Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Digitalisierung im Gesundheitswesen - Kompatibel mit dem Datenschutz?“

Digitale Akademie der VHS Bonn

8. März 2022

Online

Es gilt das gesprochene Wort

Sehr geehrter Herr Preu,
sehr geehrte Damen und Herren,

herzlichen Dank für die Einladung und Ihr Interesse. Ich freue mich, Ihnen heute meine Sicht der Dinge auf die fortschreitende Digitalisierung im Gesundheitswesen darstellen zu können.

Als Informatiker sehe ich die Digitalisierung eher positiv und freue mich über viele Fortschritte und tolle neue Möglichkeiten in diesem Bereich. Ich probiere gerne neue Anwendungen und Programme aus und alles, was ich für sinnvoll oder hilfreich erachte, nutze ich auch. Dabei achte ich – nicht erst seit ich Bundesdatenschutzbeauftragter bin - auf datenschutzfreundliche Anwendungen, weil ich weder den ganzen Tag mit vermeintlich passender Werbung vollgemüllt werden möchte und weil es die internationalen Internetunternehmen und Datenhändler überhaupt nichts angeht, welche Vorlieben oder Krankheiten ich oder meine Familienmitglieder haben.

Dieses Ausspionieren ist widerlich, ein Krebsgeschwür der Digitalisierung, das in allen Bereichen um sich gegriffen hat. Oft ist es schon heute rechtswidrig und dort versuchen wir Datenschutz-aufsichtsbehörden durchzugreifen. Und dort, wo es nicht rechtswidrig ist, muss die Politik die Regeln verschärfen. Ausspionieren unterminiert eine freie Gesellschaft.

I. Gesundheitsdaten - besonders sensibel

Daten zu unserer Gesundheit, zu unserer Konstitution, zu unseren Krankheiten sind besonders sensibel und deshalb von der Datenschutzgrundverordnung (DSGVO) besonders geschützt. Die Verarbeitung dieser Daten ist sogar verboten, wenn wir der Verarbeitung nicht ausdrücklich und unter informierter Kenntnis der Verarbeitungszwecke zugestimmt haben.

Sie kennen das sicher von Arztbesuchen. Die Datenschutzerklärung ist immer mit das erste, was Ihnen vorgelegt wird. Ohne diese könnten die Praxen weder Rechnungen noch Rezepte schreiben, ja selbst Überweisungen wären schwierig. Unter uns: Manche andere Teile der dortigen Datenschutzerklärungen sind allerdings überflüssig, weil sie Teil einer Behandlung und Behandlungsdokumentation sind.

Weil der Zahl der anfallenden Daten in Arztpraxen hoch ist, die Zusammenarbeit mit anderen Fachärzten notwendig und sinnvoll und weil man Doppeluntersuchungen insbesondere mit teuren Geräten vermeiden möchte, wurde in den letzten 20 Jahren die elektronische Patientenakte (ePA) entwickelt und vor gut einem Jahr eingeführt. Die beiden Zahlen, 20 und 1, machen schon einen Teil der Problematik der Digitalisierung in Deutschland deutlich, die weder an technischen Problemen noch am Datenschutz scheitert.

II. ePA

Ich erspare Ihnen jetzt aber die mehr als ärgerliche und lange Geschichte, warum es 20 Jahre brauchte, bis eine ePA tatsächlich umgesetzt wurde. Ich will mich auf den Teil der Geschichte konzentrieren, wo es um die jetzt verwendete ePa geht.

Zunächst möchte ich Ihnen eine Einführung in die Zielsetzung und grobe Funktionsweise der elektronischen Patientenakte als Bestandteil der Telematikinfrastruktur der elektronischen Gesundheitskarte geben und dabei auch auf ihre Chancen eingehen.

Um es deutlich zu sagen: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit befürwortet eine gutgemachte Digitalisierung im Gesundheitswesen und auch eine gutgemachte elektronische Patientenakte. Neben direkten Vorteilen für die Versorgung kann sie auch Patientenrechte stärken. Wenn Versicherte einen sicheren Datenspeicher für ihre Dokumente erstellen können, kann das ein großer Vorteil gegenüber aktuellen Lösungen wie E-Mails oder Papierausdrucken sein: Aus Versorgungs- und aus Datenschutzsicht!

Die elektronische Patientenakte ist explizit als eine von den gesetzlichen Krankenkassen ihren Versicherten anzubietende versichertengeführte Akte benannt. Völlig zu Recht hat die Bundesregierung in der Begründung zum Patientendaten-Schutz-Gesetz die Wahrung der Patientensouveränität als eine der wichtigsten Vorgaben betont.

Die elektronische Patientenakte soll dabei nicht die Behandlungsdokumentation oder andere Akten von Ärzten, Krankenhäusern oder anderen Leistungserbringern ersetzen. Auch die direkte Kommunikation zwischen Leistungserbringerinnen und Leistungserbringern ist nicht Zweck der elektronischen Patientenakte. Ich betone dass, weil das in der Öffentlichkeit immer wieder falsch dargestellt wird. Ein Beispiel: Da die elektronische Patientenakte versichertengeführt ist, entscheiden die Versicherten selbst, welche Daten sie in diese einstellen und welche nicht. Das können und müssen sie nicht ausschließlich anhand von medizinischen Gesichtspunkten tun. Daher kann die elektronische Patientenakte auch nicht als vollständige Fallakte gelten, wie sie Ärztinnen und Ärzte führen. Das sollten auch bestimmte Ärztefunktionäre und Lobbyisten endlich zur Kenntnis nehmen.

Wie bisher wird sich wohl nur in der direkten Kommunikation zwischen Arzt und Patient bei der Behandlung herausstellen, welche Dokumente benötigt werden. Die elektronische Patientenakte kann dann über die Telematikinfrastruktur ein sicherer Weg sein, um diese Dokumente zu übergeben. In der analogen Welt entspricht die sogenannte elektronische Patientenakte einem Ordner, in dem alle medizinischen Befunde, Arztberichte, etc. vom Versicherten gesammelt werden und den er zu seinen Arztbesuchen mitnimmt.

Die Regelungen des Patientendaten-Schutz-Gesetz widersprechen leider seiner eigenen Prämisse der Patientensouveränität. Ich habe deshalb gegenüber den gesetzlichen Krankenkassen drei wesentliche Punkte der elektronischen Patientenakte benannt, die gegen die Datenschutz-Grundverordnung verstoßen, wenn keine zusätzlichen Maßnahmen über die Mindestanforderungen des Patientendaten-Schutz-Gesetzes ergriffen werden.

Kritik

Aus Sicht des Datenschutzes bei der elektronischen Patientenakte gibt es **drei gravierende Schwachstellen**:

1. das Berechtigungsmanagement wegen des „Alles oder nichts Prinzips“

2. Frontend-Nicht-Nutzer, d.h. diejenigen, die kein geeignetes Smartphone oder ein Tablet haben, werden benachteiligt

3. die Umsetzung des alternativen Authentisierungsverfahrens muss verbessert werden.

1. Berechtigungsmanagement

Beginnen möchte ich mit dem defizitären Berechtigungsmanagement, das auch Inhalt einer „Anweisung“ war, die ich als datenschutzrechtlich Verantwortlicher gegenüber den in meine aufsichtsbehördliche Zuständigkeit fallenden bundesunmittelbaren gesetzlichen Krankenkassen ausgesprochen habe. (Exkurs: aufgrund der förderalen Zuständigkeit der Datenschutzaufsicht bin ich „nur“ für GKK zuständig, die in mehr als zwei Bundesländern tätig sind. Das sind allerdings 2/3 der gesetzlich Versicherten) Worum geht es?

Dokumente werden nach einem festgelegten Schema in der elektronischen Patientenakte abgelegt. In der ersten Phase 2021 gab es nur zwei Fächer. Dokumente aller Leistungserbringer, d.h. aller Ärzte, Ärztinnen, Zahnärzte, Zahnärztinnen, Therapeutinnen und Therapeuten sowie aller Krankenhäuser und Kliniken kommen gesammelt in ein Fach. Dokumente, die Versicherte selbst einstellen, in ein zweites Fach.

Die Dokumente im Leistungserbringerfach sind besonders wichtig. Sie stammen vom Hausarzt, der Hausärztin, vom Kardiologen oder vom Krankenhaus oder der Reha-Klinik. Diese sind als Einstellende auch nachweisbar. Für jedes Dokument kann auch nachgewiesen werden, dass es nicht verändert wurde und von wem es stammt.

Dokumente im Versichertenfach haben diese Eigenschaft nicht. Zwar können Versicherte natürlich auch ärztliche Dokumente einscannen und in der elektronische Patientenakte digitalisieren. Es ist aber nicht mehr nachweisbar, ob sie unverändert sind oder überhaupt vom Leistungserbringer stammen.

Wo sah nun der Bundesdatenschutzbeauftragte den Missstand beim Berechtigungsmanagement?

Als Versicherter konnte ich jedem Arzt in 2021 nur eine Berechtigung für ein ganzes Fach erteilen. Ich konnte meinem Arzt nicht nur einzelne Dokumente zuweisen. Ich konnte auch nicht einzelne Dokumente ausschließen. Die Zugrifferlaubnis erstreckte sich immer auf das komplette Fach. Das heiß, jeder zugelassene Arzt oder Therapeut sah alles oder gar nichts. Um es deutlich zu machen: der Physiotherapeut hatte dann auch Zugang etwa zu den Dokumenten, die vom Gynäkologen oder vom Zahnarzt stammen. Brauchte der Physiotherapeut dies? Das kritisierte ich unter dem Schlagwort „Alles-oder-nichts-Prinzip“.

Die Schutzbehauptung des damaligen Gesundheitsministers und der Kassenärzte-Funktionäre, die Versicherten könnten Dokumente ja in Ihr Fach auslagern, um diese zu schützen, war und ist schlichtweg falsch. Damit ist sie quasi gelöscht und kann nicht wieder eingestellt werden. Sie erinnern sich? Die Dokumente aus dem Versichertenfach sind nicht mehr gesichert gegen Veränderung und keinem Einstellenden mehr sicher zugeordnet.

Weder aus Sicht der Versicherten noch der Leistungserbringer ist so eine ausschließliche Pauschalfreigabe fachlich sinnvoll. Natürlich ist es in vielen Situationen – z. B. gegenüber einem Hausarzt – sinnvoll, möglichst viele Informationen zur Verfügung zu stellen. Und ich sage das ganz offen: die Grundeinstellung meiner ePA, wenn ich sie dann verwenden werde, wird voller Zugriff für alle Ärztinnen und Ärzte meines Vertrauens sein Es gibt aber auch Situationen, in denen eine dokumentengenaue Steuerung nötig ist. Versicherte wollen vielleicht eine psychiatrische Behandlung ihrem Zahnarzt nicht bekannt machen.

Verstärkend kommt hinzu, dass Berechtigungen für bis zu 18 Monate oder sogar unbegrenzt gültig sind und somit das Tor zum gesamten Dokumentenbestand lange offen steht. Allerdings dürfen die Leistungserbringer legal nicht jederzeit auf alle Daten zugreifen: Das Gesetz formuliert explizit den schon in der Datenschutz-Grundverordnung verankerten Grundsatz der Zweckbindung: Der Zugriff ist mit Einwilligung der Versicherten nur zulässig, soweit er für die Versorgung erforderlich ist. So weit, so gut, aber: der Versicherte kann nicht überprüfen, ob sich der Arzt, Therapeut oder das Krankenhaus daran hält.

Das „Alles-oder-nichts-Prinzip“ war auch schlicht nicht zeitgemäß. Wir wissen alle, dass eine dokumentengenaue Zugriffsfreigabe am Markt Standard und damit technisch auch leicht möglich ist. Da fallen mir viele Alltagsbeispiele ein, vom Betriebssystem über Cloudspeicher bis zum Teilen von Fotos in sozialen Netzwerken. Aber auch Hersteller medizinischer Software betonen, dass ihre Software sogenannte feingranulare Berechtigungen zulässt.

Das „Alles oder nichts Prinzip“ widerspricht der Datenschutz-Grundverordnung. Die Datenschutz-Grundverordnung definiert in Artikel 5 die Grundsätze, die eingehalten werden müssen, wenn Daten verarbeitet werden. Nach Artikel 25 Datenschutz-Grundverordnung müssen Verantwortliche – also hier die Krankenkassen – geeignete Maßnahmen ergreifen, um diese Grundsätze auch umzusetzen. Ein feingranulares, dokumentengenaues Berechtigungsmanagement ist eine solche Maßnahme. Es sorgt dafür, dass nur die notwendigen Dokumente „geteilt“ werden und alle anderen eben verborgen bleiben. Das entspricht den Grundsätzen der Rechtmäßigkeit, der Datenminimierung, der Erforderlichkeit und Zweckbindung sowie der Vertraulichkeit.

Erst seit dem 1. Januar diesen Jahres gibt es die Möglichkeit, dokumentengenaue Berechtigungen zu vergeben. Aktuell wird die neue Version ausgerollt.

Allerdings haben diese Möglichkeit nur die Nutzer der elektronische Patientenakte-App auf einem Smartphone oder einem Tablet. Fast alle anderen können das nicht (erste Ausnahmen KNAPPSCHAFT + weitere KK).

Das bringt mich zu meinem zweiten großen Kritikpunkt:

2. Benachteiligungen für Frontend-Nichtnutzer, d.h. für Menschen, die kein geeignetes Smartphone oder Tablet haben

Die elektronische Patientenakte als Akte existiert ganz ohne eine „App“. Sie ist zunächst lediglich das Aktensystem „in der Telematikinfrastruktur-Cloud“. Versicherte können sie bei ihrer Krankenkasse beantragen und sie z.B. bei ihrem Hausarzt ersteinrichten lassen. Der ist auch verpflichtet, auf Wunsch des Versicherten medizinische Daten aus der Behandlung in die elektronische Patientenakte zu kopieren. Bei einem weiteren Arztbesuch können diese Daten dann aus der elektronische Patientenakte freigegeben werden. Dazu stecken die Versicherten ihre elektronische Gesundheitskarte in das Kartenlesegerät und bestätigen die Freigabe mit ihrer PIN.

Zusätzlich stellen die Krankenkassen den Versicherten eine elektronische Patientenakte-App zur Verfügung. Versicherte, die die App nicht nutzen wollen oder können, werden als Frontend-Nichtnutzer bezeichnet.

Eine ganze Reihe von Funktionen dieser App bilden elementare Einsicht- und Kontrollrechte bzgl. der elektronischen Patientenakte ab. Zunächst ist das Berechtigungsmanagement zu sehen, über das ich schon vorher berichtet habe. Ohne App können Versicherte vor Ort in Praxis oder Krankenhaus am Kartenterminal ab 2022 lediglich „mittelgranular“ freigeben. Dazu werden Kategorien von Dokumenten gebildet. Auf diese Kategorien beziehen sich dann die Berechtigungen.

Eine dokumentengenaue Steuerung ist vor Ort in der Praxis nicht möglich. Ein konkreter Zeitpunkt für die Einführung von feingranularem Berechtigungsmanagement vor Ort in der Praxis wurde im Gesetzgebungsverfahren aus dem Entwurf gestrichen. Trotz meiner expliziten Warnung, dass dieser Schritt zu einem europarechtswidrigen Zustand führen wird. Obwohl es keine technischen Gründe für diesen Schritt gab.

Die nächste wichtige Funktion, die ohne App nicht genutzt werden kann, ist die Protokolleinsicht. Die elektronische Patientenakte protokolliert alle Zugriffe und Zugriffsversuche. Um Missbrauch aufzudecken ist es wichtig, dass ich selbst nachvollziehen kann, wer auf meine Akte zugegriffen hat. Berechtigungen werden an die ganze Institution (etwa eine Gemeinschaftspraxis oder eine Praxisgemeinschaft[1] oder das Krankenhaus) vergeben und sind ab 2022 auch in ihrer Dauer nicht begrenzt. Vielleicht habe ich ja einige Berechtigungen vergessen, die ich vor längerer Zeit vergeben habe? Auch eine Übersicht über die vergebenen Berechtigungen erhalte ich nur mit der App.

Selbst die fundamentale Funktion, Einsicht in die eigene Akte zu nehmen, setzt also die Nutzung der App voraus. Als Frontend-Nichtnutzer weiß ich also nicht mal, welche Dokumente in meiner elektronische Patientenakte liegen. An der Stelle kann man sich fragen, ob Versicherte nicht einfach von ihrem Auskunftsrecht nach

[1] Im Unterschied zu einer Praxisgemeinschaft, die sich nur die gemeinsamen Praxisräume und ggf Personal teilt (Kostengemeinschaft), aber ansonsten eigenständig sind und getrennt abrechnen, ist eine Gemeinschaftspraxis (heute Berufsausübungsgemeinschaft) in der Regel als Gesellschaft bürgerlichen Rechts (GbR) oder als Medizinisches Versorgungszentrum (MVZ) organisiert und bildet eine Abrechnungsgemeinschaft.

Datenschutz-Grundverordnung Gebrauch machen könnten. Die Krankenkassen können und dürfen die Verschlüsselung der Daten aber nicht aufbrechen – auch nicht im Rahmen einer Auskunft. Und diese technische Designentscheidung ist richtig. Diese starke Verschlüsselung befürworte ich. Sie soll auch zu Auskunftswecken nicht aufgeweicht werden.

Das heißt zusammengefasst, dass Nutzenden ohne Frontend, d.h. ohne geeignetes Smartphone oder Tablet, bisher elementare Funktionen zur Wahrnehmung ihrer Kontrollrechte nach der Datenschutz-Grundverordnung nicht zur Verfügung stehen. Neben Menschen, die kein aktuelles Smartphone besitzen, gibt es auch Menschen, die mit gutem Recht ablehnen, ihre Gesundheitsdaten auf ihrem Smartphone zu verarbeiten.

Nun kann man einwerfen, dass das dann wohl nicht zusammenpasst: Vorteile der Digitalisierung nutzen wollen und gleichzeitig Ablehnung der Smartphone-Nutzung für Gesundheitsdaten.

Da bin ich anderer Meinung: Aus grundsätzlichen ethischen, aber auch aus technischen Gründen: Tatsächlich gib es schon eine Lösung, die zumindest die gröbste Ungleichbehandlung mindern könnte. Der Gesetzesentwurf sah eigentlich ein Frontend für spezielle gesicherte (sprich konfigurierte) Tablets vor, das nahezu alle Funktionalitäten der elektronische Patientenakte-App geboten hätte. Dort hätten Versicherte – z.B. in den Geschäftsstellen der Krankenkassen – innerhalb einer gesicherten Umgebung Einblick in elektronische Patientenakte und

Protokoll nehmen können. Übrigens wäre dort auch das dokumentengenaue Berechtigungsmanagement möglich gewesen.

Diese Lösung mithilfe von sogenannten „Terminals“ ist dann in letzter Minute aus dem Gesetzentwurf gestrichen worden, wohl auf Druck der Krankenkassen-Lobbyisten, wie mir berichtet wurde. Stattdessen gibt es nun ab 2022 die Vertreterlösung, mit der ein Versicherter einen mit Smartphone ausgestatteten Vertreter mit der Frontend-Nutzung seiner elektronischen Patientenakte beauftragt. Das ist sicherlich für viele Situationen eine sinnvolle Lösung. Allerdings muss trotzdem jede und jeder die Möglichkeit haben, seine Rechte wahrzunehmen, ohne einem Dritten den vollen Zugang zu seiner elektronische Patientenakte und damit allen seinen Gesundheitsdaten zu geben. Im Übrigen hilft diese Vertreterlösung Personen, die keine Gesundheitsdaten auf privaten Endgeräten im Internet und auf Betriebssystemen mehr oder weniger vertrauenswürdiger Anbieter verarbeiten wollen, überhaupt nicht.

3. Authentisierungsverfahren ohne elektronische Gesundheitskarte

Mein dritter Kritikpunkt ist die Umsetzung des alternativen Authentifizierungsverfahrens. Der Gesetzgeber wollte zusätzlich neben der elektronischen Gesundheitskarte ein anderes Authentisierungsmittel zulassen. Schon mit dem Terminservice- und Versorgungsgesetz (TSVG) aus dem Mai 2019 wurde die rechtliche Grundlage für einen Zugang zur elektronischen Patientenakte ohne elektronische Gesundheitskarte geschaffen.

Diese rechtliche Grundlage wurde mit dem Patientendaten-Schutz-Gesetz im Fünften Buch Sozialgesetzbuch konkretisiert.

Das Gesetz gibt als Voraussetzung für den Zugriff ohne Einsatz der elektronischen Gesundheitskarte an, dass sich der Versicherte „jeweils durch ein geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet, authentifiziert hat“.

Ich habe diese Regelung als zu unspezifisch kritisiert. Der eigentliche Mangel liegt allerdings nicht im Gesetz, sondern in der konkreten Ausgestaltung des Verfahrens. Im Unterschied zu den zwei vorherigen Punkten ist dieser Missstand nicht unmittelbare Folge des Gesetzestexts.

Die gematik (also der mehrheitlich im Bundesbesitz befindliche IT-Dienstleister hinter der Gesundheits-TI) beschreibt ein Verfahren, das sie „Alternative Versichertenidentität“ (kurz: Al.VI) nennt. Hier wird für die Versicherten eine zweite kryptografische Identität erzeugt. Diese existiert zusätzlich zur kryptografischen Identität auf der elektronischen Gesundheitskarte. Dieses Verfahren entspricht einer Fernsignatur, das kryptografische Identitätsmaterial wandert aus der Hardware des Nutzers zum entfernten Dienst. Dann fallen wichtige Sicherheitsleistungen, die sonst in der elektronischen Gesundheitskarte gekapselt sind, nun in die Verantwortung der Frontendhersteller.

Bereits im Mai 2019 nach der ersten Vorstellung des Verfahrens habe ich zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) formuliert, dass dieses Verfahren nur für eine Übergangszeit geduldet werden kann. Das BSI hat Anforderungen entwickelt, die Identifizierungsverfahren für den Zugang zur Telematikinfrastruktur erfüllen müssen. Die gematik muss ein anderes Verfahren entwickeln, das all diesen Anforderungen entspricht. Bis dahin müssen die Versicherten genau über die Unterschiede der Authentisierung mit elektronische Gesundheitskarte oder mit Al.VI informiert werden.

Ich habe das alles etwas ausführlicher dargestellt, weil es für viele die erste Berührungsstelle mit der Digitalisierung im Gesundheitswesen ist und gleichzeitig die Probleme beispielhaft darstellt. Unnötiger Verzicht auf Maßnahmen zum Schutz der Gesundheitsdaten, die die Funktionalität gar nicht gemindert hätten. Faulheit oder Verspätung bei Maßnahmen der IT-Sicherheit und der Zulassung, die dann auch zu ungeschützten Servern mit CT- und MRT-Bildern im Netz oder Gesundheitsanwendungen führen, die die erhaltenen Daten munter mit Internetkonzernen und Datenhändlern teilen.

Alles das müsste nicht sein. Man kann bei der Digitalisierung des Gesundheitswesens ein Sicherheits- und ein Datenschutzniveau erreichen, dass dem in der analogen Welt ebenbürtig ist und gleichzeitig neue Möglichkeiten zur Behandlung und Versorgung öffnet.

III. Das eRezept

Seit dem 1. Januar 2022 müssen ärztliche Verordnungen elektronisch über die Telematikinfrastruktur (TI) übermittelt werden. Das sogenannte E-Rezept ist damit die erste medizinische digitale Pflichtanwendung überhaupt.

Rezepte im Rahmen der vertragsärztlichen Versorgung sollen immer in einem zentralen Speicher in der TI abgelegt werden. Patientinnen und Patienten können dann nur wählen, ob sie die Zugangsinformationen dazu in elektronischer Form oder – nach dem Vorbild eines Bahn- oder Flugtickets – als Papierausdruck mit einem Code-Block zur Einlösung in einer Apotheke ausgehändigt bekommen wollen.

Wie bei der ePA wird es auch beim E-Rezept eine Zweiklassengesellschaft geben. Menschen, die nicht die E-Rezept-App nutzen möchten oder können, erhalten keinen unmittelbaren Einblick in die über sie gespeicherten Daten oder erfolgten Zugriffe auf ihre Rezepte.

Zur Authentisierung in der E-Rezept-App gegenüber dem E-Rezept-Server sieht das Gesetz kein alternatives Verfahren ohne elektronische Gesundheitskarte (eGK) vor. Nutzende werden deshalb ihre eGK über Near Field Communication (NFC) mit dem Endgerät verbinden. Hierbei werden die Daten kontaktlos über eine kurze Strecke von wenigen Zentimetern ausgetauscht, Sie kennen das von dem berührungslosen Zahlen mit Kredit- und EC-Karten.

Im Rahmen der Einführung der Anwendung E-Rezept wird in der TI dazu ein Identity Provider aufgebaut, ein Dienst der zunächst nur für das E-Rezept - später potentiell für alle Anwendungen der TI - das Authentisieren der Nutzenden übernimmt und die Identifizierung bestätigt. Somit soll das zentrale Thema Authentisierung aus den Anwendungen ausgelagert werden.

Dies ist für die Einführung und Sicherheitsbewertung von Authentisierungsmitteln von Vorteil. Um diese Vorteile datenschutzkonform zu nutzen, fordere ich, dass die Prozesse zur Einführung von Authentisierungsmitteln im Vorfeld für die gesamte TI und alle Anwendungen darauf entwickelt und die Kriterien der Einstufung der Sicherheitsniveaus transparent festgelegt werden. Eine so zentrale Funktionalität für die Sicherheit der TI und der Gesundheitsdaten muss auch übergreifend geregelt werden und darf nicht bloß ein Annex bei der E-Rezept-Entwicklung sein.

Beim E-Rezept findet auch ein weiterer Paradigmenwechsel statt: Die gematik entwickelt die E-Rezept-App und wird sie zur Verfügung stellen. Die Aufgabe der gematik beschränkt sich demnach nicht, wie z.B. bei der ePA, auf die Erstellung von Spezifikationen und Sicherheitsanforderungen, nach denen Hersteller Komponenten oder Dienste der TI anzubieten haben. Die gematik wird selbst zum Hersteller und damit übrigens auch datenschutzrechtlich verantwortlich.

Dies hat aber auch zur Folge, dass die gematik ihre eigenen Entwicklungen zu prüfen und zuzulassen hat. Insoweit besteht zumindest die Gefahr einer potentiellen Befangenheit.

Im Rahmen der Gesetzesberatungen konnten wir zumindest erreichen, dass ein externes Sicherheitsgutachten von der gematik zu beauftragen ist und dieses durch das Bundesamt für Sicherheit in der Informationstechnik(BSI) geprüft und bestätigt werden muss, bevor die App in Betrieb gehen darf.

Die Verfügbarkeitsanforderungen an das E-Rezept sind natürlich sehr hoch und ebenfalls von zentraler Bedeutung. Während der Konzeption hatte ich für eine dezentrale Lösung plädiert. Diese hätte gegen Ausfälle zentraler Dienste robuster ausgestaltet werden können. In der Abwägung – u. a. mit dem Schutz vor Manipulation und Rezepthandel – hat sich letztlich die geltende spezifizierte zentrale Lösung durchgesetzt.

In allen angesprochenen Aspekten zeigt sich die Wichtigkeit der von mir wiederholt und frühzeitig geäußerten Forderung, die zentralen Aspekte der Anwendung E-Rezept im Gesetz zu verankern. Der Gesetzgeber muss für eine Pflichtanwendung wie das E-Rezept selbst zentrale Entscheidungen treffen und Leitplanken im Gesetz vorgeben, ohne sich auf eine spezifische Technik festzulegen.

Bedauerlicherweise wurde dies nicht umgesetzt, so dass zentrale Fragestellungen nunmehr nachgelagert, insbesondere im Rahmen der technischen Spezifikationen, von der gematik entschieden werden. Im Gesetz fehlen u. a. Regelungen zur Zweckbindung, zur Datenspeicherung und zu technischen Grundsätzen und Kontrollmöglichkeiten für alle Versicherten. Damit - und vor dem Hintergrund der herausragenden Bedeutung der Anwendung für die Versorgungssicherheit - sind die Regelungen zur Einführung der elektronischen Verordnung nicht hinreichend.

Lediglich in Bezug auf die Normierung einer Regelung zur Speicherdauer der E-Rezepte ist der Gesetzgeber meinem Petitum gefolgt. Auch die konkrete Gestaltung der Anwendung E-Rezept muss sich aber an den Vorgaben der DSGVO messen lassen. Mein Prüfschwerpunkt im Einsatz des E-Rezepts wird neben den Maßnahmen zur Sicherheit der Daten daher auch die Sicherstellung der Verfügbarkeit und der Kontrollmöglichkeiten sein.

IV. Erstattungsfähige digitale Gesundheitsanwendungen

Bereits seit Oktober 2020 regelt das Digitale Versorgungsgesetz, dass die Krankenkassen die Kosten für genehmigte, zertifizierte, digitale Gesundheitsanwendungen (DIGA) übernehmen – die Gesundheits-App auf Rezept sozusagen.

Die Prüfung und Zertifizierung der DIGA erfolgt beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). Dieses prüft, ob die DIGA die gesetzlich festgelegten Anforderungen an Sicherheit, Funktionstauglichkeit, Qualität, Datenschutz und Datensicherheit erfüllen und nachweislich einen positiven Versorgungseffekt erbringt. Die DIGAs sollen bei der Behandlung unterstützen oder der Früherkennung dienen, bei der Überwachung etwa von Medikamenteneinnahmen helfen, kurz: zur Verbesserung des Krankheitszustands beitragen. Eine Liste der zugelassenen DIGAs finden Sie auf der Internetseite des BfArM, eine Bonner Bundesbehörde übrigens.

Aus datenschutzrechtlicher Sicht waren wir bisher nicht zufrieden mit der Ausgestaltung der datenschutzrechtlichen Prüfung der DIGAs, denn die besteht zur Zeit nur aus einer Selbsterklärung des Herstellers, dass die DSGVO eingehalten wird. Ab dem nächsten Jahr wird eine Nachweisführung mittels eines Datenschutzzertifikats nach § 42 DSGVO ersetzt. Die Prüfkriterien für dieses Zertifikat werden aktuell vom BfArM, dem BSI und meiner Behörde erarbeitet.

V. Die Corona-Warn-App

Und nun mal zu etwas wirklich Positiven: die Corona Warn App. Sie ist die weltweit erfolgreichste Corona-App. Über 43 Millionen Downloads gibt es inzwischen, die Zahl der Warnmeldungen liegt bei knapp 47 Mio. und die Zahl der bereitgestellten Testergebnisse bei über 153 Mio. Evaluierungen gehen davon aus, dass über die Hälfte aller Personen, die sie einsetzen könnten (Alter, Smartphone), sie auch aktuell nutzen.

Die CWA hat im wahrsten Sinne des Wortes klein angefangen, viel mehr als zu warnen, wenn man längere Zeit neben einem Infizierten gestanden hat und dieser seine festgestellte Infektion auch an die App gemeldet hat, konnte sie zu Beginn nicht. Inzwischen wird sie auch zur Event-Registrierung, als digitales Impfzertifikat und als Speicher für das jeweils letzte Covid-Testergebnis verwendet. Und anders als in den ersten Monaten der App melden die Infizierten dies auch wirklich in großer Zahl an die App, weil es einfacher geworden ist. Übrigens: Wäre man unseren Vorschlägen gefolgt, wäre das Teilen eines positiven PCR-Tests noch viel einfacher. Leider hat sich der letzte Deutsche Bundestag dagegen entschieden, auch auf Wunsch des damaligen Bundesgesundheitsministers.

Wie funktioniert die App?

Die App nutzt das Protokoll Exposure Notifications (GAEN) von Google und Apple. Damit ist es dem Mobiltelefon möglich, in regelmäßigen Abständen im Gerät generierte Zufallsschlüssel (also eine Zahlenfolge) per Bluetooth in die Umgebung auszusenden und zu empfangen. Diese Schlüssel sind pseudonym und können ohne weitere Informationen aus sich heraus nicht einer konkreten Person zugeordnet werden.

Werden die Schlüssel von einem anderen Gerät empfangen, speichert dieses die Daten lokal auf dem Gerät selbst für 14 Tage. Anhand von Signalstärke und Dauer der Verbindung ermittelt das Gerät das Risiko einer Infektion. Dies ist keine perfekte Technologie, um eine mögliche Infektion einzuschätzen, aber die am wenigsten schlechte. Mobilfunkdaten und GPS-Daten sind wesentlich ungeeigneter, egal, was manche Philosophen, Ministerpräsidenten und Chefredakteure dazu meinen. Da würde man sich dringend mehr technischen Sachverstand wünschen.

Zudem kann über die App inzwischen das Ergebnis eines Covid-Tests übermittelt werden, wenn dies bei der Testung vom App-Nutzenden gewünscht und das testende Labor an die Infrastruktur der App angeschlossen ist. Hierbei können auf freiwilliger Basis auch Symptome angegeben werden. Diese unterstützen den Algorithmus der App beim Berechnen der Infektionswahrscheinlichkeit. Andere Nutzende erhalten jedoch keinerlei Angabe zu den gemeldeten Symptomen.

Erhält ein Nutzer ein positives Testergebnis, kann er dieses über die CWA „bekannt“ geben. Dann sendet die App den zufällig generierten Schlüssel des Gerätes als „infiziert“ an alle anderen App-Nutzenden. Deren CWA prüft dann, ob der Schlüssel in der 14-tägigen Kontaktliste auftaucht und informiert gegebenenfalls den App-Nutzenden auf Basis der oben dargestellten Parameter.

Ich bin felsenfest davon überzeugt, dass der Erfolg dieser App ganz wesentlich darin begründet ist, dass sie so datenschutzfreundlich gestaltet ist und Vertrauen geschaffen hat. Die ersten Pläne des Bundesgesundheitsministeriums sahen noch ganz anders aus und wurden binnen kürzester Zeit von Fachleuten scharf kritisiert. Das Umdenken in Richtung dezentrale und datenschutzfreundliche App-Entwicklung war den entscheidende Erfolgsfaktor und ich kann denjenigen meiner Mitarbeiterinnen und Mitarbeiter, die in den ersten drei Entwicklungsmonaten der App die Beratung der Entwicklerfirmen und des RKI übernommen haben, auch heute noch nur Dank und Anerkennung zollen, weil sie genau wie die Entwickler Tag und Nacht durchgearbeitet haben.

Ich will hier an dieser Stelle auch kurz einmal etwas zu den angeblich so viel erfolgreicheren asiatischen Corona-Apps sagen, die immer wieder angeführt werden, vor allem von den schon genannten Philosophen, Ministerpräsidenten (ja, nur die Männer) und Chefredakteuren (auch da nur Männer). Japan, Taiwan und Südkorea werden da immer als Beispiele genannt, wo der Datenschutz, angeblich anders als in Deutschland, keine besseren Corona-Tracing-Apps verhindern würde.

Kurzer Faktencheck:

Japan nutzt beispielsweise exakt die gleiche Technologie wie die CWA.

Taiwan hat gar keine App zur Kontaktverfolgung, sondern nutzt ein modernes System für das Management der Kontaktverfolgung bei den Gesundheitsämtern.

Südkorea nutzt eine GPS-basierte App, allerdings nicht zur Kontaktermittlung im Sinne der CWA und anderer europäischer Warn-Apps, sondern als eine Art elektronische Fußfessel zur Überwachung von Quarantänevorgaben (wie auch z. B. in China). Dort gibt es übrigens auch keine oder kaum Maskenverweigerer, Corona-Leugner, Impfgegner oder sonstige Post-Aufklärungs-Tendenzen

VI. Das digitale Covid-Zertifikat der EU

Ursprünglich ging es dabei um Reiseerleichterungen auf europäischer Ebene. Am Ende standen datenschutzfreundliche Nachweise der Covid-19-Zertifikate im Alltag. Datenschutzfreundlicher übrigens als jede denkbare nicht-digitale Lösung.

Am 17. März 2021 hat die EU-Kommission einen Verordnungsentwurf zum Digital Green Certificate vorgelegt. Die EU-VO soll grenzüberschreitende Reiseerleichterungen für EU-Bürger und -Bürgerinnen während der Corona Pandemie innerhalb der EU ermöglichen.

Der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) haben hierzu am 31. März 2021 eine gemeinsame Stellungnahme (Joint Opinion) verabschiedet. Demnach sollte jede auf nationaler Ebene oder auf EU-Ebene erlassene Maßnahme, die die Verarbeitung personenbezogener Daten beinhaltet, im Einklang mit den allgemeinen Grundsätzen der Wirksamkeit, Notwendigkeit und Verhältnismäßigkeit stehen. Außerdem sollten die Datenverarbeitungen auf einer angemessenen Rechtsgrundlage in den Mitgliedstaaten basieren. Gleichzeitig ersuchten der EDSA und der EDSB die EU-Kommission klarzustellen, dass die Mitgliedstaaten alle drei Arten von Zertifikaten (geimpft, genesen oder getestet) akzeptieren sollten. Sollten sie dies nicht tun, läge eine Diskriminierung aufgrund von Gesundheitsdaten und somit eine Verletzung der Grundrechte vor.

Die Verordnung über das digitale COVID-Zertifikat der EU ist am 1. Juli 2021 in Kraft getreten. Drei Zertifikate werden definiert: Impfung, Test und Genesen. Die Mitgliedstaaten müssen die Zertifikate in Papierform und digital anbieten. Die Verwendung der Zertifikate ist freiwillig. Sie sind diskriminierungsfrei, da sie keine Reisebeschränkungen in Europa schaffen, sondern vielmehr den grenzüberschreitenden Verkehr für die Inhaber erleichtern, indem gegebenenfalls auf weitere Maßnahmen der einzelnen Mitgliedstaaten während der Corona Pandemie (z. B. Quarantäneregelungen) verzichtet werden kann. Es findet weder Tracking (zeitgleiche Nachverfolgung) noch Tracing (nachträgliche Nachverfolgung) statt. Die Zertifikate dienen der Authentifizierung sowie der Feststellung des Status der Inhaber beim Grenzübertritt. Personenbezogene Daten werden von den kontrollierenden Stellen nicht gespeichert.

Die Verordnung und damit die Zertifikate sind zeitlich befristet. Sobald die WHO die Corona-Pandemie für beendet erklären wird, setzt die EU-Kommission die Verordnung mit einem legislativen Akt außer Kraft. Die Verordnung selbst erlaubt die Nutzung der Zertifikate lediglich zu einem Zweck – die Erleichterung der Reisefreiheit.

Sie eröffnet den Mitgliedstaaten zusätzlich die Möglichkeit einer weiteren Nutzung (z. B. Zugang zu Veranstaltungen, öffentlichen Einrichtungen etc.). Davon hat der deutsche Gesetzgeber Gebrauch gemacht und ebenfalls zeitlich befristete Regelungen im Infektionsschutzgesetz getroffen, beispielsweise für den Zugang von Einrichtungen des Gesundheits- und Sozialwesens, des Nah- und Fernverkehrs oder im Hotel- und Gaststättenbereich.

In Deutschland werden die Zertifikate im Auftrag des Robert Koch-Instituts (RKI) technisch generiert. Dabei werden keine Daten gespeichert. In der CovPassApp und der Corona-Warn-App können die Zertifikate angezeigt werden. Eine Kontrolle der Gültigkeit der Nachweise kann mit der CovPassCheck-App erfolgen.

VII. SORMAS

Um endlich von Papier und Fax zu einer effizienten und datenschutzkonformen digitalen Kontaktnachverfolgung in den Gesundheitsämtern zu kommen, wurde dort SORMAS installiert. Ganz nebenbei: Anders als öffentlich behauptet, hassen wir Datenschützer Fax, wir hassen es abgrundtief. Die Medienbrüche sorgen für falsche Daten, für Verzögerungen, für mangelnde Protokollierung von Zugriffen, die Faxe fliegen durch die Gegend und sind nicht vor Einblicken geschützt.

In einer Welt von IP-basierten Telekommunikationsnetzen ist nicht gesichert, wer und wo die Gegenstelle ist. Verbrennt die Faxe, zerschlagt die Fax-Maschinen ☺

Bei der Software SORMAS handelt es sich um ein Kontaktpersonen-management im Rahmen der SARS-CoV-2- Pandemie. Die Gesundheitsämter sollen durch die Software bei der Identifizierung und Überwachung von Kontaktpersonen unterstützt werden, indem Symptomangaben von Kontaktpersonen ohne telefonische Rückfragen erfasst und Daten zu Fallmeldungen mit anderen Gesundheitsämtern ausgetauscht werden können. Neben dem digitalen Empfang von Labormeldungen sollen darüber hinaus auch Falldaten digital an die Landesbehörden gemeldet werden. Bereits auf der Ministerpräsidentenkonferenz am 16. November 2020 wurde der bundesweite Einsatz von SORMAS in den Gesundheitsämtern beschlossen.

In Abstimmung mit den beteiligten Datenschutzaufsichtsbehörden der Länder habe ich nach gemeinsamer Erörterung der eingereichten Unterlagen im Januar 2021 einem Betrieb von SORMAS-X in den Gesundheitsämtern unter Vorbehalt zugestimmt.

Voraussetzung dafür war eine schriftliche Zusicherung, dass die Unterlagen im laufenden Betrieb nachgebessert und vervollständigt werden. Das sollte ermöglichen, im Zuge der Risikobewertung Risiken zu erkennen und nötige technische und organisatorische Maßnahmen zu ergreifen. Dieses sollte schnellstmöglich unter Einsatz hinreichender Ressourcen erfolgen.

Die Datenschutzfolgeabschätzung wurde nur als Entwurf vorgelegt. Nötig war auch ein Kryptographiekonzept. Die Beratung wurde ab Juli 2021 noch einmal intensiviert und eine Arbeitsgruppe unter meiner Beteiligung und der mehrerer Landesdatenschutzbeauftragten eingerichtet. Hintergrund war, dass die Fortschritte seitens des Helmholtz-Zentrum für Infektionsforschung (HZI) über einen längeren Zeitraum nicht den Erwartungen entsprachen, die die Landesbeauftragten und ich an ein solches Projekt gestellt haben.

Wie Sie vielleicht am Wochenende gelesen haben, gibt es nach wie vor große Probleme in den Gesundheitsämtern mit der Software. So bricht das System wohl regelmäßig zusammen, wenn viele Mitarbeiterinnen und Mitarbeiter gleichzeitig die Daten eingeben und erfassen wollen. Dass dies in den letzten Woche bei der sehr hohen Zahl von Neuinfektionen regelmäßig passierte, führte dies – verständlicherweise – zu Frust bei den Mitarbeiterinnen und Mitarbeitern und zum Datenstau auf den Schreibtischen. Die Landesregierung NRW erwägt deshalb bereits, SORMAS wieder von den Rechnern der Gesundheitsämter zu verbannen, jedenfalls aber die verpflichtende Nutzung aufzuheben.

Was wir aber dringend brauchen, nicht nur für diese Pandemie: Einen schnellen digitalen Meldeweg zwischen allen beteiligten Ebenen. Eine sichere digitale Erfassung, die sich mit anderen Daten verknüpfen lässt. Die Zeit von Einzellösungen in jeder Kommune und Faxen müssen wir hinter uns lassen. Deutschland ist hier nicht für die Zukunft und zukünftige Gefährdungen gewappnet. Wir schöpfen die digitalen Chancen nicht aus.

VIII. Zum Schluss

Wie ich schon am Anfang sagte, ich bin ein großer Freund digitaler Anwendungen, die uns Dinge erleichtern, die helfen, erinnern, einordnen, Muster erkennen oder unterstützen. Forschung auf Gesundheitsdaten ermöglicht bessere Versorgung, zielgenauere Diagnostizierung und neue Behandlungsmethoden.

Und daher sage ich in fast jeder meiner Reden den gleichen Satz: Datenschutz muss bei der Entwicklung neuer Anwendungen, Software oder Apps immer von Anfang an mitgedacht und „eingebaut“ werden. Nur so lassen sich teure, nachträgliche Reparaturen und Ergänzungen verhindern. Und nur dann können die Menschen genügend Vertrauen in diese Anwendungen entwickeln, um sie dann auch tatsächlich zu nutzen.

Ich habe eine Reihe von Beispielen aus dem Bereich „Wir digitalisieren das Gesundheitswesen“ vorgestellt, dabei trotzdem nur die Oberfläche angekratzt und dabei hoffentlich deutlich machen können, dass es mir und meiner Behörde nicht darum geht, irgendeine dieser Entwicklungen zu verhindern oder zu verbieten.

Im Gegenteil, wir sind überzeugt, dass digitale Lösungen oft viel datenschutzfreundlicher, ja sogar – so absurd das klingt – datensparsamer sind als analoge, aber sie müssen eben gut gemacht sein. Und gut werden sie in aller Regel nur, wenn der Datenschutz von Anfang an mit drin steckt.

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf Nachfragen und Kommentare und Anregungen.