PB.S-01-566-2 Kapitel 3: Solidarität sichern

Antragsteller*in: BAG Arbeit Soziales Gesundheit
Beschlussdatum: 18.04.2021

Änderungsantrag zu PB.S-01

Von Zeile 566 bis 581:
Digitalisierung im Gesundheitswesen - aber sicher

~~Wir wollen die Chancen der Digitalisierung – ob Robotik zur Unterstützung in der Pflege, Telemedizin oder die elektronische Patientenakte – nutzen, um das Gesundheitssystem zukunftsfähig zu machen. Per App sollen Patient*innen sicher auf den digitalen Impfpass, Gesundheitsinformationen wie die eigene Blutgruppe, die Krankheitsgeschichte oder die neuesten Blutwerte zugreifen können. Damit sie den Patient*innen wirklich nützt, muss die digitale Patientenakte weiterentwickelt werden. Dabei sind unter anderem Patient*innenorganisationen stärker einzubinden. Gesundheitsdaten sollen anonymisiert der Forschung zur Verfügung gestellt werden, um die Gesundheitsversorgung in Deutschland zu verbessern. Eine Weitergabe der Daten erfolgt dabei nicht gegen den Willen der Patient*innen. Ihre eigenen Gesundheitsdaten müssen für Patient*innen möglichst barrierefrei und sicher zugänglich sein. Die ärztliche Schweigepflicht und das Patient*innengeheimnis müssen auch für digitalisierte Gesundheitsdaten jederzeit gewahrt bleiben. Um administrativen Aufwand für medizinisches und pflegerisches Personal zu verringern und Innovationen anzureizen, sollen Hersteller von Medizinprodukten und Software offene Schnittstellen anbieten.~~

Digitalisierung kann helfen, die Abläufe im Gesundheitssystem im Interesse der Patient*innen zu verbessern. Sie soll die Zusammenarbeit der im Gesundheitswesen Tätigen erleichtern. Die Speicherung der Gesundheitsdaten darf aber nicht zum Selbstzweck werden. Eine ausschließlich dezentrale Speicherung der Daten ist erforderlich. Gesundheits- und Sozialdaten von Menschen gehören zu den intimsten Daten überhaupt, sie stellen die höchste Schutzkategorie personenbezogener Daten dar. Wir wollen sie vor Missbrauch, Datenhandel und Kommerzialisierung schützen. Wir sorgen dafür, dass bei Verwendung personenbezogener Daten das Patient*innengeheimnis sowie die ärztliche Schweigepflicht auch in der digitalen Welt gewahrt bleiben. Eine sichere elektronische Punkt-zu-Punkt-Kommunikation der im Gesundheitswesen Arbeitenden ist längst überfällig.

Grundsätzlich wollen wir, dass die Gesundheitsdaten von Menschen ohne eigenen, selbstbestimmten Zugang zur digitalen Welt am Ort ihrer Ersterhebung bleiben und nicht weitergeleitet werden. Die Einwilligung zur Datenweitergabe über diesen Ort hinaus erfolgt nach dem Opt-In Prinzip, indem die Patient*innen aktiv zustimmen müssen, wem und wann ihre Daten weitergeleitet werden. Der Gebrauch sensibler Gesundheitsdaten muss besonders geschützt und überwacht werden. Ein neuer, daraus abgeleiteter Informationsgewinn für Medizin- und Pharmaforschung, sowie die mit der Datenverarbeitung verbundenen Algorithmen und Vorgehensweisen bei der Digitalisierung werden für Patient*innen öffentlich zugänglich und transparent, um sicherzustellen, dass ein med.- techn. Fortschritt sie auch nachvollziehbar erreicht.

Begründung

Die Vielzahl und Vielfalt der Digitalisierungsverfahren im Gesundheitswesen braucht einen besseren Kompass mit einer klaren Ausrichtung auf einen starken Datenschutz und mehr Verantwortung im Umgang mit personenbezogenen Daten, eine klare rechtliche Verantwortlichkeit und dafür eine bessere Politik die den Menschen und nicht die Kommerzialisierung in den Mittelpunkt stellt.

Ohne uns in den Dienst von Gerechtigkeit und Teilhabe, auch bei der Digitalisierung des Gesundheitswesens, zu stellen, werden wir die damit verbundenen Aufgaben nicht gut und sicher lösen können. Wir wollen die Digitalisierung im Gesundheitswesen auf Augenhöhe. Wir brauchen eine gleichberechtigte und selbstbewusste Teilnahme der Patient*innen im Rahmen der bisherigen Regeln und Schutzmechanismen für die persönlichen Patientendaten sowie Aufrechterhaltung der ärztlichen Schweigepflicht in Wort und Tat.

Wir müssen die offenen rechtlichen und verfahrenstechnischen Fragen zur dauerhaften Wahrung der Persönlichkeitsrechte zur Gewährleistung einer der funktionalen Teilhabe am weiteren medizinischen-technischen Fortschritt durch die Digitalisierung, sowie zur repräsentativen Verfahrensbeteiligung bei der Digitalisierung durch die Betroffenen, klären .

In dem Maße, in dem Menschen keinen echten barrierearmen und sicheren Zugang zur digitalen Welt haben, bleiben sie mit ihren persönlichen Daten soweit in dieser digitalen Welt bei Weiterverarbeitung und Weiterleitung außen vor, der über den gewollten und eigenverantwortlichen Teil einer Erfassung und Erhebung am Ort der Handlung (d.h. der medizinischen Dienstleistung bei Arzt, Apotheke, KH, KV, Gesundheitsamt, Behörde) hinausgeht. Eine Weiterverarbeitung oder Weiterleitung von diesen persönlichen Daten wird solange für diesen Personenkreis generell ausgeschlossen, solange sie als Betroffene nicht über einen funktionalen, eigenen, selbstbestimmten Zugang zur digitalen Welt verfügen. Wenn Menschen nicht eigenverantwortlich digital handelnde Teilhabende sein können, können sie auf diesem Wege auch nicht von „digitalen Verfahrensvorteilen“ im erforderlichen und selbst-kontrollierenden Maße digital erreicht werden. Kriterien der Anonymisierung, Weiterverarbeitung, Auswertung und Zusammenführung der Daten müssen offengelegt werden. Kriterien und dafür eingesetzte Programme müssen von einer unabhängigen Kontrollstelle geprüft und freigegeben werden.

Hackerangriffe und Datenklau sind heute häufig zu vermelden und offensichtlich leider unvermeidbar. Zentrale Datenspeicher mit Gesundheitsdaten der Bevölkerung sind lohnende Ziele für professionelle Hacker, die sich hohen Ressourceneinsatz leisten können. Bei dezentraler Speicherung bilden sich geringere Datenmengen die dadurch unattraktiver für Angriffe werden. Hohe technische Standards, klare Verantwortlichkeit, Datenminimalismus und eine verteilte dezentrale Speicherung sind daher notwendig.

Die Datenmengen beim Umgang mit personenbezogenen Gesundheitsdaten müssen gut geschützt und im Regelbetrieb möglichst gering gehalten werden (z. B. nur am Ort der Erhebung der Daten bei Patient*iinnen gespeichert, bzw. nur vor Ort in der Klinik oder der Praxis). Jegliche Form der Datenverarbeitung und Datenweiterleitung darf nur mit sicherer Verschlüsselung und Signatur und somit der Einwilligung der Datengeber*innen erfolgen.

Patient*innen sollen die Hoheit über ihre Daten haben, was bei der aktuellen Form der ePA nicht der Fall ist, wie sowohl der CCC als auch der Bundesdatenschutzbeauftragte

heftig kritisieren. (https://www.br.de/nachrichten/bayern/datenschutzbeauftragter-warnt-vor-elektronischer-patientenakte , SGtl5tU). Die jetzt zur Einführung der ePA verwendete Telematik-Infrastruktur ist diesen Aufgaben nicht gewachsen und daher abzulehnen.

Für Menschen ohne Digital-Zugang oder -Kompetenz muss eine Form von Besitz an den eigenen Daten ermöglicht werden. Dies kann über papiergebundene Dokumente geschehen. Exemplarisch ist dies z.B. beim Medikationsplan seit 2017 realisiert. Auf dem Papierausdruck der Medikationsliste ist ebenfalls ein QR Code aufgedruckt, den jeder Leistungserbringer mit einem einfachen Handscanner in sein vor Ort befindliches Datenverwaltungssystem importieren kann. Exemplarisch wurden per Gesetzt die Softwarehersteller verpflichtet dafür eine Schnittstelle zu schaffen, die dies herstellerunabhängig ermöglicht. So ist gleichzeitig gewährleistet, dass Patienten das Verfügungsrecht und die Transporthoheit über die eigenen Daten behalten Diese Lösung ist auch offen für digitale Weitergabe. Wir befürchten, dass man Patient*innen eine Einwilligungserklärung zur Unterschrift vorlegt, und dass diese das unreflektiert tun .

Aktuell und auch künftig benötigen viele Bereiche der Digitalisierung von Gesundheitsdaten nach den o.g. Grundsätzen eine Vielzahl von rechtskonformen Weiterentwicklungen und Anpassungen im Sinne eines modernen Datenschutzes wie ihn Jan-Philipp Albrecht als Europarlamentarier von Bündnis 90 /Die Grünen bei der Entstehung und Verabschiedung (Dokumentarfilm) der DSGVO (EU-VO 20916/67) als wichtige Grundlage geleistet hat. Auch die Initiative zur Verabschiedung einer europäischen Charta digitaler Grundrechte (pdf) bildet ein weiteres Fundament künftiger Entwicklung. Die grüne Bundestagsfraktion unterstützt den Anspruch auf einen effektiven und starken Datenschutz.

Zum Art. 5 der DSGVO (für schnelle Leser - Quelle/link: Wikipedia):

Grundsätze der Verarbeitung personenbezogener Daten

Die DSGVO führt in Art. 5 explizit folgende sechs Grundsätze für die Verarbeitung personenbezogener Daten auf:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)
- Datenminimierung („dem Zweck angemessen und erheblich sowie auf das […] notwendige Maß beschränkt“)
- Richtigkeit („es sind alle angemessenen Maßnahmen zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden“)
- Speicherbegrenzung (Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es […] erforderlich ist“)
- Integrität und Vertraulichkeit („angemessene Sicherheit der personenbezogenen Daten […], einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“)

Der Verantwortliche muss die Einhaltung all dieser Grundsätze nachweisen. Die Nichteinhaltung dieser Grundsätze und der Rechenschaftspflicht kann mit einem angemessenen Bußgeld in Höhe von bis zu 20 Millionen EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes geahndet werden (Art. 83 Abs. 5 lit. a).