Stellungnahme zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Drucksache 19/18792)

Prof. Dr. Dominique Schröder
Friedrich-Alexander-Universität
Erlangen-Nürnberg

Diese Stellungnahme entspricht meiner persönlichen Meinung und spiegelt nicht zwingend die Ansichten der Friedrich-Alexander-Universität Erlangen-Nürnberg wider.

https://dominique-schroeder.de

Inhaltsverzeichnis

1 Executive Summary

Der vorliegende Entwurf zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur weist aus meiner Sicht erhebliche Mängel im Bereich des Schutzes der Privatsphäre und der Selbstbestimmung von Patienten auf. Insbesondere sehe ich großen Nachbesserungsbedarf in folgenden Punkten:

- Die elektronische Patientenakte muss direkt mit einem feingranularen Zugriffskonzept für die medizinischen Daten ausgeliefert werden und nicht erst, wie aktuell geplant, nach einem Jahr.
- Der Zugriff von Krankenkassen auf medizinische Daten darf nur unter strengsten Auflagen erfolgen und ein direkter Zugriff auf die Rohdaten sollte nicht gestattet werden.
- Die Nutzung der medizinischen Daten im Forschungsdatenzentrum darf nur nach expliziter Freigabe (pro Zugriff) der Patienten erfolgen. Dabei muss sichergestellt werden, dass die Privatsphäre des Patienten und dessen Angehörigen gewahrt bleibt.
- Es muss ein formales Sicherheitskonzept zum Schutz der medizinischen Daten durch ein unabhängiges Gremium erstellt und jährlich aktualisiert werden. Basierend auf dem Konzept erfolgt die jährliche Evaluation durch Experten, die von diesem Gremium eingesetzt werden.

2 Einführung

Am 27.05.2020 fand die öffentliche Anhörung der Einzelsachverständigen zum Patientendaten-Schutz-Gesetz im Gesundheitsausschuss des Bundestags statt. In diesem neuen Gesetz sollen verschiedene Aspekte der fortschreitenden Digitalisierung des Gesundheitswesens rechtlich geregelt werden, wie zum Beispiel die elektronische Patientenakte, die Verarbeitung von medizinischen Daten der Patienten und die Gestaltung der Zugriffsberechtigungen. Im Zuge dieser Anhörung wurde ich als Einzelsachverständiger geladen und beziehe nun Stellung zu diesem Entwurf. Insgesamt sehe ich die Entwicklung der Digitalisierung als etwas Positives und bin der Meinung, dass ein entscheidender Mehrwert durch die Sammlung, Verknüpfung und Verarbeitung von medizinischen Daten erzeugt werden kann. Allerdings darf diese Entwicklung nicht zu Lasten der Privatsphäre von Individuen führen. Gerade in diesem Bereich sehe ich verschiedene Aspekte des Entwurfs eines Gesetzes zum Schutz elektronischer Patientendaten als sehr kritisch an. Zunächst erläutere ich, warum aus meiner Sicht medizinische Daten eines besondern Schutz bedürfen und diskutiere die einzelnen Aspekte des Gesetzes im Anschluss.

3 Medizinische Daten sind besonders schützenswert

Der Schutz von personenbezogenen Daten im Allgemeinen ist beispielsweise in der Charta der Grundrechte der Europäischen Union gemäß Art. 8 Abs. 1 verfestigt und schließt natürlich medizinischen Daten ein. Des Weiteren wird die Privatsphäre der Patienten durch das Recht der informationellen Selbstbestimmung gestärkt und das Grundrecht auf Integrität und Vertraulichkeit (persönlicher) informationstechnischer Systeme. Zwar schützen diese Gesetze bereits die Privatsphäre der Bürger, jedoch bedürfen medizinische Daten meiner Meinung nach einem besonderen Schutz, da das Interesse und die industrielle Verwertbarkeit dieser Daten deutlich höher ist als an allen anderen Daten. Dies wird unter anderem durch die jährliche Studie von IBM und dem Ponemon Institut belegt, die den wirtschaftlichen Schaden, und damit den Wert der Daten, nach einem Cyberangriff ermittelt. Die Studie zeigt, dass der Wert eines einzelnen Datenbankeintrags im medizinischen Bereich bei ca. 400USD liegt[1].

Medizinischen Daten beschreiben nicht nur den ist-Stand einer Person, sondern erlauben teilweise auch, Vorhersagen auf zukünftige Entwicklungen zu treffen. Leidet eine Person zum Beispiel an Übergewicht so ist die Wahrscheinlichkeit, dass diese Person an Begleiterkrankungen wie Bluthochdruck, Herzleiden oder Diabetes erkrankt, deutlich höher. Darüberhinaus lassen sich teilweise auch Vorhersagen über (direkte) Verwandte treffen. Heute wissen wir, dass dies der Fall bei der Preisgabe von Erbkrankheiten und der DNA ist. Was wir zukünftig aus den zusätzlichen Informationen noch ableiten können, kann heute kaum abgeschätzt werden. Aus diesem Grund halte ich eine pauschale Freigabe der Daten für nicht tragbar. Stattdessen

[1] https://www.ibm.com/security/data-breach

sollte der Patient bei jedem Zugriff erneut befragt werden und über den aktuellen Stand des Wissens verständlich aufgeklärt werden.

4 §217f Beauftragung eines Sicherheitsgutachters

Entwurf. Die Neufassung des §217f Absatz 4b sieht vor, dass alle zwei Jahre ein Sicherheitsgutachten in Benehmen mit dem BSI in Auftrag gegeben werden muss.

Stellungnahme. Ein einzelnes Sicherheitsgutachten kann nicht alle relevanten Aspekte der IT Sicherheit abdecken. Ausserdem ist dies ein sehr junges und dynamisches Gebiet, so dass eine Untersuchung nach zwei Jahren nicht ausreichend ist.

Forderung. Die Sicherheit sollte von einem umabhängigen Gremium analysiert werden. Dieses Gremium sollte aus unabhängigen Experten der IT Sicherheit, der Kryptographie und des BSIs bestehen. Im ersten Schritt sollte hier ein formales Sicherheitskonzept entwickelt werden, welches die Schutzziele präzise festlegt. Ohne eine solide Basis hierfür ist nicht klar, wann ein System als sicher und wann als unsicher gilt. Dieses Sicherheitskonzept muss jährlich auf seine Aktualität überprüft werden. Sind beispielsweise neue Angriffe auf ein System bekannt geworden, so müssen die Möglichkeiten von dem formalen Modell abgedeckt werden. Des Weiteren müssen die Sicherheit des Systems und alle Änderungen formal nachgewiesen werden (Stichwort beweisbare Sicherheit). Nach dieser formalen Analyse muss die Implementierung, also die Umsetzung des Systems, ebenfalls evaluiert werden. Dies geschieht typischerweise durch sogenannte “penentration test”. Alle verwendeten kryptographischen Komponenten des Systems müssen durch das BSI zertifiziert sein. Aus meiner Sicht müssen diese Punkte im Einvernehmen mit dem BSI und nicht nur im Benehmen getroffen werden, da rechtlich gesehen “im Benehmen” nicht bindend ist.

5 §342 Berechtigungskonzept

Entwurf. Der aktuelle Entwurf sieht eine zweistufiges Konzept zur Freigabe von medizinischen Daten in der elektronischen Patientenakte vor. Im ersten Jahr hat der Patient lediglich die Möglichkeit "alles" oder "nichts" freizugeben. Ein feingranuläres Konzept zur Freigabe der Daten wird erst ab dem zweiten Jahr verpflichtend.

Stellungnahme. Die stufenweise Realisierung der Zugriffsrechte halte ich für höchst problematisch, und es müssen aus meiner Sicht drei Aspekte beachtet werden: technische Realisierbarkeit, rechtliche und langfristige Aspekte.

1. Technisch halte ich die Umsetzung feingranularer Zugriffsstrukturen für ein gelöstes Problem. Diese Techniken werden nicht nur seit Jahrzehnten in verschiedenen Betriebssystemen umgesetzt, sondern sind auch ein wesentlicher Bestandteil von unterschiedlichen Datenbanken. Zum Beispiel können bei dem Datenbanksystem "PostgreSQL" genaue Zugriffsstrukturen festgelegt werden. Des Weiteren bedeutet eine schrittweise Umsetzung, dass diese Rechte nachträglich hinzugefügt werden. Nachträgliche Änderung sind immer sehr fehleranfällig was zum Verlust von sensitiven Daten führen kann und die Beseitigung dieser Fehler führt dann unweigerlich zum einen Anstieg der Kosten.
2. Als Kryptograph stelle ich mir hier die Frage, wie die eine pauschale Freigabe der Daten mit dem Recht auf informationelle Selbstbestimmung vereinbar ist. Natürlich möchte ich meinem Kieferorthopäden Zugriff auf die Röntgenbilder meines Zahnarztes geben, jedoch sehe ich nicht, warum ich damit auch die Freigabe einer potentiellen Krebserkrankung und/oder einer psychologischen Behandlung erteilt habe. Insbesondere wenn die zusätzliche Freigabe Informationen betrifft, die einen Rückschluss auf Dritte erlauben (z.B. Erbkrankheiten).
3. Ich bin der Meinung, dass die langfristigen Folgen für die Freigabe von diesen Daten für den einzelnen Patienten oftmals nicht absehbar sind. Dies folgt daraus, dass die Patienten nicht jede Erbkrankheit kennen und dass wir heute nicht abschätzen können, welche Informationen aus den Daten in den nächsten Jahrzehnten abgeleitet werden können. Und dies betrifft wieder nicht nur einen einzelnen Patienten, sondern auch die (nahen) Angehörigen.

Forderung. Die elektronische Patientenakte soll direkt ein feingranulares Zugriffskonzept realisieren. Der Patient muss über jeden Zugriff informiert werden und diesen auch freigeben. Der Patient muss nach dem aktuellen Stand des Wissens über die möglichen Konsequenzen der Freigabe informiert werden. Jeder Zugriff darf nur einmal erfolgen und kein pauschales Zugriffsrecht auf einen Eintrag darstellen. Der Patient muss die Möglichkeit haben, einzelne Informationen zu schwärzen. Gibt die Freigabe von Informationen ebenfalls Informationen über Dritte preis, so darf diese Freigabe nur unter strengen Auflagen erfolgen und muss ebenfalls bei den Angehörigen dokumentiert werden.

6 §345 Angebot und Nutzung zusätzlicher Inhalte und Anwendungen

Entwurf. Dieser Paragraph gestattet es den Krankenkassen, Daten aus der digitalen Patientenakte "zum Zweck der Nutzung zusätzlicher [...] Anwendungen" zu nutzen, sofern die Patienten dieser Nutzung vorher zugestimmt haben.

Stellungnahme. Aus meiner Sicht ist die Freigabe dieser zusätzlichen Daten extrem problematisch, da dieser Paragraph auch den Zugriff auf Daten ermöglicht, die der ärztlichen Schweigepflicht unterliegen. Ausserdem sind die Auswirkungen der Nutzung dieser Daten für den Patienten nicht absehbar und können gegebenenfalls auch Angehörige des Patienten betreffen, die kein Einverständnis erteilt haben. Das Argument, dass die Patienten dem Zugriff vorher zustimmen müssen, ist fadenscheinig, da man dieses Einverständnis durch finanzielle Anreize sicher leicht erhalten kann.

Forderung. Die Daten dürfen nur dann genutzt werden, wenn der Schutz der Privatsphäre von Dritten sichergestellt werden kann. Ausserdem sollen die Krankenkassen keinen direkten Zugriff auf die Daten erhalten. Stattdessen soll eine vertrauenswürdige Einrichtung geschaffen werden, die die Hoheit über diese Daten erhält. Dort können die Krankenkassen dann Anfragen stellen, die von einer Kommission vorher begutachtet werden. Der Patient muss zu jedem Zeitpunkt genauestens über die Nutzung seiner Daten im Bilde sein.

7 §345 Verarbeitung von Daten der elektronischen Patientenakte zu Forschungszwecken

Entwurf. Der vorliegende Entwurf sieht vor, dass Patienten Daten der elektronischen Patientenakte freiwillig zu Forschungszwecken zur Verfügung stellen können. Diese Daten werden dann an das Forschungsdatenzentrum übertragen.

Stellungnahme. In meiner Stellungnahme zum Entwurf des Digitale-Versorgungs-Gesetzes (DVG) habe ich bereits deutlich gemacht, dass ich die Verarbeitung von medizinischen Daten zu Forschungszwecken prinzipiell unterstütze, jedoch muss die Privatsphäre der Patienten geschützt werden.

Forderung. Die aktuelle Formulierung folgt dem DVG und ist nicht ausreichend: Die Pseudonymisierung dieser Daten muss den Rückschluss auf Individuen ausschließen. Auch muss sichergestellt werden, dass Patienten nicht durch wiederholte Anfragen auf die Forschungsdaten deanonymisiert werden können. Der Zugriff sollte nicht direkt erfolgen, sondern es sollten lediglich aggregierte und ggf. verrauschte Daten zur Verfügung gestellt werden. Die Patienten sollten über jeden Zugriff und jede Verarbeitung informiert werden und diese auch freigeben. Insbesondere sollte es keinen Freifahrtsschein für zukünftige Untersuchungen geben. Anfragen, die die Anonymität und Privatsphäre von Dritten gefährden könnten, sollten generell nicht freigegeben werden.