Jugendsession
Session des jeunes
Sessione dei giovani
Sessiun da giuvenils

Jugendsession 2019

07. - 10. November

Dossier

Datenschutz im Gesundheitswesen

Autorin: Laura Hagen

Inhaltsverzeichnis

Um was geht es?

Tagtäglich geben wir privaten Unternehmen und dem Staat Informationen zu unserer Person preis: Apps zeichnen unser Bewegungsverhalten auf und Kundenkarten erfassen unsere Einkäufe und versorgen uns mit gezielter Werbung. Diverse Akteur*innen besitzen unvorstellbare Mengen an Daten über uns, die wir ihnen häufig liefern, ohne es überhaupt zu merken. Das ist im Gesundheitsbereich aufgrund der sensiblen Daten besonders kritisch. Es kann zwar meist ausgewählt werden, ob die eigenen Daten übermittelt werden sollen oder nicht. Jedoch muss der Freigabe von Daten oft zugestimmt werden, um überhaupt Zugang zu einer Dienstleistung zu erhalten. Wie kann in einer stark vernetzten Welt mit derart wertvollen Daten sichergestellt werden, dass diese Informationen nicht missbraucht werden? Wie ist die Bevölkerung zu schulen, damit sie die neuen Instrumente sicher nutzen kann?

Wichtige Begriffe und Definitionen

Daten	Informationen, die von einem Computer verarbeitet werden. Können in Text-, Bild-, Video- oder Audio-Format sein (Techfacts).
Personendaten (personenbezogene Daten)	Jegliche Daten, von denen auf eine bestimmte Person geschlossen werden kann (Vetter 2016).
Anonymisierte Daten	Daten die verändert, ersetzt oder weggelassen wurden, sodass davon nicht auf eine bestimmte Person geschlossen werden kann (Vetter 2016).
Pseudonymisierte Daten	Personendaten, bei welchen der Name oder andere Merkmale durch ein Pseudonym oder Alias ersetzt werden, damit die Daten nicht, oder nur erschwert, mit einer Person verbunden werden können (Vetter 2016).
Aggregierte Daten	Daten, die zusammengefasst wurden, beispielsweise der Durchschnitt eines Wertes; das erschwert den Rückschluss auf eine bestimmte Person (Vetter 2016).
Analoge Daten	Beinhalten theoretisch unendlich viele Informationen, z.B. können einer analogen Uhr verschiedene Informationen von Stunden-, Minuten- und Sekundenzeiger entnommen werden, zudem können sich die Zeiger auch zwischen zwei Zahlen befinden (Peters 2017).
Digitale Daten	Im Gegensatz zu analogen Daten bezeichnen digitale Daten ausgewählte Informationen, die von der Betrachtungsart unabhängig sind, z.B. gibt eine digitale Uhr eine eindeutige Uhrzeit an. (Peters 2017).

Privacy-by-Default	Stehen verschiedene Datenschutzniveaus zur Auswahl, dann muss das höchste voreingestellt sein.
Privacy-by-Design	Bei der Entwicklung von Software, die Personendaten verarbeitet, muss von Beginn weg auf die Einhaltung des Datenschutzes geachtet werden.
Besonders schützenswerte Personendaten (SR DSG)	Daten über: 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten 2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit 3. Massnahmen der Sozialhilfe 4. administrative oder strafrechtliche Verfolgungen und Sanktionen
Persönlichkeitsprofil	Eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt.
Datensammlung	Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.
Zentrale Speicherung	Zentrale Speicherung bedeutet, dass alle Daten am gleichen Ort gespeichert sind. Wer Zugriff auf eine zentrale Datenbank hat, kann theoretisch alle darin gespeicherten Daten einlesen.
Dezentrale Speicherung	Dezentrale Speicherung bedeutet, dass eine Datenbank auf verschiedene Standorte verteilt ist. Sie sind nicht alle am gleichen Ort, daher muss gezielt die jeweilige Datenbank abgefragt werden, um an bestimmte Daten ranzukommen.

Von Daten, Big Data und dem Gesundheitswesen

Wir leben im Zeitalter der Digitalisierung. Ob wir beim Einkaufen unser Kundenkärtchen vorweisen, um später Rabatte oder Gutscheine zu erhalten, auf Sicherheitskameras gefilmt werden oder daheim im Internet surfen – ständig werden Daten über unseren Alltag gesammelt. Dabei kann bezüglich der Art zwischen digitalen und analogen Daten differenziert werden. *Digitale Daten* bestehen aus einzelnen Elementen, die beim Zusammenfügen eine Information repräsentieren. Hingegen sind *analoge Daten* eine weiterführende Aneinanderreihung von einzelnen Daten, die zusammen eine physikalische Grösse inklusive ihrer Änderungen repräsentieren. Zusätzlich existieren unterschiedliche Datentypen – personenbezogene, anonymisierte, pseudonymisierte und aggregierte Daten.

Wer von Daten spricht, sollte zudem mit dem Konzept *Big Data* vertraut sein. Big Data beschreibt eine Menge von unstrukturierten und semi-strukturierten Daten, diese müssen aber nicht zwingend personenbezogen sein (Rouse 2013). Charakterisiert wird Big Data durch Informationen, auf die mittels riesiger Datensammlungen aus verschiedenen Quellen schnell zugegriffen werden kann. So können beispielsweise Effizienzanalysen durchgeführt oder datengestützte Entscheidungen getroffen werden (Salzig 2016).

Aktuell wird die Anwendung von Big Data im Gesundheitswesen zu Zwecken besserer medizinischer Prognosen und Behandlungen diskutiert und in verschiedenen Projekten auch bereits angewendet. Zudem ist von einem enormen Forschungspotential die Rede z.B. wurden im Rahmen einer Studie Daten über das Erbgut der Teilnehmenden aufgenommen, anonymisiert, und mehrfach gesichert. Jedoch gelang es einem Team des *Data Privacy Lab* der Harvard-Universität, diese Daten zu de-anonymisieren und so 40% der Teilnehmenden zu identifizieren (SRF 2017).

Hier wird auch der Konflikt mit dem Datenschutz deutlich, denn Gesundheitsdaten gelten als besonders schützenswert. Informationen über die DNA könnten auch zum Nachteil der Patient*innen verwendet werden. Beispielsweise wenn eine Krankenkasse diese Informationen auswertet und jemandem gewisse Versicherungsleistungen vorenthält, um das eigene Risiko zu minimieren. Zudem besteht die Gefahr, dass heikle Daten, beispielsweise über eine Erkrankung, an die Öffentlichkeit gelangen. Ein solches Datenleck kommt einer Persönlichkeitsverletzung gleich und kann für die Betroffenen gravierende Konsequenzen haben. Wir sollten uns also gut überlegen, welche Daten wir preisgeben wollen, welche Folgen dies haben kann und welche Rolle der Datenschutz dabei spielt.

Datenschutz und Datensicherheit

Privatsphäre ist ein Menschenrecht. Alle haben ein Recht darauf, dass die eigene Privatsphäre respektiert, geschützt und sorgfältig behandelt wird. Dies gilt auch für Daten, denn diese können vieles über uns aussagen. Oft sind wir uns gar nicht bewusst, wie viel wir in unserem Alltag an Dritte preisgeben und welche Auswirkungen dies haben kann. Deshalb ist es umso wichtiger, dass wir uns mit Datensicherheit und Datenschutz befassen. Datensicherheit beschäftigt sich mit der Sicherheit von Systemen und Prozessen, welche auf Daten angewiesen sind und diese verarbeiten. Das Ziel ist es, Daten vor unbefugtem Zugriff, Schäden oder versehentlichem Löschen zu schützen. Der Datenschutz hat hingegen zum Ziel, die Privatsphäre und personenbezogene Daten vor unrechtmässiger Nutzung zu schützen.

Datenmissbrauch liegt vor, wenn Daten nicht für den Zweck verwendet werden, für den sie erhoben wurden oder wenn sie unrechtmässig an Dritte weitergegeben werden. Oder wenn mehr Daten gesammelt werden als nötig, was einer Verletzung des Prinzips der Datensparsamkeit gleichkommt. Eine weitere Gefahr sind Datenlecks, die zu einem ungewollten, unerlaubten Datenzugriff führen können.

Um einen hohen Datenschutz zu gewährleisten gibt es mehrere Ansätze:

1. Datensparsamkeit: Es werden nur Daten gesammelt, die für die Funktionsfähigkeit des Unternehmens notwendig sind.

2. Zweckgebundenheit: Daten werden nur für die angegebenen Zwecke genutzt und weder unerlaubt an Dritte weitergegeben noch für andere Zwecke verwendet.
3. Anonymisierung: Personenbezogene Daten werden verändert, ersetzt oder teilweise nicht angegeben (z.B. gibt man keine Namen, Adressen, Geburtsdatum etc. an)
4. Pseudonymisierung: Namen oder andere Merkmale, die auf eine Person zurückführen können, werden durch Codes oder Pseudonyme ersetzt.
5. Aggregation von Daten: Daten werden zusammengeführt und Durchschnitte oder sonstige allgemeine Aussagen aus dem Total der Daten abgeleitet (Datenschutz.org 2018)

Was sollte beim Datenschutz sonst noch beachtet werden?
Zunächst ist es wichtig, dass Grundsätze wie Datensparsamkeit, Privacy-by-Default, Privacy-by-Design, Transparenz und Einwilligungspflicht berücksichtigt werden. Wenn eine Einzelperson ein Unternehmen wegen Datenschutzverletzungen anklagen will, sieht das Schweizerische Datenschutzgesetz bisher eine zivilrechtliche Klage vor. Das heisst, dass jede Person einen eigenen Prozess gegen das Unternehmen führen muss. Sie trägt damit aber das ganze Prozessrisiko und im Fall einer Niederlage die gesamten Prozesskosten.

Eine Zivilklage kann verlangen:
- Dass man für allfällige Schäden entschädigt wird. Jedoch ist der Nachweis von Datenschutzverletzungen relativ kompliziert und der entstandene Schaden nur schwer feststellbar.
- Dass die Bearbeitung der Daten angepasst oder beendet wird.
- Dass die Daten gelöscht werden.
- Dass die Daten nicht mehr an Dritte weitergegeben werden.

Datenschützer*innen befürworten die Einführung einer Kollektivrechtsdurchsetzung, welche die Möglichkeit einer Sammelklage oder ein Verbandsbeschwerderecht beinhaltet. *Verbandsbeschwerderecht* meint, dass Organisationen oder Verbände die im betroffenen Bereich tätig sind, z.B. im Umweltschutz, in eigenem Namen eine Beschwerde für Betroffene führen können, auch wenn die Organisation selbst nicht betroffen ist. Dieses Recht ist im Datenschutz und im Bereich der Privatsphäre noch nicht gegeben. Bei einer *Sammelklage*, können sich Betroffene zusammenschliessen, gemeinsam einen Anwalt anstellen und einen Prozess führen. Die Sammelklage bietet eine Möglichkeit, potentiell hohe Prozesskosten zu teilen. Dadurch wird die Wahrscheinlichkeit erhöht, dass Betroffene überhaupt Klage erheben. (Schönenberger 2019)

Das Datenschutzgesetz (DSG) erteilt dem Eidgenössischen Öffentlichkeitsbeauftragten (EDÖB) u.a. die Aufgabe, Bussen für Missbräuche und Datenschutzverletzungen auszusprechen. Die Bestrafungsmittel sind jedoch sehr eingeschränkt, da der EDÖB nicht als Datenpolizei fungiert sondern seine Hauptaufgabe darin besteht, bezüglich der Einhaltung des DSG zu beraten (Meier 2019).

Falls in einem Unternehmen ein ungewollter, unerlaubter Datenzugriff auftritt, muss die zuständige Datenschutzbehörde informiert werden. Informationen über die Ursachen, den Ablauf und ergriffene Schutzmassnahmen werden jedoch nur der Behörde und nicht den Betroffenen kommuniziert. Eine Informationspflicht an Betroffene bei Datenverlust oder

ungewolltem Datenfluss ist gesetzlich also nicht vorgeschrieben. Datenschützer*innen fordern die Einführung einer solchen Informationspflicht. Sie hätte zur Folge, dass zumindest ein Teil der Betroffenen über den Datenfluss informiert würde (Müller 2017).

Datenschutz und Krankenkassen

Wie bereits erwähnt, sind Gesundheitsdaten besonders schützenswerte Daten. Deshalb existiert auch eine Schweigepflicht für Ärzte und es wird besondere Aufmerksamkeit auf den Schutz dieser Daten gelegt. Denn diese Daten sind potentiell wertvoll. So wird oft argumentiert, dass anhand genauerer Daten beispielsweise bessere Prognosen ausgestellt werden könnten, was sich wiederum positiv auf das Risikomanagement auswirken kann. Deshalb verfolgen verschiedene Institutionen aus dem Gesundheitswesen, etwa die Krankenkassen, die Entwicklung des Datenschutzes in diesem Bereich mit grossem Interesse.

In der Schweiz gibt es zwei Arten von Krankenversicherungen – die obligatorische Krankenversicherung und die freiwillige Zusatzversicherung. Alle in der Schweiz wohnhaften Personen müssen die obligatorische Krankenversicherung, auch Grundversicherung genannt, abschliessen. Die Prämienhöhe variiert abhängig vom Wohnort, dem Alter und den wirtschaftlichen Verhältnissen. Personen mit beschränkten finanziellen Mitteln können eine Prämienverbilligung beantragen. Gewisse Leistungen wie Brillen, Zahnarztkosten oder Alternativmedizin werden von der Grundversicherung nicht übernommen. Sie können bei Bedarf aber mit einer freiwilligen Zusatzversicherung abgedeckt werden. (SR KVG)

In letzter Zeit ist es immer üblicher geworden, dass Krankenkassen ihren Kund*innen Apps zur Verfügung stellen. Diese funktionieren oft als Bonusprogramm, mit welchen die Kund*innen ihre sportliche Aktivitäten messen können – wer sich mehr bewegt, erhält einen grösseren Bonus. Dies hat die Frage aufgeworfen, welche Gesundheitsdaten von einer App überhaupt gesammelt und bearbeitet werden dürfen. So sorgte das Programm *Helsana Plus* für ziemlichen Aufruhr. Das Bonusprogramm griff nämlich auch auf die Grundversicherung zu, d.h. dass durch sportliche Aktivitäten die Möglichkeit bestand, Bonuspunkte zu sammeln, welche anschliessend in Form von Rabatten oder Sachwerten bezogen werden konnten. Dadurch konnte eine indirekte Vergünstigung auf die monatliche Prämie erzielt werden. Das verletzt jedoch den Solidaritätsgedanken und damit das Grundprinzip des Schweizerischen Krankenversicherungssystems (bwg 2019).

Elektronisches Patientendossier (EPD)

Die gesetzlichen Rahmenbedingungen für die Einführung und Verbreitung des EPDs sind bereits gegeben und seit dem 15. April 2017 in Kraft. Ab dem Jahr 2020 müssen Spitäler ihren Patient*innen die elektronische Form des Patientendossiers anbieten. Doch was genau ist das EPD? Es handelt sich dabei um ein Dossier, welches jegliche Gesundheitsdaten und gesundheitlich relevanten Dokumente einer Person in elektronischer Form beinhaltet, etwa Röntgenbilder, den Impfausweis, Medikamentenrezepte oder Austrittsberichte des Spitals. Auf diese Dokumente kann der Patient oder die Patientin immer und von überall zugreifen.

Die Erstellung eines EPD ist freiwillig. Es muss eigenhändig unterschrieben und bewusst und mit Kenntnis über die genauen Bedingungen eingewilligt werden. Die Anforderungen an den Datenschutz sind beim EPD hoch, da der Erfolg des Systems vom Vertrauen in das Dossier abhängig ist. Je nach Präferenz sind die Gesundheitsdaten nur für Nutzer*in sowie

Behandlungspersonal zugänglich. Ausserdem müssen sich Gemeinschaften zertifizieren lassen und aufzeigen, dass ihre technischen und organisatorischen Massnahmen den Sicherheitsstandart erfüllen.

Die standardmässigen Zugriffsberechtigungen berücksichtigen den Datenschutz für den Zweck des EPDs in sinnvollem Masse, können aber weiter eingeschränkt werden. Kritisiert wird zum Beispiel, dass die Daten von der Post und Swisscom gespeichert würden, welche sich mit unterschiedlichen Informatikplattformen als Dienstleister*innen positionieren. Über diese Plattformen sollen Patienten digital auf ihre Krankenakten zugreifen. Damit die Daten abgerufen werden können, ist ein sicherer Log-In vorgesehen, der über einen simplen Benutzernamen mit Passwort herausgeht.

Bei der Erstellung eines EPD werden alle Daten übertragen. Den Patient*innen bleiben aber einige Möglichkeiten offen, das Datenschutzniveau anzupassen, beispielsweise kann die Zugriffserlaubnis selber eingestellt werden. Dabei gibt es folgende Sensibilisierungsstufen: (Patientendossier.ch 2019)

1. alle behandelnden Personen können die Informationen abrufen
2. nur der Hausarzt oder die Hausärztin kann die Informationen abrufen
3. nur der Patient oder die Patientin selbst kann die Informationen abrufen

Das EDP beruht auf dezentraler Datenspeicherung. Das bedeutet, dass es keine zentrale Datenbank gibt, auf der alle Informationen abgespeichert sind. Jede Datenbank beinhaltet nur eine gewisse Art von Daten. Abhängig davon, welche Daten benötigt werden, muss die dazugehörige Datenbank kontaktiert werden. Hinzu kommt, dass Patient*innen den Zugriff auf das EPD, und damit den Datenaustausch, bewusst erlauben müssen. Im Notfall, beispielsweise bei Bewusstlosigkeit, dürfen die Daten nur mit nachvollziehbarer Begründung abgerufen werden. Die Hauptmotivation für das EPD ist die Vereinfachung der Kommunikation und des Datenaustausches zwischen den Behandelnden, sowie eine vereinfachte Verwaltung der Daten (Raymann & Binder 2016).

Zudem existiert auch wirtschaftspolitischer Druck. Bereits heute stellen Spitäler Datenbanken mit anonymisierten Daten für Forschungszwecke zur Verfügung, um Therapien zu verbessern oder Krankheitsursachen aufzudecken. Hierfür wird das Einverständnis der Behandelten aufgrund der Anonymisierung nicht benötigt. Wenn aber verschiedene Datensätze zusammengefügt werden, kann von diesen Daten möglicherweise auf eine Person zurückgeschlossen werden. Dadurch entsteht das Risiko einer Diskriminierung von Einzelpersonen durch Konzerne mit Zugriff auf die Daten. Beispielsweise könnten gesundheitlich Angeschlagenen gewisse Versicherungen oder eine Anstellung verweigert werden.

Auch wenn das EPD voraussichtlich unter Verschluss bleiben soll, ist auch die Weitergabe der Gesundheitsdaten für Forschungszwecke ein Ziel. Eine solche Weitergabe von Daten könnte zu Beginn das Vertrauen in das System schwächen, da die Daten nicht nur bei Behandelnden und Behandelten bleiben würden. Letztlich soll die Entscheidung darüber, was mit den Daten geschieht aber bei den Patient*innen bleiben (John 2019).

Gesetzliche Grundlagen

BV Art. 13 Abs. 1 und 2 Schutz der Privatsphäre
Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs. Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

DSG (Bundesgesetz über den Datenschutz) Art. 7 Abs. 1 Datensicherheit
Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugten Zugriff geschützt werden.

DSG Art. 10a Abs.1-3 Datenbearbeitung durch Dritte
Es ist erlaubt, Personendaten durch Vereinbarungen Dritten zu überlassen, wenn «die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte» und die Bearbeitung nicht durch gesetzliche oder vertragliche Geheimhaltungspflicht verboten ist. Dabei ist zu beachten, dass der Auftraggeber sicher sein muss, dass die Datensicherheit durch die Drittpartei gewährleistet ist.

DSG Art. 12 Abs. 1-3 Persönlichkeitsverletzungen
Die Persönlichkeit der Betroffenen darf von Personendatenbearbeitenden nicht widerrechtlich verletzt werden. Es ist verboten, die Daten einer Person «ohne Rechtfertigungsgrund» oder «gegen ihren ausdrücklichen Willen» zu bearbeiten oder an Dritte weiterzugeben. Wenn die die Daten der betroffenen Person allgemein zugänglich sind und sie die Bearbeitung nicht ausdrücklich (z.B. schriftlich) verbietet, kann nicht von einer Persönlichkeitsverletzung die Rede sein. Problem: Dieses Recht kann nur mit Wissen um die Datenbearbeitung ausgeübt werden.

ZGB Art. 43a1A. Register / V. Datenschutz und Bekanntgabe der Daten
Der Bundesrat ist verpflichtet, den Schutz der Persönlichkeit und die Grundrechte der Person, von der die Daten handeln, zu beachten. Daten dürfen nur an Private bekanntgegeben werden, die ein *unmittelbares schutzwürdiges Interesse* nachweisen können. Mit einem schutzwürdigen Interesse ist gemeint, dass die Gründe den Persönlichkeitsschutz überwiegen. Behörden ausserhalb des Zivilstandwesens, welche regelmässig oder auf Anfrage Daten für die Erfüllung ihrer gesetzlichen Aufgaben benötigen, werden vom Bundesrat bestimmt. Jedoch sind die Vorschriften über die Bekanntgabe kantonal geregelt.

Was läuft aktuell in der Politik

DSG Revision
Im Mai 2018 ist von der EU die neue Datenschutzgrundverordnung erlassen worden. Diese hat die Regeln bezüglich der Erfassung, Speicherung und Bearbeitung personenbezogener Daten an die momentanen Rahmenbedingungen angepasst. Aktuell ist die Schweiz nicht so weit wie die EU, weshalb ein gewisser wirtschaftspolitischer Druck zur Anpassung der Gesetzgebung in der Schweiz besteht. 2018 begann denn auch die Revision des Schweizerischen Datenschutzgesetzes, welche in zwei Etappen ablaufen soll.

Während der ersten Etappe wurden Ausnahmefälle im Datenschutz untersucht, beispielsweise in Bezug auf die Verfolgung von Straftätern oder Asylsuchenden. Infolge

dessen wurde eine gesetzliche Grundlage für übergreifende Datenbanken geschaffen. In der zweiten Etappe wird die Vereinbarkeit des Schweizer DSG mit der neuen EU-Datenschutzverordnung geprüft. Bereiche, die primär Individuen betreffen, werden anhand kollektiver Rechtsdurchsetzung – beispielsweise mittels der bereits erwähnten Sammelklage – und weiterer Massnahmen geregelt, welche bei Missbräuchen und Datenschutz-verletzungen Bussen oder andere Strafen vorschreiben.

Aufwendung von Ressourcen
Die Schweiz wird dafür kritisiert, dass sie nicht ausreichend Ressourcen für den Datenschutz bereitstellt. Es sei zu wenig Personal vorhanden, welches zudem nicht über die notwendigen Entscheidungskompetenzen verfüge. Deshalb fordert die EU, dass kantonale Datenschützer*innen verbindliche Verfügungen erlassen können. Bislang seien sie lediglich in der Lage, Empfehlungen abzugeben. (Schneider 2018)

Hier spielt die Digitalisierung eine Schlüsselrolle. Da im Alltag, z.B. beim Einkaufen oder beim Lösen eines ÖV-Billets, aus Gründen der Effizienz mehr und mehr digitalisiert wird, werden auch mehr Daten gesammelt und bearbeitet. Dies hat zur Folge, dass auch die Arbeit des EDÖB immer wichtiger und gefragter, aber auch aufwändiger geworden ist. Da die Zahl der Angestellten aber ungefähr konstant blieb, herrscht aktuell ein Personalmangel. Es fehlen also die nötigen Mittel, um alle Fälle im Zusammenhang mit Datenschutz auch wirklich zu behandeln. (Curia Vista 2019)

Patientendaten und das EPD
Nationalrat Mathias Reynard drückte seine Besorgnis zur Kommerzialisierung der im EPD abgespeicherten Gesundheitsdaten und deren Zugänglichkeit in Form einer Interpellation aus. Die Antwort des Bundesrates lautete, dass die Patient*innen die Zugriffsberechtigungen für ihr EPD frei einstellen könnten und dass weder Krankenversicherungen noch andere Unternehmen Zugriff auf die Daten haben. Jedoch bestünde die Möglichkeit, die eigenen Daten für Forschungszwecke zur Verfügung zu stellen. (Curia Vista 2019)

Jugendsession
Im Rahmen der Jugendsession wurden drei Petitionen zum Thema Datenschutz verabschiedet:

Die Petition *Internetfreiheit und Urheberrecht*, welche vom Schulwesen bessere Aufklärung und Sensibilisierung hinsichtlich der Themen *Privatsphäre*, *Anonymität* und *Gefahren im Internet* forderte. (Jugendsession 2012)

Die Petition *Transparente Datenschutzbestimmungen in den AGB* fordert eine verständliche und klare Festlegung des Umgangs mit personenbezogenen Daten sowie eine Sensibilisierung der Bürger*innen. (Jugendsession 2015)

Die letzte eingereichte Forderung verlangt, dass das EPD obligatorisch und unter hohen Sicherheitsauflagen ausgedehnt wird. (Jugendsession 2017)

Nützliche Links

Links	QR Code
Datenschutz bei der Digitalen Gesellschaft Schweiz	
Datenschutz im Gesundheitswesen	
Allgemeine Informationen zum EPD	
Big Data im Gesundheitswesen auf *eHealth*	
Kritischer Artikel zum Umgang mit Patientendaten	

Quellenverzeichnis

BAG. (2017). *Gesetzgebung elektronisches Patientendossier*. Stand 13.09.2019 [online] https://www.bag.admin.ch/bag/de/home/gesetze-und-bewilligungen/gesetzgebung/gesetzgebung-mensch-gesundheit/gesetzgebung-elektronisches-patientendossier.html [19.09.2019]

bwg. (2019). *Gericht verurteilt die Helsana-Versicherung*. In: Medinside, 01.04.19 [online] https://www.medinside.ch/de/post/gericht-verurteilt-die-helsana-versicherung [19.09.2019]

Curia Vista (2019). *Sollen Patienten an den Meistbietenden verkauft werden?* In: Interpellation 19.3330 vom 22.03.2019 [online] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193330 [19.09.2019]

Datenschutz.org. (2018): *Datensicherheit: Massnahmen für den Schutz von Daten*. Stand 24.05.2018 [online] https://www.datenschutz.org/datensicherheit-massnahmen/ [19.09.2019]

John, Simon. (2019). *Die Gier nach Gesundheitsdaten*. In: Beobachter, 24.05.2019 [online] https://www.beobachter.ch/gesundheit/medizin-krankheit/elektronisches-patientendossier-die-gier-nach-gesundheitsdaten [19.09.2019]

Jugendsession. (2012). *Internetfreiheit und Urheberrecht*. In: Forderungsheft 2012 [online] http://forderungen.jugendsession.ch/de/demand/49/show [19.09.2019]

Jugendsession. (2015). *Transparente Datenschutzbestimmung in den AGB*. In: Forderungsheft 2015 [online] http://forderungen.jugendsession.ch/de/demand/288/show [19.09.2019]

Jugendsession. (2017). *Digitalisierung und Gesundheitswesen*. In: Forderungsheft 2017 [online] http://forderungen.jugendsession.ch/de/demand/285/show [19.09.2019]

Meier, Thomas. (2019). *Persönliches Gespräch mit der Verfasserin*. Bern, am 25.04.2019

Müller, Giorgio V. (2017). *Schweizer Firmen sind gezwungen, Daten ihrer Kunden besser zu schützen – sonst drohen drakonische Strafen*. In: NZZ, 17.07.2017 [online] https://www.nzz.ch/wirtschaft/in-knapp-einem-jahr-gilt-es-ernst-die-schweiz-wird-eu-datenschutz-konform-ld.1305383 [19.09.2019]

Patientendossier.ch. (2019). *Das Elektronische Patientendossier einfach erklärt*. Stand 28.05.2019 [online] https://www.patientendossier.ch/de/bevoelkerung/informationen [19.09.2019]

Peters, Marcel. (2017). *Analog und digital: das ist der Unterschied*. In: Praxistipp Chip, 28.08.2017 [online] https://praxistipps.chip.de/analog-und-digital-das-ist-der-unterschied_95532 [19.09.2019]

Raymann, Felix; Binder, Urs. (2016). *Digitale Medizin bringt bessere Qualität für alle*. In: Swisscom Magazin, 26.08.16 [online] https://magazin.swisscom.ch/digitale-transformation/digitale-medizin-bringt-bessere-qualitaet-fuer-alle/ [19.09.2019]

Rouse, Margaret. (2013). *Big Data*. In: Wörterbuch [online] https://www.computerweekly.com/de/definition/Big-Data [19.09.2019]

Salzig, Christoph. (2016). *Was ist Big Data?* In: *umBlog, 04.05.2016 [online] https://blog.unbelievable-machine.com/was-ist-big-data-definition-f%C3%BCnf-v [19.09.2019]

Schneider, Oliver. (2018). *Was mit der EU-DSGVO auf das Schweizer Gesundheitswesen zukommt*. In: Netzwoche, 26.03.2018 [online] https://www.netzwoche.ch/news/2018-03-26/was-mit-der-eu-dsgvo-auf-das-schweizer-gesundheitswesen-zukommt [19.09.2019]

Schönenberger, Erik. (2019). *Persönliches Gespräch mit der Verfasserin*. Zürich, am 10.04.2019

Schweizerische Eidgenossenschaft. *Krankenkasse – Abschluss, Kosten und Leistungen der Grundversicherung*. In: Die Schweizer Behörden Online [online] https://www.ch.ch/de/krankenkassen-kosten-leistungen-der-grundversicherung/ [19.09.2019]

SR 101 BV. *Bundesverfassung*. Stand 23.09.2018 [online] https://www.admin.ch/opc/de/classified-compilation/19995395/index.html [19.09.2019]

SR 210 ZGB. *Schweizerisches Zivilgesetzbuch*. Stand 01.01.2019 [online] https://www.admin.ch/opc/de/classified-compilation/19070042/index.html [19.09.2019]

SR 235.1 DSG. *Bundesgesetz über den Datenschutz*. Stand 01.03.2019 [online] https://www.admin.ch/opc/de/classified-compilation/19920153/index.html [19.09.2019]

SR 832.10 KVG. *Bundesgesetz über die Krankenversicherung*. Stand 01.07.2019 [online]

https://www.admin.ch/opc/de/classified-compilation/19940073/index.html [19.09.2019]
SRF. (2017). *Das Milliarden-Geschäft der anderen.* In: Beitrag vom 24.02.2017 [online] https://www.srf.ch/news/schweiz/das-milliarden-geschaeft-der-anderen [19.09.2019]
Techfacts. *Was sind Daten?* In: Ratgeber [online] https://www.techfacts.de/ratgeber/was-sind-daten [19.09.2019]
Vetter, Anita. (2016). *Datenschutz, Datensicherheit und Arten von Daten*. In: Blogbeitrag vom 09.02.2016 [online] https://www.polyas.de/blog/de/online-wahlen/sicherheit/datenschutz-datensicherheit-und-arten-von-daten [19.09.2019]

Notizen

SAJV | Projektleitung
Jugendsession
projektleitung@jugendsession.ch
www.jugendsession.ch

Schweizerische Arbeitsgemeinschaft der Jugendverbände
Conseil Suisse des Activités de Jeunesse
Federazione Svizzera delle Associazioni Giovanili
Federaziun Svizra da las Uniuns da Giuventetgna

Dieses Thema wurde erarbeitet mit der Unterstützung der Digitalen Gesellschaft Schweiz und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB