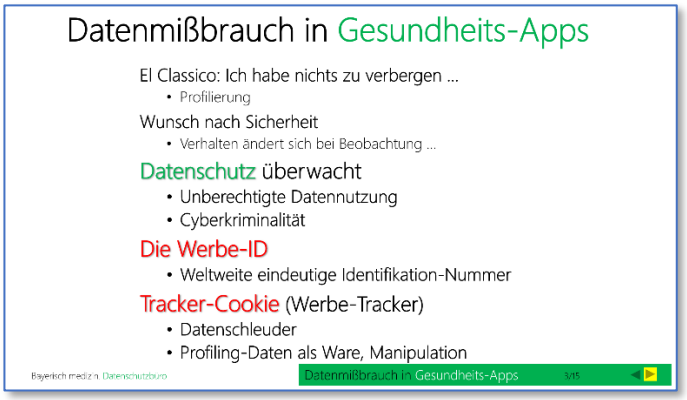
Folie 1

Folie 2

Agenda: 2020

- Datenmißbrauch bei Gesundheits-App
- Corona-App
- Debakel Telematik-Infrastruktur
- Hoch intelligente Trojaner
- Einwilligungen rechtssicher gestalten

Folie 3



El Classico: „Ich habe nichts zu verbergen“ erzeugt eine ungehemmte Weitergabe von Daten.

Aber daraus werden Benutzer-Profile erstellt:

- Wie oft wird die Webseite besucht, zu welcher Zeit, in welchen Perioden -> Interessen-Profil
- Wie intensiv beschäftigt man sich mit dem Inhalt -> Prioritäten der Interessen
- Woher kommt der Nutzer geografisch -> Bewegungsprofil
- Welche IT-Technik wird verwendet -> Aufgeschlossenheit gegenüber Neuerungen
- Wurde „gelikt“ -> soziales Engagement

Fazit: Rückschlüsse auf politischen Affinitäten, Charakter, Ängste, Alter, Geschlecht, Konfession, Ethnie, Beruf, besondere Vorlieben, usw.

Wunsch nach Sicherheit

- Sonderrolle Staat: Video-, E-Mail-, Internet-, PC-Überwachung, Regierungstrojaner, Alexa & Co.
- Ist Datenschutz Täterschutz? Wie anonym darf man in Internet sein. Wie weit dürfen Ermittlungsbefugnisse gehen
  Verhalten ändert sich bei Beobachtung
- Wenn ich weiß, andere beobachten mich oder haben Daten von mir, verhalte ich mich anders (Devianz).
- Beispiel: Video-Überwachung, Polizei fährt hinter einem her. Polizist trägt Body-Cam, usw.
- Deswegen kleben wir die Kameras am Laptop zu
- Verlust der Individualität.
- Das Verhalten wird konformer, es kann Demokratie gefährdend sein, Beispiel, Überwachungs-Phobie in China, usw.

Der Datenschutz überwacht und stellt die Regeln auf

- gegen unberechtigte Abschöpfung und Kommerzialisierung von Personendaten,
- regelt die Befugnisse zur Datensammlung bei GesundheitsApps, oder zur Strafverfolgung von Cyber-Kriminalität, Beleidigung und Verleumdung.

Die Werbe-ID

Sie ist die Erkennungsnummer, mit der der Anwender in jeder Internet-Berührung wiedererkannt wird. Sie ist für jedes Gerät einzigartig. Damit soll dem Benutzer eine individuelle Werbung oder Benachrichtigung übermittelt werden können, so die Industrie. Ganz nebenbei entstehen aber sehr genaue Persönlichkeits-Profile, die Rückschlüsse auf politischen Affinitäten, Charakter, Ängste und soziale Stellung wiedergeben.
Die Werbe-ID kann zurückgesetzt oder abgeschaltet werden. Für eine Anleitung dazu geben Sie unter Google ein:

- Windows 10 Werbe-ID deaktivieren.
- IPhone Werbe-ID deaktivieren: Bei Apple heißt die Werbe-ID -> Ad-ID (Advertising-Identifier), gehen Sie zu „Einstellungen“ – „Datenschutz“
- Android Werbe-ID deaktivieren

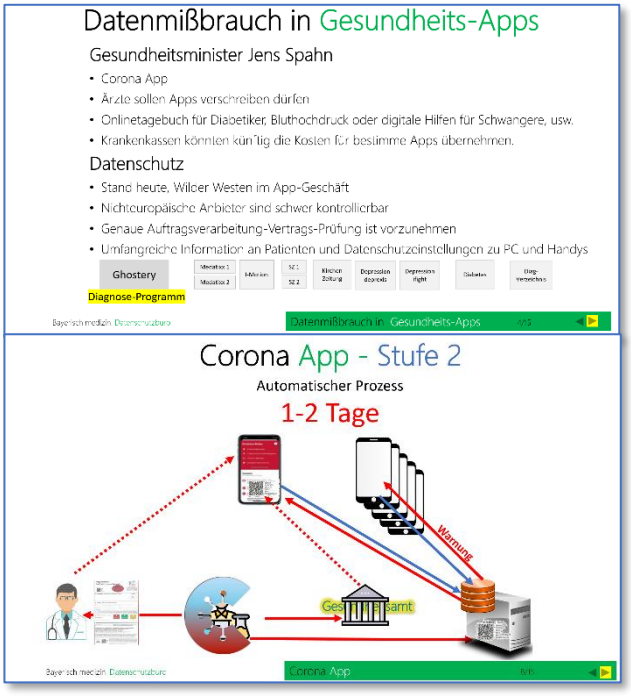
Tracker-Cookies

Das sind kleine Programme, die in die Webseite vom Programmierer eingebaut wurden. Sie haben nichts mit dem Seitenaufbau zu tun, sondern dienen alleine der Übersendung der Clicks auf der aktuell besuchten Webs-Seite usw. an Marketing-Firmen. Seit Juli 2019 hat der EUGH per Urteil verkündet, dass für jedes einzelne Tracker-Cookie vor Aktivierung die Anwender-Einwilligung eingeholt werden muss.

Daten das neue Öl

- Durch die Digitalisierung gewinnen Daten einen anderen Wert als früher. Von der Ressourcen-Planung des Staates zur globalen privatisierten Interessenssteuerung.
- Geschäftsmodell: Profile werden durch jeden Internetkontakt granularer und erbringen einen steigenden monetären Wert durch Individual-Werbung,
- Microtargeting: Bei dieser Form der Kommunikation werden Botschaften an möglichst genau definierte Zielgruppen angepasst z.B. zur Meinungs-Manipulation: US-Wahl, EU-Wahl, Sheet-Storm

Folie 4 - 8



Gesundheitsminister Jens Spahn

Verschreibt der Arzt bald nicht mehr nur Tabletten oder Krücken, sondern auch mobile Anwendungen für Smartphones, Smartwatches oder Tablets? Genau das sieht ein Entwurf für ein neues Digitalisierungsgesetz von Bundesgesundheitsminister Jens Spahn vor. Die Kosten sollen von den Krankenkassen übernommen werden. "Patienten sollen sich darauf verlassen können, dass sinnvolle digitale Anwendungen - z. B. Apps oder Diagnose-Tools - schnell in die Versorgung kommen", schreibt der CDU-Politiker auf Twitter.

Gemeint seien Gesundheits-Apps wie digitale Tagebücher für Diabetiker oder Apps für Menschen mit Bluthochdruck. Spahn will auch weitere digitale Angebote stärken. So sollen Patienten künftig leichter Arztpraxen finden können, die auch Videosprechstunden anbieten. "Der Patient von morgen wird immer noch einen Arzt brauchen",

argumentiert Spahn. "Aber er wird keinen Arzt mehr ernst nehmen, der nur noch über Karteikarten arbeitet."

Diag-Liste

Hersteller von Digitalen Gesundheitsanwendungen (DiGA) können einen Antrag zur Aufnahme in das DiGA-Verzeichnis beim Bundesamt für Arzneimittel und Medizinprodukte (BfArM) stellen. Sie werden in einem Verfahren, das als zügiger „Fast-Track“ konzipiert ist bewertet: Die Bewertungszeit für das BfArM beträgt drei Monate nach Eingang des vollständigen Antrags. Kern des Verfahrens sind die Prüfung der Herstellerangaben zu den geforderten Produkteigenschaften – vom Datenschutz bis zur Benutzerfreundlichkeit – sowie die Prüfung eines durch den Hersteller beizubringenden Nachweises für die mit der DiGA realisierbaren positiven Versorgungseffekte. Liste der bereits gemeldeten Apps, siehe am Ende.

Datenschutz

haben ein Ausmaß angenommen, das für den Anwender ohne Fachkenntnisse nicht zu durchschaubar ist. Hier benötigt der Arzt/Apotheker Beratungs-Know-how, um den Patienten zu warnen.

Kann man europäische Anbieter noch relativ gut kontrollieren und zur Räson bringen, ist dies bei außereuropäischen Anbietern sehr schwer.

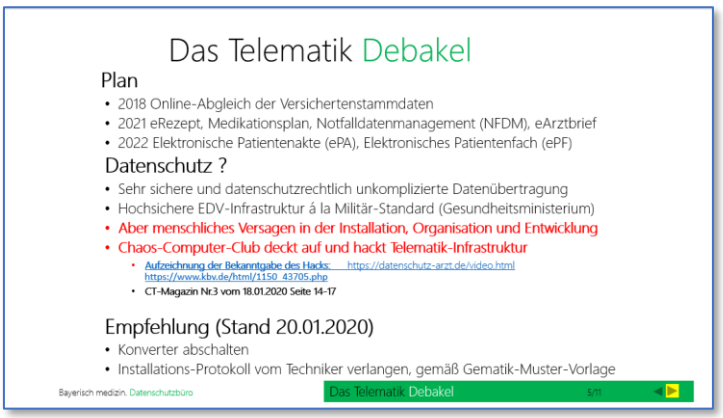
Die derzeit meisten Apps werden von amerikanischen Anbietern geliefert. Diese haben ein anderes Verständnis zum Datenschutz und werden zusätzlich durch das Gesetz “US Claud Act„ vom amerikanischen Staat gezwungen, umfassende Zugriffsrechte auf die Daten, selbst wenn sie in Europa liegen, zu gewähren.

Rechtliche Mittel, um gegen den „Claud Act“ vorzugehen, haben US-fremde Personen nicht. Datenübermittlungen sind nur dann zulässig, wenn die Bedingungen der DSGVO für einen Drittlandtransfer eingehalten werden. Dies wird zurzeit nicht erfüllt.

Diagnose-Programm:

Ghostery ist ein Diagnose Programm, das die versteckten Datenweiterleitungen durch Tracker-Cookies aufdeckt. Es listet sie auf und blockiert diese gleichzeitig. Es ist als kostenfreies Browser-Add-In für Windows und als eigenständiger Browser auf Handys mit IOS und Android im Shop verfügbar. Unter Windows kann es unter dem folgenden Link für jeden Browsertyp heruntergeladen und mit wenigen Klicks installiert werden: **https://www.ghostery.com/de/.** Es ist danach in der Kopfzeile obenrechts als blaues Geistsymbol sichtbar. Die kleine Zahl dabei zählt die von der Webseite erkannten Werbe-Tracker auf und blockiert sie.

Folie 9



(Siehe auch Link-Liste am Ende)

Der Plan, Daten zwischen den Ärzten, Krankenhäuser, Leistungsträger und Apotheken auf digitalem Weg abzuwickeln, nimmt langsam Fahrt auf.

So fällt ab 2018 die umständliche Prozedur der Versicherten Karten Aktualisierung über den Postweg und Austausch und Vernichtung der alten Karten weg.

2021 wird auch das Rezept sicherer. Elektronisch übermittelt gibt es keine schwer lesbaren Rezepte, oder fragwürdige unsichere über Sendungen dieser von der Arztpraxis in die Apotheke. Das gleiche trifft den Arztbrief, der oft mit dubiosen Einwilligungen und unsicheren Übermittlungswegen mit den Kollegen ausgetauscht wird. Die Übermittlung mit einer immer gültigen Krankenversicherungskarte ist sicher, da verschlüsselt, und

macht die jetzt komplizierte Einwilligungspraxis zu einer einfachen und natürlichen, transparenten Sache. Der Patient bleibt Herr seiner Daten und nur berechtigte können die Daten in Empfang nehmen.

Datenschutz ist gewährleistet?

Eine wichtige grundlegende Entscheidung bei der Konzeption der Karte trägt dem Datenschutz Rechnung: Die freiwilligen Anwendungen der elektronischen Gesundheitskarte (Notfalldaten, Arzneimitteldokumentation, elektronische Patientenakte, elektronischer Arztbrief, Patientenfach und Patientenquittung) sind klar von den Pflichtanwendungen (administrative Versichertendaten wie Name, Adresse, Versichertenstatus etc. und das eRezept) getrennt. Zum Einlesen von Verwaltungsdaten wie etwa Name und Adresse des Versicherten sind keine zusätzlichen Sicherheitsmaßnahmen erforderlich. Das entspricht dem heutigen Verfahren in den Arztpraxen. Der Zugriff auf sensible Daten, wie etwa Zuzahlungsstatus, das elektronische Rezept oder Arztberichte, ist jedoch durch ein strenges Sicherheitssystem geschützt.

Versprechen des Gesundheitsministerium:

Herzstück der digitalen Gesundheitsversorgung für 73 Millionen Versicherte ist die hochsichere, kritische Telematik-Infrastruktur mit bereits 115.000 angeschlossenen Arztpraxen. Nur berechtigte Teilnehmer haben über dieses geschlossene Netz Zugang zu unseren medizinischen Daten.

- Ein "Höchstmaß an Schutz"
- Schon in 12 Monaten können 73 Millionen gesetzlich Versicherte ihre Gesundheitsdaten in einer elektronischen Patientenakte speichern lassen. Dazu werden zurzeit alle Arztpraxen, Krankenhäuser und Apotheken Deutschlands über die neu geschaffene kritische Telematik-Infrastruktur verbunden.
- Dieses hochverfügbare Netz genügt "militärischen Sicherheitsstandards",
- bietet ein "europaweit einzigartiges Sicherheitsniveau" und
- verspricht ein "Höchstmaß an Schutz für die personenbezogenen medizinischen Daten" wie Arztbriefe, Medikamentenpläne, Blutbilder und Chromosomenanalysen.
- "Wir tun alles, damit Patientendaten sicher bleiben."
- "Selbst dem Chaos Computer Club ist es nicht gelungen, sich in die Telematik-Infrastruktur einzuhacken."
- "Nach den Lehren aus PC-Wahl, Ladesäulen und dem besonderen elektronischen Anwaltspostfach brauchen wir kein weiteres Exempel."

Chaos-Computer-Club widerspricht:

Es ist nicht so, wie es das Gesundheitsministerium behauptet! Bewaffnet mit 10.000 Seiten Spezifikation und einem Faxgerät lassen wir Illusionen platzen und stellen fest: Technik allein ist auch keine Lösung. Braucht es einen Neuanfang?

- Video-Aufzeichnung der Bekanntgabe des Hacks: https://datenschutz-arzt.de/video.html
- Was die KV dazu schreibt: https://www.kbv.de/html/1150_43705.php
- Fachbericht CT-Magazin Nr.3 vom 18.01.2020 Seite 14-17

Feststellung:

In der Pflichtenheft-Erstellung hat die Gematik alles richtig gemacht!

Fehlerhaft:

- Entwicklungsfehler von den Herstellern in den Geräten (Konnektor, Chipkartenlesegerät)
- Berechtigung zum Bestellen und Verteilung von Karten (eGK, HBA, SMC-B) ungenügend
- Installation des Konnektors teils mangelhaft

Empfehlung:

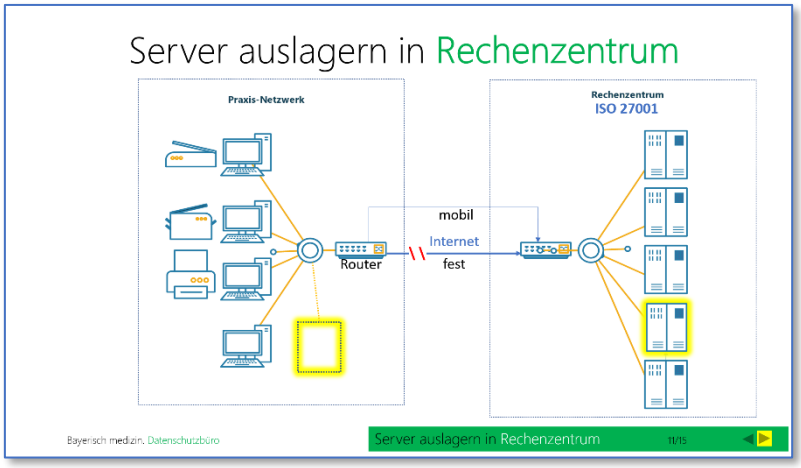
- Konverter abschalten bis die Gematik ihr Lieferstopp zurücknimmt.
- Nach der Installation des Converters sollte der Techniker, das von der Gematik empfohlene Protokoll aushändigen.

Folie 10

Der Ransomware-Virus ist ein Trojaner. Das heißt er ist in erster Linie ein scheinbar unverfängliches Programm, dass die Fähigkeit besitzt sich so zu verändern, dass herkömmlichen Virenprogrammen, die rein nach Signatur Basis arbeiten, ihn nicht erkennen. Erst in zweiter Linie, wenn die Krieger aus dem trojanischen Pferd herauskriechen und die Tore öffnen, wird das tatsächliche Standardprogramm nachgeladen. Programme die nicht auf unbekannte Prozesse oder böse Prozesse reagieren können, können dieser Strategie nicht folgen.

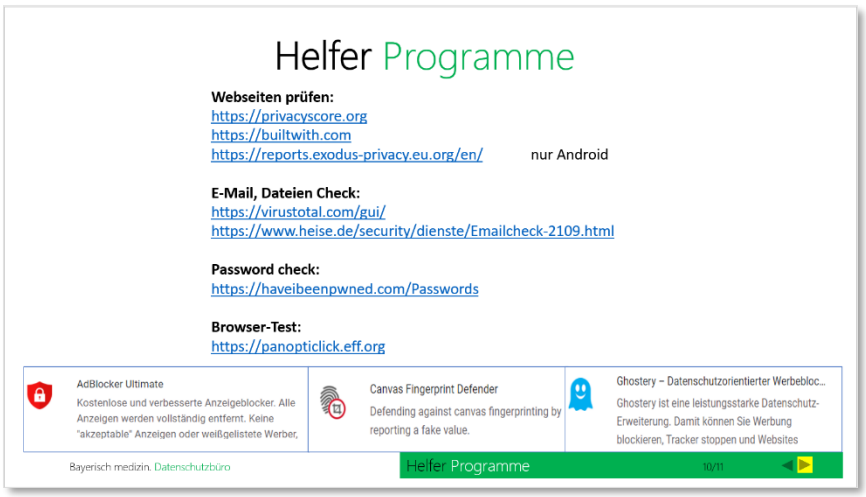
- Die einfachste und preiswerteste Lösung ist aber das Praxisnetzwerk mit den Patientendaten von Internet-Recherche und E-Mail-Belangen zu trennen und auf Computer außerhalb des Praxisnetzwerkes zu legen, man spricht von einem anderen Netzwerksegment.
- Die spanische Firma Panda arbeitet seit vielen Jahren nach diesem Prinzip Anomalie-Erkennung durch Prozessanalyse, und hatte bei seinen Usern in den letzten fünf Jahren keinen einzigen Crypto-Virus-Vorfall ertragen müssen. Andere Hersteller ziehen aber mittlerweile mit dieser Methode nach. Bei der Auswahl von Antivirusprogrammen sollte daher auf diesen Umstand geachtet werden.
- Eine Lösung wäre mit externer Expertenhilfe das Praxisnetzwerk live zu monitoren. Diese sogenannten Managed Service Provider schreiten automatisch und sofort bei erkennbaren Anomalien ein und blockieren bösartige Prozesse und benachrichtigen die Praxis.
- In Bayern gibt es eine Cyberschutzhotline, an die man sich wenden kann, um Hilfe zu richtiger Vorgehensweise zu erhalten: 089 31201-222
  http://www.stmi.bayern.de/sus/datensicherheit/cybersicherheit/
- Computer-Magazin CT liefert Sicherheitschecklisten:
  https://www.heise.de/ct/downloads/04/2/7/4/2/6/2/6/ct-sicherheits-checklisten-2020.pdf

Folie 11



Den Server in einen sicheren Bereich auslagern. Wird der Server, oder der PC, der die Datenbank und andere schützenswerte Dateien beherbergt in einem Rechenzentrum ausgelagert, das der ISO 27001 Norm entspricht, kann höchste Verfügbarkeit und Schutz erreicht werden. Dabei kann das Rechenzentrum zusätzlich die Last der Datensicherung und einen ständig überwachenden Schutz der Endgeräte in der Arztpraxis übernehmen. In der Regel sind die Kosten dafür günstiger als eine Neuanschaffung, Unterhalt und Pflege eines lokalen Servers, bei zusätzlich einem Vielfachen an Ausfallsicherheit.

Folie 12



Privacy-Score überprüft die Sicherheit des Webseiten-Zuganges für den Besucher.

Builtwith überprüft die Sicherheit der Webseite-Module, ob diese vor Angriffen geschützt sind und in welchem Land die Webseiten vom Provider gespeichert worden sind. Europäischen Ländern, die der DSGVO unterliegen sollte der Vorzug gegeben werden.

(Siehe auch Link-Liste letzte Seite)

Report **Exodus** ist eine Prüfstelle für Android-Programme, die die Geschwätzigkeit und Datenweitergabe aufdeckt.

Virustotal überprüft E-Mails und deren Anhänge. Ein Beispiel dazu. Ich hole eine Virusverseuchte E-Mail und schiebe sie einfach in den Testbereich. Mit bestätigen des Upload-Knopf wird die komplette E-Mail hochgeladen und mit zig Virenscannern überprüft. Sollte auch nur einer dieser Virenscanner anschlagen ist Vorsicht geboten und das E-Mail sofort zu löschen.

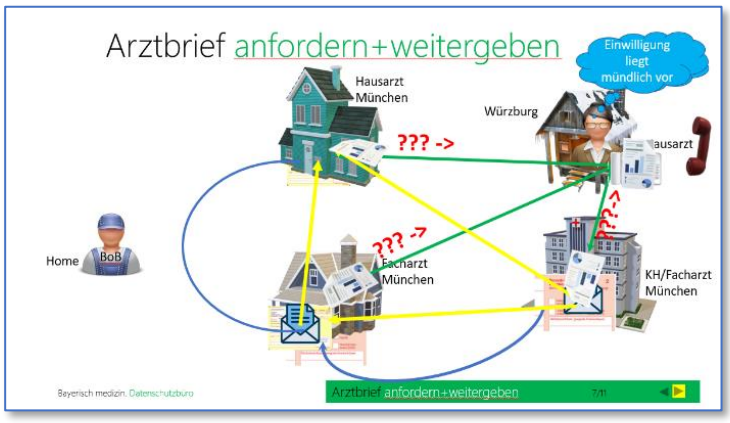
Heise-Plattform, von dort kann man sich Test-Virus-E-Mails zuschicken lassen. Um keinen Missbrauch damit machen zu können, wird jedoch zuvor an die angegebene Adresse ein Einwilligungs-E-Mail gesendet und der Sachverhalt nochmals erläutert, erst dann wird in einer darauffolgenden E-Mail der Virus tatsächlich verschickt, der aber keinen Schaden anrichtet, falls doch die eigene Sicherheit noch schwächelt.

Have I been passworded, verwende ich aufgedeckte, bekannte Passwörter.

Diese Prüfseite sagt, ob mein Passwort in der Liste bekannter Passwörter steht, die von Hackern zum Verkauf angeboten werden.

Panopti Click, überprüft die Sicherheit meines Browsers gegenüber Werbetracker und Angriffe.

Folie 13



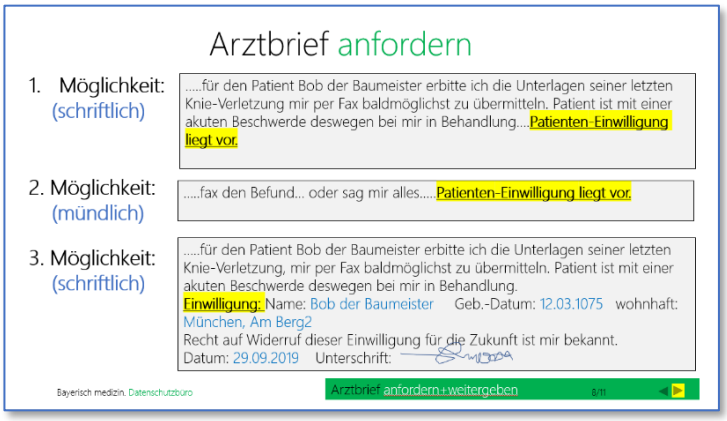
BUNDESÄRZTEKAMMER KASSENÄRZTLICHE BUNDESVEREINIGUNG, Deutsches Ärzteblatt | 09. 03. 2018 | DOI: 10.3238/aerztebl. 2018.ds01

Einschränkungen der ärztlichen Schweigepflicht

Ausnahmen von der ärztlichen Schweigepflicht sind gegeben, wenn gesetzliche Vorschriften dem Arzt eine Pflicht oder ein Recht zur Offenbarung auferlegen bzw. einräumen (vgl. 5.2). Der Arzt ist des Weiteren berechtigt, Informationen weiterzugeben, wenn der Patient ausdrücklich oder konkludent seine Einwilligung erteilt hat. Die ausdrücklich erteilte Einwilligung des Patienten ist nur wirksam, wenn sie auf der freien Willensbildung und Entscheidung des Patienten beruht. Hierzu muss der Patient wissen, zu welchem Zweck er den Arzt legitimiert,

patientenbezogene Informationen weiterzugeben. Die Einwilligung ist nur gültig, wenn sie hinreichend konkret bestimmt ist. Der Arzt sollte deshalb den Patienten auch auf die Folgen der Verweigerung seiner Einwilligung hinweisen. Das Sozialgesetzbuch und das Bundesdatenschutzgesetz verlangen darüber hinaus in bestimmten Fällen die **schriftliche oder elektronische Form der Einwilligung** (insb. § 67b SGB X und § 51 BDSG). Gleiches gilt im Rahmen der vertragsärztlichen Versorgung für den Austausch von Behandlungsdaten zwischen Hausarzt, Facharzt und sonstigen Leistungserbringern (§ 73 Abs. 1b SGB V).

Folie 14



Allerdings ist insoweit von einer **stillschweigenden Einwilligung** auszugehen, wenn die Übermittlung von Behandlungsdaten und Befunden im normalen Behandlungsablauf stattfindet, z. B. im Rahmen einer Überweisung durch den Hausarzt oder die Rückübermittlung der fachärztlichen Untersuchungsergebnisse.

Eine **konkludente bzw. stillschweigende Einwilligung** liegt grundsätzlich dann vor, wenn der Patient aufgrund der Umstände von einer Informationsweitergabe durch den Arzt an Dritte ausgehen muss und nicht widerspricht. Eine Offenbarungsbefugnis kann sich darüber hinaus aus einer sog. mutmaßlichen Einwilligung ergeben, wenn der Patient seine Einwilligung nicht erklären kann, beispielsweise weil er bewusstlos ist. Die **mutmaßliche Einwilligung** ist gegeben, wenn der Arzt davon ausgehen kann, dass der Patient im Fall seiner Befragung mit der Offenbarung einverstanden wäre oder wenn offenkundig ist, dass der Patient auf eine Befragung keinen Wert legt.

Liegt weder eine gesetzliche Befugnis noch eine Einwilligung zur Offenbarung patientenbezogener Daten vor, kann dennoch ausnahmsweise eine Offenbarung gegenüber Dritten zulässig sein. Grundsätzlich kommen solche Ausnahmen in Betracht, wenn das Vertrauen in die ärztliche Schweigepflicht gegenüber anderen Rechtsinteressen zurücktritt (**Notstand** gemäß § 34 StGB) oder der Arzt zur Wahrnehmung berechtigter Interessen handelt. So darf der Arzt zur **Abwendung einer anhaltenden Gefahr** dem Sexualpartner eines Patienten dessen HIV-Infektion mitteilen, wenn er zuvor erfolglos versucht hat, den Patienten zu bewegen, selbstständig seine Krankheit zu offenbaren. Ebenso kann die Schweigepflicht zurücktreten, wenn es um die Abwendung besonders **schwerer Verbrechen** geht (vgl. § 138 StGB).

Die Schweigepflicht kann ausnahmsweise auch hinter die persönlichen Interessen des Arztes zurücktreten. Dies kommt beispielsweise in Betracht, wenn der Arzt gezwungen ist, seine **Honorarforderung** gegenüber einem Patienten gerichtlich durchsetzen oder der Arzt sich gegen **Strafverfolgungsmaßnahmen** nur durch Offenbarung von Patientengeheimnissen effektiv verteidigen kann.

<u>Berufsordnung der Ärzte</u>

§9 Schweigepflicht

(5) Wenn mehrere Ärztinnen und Ärzte gleichzeitig oder nacheinander dieselbe Patientin oder denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis der Patientin vorliegt oder **anzunehmen** ist.

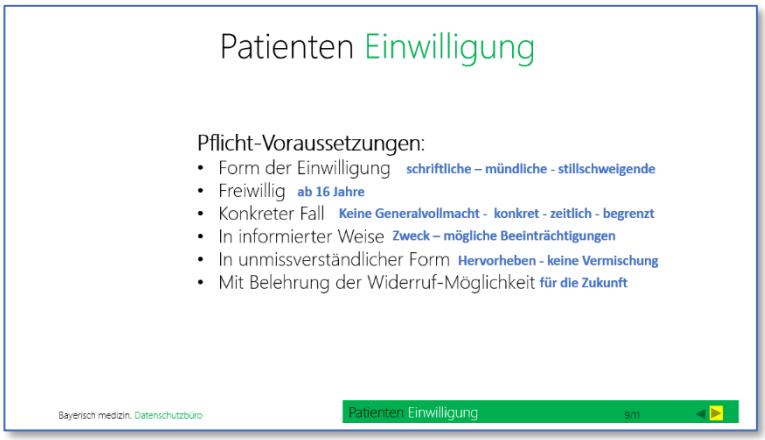
§ 7 Behandlungsgrundsätze und Verhaltensregeln

(7) Bei der Überweisung von Patientinnen und Patienten an Kolleginnen oder Kollegen oder ärztlich geleitete Einrichtungen, haben Ärztinnen und Ärzte rechtzeitig die erhobenen Befunde zu übermitteln und über die bisherige Behandlung zu informieren, soweit das Einverständnis der Patientinnen und Patienten vorliegt oder **anzunehmen** ist. Dies gilt insbesondere bei der Krankenhauseinweisung und –Entlassung. Originalunterlagen sind zurückzugeben.

DSGVO Erwägungsgrund 32

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung.
Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.
Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.

Folie 15
DSGVO: Voraussetzungen für die rechtssichere Einwilligung



Wichtig: Alle Voraussetzungen müssen nachgewiesen, dokumentiert werden!

Eine Einwilligung muss von einer einwilligungsfähigen Person,

- **formgerecht**
- **freiwillig,**
- **zu einem konkreten Fall,**
- **in informierter Weise**
- **in unmissverständlich in Form,**
- **mit Belehrung der Widerruf-Möglichkeit**,

abgegeben werden.

1. Form der Einwilligung

Die Einwilligungserklärung bedarf nicht zwingend der Schriftform. Diese kann ebenfalls mündlich oder elektronisch erfolgen. Jede Form bringt jedoch eigene Vor- und Nachteile mit sich.
Wichtig ist jedoch, dass die Einwilligungserklärung klar verständlich und eindeutig formuliert sein muss. Zur Erhöhung der Verständlichkeit darf man sich dabei visuelle Elemente bedienen. Optisch muss die Einwilligungserklärung klar von anderen Sachverhalten abgegrenzt werden.
Bloßes Schweigen oder Untätigkeit können nicht zu einer wirksamen Einwilligung führen.
So werden zum Beispiel bereits vorangehakte Kontrollkästchen (etwa zum Einverständnis mit Newsletter Zusendung) nicht für eine Einwilligung ausreichen. Deren Nicht-Weg-Klicken ist eine bloße Untätigkeit, die keine Einwilligung begründen kann.

2. Freiwilligkeit setzt eine Wahlmöglichkeit voraus

Freiwillig handelt nur, wer ohne Konsequenzen Nein sagen kann.
Das heißt die Person darf sich nicht gezwungen fühlen, eine Einwilligung abgeben zu müssen. An eine Einwilligung gekoppelte Vergünstigung macht die Einwilligung ungültig.
Hier ist auf die Minderjährigen zwischen 16 und 18 Jahren zu achten.

3. Konkreter Fall und in Kenntnis der Sachlage

ist die Voraussetzung einer gültigen Einwilligungserklärung. Hiernach muss der Patient die Möglichkeit erhalten, sich über die Konsequenz seiner Einwilligung zu informieren. Es muss für ihn klar sein, welche Dienstleistungen die Einwilligung konkret erfasst. Sie muss zeitlich überschaubar und verständlich für den Nutzer sein. Der Bezug auf künftige, mögliche Ereignisse ist nicht statthaft,

sogenannte General- oder Dauer-Einwilligungen. Typisch muss der zeitliche Bezug, bzw. Gültigkeit einen engen Zeitraum beschreiben, z.B. aktuelle Behandlung, oder 2-3 Monate.

4. Informiertheit

Nutzer müssen immer verständlich darüber informiert werden, zu welchem Zweck ihre Daten verarbeitet werden, auf welche Art, in welchem Umfang, ob deren Daten an Dritte weitergegeben und wann sie gelöscht werden. Im Regelfall ist es ausreichend, wenn diese Hinweise in der Datenschutzerklärung platziert werden.

Handelt es sich um eine Einwilligung, die besondere Beeinträchtigungen oder Belästigungen nach sich ziehen könnte, sollte jedoch schon im Rahmen der Einwilligung darauf hingewiesen werden.

5. Unmissverständliche Form

Dem Betroffenen muss bei der Abgabe einer Einwilligungserklärung klar sein, dass es sich hierbei um eine solche handelt. Dies kann etwa dadurch erfolgen, dass die Erklärung die Überschrift „Einwilligung" trägt oder der Inhalt wiedergibt, dass man bei etwas „zustimmt" oder in etwas „einwilligt". Einwilligungen die zudem zwischen anderen Klauseln stehen (Anmelde- Anamnese-Bogen, usw.), sollten beispielsweise durch Fettschrift, Rahmen oder Schriftfarbe besonders hervorgehoben werden.

6. Widerrufsmöglichkeit der Erklärung

Der Patient kann darüber hinaus jederzeit ohne Angabe von Gründen von seinem **Widerspruchsrecht** Gebrauch machen und die erteilte Einwilligungserklärung mit Wirkung für die Zukunft abändern oder gänzlich widerrufen. Er kann den Widerruf mündlich, postalisch, per E-Mail oder per Fax übermitteln. Es dürfen ihm dabei keine anderen Kosten als die Portokosten bzw. die Übermittlungskosten nach den bestehenden Basistarifen entstehen.
Eine Einwilligung ist nur dann freiwillig, wenn Nutzer wissen, dass sie die Einwilligung widerrufen können.

Minderjährige können erst ab 16 Jahren einwilligen

Art. 8 der DSGVO sagt, dass Minderjährige überhaupt erst ab dem 16ten Lebensjahr fähig sind, eine Einwilligung abzugeben (einzelne EU-Länder dürfen diese Grenze bis auf 13 Jahre senken, was in Deutschland jedoch nicht passiert ist). Dies gilt zwar nur, wenn sie „Dienste der Informationsgesellschaft" in Anspruch nehmen, doch wird das zumindest im Internet der Regelfall sein.
Das heißt unter 16 Jahren müssen die Eltern einwilligen. Hierzu existieren keine einfachen und praktikablen Mechanismen, wie zum Beispiel ein Double-Opt-In, bei dem mit hinreichender Sicherheit nur die Eltern zustimmen können. Es ist daher damit zu rechnen, dass viele Onlinedienste das Mindestalter schlicht auf 16 Jahre erhöhen werden.
Die Grenze von 16 Jahren bedeutet jedoch nicht, dass Daten Minderjähriger sonst nicht verarbeitet werden dürfen. Die Einwilligung ist nur einer der vielen Erlaubnisse der Verarbeitung von Daten.

Fazit

Eine Einwilligung sollte erst dann in Betracht gezogen werden, wenn andere Erlaubnisse der Datenverarbeitung nicht greifen.

Eine Einwilligung wird auch nach der Datenschutzreform bedeutend bleiben. Sie ist allerdings kein Allheilmittel. Zum einen sind die Anforderungen an deren Wirksamkeit sehr hoch. Zum anderen kann eine Einwilligung jederzeit widerrufen werden.
Aus diesem Grund sollte immer zuerst geprüft werden, ob nicht eine gesetzlichen Erlaubnisgrundlagen greift und man selbst von den Nutzern, bzw. Kunden weniger abhängig ist. Angesichts der Bußgelder von bis zu vier Prozent des Jahresumsatzes, solltest hier sehr sorgfältig gearbeitet oder eine rechtliche Beratung herangezogen werden.
Was Einwilligungen und gesetzliche Erlaubnisse jedoch gemeinsam haben, sind die hohen Anforderungen an deren Dokumentation und Nachweis.

Linkliste:

Allgemein:

Aufzeichnung der Bekanntgabe des Telematik-Hacks: https://datenschutz-arzt.de/video.html
Kommentar der KV HBA-Ausweis – Ausgabe: https://www.kbv.de/html/1150_43705.php

Kleine Helfer:

Webseiten-Aufbau prüfen:

https://webbkoll.dataskydd.net/de/

https://privacyscore.org

https://builtwith.com

Gefährliche Webseiten prüfen

https://global.sitesafety.trendmicro.com/result.php

App-Prüfer: (nurAndroid-App)

https://reports.exodus-privacy.eu.org/en/

E-Mail, Dateien Check:

https://virustotal.com/gui/

https://www.heise.de/security/dienste/Emailcheck-2109.html

Password check:

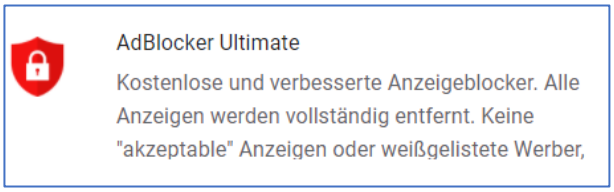
https://haveibeenpwned.com/Passwords

Browser-Test:

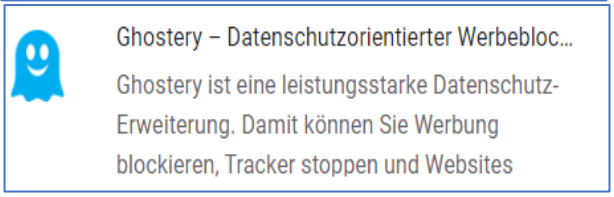
https://panopticlick.eff.org

Browser-Erweiterungen im jeweiligem Browser-Shop erhältlich:

Pop-Up-Blocker:



Tracker-Blocker:



DIGA-Verzeichnis

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

Diga für Leistungserbringer:	Für Diga-Nuzer:	Diga-Verzeichnis:
https://diga.bfarm.de/de/leistungserbringer	https://diga.bfarm.de/de/diga-nutzer	https://diga.bfarm.de/de/verzeichnis