www.datenschutzzentrum.de

ULD · Postfach 71 16 · 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200

Aktenzeichen:
LD -

Deutscher Bundestag
Ausschuss Digitale Agenda
Der Vorsitzende, Jens Koeppen, MdB
Platz der Republik 1
11011 Berlin

Kiel, 4. November 2014

Öffentliches Fachgespräch des Ausschusses Digitale Agenda zum Thema "eHealth" am Mittwoch, dem 12.11.2014
Ihre Einladung vom 29.10.2014

Sehr geehrter Herr Vorsitzender Koeppen,
sehr geehrte Damen und Herren Abgeordnete,

für die Einladung zur Teilnahme an dem im Betreff genannten Fachgespräch bedanke ich mich. Ich werde der Einladung gerne folgen. Zur inhaltlichen Vorbereitung des Fachgesprächs erlaube ich mir, Ihnen die folgenden Ausführungen zukommen zu lassen:

Gesundheitsdaten bedürfen eines besonderen staatlichen Schutzes

Es ist eine wichtige staatliche Aufgabe, den Schutz von personenbezogenen Gesundheitsdaten langfristig und nachhaltig zu gewährleisten. Die Verarbeitung dieser besonderen Art personenbezogener Daten (vgl. § 3 Abs. 9 BDSG) setzt wegen deren Sensibilität und der zugrunde liegenden, durch das Patienten- und durch das Sozialgeheimnis besonders geschützten Vertrauensbeziehung (§ 35 SGB I, § 203 Abs. 1, 2 StGB, Berufsordnungen) besonders hohe technische, organisatorische und rechtliche Schutzvorkehrungen voraus. Die Vorschläge für eine Europäische Datenschutz-Grundverordnung sehen insofern einen nationalen Regelungsvorbehalt vor. Deshalb steht die bundesdeutsche Gesetzgebung vor der Aufgabe, ein umfassendes hohes Schutzniveau festzulegen, das den technischen Gegebenheiten und Möglichkeiten gerecht wird. Sie kann damit Vorbild für andere Staaten sein.

Mit der Ankündigung eines E-Health-Gesetzes im Sommer 2014 hat Bundesgesundheitsminister Hermann Gröhe signalisiert, dass es ihm am Herzen liegt, das Potenzial der Informationstechnik (IT) für das Gesundheitswesen auszuschöpfen, um Verbesserungen und eine Effektivierung bei der Gesundheitsversorgung zu erreichen und hierfür die gesetzlichen

Grundlagen zu schaffen. Dies kann nur gelingen, wenn hierbei personenbezogene Gesundheitsdaten angemessen und technikadäquat geschützt werden.

Durch die zunehmende Digitalisierung des Gesundheitswesens eröffnen sich zunehmende Erkenntnismöglichkeiten durch die Auswertung der anfallenden personenbezogenen Daten. Die Digitalisierung erfasst nicht nur Krankenhäuser, Arztpraxen und Apotheken, sondern auch Alten- und Pflegeheime, sonstige Stellen und freiberuflich Tätige in den Bereichen der Pflege, der psychologischen Betreuung und Behandlung sowie der technischen sowie der informationstechnischen Unterstützung. Im Internet wie im analogen Leben ist ein Wellness-Wirtschaftssektor entstanden, in dem in großem Maße biometrische und sonstige gesundheitsrelevante Daten anfallen.

Diese Daten können zur Erlangung neuer medizinischer Forschungsergebnisse, zur Sicherung der Wirtschaftlichkeit und der Qualität der medizinischen Versorgung und zur Verbesserung der Behandlung verwendet werden. Sozial- und Gesundheitsdaten sind für viele Beteiligte im Gesundheitswesen von hohem wirtschaftlichem Wert, was z. B. die Diskussion um die Veräußerung von Abrechnungsdaten durch Apothekenrechenzentren zeigt, von denen sich einige weigern, ihre Verfahren transparent und damit kritikfähig zu machen (vgl. PE ULD 05.03.2014, OVG Schleswig: Kein Maulkorb für ULD). Das Geschäft mit Gesundheitsdaten spielt sich teilweise in einem grauen Markt ab. Krankenkassen und auch andere Sozialleistungsträger erheben oft über das erforderliche Maß hinaus Daten von Betroffenen, mit dem Ziel Ausgaben zu reduzieren, und umgehen dabei gesetzlich vorgesehene Verfahren wie z. B. die Einschaltung des Medizinischen Dienstes der Krankenversicherung (vgl. 24. Tätigkeitsbericht (TB) BfDI 2011/2012, Kap. 11.1.7 u. 11.1.8; schon 22. TB ULD 2000, Kap. 4.7.3). Private Krankenversicherungen etablieren Datensammlungen, mit denen „Versicherungsrisiken" minimiert werden sollen. Es besteht die Gefahr, dass die Daten zur Beeinflussung des medizinischen Versorgungsgeschehens sowie für vorrangig kommerzielle Zwecke verwendet und hierdurch die Vertraulichkeit der Daten und damit das Vertrauen der Betroffenen beeinträchtigt werden. Diese Gefahr wird durch folgende Entwicklungen verstärkt:

- Die Arbeitsteilung im Medizinbereich und die Einschaltung von informationstechnischen Dienstleistern verunklart Verantwortlichkeiten und verstärkt über duplizierte Datenbestände das Risiko zweckwidriger Nutzungen.

- Durch biotechnologische (gentechnische) Verfahren fallen immer mehr Daten an, die für die Betroffenen schicksalhaft sind und von denen für diese ein hohes Diskriminierungsrisiko ausgeht.

- Die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, z. B. durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Technologien, erhöht das Risiko für die Vertraulichkeit und die Integrität der Daten.

- Angesichts des Kostendrucks im Gesundheitswesen und der Möglichkeit der zentralen Auswertung und Nutzung von Behandlungs- und Abrechnungsdaten droht die Dis-

kriminierung von bestimmten Personengruppen bei der Versorgung und der unzulässigen Beeinflussung des Behandlungsgeschehens.

Es ist Aufgabe der Gesetzgebung, die Potenziale der Informationsverarbeitung zur Verbesserung der Gesundheit in der Gesellschaft wie individuell zu nutzen und zugleich die damit verbundenen Gefahren für Wahlfreiheit und Vertraulichkeit zu vermeiden:

- Die Telematik-Infrastruktur ist zeitnah und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Gesundheitsdienstleistern vertraulich und zuverlässig ermöglicht wird und die Patientinnen und Patienten praktisch in die Lage gesetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

- Da elektronische Kommunikation im gesamten Gesundheitssektor genutzt wird, dürfen sich zu schaffende datenschutzrechtliche Regelungen nicht auf einzelne Teilbereiche beschränken, sondern sollten den gesamten Gesundheitsbereich unter Einbeziehung unter anderem der niedergelassenen Ärzteschaft, des Pflegewesens und anderer Gesundheitsberufe erfassen.

- Die Datenverarbeitung im gesetzlichen wie im privaten Versicherungsbereich ist so zu regeln und zu gestalten, dass dort Transparenz, Datensparsamkeit und eine wirksame Kontrolle gewährleistet werden.

- Ökonomische Veränderungen bei Leistungserbringern, z. B. Betriebswechsel, Forderungsabtretungen, Fusionen (z. B. zu bundesweiten Krankenhauskonzernen) und Abspaltungen, dürfen nicht zu einer Beeinträchtigung von Vertraulichkeit, Transparenz und Wahlfreiheit führen, wozu neue technische, organisatorische und rechtliche Vorkehrungen getroffen werden müssen. Änderungen in der Konzernstruktur dürfen nicht dazu führen, dass Datenzugriffe aus Drittstaaten ermöglicht werden. Vor gesetzlichen Zugriffsrechten aus Drittstaaten sind geeignete technische und organisatorische Schutzmaßnahmen vorzusehen.

- Die Abrechnung im Bereich der gesetzlichen Krankenversicherung ist auch aus Gründen des Datenschutzes vorrangig eine hoheitliche Aufgabe, die nur begrenzt und unter hohen Anforderungen an Private delegiert werden kann.

- Durch eine Verbesserung der Koordinierung und Intensivierung der Kontrolle von Informationsdienstleistern im Medizinbereich ist dafür zu sorgen, dass bei zweckändernder Weiternutzung der Daten die Anonymität der Verarbeitung wirksam realisiert wird.

- Die Bereitstellung von aggregierten Gesundheitsdaten für Zwecke der Versorgungsplanung und zur Herstellung demokratischer Transparenz des Gesundheitswesens ist eine staatliche Aufgabe, die Bund und Länder unter Einbeziehung der Krankenversicherungen und der Gesundheitsdienstleister zu erfüllen haben.

- Die Einschaltung von Dienstleistern im Bereich von Krankenhäusern und sonstigen heilberuflich Tätigen ist durch gesetzliche Regelungen so rechtssicher zu gestalten, dass die Funktionalität der Dienstleistungen ebenso wie das Patientengeheimnis gewährleistet werden. Daten, die beim Behandelnden einer gesetzlichen Schweigepflicht unterliegen, müssen auch bei externen Dienstleistern dem gleichen Schutzniveau unterliegen einschließlich einem umfassenden Beschlagnahmeschutz.

- Die Krankheitsregistrierung für Zwecke der klinischen und epidemiologischen Forschung wie der Qualitätssicherung und Behandlungsunterstützung ist auf Bundes- und Landesebene möglichst einheitlich gesetzlich so zu regeln, dass Transparenz und Selbstbestimmung der Betroffenen gewahrt bleiben.

- Durch ein gesetzliches Forschungsgeheimnis sowie durch Anonymisierungs- und einheitliche Genehmigungserfordernisse kann die Bereitstellung der nötigen Datengrundlagen für die medizinische Forschung gesichert werden, ohne die Vertraulichkeit der Daten übermäßig zu beeinträchtigen.

- Die Bundesregierung soll sich dafür einsetzen, dass Standards für eine datenschutzkonforme Gestaltung von medizinischen IT-Produkten und -Verfahren erarbeitet (vgl. z. B. für Krankenhausinformationssysteme die KIS-Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder) und deren Einsatz z. B. durch gesetzlich regulierte Zertifizierungsangebote gefördert werden.

Für Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)