

Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) vom 11.02.2015 zum

## **Referentenentwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz)**

des Bundesgesundheitsministeriums (BMG) vom 19.01.2015 (71.03/14.022)

Im Januar 2015 legte Bundesgesundheitsminister Gröhe den Entwurf eines „Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen“, kurz eines „E-Health-Gesetzes“ vor. Den Ankündigungen gemäß sollte damit ein Durchbruch für E-Health, also für die **Einführung der Informationstechnik (IT) im Gesundheitswesen**, erreicht werden. Dieser Anspruch erscheint in zweierlei Hinsicht etwas überzogen: Zum einen hat die IT das Gesundheitswesen schon voll im Griff; dafür ist kein Gesetz nötig. Zum anderen ist der Entwurf kein großer Wurf, sondern nicht viel mehr als der gesetzgeberische Versuch, die elektronische Gesundheitskarte (eGK) und die Telematik-Infrastruktur (TI), die gemäß dem derzeit geltenden § 291a Abs. 1 SGB V „bis spätestens zum 1.1.2006 zur Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz“ eingeführt sein sollte, endlich zum realen Leben zu erwecken.

Es kam anders, als es im für die gesetzliche Krankenversicherung geltenden Sozialgesetzbuch V (SGB V) vorgesehen war. Bis Ende 2014 wurden für das **Projekt eGK/TI** über eine Milliarde Euro ausgegeben, doch hat die Technik immer noch nicht richtig abgehoben. Wer die Schuld hierfür bei der Technik oder bei der Politik sucht, wird nicht fündig. Die Politik hatte mit dem Gesetz die normativen Grundlagen geschaffen; das Bundesgesundheitsministerium (BMG) hat immer getrieben, um voranzukommen. Auch die Technik war im Prinzip entwickelt und musste bzw. muss für die Praxis allenfalls spezifiziert werden, um konkret programmiert, installiert und ausgerollt werden zu können.

### **Ärztlicher Widerstand**

Die Hauptursache für die teuren Verzögerungen liegen bei der Ärzteschaft. Diese schaffte es über ein Jahrzehnt, mit falschen Argumenten die Bevölkerung, die Medien und letztlich die Politik zum Narren zu halten und dadurch das Gelingen eines äußerst ambitionierten, und zugleich dringend nötigen und sinnvollen Projektes hinauszuzögern. Die Ärzteschaft – genauer: ein großer Teil davon – behauptete, die eGK brächte den „**gläsernen Patienten**“. Die Vertrauensbeziehung des Arztes zu seinen Patienten würde zusammenbrechen, weil medizinische Daten in riesigen Datenzentren ungenügend geschützt zentral abgespeichert würden, wo sich dann so mancher bedienen könnte. Diese Behauptungen wurden durch ihre starke Verbreitung zwar nicht wahrer, sind aber bis heute ein Grund, weshalb vielen Menschen vor der eGK Angst haben.

Tatsächlich ist die gesetzliche Regelung von eGK und TI **aus Datenschutzsicht fast vorbildlich**. Die Speicherung der Daten erfolgt – wie bisher, bei den

Leistungserbringern – dezentral. Zentrale Datenspeicherungen sind nicht vorgesehen. Die in § 291a Abs. 3 Nr. 4 vorgesehene „fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte)“ ist noch nicht in der praktischen Umsetzung. Auch insofern sind Transparenz und Bestimmungsrecht der Betroffenen voll umsetzbar. Die TI ist eine reine Netzstruktur, deren wichtigstes Ziel eine abgeschottete verschlüsselte Übermittlung zwischen medizinischen Leistungserbringern ist. Die dafür vorgesehene Technik ist ausgereift und bewährt. Eigentlich hätte insbesondere die Ärzteschaft jubilieren müssen und können, die ihre elektronischen Praxissysteme endlich sicher vernetzt bekommt und nicht auf proprietäre und unsichere Sonderlösungen zurückgreifen muss.

Dass die Ärzteschaft sich gegen die eGK teilweise bis heute zur Wehr setzt, beruht auf einem richtigen Grund und einer falschen Erwägung: Die Ärzteschaft befürchtet zu Recht die Gängelung und übermäßige **Kontrolle durch die Krankenkassen**, die aus Gründen der Kosteneinsparung die Behandlungs- und Verschreibungspraxis zu überwachen und die Therapiefreiheit zu beeinträchtigen versuchen. Dies tun die Kassen aber nicht über die eGK oder die TI. Diese technische Infrastruktur ist für diesen Zweck auch nur begrenzt geeignet. Sie soll gemäß den bisherigen Planungen hierfür auch nicht genutzt werden, da außer dem Stammdatenmanagement bei den Kassen überhaupt keine Daten über die TI anfallen. Die Übernahme der Kontrolle des Gesundheitswesens durch die Krankenkassen erfolgt erheblich raffinierter durch verborgene Big Data-Auswertungen der Abrechnungen und über die Beschaffung weiterer medizinischer Daten über so verführerische Versprechen wie Prävention, Qualitätssicherung und Patientenberatung. Dieser Trend hält seit Jahren an, ohne dass die Ärzteschaft dies lautstark kritisieren würde. Die aktuellen Entwürfe für ein Präventionsgesetz und ein Gesundheitsversorgungsstärkungsgesetz, die sich derzeit als SGB-V-Änderungen im Gesetzgebungsprozess des Bundes befinden, blieben insofern bisher – außer von Patientenvertretern und Datenschützern – unkommentiert.

[https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Entschlie%DFung\\_DSK\\_GK\\_V-Versorgungsst%E4rkungsgesetz.pdf](https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Entschlie%DFung_DSK_GK_V-Versorgungsst%E4rkungsgesetz.pdf)

## **Grundrechtsschutz - missverstanden**

Aus Datenschutzsicht ärgerlich ist, dass der Widerstand gegen die eGK und die TI aus einer Richtung Unterstützung bekam und teilweise immer noch bekommt, die für sich besondere Glaubwürdigkeit in Anspruch nimmt. Teile der **Bürgerrechts- und Datenschutzszene** profilieren sich mit wenig sachlichen Argumenten, aber griffigen Parolen wie „Stoppt die E-Card!“, ohne zu bemerken, dass ihre Kampagne grundrechtsschädlich ist, weil sie halbseidene IT-Anbieter im Gesundheitsbereich den Weg bereitet, und kurzfristig, weil sie damit nichts anderes tat, als ärztliche Standesinteressen zu befördern.

Inzwischen ist die Informatisierung des Gesundheitswesens weit fortgeschritten. Google, Microsoft und andere Anbieter breiten sich hier aus, ohne dass ein effektiver Datenschutz besteht. Die elektronische **medizinische Kommunikation erfolgt**

**weitgehend ungesichert**, weil unverschlüsselt und über offene Netze. Platzhirsche, oft mit US-amerikanischem Hintergrund, haben sich auf dem Markt mit Gesundheits-IT und -daten etabliert, ausgebreitet und verfolgen mit teilweise datenschutzrechtlich unzulässigen Geschäftsmodellen eine erfolgreiche ökonomische Strategie.

## **Anreize und Sanktionen**

Es ist also positiv zu bewerten, wenn das Bundesministerium für Gesundheit (BMG) versucht, endlich den Knoten zu zerschlagen und eGK sowie TI wirklich ins Leben zu bringen. Das tut der E-Health-Gesetzentwurf mit dem wohl wirksamsten Gestaltungsmittel im Gesundheitswesen: mit finanziellen **Anreizen und Sanktionen**. Als Anreiz ist vorgesehen, dass Ärzte für die Erstellung und Aktualisierung des Notfalldatensatzes eine Vergütung erhalten. Ärzte und Einrichtungen bekommen für eine gewisse Zeitspanne (2016 bis 2017 bzw. 2018) für die Übermittlung von elektronischen Entlass- und Arztbriefen einen beachtlichen „Telematikzuschlag“ von 1 Euro bzw. 55 Cent pro Fall (§§ 291f Abs. 4, § 291h Abs. 1 SGB V). Die Nichtnutzung von IT-Angeboten oder das Nichteinhalten von Fristen für die technische Umsetzung von Maßnahmen wird bestraft.

Das Prinzip „Zuckerbrot und Peitsche“ wird auch in **organisatorischen Fragen** umgesetzt: Die Aufgaben und Befugnisse der Gesellschaft für Telematik (Gematik) werden erweitert und präzisiert (§ 291b Abs. 1 SGB V). Einigt sich die Selbstverwaltung im GKV-System nicht, so erhält das BMG als Ministerium Zwangsbefugnisse.

## **Funktionalitäten**

Das Ziel, der TI mit praktischen Anwendungen Leben einzuhauchen, wird mit Spezialregelungen zum elektronischen **Entlassbrief** (§§ 291f f. SGB V), zum elektronischen **Arztbrief** (§ 291h SGB V) und zur **konsiliarischen Befundbehandlung** (§§ 87 Abs. 2a, 291i SGB V) verfolgt. Die Festlegungen hierzu erfolgen durch die KBV, die Deutsche Krankenhausgesellschaft (DKG), die Gematik und den Spitzenverband der Krankenkassen, wobei die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) eingebunden werden muss (§§ 291g Abs. 3 S. 2, 291h Abs. 2 S. 2, 291i Abs. 1 S. 2 SGB V). Von der DKG und der KBV erfolgt eine Bestätigung der zugelassenen Systeme, die auf einer Liste veröffentlicht werden.

In § 291b Abs. 1 SGB V werden die **Aufgaben der Gesellschaft für Telematik** (Gematik) präzisiert und erweitert, u. a. um Funktionalität und Sicherheit der TI zu gewährleisten, wozu die Erstellung eines Sicherheitskonzeptes ebenso gehört wie Test- und Zertifizierungsmaßnahmen.

Einen weiteren Schritt nach vorne in der TI sollen „**weitere elektronische Anwendungen** des Gesundheitswesens“ gemäß § 291a Abs. 7 S. 2 SGB V bringen, „soweit dadurch die Nutzbarkeit der Telematikinfrastruktur nicht beeinträchtigt wird, insbesondere im Hinblick auf Datenschutz, Datensicherheit und Verfügbarkeit.“ Der Vorbehalt ist zu begrüßen, wenngleich die Terminologie wenig systematisch ist. Mit

dieser Öffnungsregelung sind Innovationen möglich, ohne dass jeweils das Gesetz geändert werden muss.

Mit der Öffnung sollen **weitere Leistungserbringer**, etwa nicht-aprobierte Gesundheitsberufe im Bereich der Pflege in die TI-Kommunikation integriert werden. Da elektronische Kommunikation im gesamten Gesundheitssektor genutzt wird, sollte sich die zu schaffende datenschutzfreundliche und sichere Infrastruktur nicht auf einzelne Teilbereiche beschränken, sondern den gesamten Gesundheitsbereich unter Einbeziehung des Pflegewesens und anderer Gesundheitsberufe erfassen.

In § 291a Abs. 1b SGB V wird für die neuen Anwendungen ein „**diskriminierungsfreier**“ **Zugang zur TI** zugesichert. Hierzu erfolgen durch das BSI und Gematik gemeinsame Festlegungen, die veröffentlicht werden müssen. Anbieter werden über ein Bestätigungsverfahren zur TI zugelassen, was auch im Internet veröffentlicht wird (ebenso für den operativen Betrieb Abs. 1c). Werden Betreibern Störungen bekannt, so sind sie nach § 291b Abs. 6 SGB V zu entsprechenden Meldungen an die Gematik bzw. an das BSI verpflichtet.

In § 291d SGB V ist vorgesehen, dass für die vertrags(zahn)ärztliche Versorgung und Krankenhäuser **offene und standardisierte Schnittstellen** für den Datenaustausch integriert werden, deren Festlegung durch die K(Z)BV und die Deutsche Krankenhausgesellschaft (DKG) im Benehmen mit der Gematik erfolgt.

Nach § 291e SGB V richtet die Gematik ein öffentlich über das Internet verfügbares **Interoperabilitätsverzeichnis** „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein (Abs. 1). Die Gematik wird dabei von „Experten“ beraten, bei deren Auswahl „Vertreter der Anwender der informationstechnischen Systeme, der für die Wahrnehmung der Interessen der Anbieter informationstechnischer Systeme maßgeblichen Bundesverbände, der Länder, fachlich betroffener Standardisierungs- und Normungsorganisationen sowie Vertreter wissenschaftlicher Einrichtungen zu berücksichtigen“ sind. Es ist nicht ersichtlich, weshalb hier Experten aus dem Datenschutzbereich nicht erwähnt werden, zumal die Festlegungen zur Interoperabilität von großer datenschutzrechtlicher Relevanz sind. Zu begrüßen ist die Öffentlichkeit der Verfahren zu dem Verzeichnis, die eine fachöffentliche Debatte zu spezifischen Einzelfragen ermöglicht.

Die Regelungsvorschläge sind stark auf die Bedürfnisse der medizinischen IT-Industrie ausgerichtet. Es gesteht die große Gefahr, dass hier **wirtschaftliche Machzentren** entstehen, deren Geschäftsmodell nicht nur darin besteht, Informationstechnik in Gesundheitswesen zu implementieren und effektiv zu nutzen, sondern auch, personenbezogene oder -beziehbare Medizindaten zu erfassen, auszuwerten und kommerziell zu nutzen, ohne dass eine wirksame Kontrolle gewährleistet ist.

## **Patientenorientierung**

Für die Patienten direkt bringt das E-Health-Gesetz nur wenig. In § 31a SGB V ist ein **Medikationsplan** vorgesehen, der den Patienten mehr Verschreibungssicherheit und

-transparenz bringen soll. Versicherte haben ab Oktober 2016 einen Anspruch darauf, wenn sie mindestens fünf verordnete Arzneimittel anwenden. Das Grundprinzip, dass für eine Datenverarbeitung mit der eGK eine Autorisierung sowohl durch den Patienten wie auch einen medizinischen Leistungserbringer nötig ist, wird – aus Praktikabilitätsgründen – aufgehoben, wenn der Medikationsplan auf die eGK gespeichert werden soll (§ 291a Abs. 5 S. 2 SGB V). Diese Erleichterung erscheint sinnvoll.

Eine Krux des korporativen GKV-Systems spiegelt sich im E-Health-Gesetz wieder: Der **Patient** spielt nur eine Randrolle. Im Zentrum stehen die Leistungserbringer, deren Vereinigungen, die Kassen und neuerdings die IT-Anbieter, allenfalls noch die staatliche Bürokratie in Form des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) oder des BMG. Der Datenschutz wird nur am Rande, der Verbraucherschutz überhaupt nicht erwähnt.

Eine weitere Krux des GKV-Systems kommt in dem Entwurf zum Tragen: Die **Formulierungen der Regelungsvorschläge** sind derart komplex und unübersichtlich, dass sie von den Betroffenen, also den Patientinnen und Patienten definitiv nicht verstanden und mit Leben gefüllt werden können. Selbst für Juristen sind die bestehenden Regelungen wie auch die Vorschläge nur nach einer intensiven Einarbeitung nachvollziehbar und verstehbar. Damit geht eine wichtige Funktion von Gesetzgebung, nämlich demokratische Transparenz in Prozesse und Entscheidungen zu bringen, verloren.

### **Weiterer Regelungsbedarf**

Mit dem Entwurf für ein E-Health-Gesetz signalisiert das BMG, dass es wichtig ist, 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.

Digital anfallende Gesundheitsdaten werden zu vielen **sinnvollen Zwecken** – zur Erlangung neuer medizinischer Forschungsergebnisse, zur Sicherung der Wirtschaftlichkeit und der Qualität der medizinischen Versorgung und zur Verbesserung der Behandlung – verwendet und benötigt. Sozial- und Gesundheitsdaten sind für viele Beteiligte im Gesundheitswesen von hohem wirtschaftlichem Wert.

Es besteht mangels hinreichender Regelungen 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 in die Datenverarbeitung und letztlich in die Behandlung 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 Diskriminierung 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. Hierfür muss die TI zeitnah und funktionsfähig so realisiert werden, 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. Hierzu macht der Entwurf für das E-Health einige wichtige Vorgaben. Darüber hinausgehend sind weitere Maßnahmen und Regelungen nötig:

**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.

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 **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.

<https://www.datenschutzzentrum.de/artikel/828-.html>

<https://www.datenschutzzentrum.de/uploads/medizin/20141112-FachgespracheHealth.pdf>

### **Insbesondere: Regulierung des medizinischen IT-Outsourcings**

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 Patienten- und das Sozialgeheimnis gewährleistet werden. Daten, die beim Behandelnden einer gesetzlichen Schweigepflicht unterliegen, müssen auch **bei externen Dienstleistern** dem gleichen Schutzniveau unterliegen einschließlich einem umfassenden Beschlagnahmeschutz.

Es bedarf hierfür einer Regelung zur Auslagerung von Dienstleistungen mit personenbezogener Datenverarbeitung für Berufsgeheimnisträger oder auch für Sozialleistungsträger, mit welcher der **Vertraulichkeitsschutz** bei den Dienstleistern gewahrt wird. Eine solche Regelung käme Heilberufen wie (Zahn-)Ärzten, Apothekern oder Psychologen zugute, deren elektronische Vernetzung durch das E-Health-Gesetz erleichtert und verbessert werden soll. Derzeit ist wegen der beruflichen Schweigepflicht in Form des Patientengeheimnisses für die Verarbeitung von Patientendaten bei Dienstleistern zumeist eine Einwilligung erforderlich, die in vielen Fällen faktisch nicht eingeholt werden kann. Die Einschaltung von Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn diese moderne Informationstechnik nutzen wollen. Dies führt dazu, dass durch deren Einschaltung in der Praxis oft massenhaft gegen die Pflicht zur beruflichen Verschwiegenheit verstoßen wird.

Die notwendige rechtliche **Regelung** sollte gewährleisten, dass die Verarbeitung von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister insofern einer Schweigepflicht unterworfen und durch ein Beschlagnahmeverbot abgesichert werden und dass durch Kontroll- und Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Durch weitergehende Anforderungen an die Art der Datenverarbeitung, etwa über technisch-organisatorische Maßnahmen und über das Herstellen von Transparenz, kann das für sensible Daten erforderliche Schutzniveau hergestellt werden.

Mit einer solchen Regelung kann die für die Verarbeitung dringend notwendige Vertraulichkeit bei der Verarbeitung von Berufsgeheimnissen gewährleistet und die für die Berufsgeheimnisträger und deren Dienstleister notwendige Rechtssicherheit geschaffen werden. Von ihr kann zugleich der auch mit dem E-Health-Gesetz intendierte **Modernisierungsschub** bei der Verarbeitung besonders geschützter personenbezogener Daten ausgehen.