1TB Festplatten.
- In der Regel läuft die Datensicherung zeitgesteuert, automatisch ab.
- Es fällt das Verwalten, Wechseln und Überprüfen durch eine Test-Rückspielung der Datenträger weg.
- Es entstehen keine unlesbaren Datensicherungen durch physikalische Speicherfehler auf veralteten Datenträger.

Folie 13



PVS in der Cloud

Der Server wird in die Cloud verschoben.

Es ist ein Auftragsverarbeitungsvertrag mit dem Rechenzentrum notwendig.

Voraussetzung dafür ist, dass der Vermieter im Einflussbereich der DSGVO und nach ISO 27001 zertifiziert ist und dass der physikalische Server in der EU steht und der Eigentümer des Rechenzentrums europäisch ist.

Damit scheiden alle Provider wie Microsoft, Amazon, Alibaba, usw. aus, auch wenn diese Niederlassungen in der EU haben und behaupten die Server stünden in der EU.

In München betreue ich datenschutzrechtlich 2 Arztpraxen, die zur Cloud auf meine Empfehlung gewechselt sind.

- die HNO-Praxis Dr.Edelmann (https://hno-muenchen.de)mit 18 Arbeitsplätzen, 4 Ärzten, 7 Diagnose-Geräte, mit dem Programm Medatixx. Ausführende Firma Worxeasy (https://worxeasy.de) mit Rechenzentrum in München.
- das Diabeteszentrum, Dr.Grünerbel (diabeteszentrum-muenchen-sued.de) 16 Arbeitsplätze, 3 Ärzte, 3 Diagnose-Geräte, mit dem Programm Medistar. Ausführende Firma Worxeasy (https://worxeasy.de) mit Rechenzentrum in München.

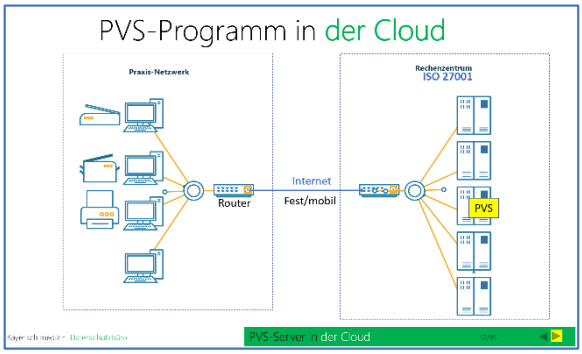
Vorteile

- Es wird höchste Verfügbarkeit und Schutz erreicht. Dabei kann das Rechenzentrum zusätzlich die Last der Datensicherung und einen ständig überwachenden Schutz der Endgeräte

übernehmen. In der Regel sind die Kosten günstiger als eine Neuanschaffung, Unterhalt und Pflege eines lokalen Servers, bei einem Vielfachen an Sicherheit.

- Niedriger Installationsaufwand. Der lokale Server wird gespiegelt und im Rechenzentrum installiert. Ein spezieller Router wird konfiguriert.
- Es sind keine Installations-Änderungen an den Arbeitsplätzen notwendig, oder an den Diagnosegeräten, die Ihre Daten zum Server übertragen.
- Ein intelligenter Router übernimmt alle lokalen Serveranfragen auf und leitet sie an den virtuellen Server im Rechenzentrum weiter. Bei Ausfall der Internet-Kabel-Verbindung schaltet er unterbrechungsfrei auf eine mobile Verbindung um. Als Kabel-Geschwindigkeit sind bei ca. 20 Arbeitsplätzen eine 100kB-Internet-Leitung notwendig und als Mobile-Verbindung LTE.
- Die Wartungsarbeiten der PVS-Hersteller werden nicht beeinträchtigt, da so auf dem Server gearbeitet werden kann, als stünde er in der Praxis.
- Es funktioniert mit jedem Arztprogramm.

Folie 14



Das Programm in der Cloud

Der Arzt hat mit dem Server nichts mehr zu tun. Er mietet lediglich das Programm in der Cloud mit einer Anzahl von Zugängen pro Arbeitsplätze.
Jeder Arbeitsplatz verbindet sich über eine kleine Clientsoftware mit dem Programm in der Cloud.
Es ist ein Auftragsverarbeitungsvertrag notwendig.
Diese Variante bietet die Firma RedMedical (https://www.redmedical.de) an.

Vorteile

- Es fällt eine Server- und eine Betriebssystem-Verwaltung in Gänze weg.
- Höchste Verfügbarkeit und Zugriff von überall her.
- Geringer Installationsaufwand. Über Fernwartung wird auf den Arbeitsplätzen eine kleine Client-Installation getätigt.
- Die Erneuerung eines Arbeitsplatzes dauert 5 Minuten, wenn keine Diagnose-Geräte installiert werden müssen.
- Die Daten sind Ende zu Ende verschlüsselt. Eine Ver- und Entschlüsselung findet im Client statt.

Nachteile

- Alle Clients arbeiten mit dem selben Geheimschlüssel. Bei Verlust des Schlüssels hat der Arzt keinen Zugriff mehr auf die Daten. Auch RedMedical kann dann die Daten nicht wiederherstellen.
- Ein PVS-Wechsel ist ungeklärt, keine Angaben sind dazu verfügbar.
- Beendet der Arzt seine Praxis-Tätigkeit, hat er keinen strukturierten Zugriff auf die Patientendaten mehr (Abbo-Ende=Zugriff-Ende)
- Er bekommt zwar alle zig Tausend Patientenakten als PDF-Datei, aber dadurch ist es extrem aufwendig, fast unmöglich seinen Löschpflichten nach Aufbewahrungsende nach zu kommen, oder das Erledigen von Patienten-Rechten gemäß DSGVO zu gewährleisten.
- Es fehlt ein minimales lokales Patientenverwaltung-Programm für nach Praxis-Ende/Aufgabe
- Eine Umschaltung auf mobile Internetverbindung bei Kabel-Unterbrechung wird von RedMedical nicht geliefert.

Link-Liste

Schulung 2020
Video: https://www.datenschutz-arzt.de/video/pegamed/2020.html
Dokumentation+Links: https://www.datenschutz-arzt.de/video/pegamed/2020.pdf

Hilfsprogramme gegen Werbetracker
Ghostery: www.ghostery.com oder über den jeweiligen Browser-Shop
Canvas Fingerprint Defender: Canvas Fingerprint Defender :: MyBrowserAddon oder über den jeweiligem Browser-Shop

DiGA (Digitale Gesundheit App)
Spitzenverband Gesundheitsversorgung https://digitalversorgt.de/diga-verzeichnis/
TIM – Telemonitoring Interventions in Medicine UG https://scitim.de/
BfArM https://diga.bfarm.de/de
BfArM DiGA-Verzeichnis https://diga.bfarm.de/de/verzeichnis

Cloud Referenzen:
Dr.Edelmann https://hno-muenchen.de
Dr.Grünerbel diabeteszentrum-muenchen-sued.de

Lieferant Rechenzentrum:
H.Landthaler https://worxeasy.de

DIGA-Verzeichnis-Linkliste

Hersteller von Digitalen Gesundheitsanwendungen (DiGA) können einen Antrag zur Aufnahme in das DiGA-Verzeichnis beim Bundesamt für Arzneimittel und Medizinprodukte (BfArM) stellen.
Folgende Mitgliedsunternehmen haben in der ersten Phase eine DiGA eingereicht oder werden in Kürze einreichen.
Diese Liste erhebt keinen Anspruch auf Vollständigkeit. Es ist möglich, dass sich weitere Mitgliedsunternehmen, die sich nicht auf dieser Liste befinden, einen Antrag beim Bfarm stellen werden.

Unternehmen	Anwendung	Kontakt
1. ADA Health GmbH	Ada: Deine Gesundheitshelferin (allg.Gesundheitsberater)	Anisa Idris
2. aidhere GmbH	zanadio: Das digitale Adipositasprogramm	Henrik Emmert
3. Antaris Digital Health Solutions GmbH	mentalis: Plattform für die psychische Gesundheit	Dr. Christian Aljoscha Lukas
4. Emperra GmbH E-Health Technologies	ESYSTA (Diabetes-Tagebuch)	Dr. med. Janko Schildt
5. GET.ON Institut für Online Gesundheitstrainings GmbH	HelloBetter (psychologische Begleitung)	Philip Ihde
6. HiDoc Technologies GmbH	CARA CARE (Reizdarm)	Jesaja Brinkmann
7. klier.net GmbH & Co. KG	BlutdruckDaten + SciTIM	Horst Klier
8. Lindera GmbH	Lindera Mobilitätsanalyse per App	Diana Heinrichs
9. mementor DE GmbH	somnio: Das digitale Schlaftraining	Noah Lorenz
10. mySugr GmbH	mySugr Tagebuch (Diabetes)	Sarah-Maria Richter
11. Newsenselab GmbH	M-sense Migräne	Diana Hagenberg
12. Perfood GmbH	sinCephalea: Migränetherapie von MillionFriends	Dominik Burziwoda
13. Selfapy GmbH	Selfapys Online Programme bei psychischen Erkrankungen	Farina Schurzfeld
14. TIM – Telemonitoring Interventions in Medicine UG	**SciTIM (Tele-Datenschnittstelle von Apps zum PVS)**	**Tino Römer**
15. Vivira Health Lab GmbH	Vivira: Therapeutisches Training für zu Hause	Philip Heimann