IGZ
DIE ALTERNATIVE
20. Jahrgang
VKZ 17248
2
2015

Daten- und Patientenschutz im digitalen Gesundheitswesen

Interessengemeinschaft Zahnärztlicher Verbände in Deutschland IGZ e.V.

Weil uns mehr verbindet.

Spezialisierte Beratung für Apotheker und Ärzte.

Ob beruflich oder privat: Die meisten Apotheker und Ärzte in Deutschland vertrauen auf unsere Leistung und spezialisierte Beratung.

Mehr Informationen erhalten Sie unter: **www.apobank.de**

Weil uns mehr verbindet. deutsche apotheker- und ärztebank

Dr. Christian Georg, Radiologe

Antonia Zimmer, Studentin der Zahnmedizin

Markus Felber, Zahnarzt

Masoumeh Hediehlou, Apothekerin

Benn Roolf

Fortschritt muss gestaltet werden.

Liebe Leserinnen und Leser,

die Digitalisierung hat den Industriegesellschaften in den letzten Jahrzehnten einen ungeheuren Zuwachs an Produktivität und neuen Möglichkeiten gebracht. Was mit der Einführung einfacher Rechenmaschinen für industrielle und militärische Spezialanwendungen begann, hat in historisch atemberaubendem Tempo Einzug in nahezu alle Bereiche der Arbeits- und Lebenswelt gehalten. Auch die Medizin und das Gesundheitswesen haben von dieser Entwicklung profitiert. Der Nutzen ist offensichtlich und unbestritten: Die Möglichkeiten, Krankheiten zu diagnostizieren und zu behandeln, haben sich enorm erweitert. Und die komplexen Prozesse von Verwaltung, Abrechnung und Dokumentation wären wohl ohne Digitaltechnik kaum noch denkbar.

Es erscheint daher auf den ersten Blick nur folgerichtig, wenn in einem nächsten Entwicklungsschritt all die verschiedenen Akteure im Gesundheitswesen über eine Telematikinfrastruktur (TI) vernetzt werden sollen. Proprietäre Systeme sollen künftig über einheitliche Schnittstellen Daten sicher miteinander austauschen können. Die Vernetzung schafft noch einmal zusätzlichen Mehrwert und schreibt das Innovationstempo fort. Notfalldaten, Röntgenbilder, Befunde, Behandlungsverläufe eines Patienten sind in einer elektronischen Patientenakte gespeichert und jedem behandelnden Arzt jederzeit zugänglich. Telemedizin überbrückt räumliche Entfernungen. Data mining bietet die Chance, die vielfältig erhobenen Gesundheitsdaten für die Erforschung von Krankheitsursachen zu nutzen - faszinierende Möglichkeiten.

Neben den vielen Chancen birgt die Entwicklung jedoch auch ganz neuartige Risiken. Im Unterschied zu einer herkömmlichen Patientenakte in Papierform lassen sich digitale Daten quasi unbegrenzt kopieren und in wenigen Minuten weltweit veröffentlichen. Allein diese Möglichkeit schafft bisher kaum vorstellbare Missbrauchsmöglichkeiten. Datenschützer führen seit Jahren einen zähen Kampf für das „digitale Vergessen“, um Betroffenen ein Löschen ihrer ins Internet gelangten Daten zu ermöglichen.

Zurecht wird in der Debatte um die Telematikinfrastruktur darauf verwiesen, dass es trotz hoher Sicherheitsstandards keine einhundertprozentige Sicherheit geben kann - weder in der analogen noch in der digitalen Welt. Richtig ist aber auch, dass die Konsequenzen einer Datenpanne in der digitalen Welt ungleich größer sind, schon allein wegen der hohen Zahl an Betroffenen. So ist es schwer vorstellbar, dass beispielsweise die Datendiebe, die sich Anfang diesen Jahres ins System des amerikanischen Krankenversicherers Anthem gehackt haben, die entwendeten Daten von Millionen Versicherten auch in analoger Form als Aktenberge aus einem Bürogebäude hätten tragen wollen.

Nun wird niemand dafür plädieren wollen, zur analogen Datenhaltung zurückzukehren. Eine Möglichkeit, die Risiken der Digitalisierung aufzufangen, ist die klassische Versicherungsidee. Und in der Tat: Die Versicherungsbranche ist im Aufwind: Dem aktuell noch jungen Markt für sogenannte Cyberversicherungen wird bereits ein rasantes Wachstum prognostiziert. Interessant wäre in diesem Zusammenhang der Gedanke, ob und zu welchen Kosten sich die Cyberrisiken der Telematikinfrastruktur absichern lassen. Die Höhe einer seriös kalkulierten Versicherungsprämie würde uns den Preis für die bislang nur spekulativ diskutierten Cyberrisiken aufzeigen.

Neben den Abwägungen zur Sicherheit hochsensibler Patientendaten gibt es noch viele offene Fragen bezüglich der Telematikinfrastruktur: Welcher Nutzen kann in der medizinischen Versorgungswirklichkeit konkret generiert werden? Mit welchen laufenden Kosten - da sollten Kosten für die Risikoabsicherung korrekterweise berücksichtigt werden - ist beim Betrieb der TI zu rechnen? Wie soll das Zugriffsrecht der Patienten auf ihre Daten aussehen? Welche Ansprüche sollen Patienten rechtlich erhalten, die durch die Nutzung der TI Nachteile erleiden? Und nicht zuletzt: Welche Auswirkungen hat die Digitalisierung im Gesundheitswesen auf die Kultur unseres Gemeinwesens? Hier sind Stichworte wie „Entsolidarisierung des Versicherungsgedankens“, „Arzt-Patienten-Verhältnis“ und „Konformitätsdruck durch Selbstvermessung mittels Gesundheits-Apps“ angesprochen. In unserem Schwerpunktthema finden Sie inhaltsreiche Beiträge, die diese vielfältigen Facetten der Diskussion aufgreifen.

Ich wünsche Ihnen eine interessante Lektüre.
Benn Roolf

Benn Roolf
Chefredakteur

Günther E. Buchholz

Chancen und Herausforderungen der Digitalisierung in der zahnärztlichen Praxis

Dr. Günther E. Buchholz, *Stellvertretender Vorsitzender des Vorstandes der Kassenzahnärztlichen Bundesvereinigung (KZBV)*

Ob E-Mails, Smartphones oder Online-Banking – die Errungenschaften fortschreitender Digitalisierung im beruflichen und privaten Umfeld werden vielfältig genutzt und finden weithin Verbreitung. Auch in der modernen Zahnmedizin ist der Einsatz digitaler Infrastrukturen nicht mehr wegzudenken.

In nahezu jeder zahnärztlichen Praxis werden Aufgaben der Praxisverwaltung und der Abrechnung zahnärztlicher Leistungen mittels eines Dentalsoftwaresystems organisiert. So wurden im 4. Quartal 2013 beispielsweise 99,8 Prozent der konservierend-chirurgischen Leistungen und 98,8 Prozent der kieferorthopädischen Leistungen auf elektronischem Wege abgerechnet. Die Software bereitet dabei die Daten zu den Leistungen für die Abrechnung mit den Kassenzahnärztlichen Vereinigungen (KZVen) auf und übermittelt diese hauptsächlich in Form von Online-Abrechnungen oder Datenträgeraustausch. Um dabei die Kompatibilität zu gewährleisten, müssen spezifische Anforderungen an die Programme berücksichtigt werden. Die Kassenzahnärztliche Bundesvereinigung stellt den Softwareherstellern daher definierte Vorgaben in Form von Modulen zur Verfügung, die in die Programme integriert werden.

Auch praxisorganisatorische Aufgaben wie die Verwaltung von Terminen oder die zahnmedizinische Dokumentation werden heute meistens über EDV-Systeme abgewickelt. Dies kommt auch den Patienten unmittelbar zugute, etwa in Form eines Terminmanagements, das dabei hilft, lange Wartezeiten zu vermeiden.

Einsatz von digitaler Medizintechnik

Zunehmend mehr Arbeitsschritte von Behandlungsprozessen werden durch Einsatz digitaler Medizintechnik unterstützt. So können durch Kamerasysteme Aufnahmen von Zahndefekten oder Schleimhautveränderungen gemacht werden. Diese helfen Zahnärztinnen und Zahnärzten bei der Befunddokumentation. Zugleich können Patienten die nötigen Behandlungsschritte anschaulich präsentiert werden. Digitales Röntgen und damit auch die digitale Archivierung von Röntgenaufnahmen in den Informationssystemen stellt ein weiteres, verbreitetes Anwendungsfeld digitaler Technik in der Praxis dar. Die Verknüpfung der medizinischen Patientendaten mit der zugehörigen Röntgenaufnahme kann hierdurch verbessert werden.
Im Markt werden heute auch CAD/CAM-Systeme zur 3D-Modellierung und Erstellung von Zahnersatz angeboten. Mit dem Einsatz dieser Techniken können Kronen beispielsweise direkt in der Praxis passgenau hergestellt werden.

Die Telematikinfrastruktur – Vernetzung auf allen Ebenen

Ein zentrales Thema für das Gesundheitswesen der Zukunft ist der Einsatz einer umfassenden Telematikinfrastruktur. Diese dient dazu, die IT-Systeme von Zahnarzt- und Arztpraxen, Apotheken, Krankenhäusern und Krankenkassen miteinander zu vernetzen und einen systemübergreifenden Austausch von Informationen zu ermöglichen. Der Zugang zu diesem Netzwerk erfolgt durch die elektronische Gesundheitskarte des Versicherten und/oder den Heilberufsausweis des Zahnarztes oder Arztes.

Derzeit wird die Erprobung der Telematikinfrastruktur vorbereitet. In einem ersten Schritt wird das elektronische Versichertenstammdatenmanagement aufgebaut. Hierdurch ist eine Onlineprüfung und -aktualisierung grundlegender Daten der Patienten wie Name oder Anschrift möglich. Bezeichnend ist, dass diese Anwendung in erster Linie als Verwaltungsanwendung den Krankenkassen zum Vorteil gereicht – weder Patienten noch Zahnärzte oder Ärzte profitieren hiervon. Erst die für die weitere Zukunft angedachten medizinischen Anwendungen werden auch für Zahnärztinnen und Zahnärzte sinnvolle Hilfen sein, wobei der Stellenwert der Arzneimitteltherapiesicherheit und des Notfalldatenmanagements sicherlich nicht das Ausmaß des Nutzens wie in humanmedizinischen Praxen erreichen wird.

Zahnärzte werden daher auch im Gegensatz zu Hausärzten keine aktive Funktion im Sinne großer Datenlieferanten haben. So ist zum Beispiel die Erfassung und die Pflege der Notfalldaten eher in der Obhut des Hausarztes angesiedelt, der den Überblick über die gesamten Behandlungsdaten seines Patienten hat. Ebenso ist der Beitrag zu den Daten der Arzneimitteltherapiesicherheitsprüfung und des Medikations-

plans wegen der geringen Anzahl von Verordnungen in der zahnärztlichen Praxis eher gering. Speziell vor dem Hintergrund einer zunehmenden Überalterung der Gesellschaft liegen die Vorteile solcher medizinischen Anwendungen für multimorbide Patienten jedoch auf der Hand.

Eine auch für die Zahnarztpraxis zentrale Funktion wird hingegen der Austausch von Sozialdaten sein. Darunter fallen zum Beispiel Abrechnungsdaten, die letztlich auf die zahnmedizinische Behandlung zurückzuführen sind und damit geschützt werden müssen. Künftige Anwendungen sollen nicht nur die sichere Kommunikation zwischen den Zahnärzten, sondern auch zwischen KZVen und Praxen ermöglichen. Die KZBV hat sich daher besonders dafür stark gemacht, dass auch KZVen in den Testregionen im Rahmen der Erprobung mit dieser Technik ausgestattet werden.

Fest steht: das ambitionierte Großprojekt der Telematikinfrastruktur birgt also einiges Potential, um Praxis- und Behandlungsabläufe weiter zu optimieren und zu vereinfachen. Allerdings darf dabei nicht außer Acht gelassen werden, dass die Integration in eine bereits vorhandene Praxis-EDV komplex ist und erhebliche Kosten und Aufwände verursachen kann.

Daneben muss natürlich immer der Sicherheitsaspekt beachtet werden. Eine Online-Anbindung des Praxissystems stellt ein Risiko für das Einbringen von Schadsoftware oder ein Einfallstor für Hacker dar. Damit diese Risiken bei der Online-Anbindung minimiert werden, sind Sicherheitsmaßnahmen beim Aufbau der Telematikinfrastruktur wie sichere Zugangsnetze mit Nutzung von VPNs („virtual private network“) auf der Basis moderner Verschlüsselungs-Technik erforderlich. Um den Sicherheitsanforderungen zu genügen, ist eine Zertifizierung von Komponenten wie Kartenterminals und Konnektoren durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erforderlich. Dieser hohe Sicherheitsstandard mit der damit verbundenen und von der Industrie unterschätzten Komplexität ist eine der Ursachen für die verzögerte Realisierung der Telematikinfrastruktur. Es bleibt weiter zu hoffen, dass sich der enorme Aufwand letztendlich lohnt und am Ende ein solider Sicherheitsstandard Einzug in alle Praxen hält, der den ebenso sicheren wie einfachen Austausch von Informationen erlaubt. Probleme wie Spähangriffe oder versehentlich falsch ausgewählte E-Mail-Adressen sollten dann der Vergangenheit angehören. Unsichere Kommunikationswege für Befunde oder Röntgenbilder wie E-Mails oder Fax-Geräte werden mit der neuen Vernetzung schrittweise ersetzt.

Die Telematikinfrastruktur birgt einiges Potential, um Praxis- und Behandlungsabläufe weiter zu optimieren und zu vereinfachen. Vermieden werden muss aber in jedem Fall der „gläserne Patient“. Daher setzen wir Zahnärzte uns auch für eine dezentrale Datenspeicherung ein. [...] Zudem sollte es nicht um wahllose Datensammelei oder das Anlegen lebenslanger Akten gehen - im Vordergrund sollte der bedarfsorientierte Informationsaustausch im Behandlungskontext stehen.

Nein zum „gläsernen Patienten“!

Vermieden werden muss aber in jedem Fall der „gläserne Patient“. Daher setzen wir Zahnärzte uns auch für eine dezentrale Datenspeicherung ein, etwa mit Blick auf Notfalldaten oder die Arzneimitteltherapiesicherheit. Zudem sollten eine wahllose Sammelwut sowie lebenslange Akten nicht im Vordergrund stehen, sondern vielmehr der bedarfsorientierte Informationsaustausch im Behandlungskontext. Eine zielgerichtete Datenweitergabe erhöht gleichzeitig die Sicherheit der übermittelten Informationen. Es macht im Hinblick auf die Vertrauenswürdigkeit der Diagnose- und Behandlungsdaten durchaus einen Unterschied, ob der Zahnarzt oder Arzt, der die Information benötigt, diese zeitnah von einem Kollegen erhält oder aus einer zentralen Datensammlung abruft, bei der im Zweifelsfall nicht ersichtlich ist, wer die Information wann eingestellt oder geändert hat. Der Empfänger kann demzufolge auch nicht beurteilen, ob die Daten aktuell, vollständig und für den vorgesehenen Behandlungszweck überhaupt relevant sind.

Ein zweifellos bestehendes Sicherheitsrisiko ergibt sich an dieser Stelle jedoch aus dem bekannten Kontrollbedürfnis der Krankenkassen, wenn künftig auch andere Prozesse im Datenaustausch mit den Versicherungen elektronisch abgewickelt werden. Natürlich darf es hier zu keiner Einschränkung der Therapiefreiheit kommen. Mögliche Gefährdungen durch eine „Big Data-Auswertung“ müssen frühzeitig erkannt und kategorisch ausgeschlossen werden. In diesem Bereich sehen wir den Bundesbeauftragten für den Datenschutz gefordert, auf rechtliche Vor-

kehrungen hinzuwirken, die einen solchen Missbrauch verhindern.

Komplexe Systeme, Datensicherheit und Datenschutz

Bereits die heutige IT-Infrastruktur in den Praxen ist häufig eine Herausforderung für die Anwender. Die Vernetzung unterschiedlicher Systeme von unterschiedlichen Hard- und Softwareherstellern erhöht das Risiko von Fehlern und Schwachstellen für den Datenschutz und die Datensicherheit. Das beginnt schon bei der Konfiguration des PC-Betriebssystems: So wird mit dem neuen Microsoft-Produkt Windows 10 der Trend erkennbar, Nutzerdaten direkt an den Hersteller zu versenden, ohne dass der Nutzer dies für den Einzelfall autorisiert. Zwar sind die Einstellungen zum Systemverhalten prinzipiell konfigurierbar, aber dies verlangt schon die notwendigen Kenntnisse bei dem verantwortlichen Zahnarzt und geht in der Vielschichtigkeit der IT-Landschaft leicht unter. Dieser Trend zum „Aushorchen“, der sich leider auch bei anderen IT-Produkten und Betreibern zunehmend zeigt, kann auf die Sicherheit und den Schutz sensibler Patientendaten sowie auf das Nutzerverhalten negativen Einfluss haben. Hinzu kommt, dass die Vielfalt verwendeter Soft- und Hardware kontinuierlich gepflegt und aktualisiert werden muss. Updates müssen verlässlich eingespielt werden. Bei mangelhafter Pflege drohen Sicherheitslücken.

Das Thema Datenschutz spielt also sowohl innerhalb einer künftigen Telematikinfrastruktur als auch bei bereits bestehenden Praxis-EDV-Systemen eine wachsende Rolle. Unberechtigte Zugriffe Dritter auf den Praxisrechner und damit auf Patientendaten müssen ebenso ausgeschlossen werden, wie der Verlust der Daten, etwa durch technische Ausfälle. Als unterstützende Maßnahme haben KZBV und Bundeszahnärztekammer (BZÄK) darum einen Leitfaden entwickelt, der die Praxen bei der Erfüllung der Anforderungen an Datenschutz und Datensicherheit ihrer EDV-Systeme unterstützt. Angesichts der fortschreitenden technischen Entwicklungen muss dieser allerdings ständig aktualisiert werden. Die aktuelle Fassung des Leitfadens kann unter www.kzbv.de abgerufen werden.

Künftig werden Arbeitsabläufe in den Zahnarztpraxen durch die Digitalisierung weiter ausgebaut und unterstützt. Die Digitaltechnik ist dabei jedoch nur ein weiteres Werkzeug, welches sowohl Chancen als auch Risiken mit sich bringt. Die eigentliche zahnmedizinische Leistung wird nach wie vor durch das Geschick und die Expertise von Menschen erbracht. Und diese kann auch in absehbarer Zukunft weder durch Computer noch durch Roboter ersetzt werden.

Künftig werden Arbeitsabläufe in den Zahnarztpraxen durch die Digitalisierung weiter ausgebaut und unterstützt. Die Digitaltechnik ist dabei jedoch nur ein weiteres Werkzeug, welches sowohl Chancen als auch Risiken mit sich bringt. Nicht zu vergessen ist, dass die eigentliche zahnmedizinische Leistung nach wie vor durch das Geschick und die Expertise von Menschen erbracht wird. Und diese kann auch in absehbarer Zukunft weder durch Computer noch durch Roboter ersetzt werden.

Jürgen Herbert

Die Digitalisierungswelle rollt

Und sie wird uns alle erfassen. Die entscheidende Frage ist, ob wir auf ihr surfen wollen, oder uns von ihr wegtragen lassen. Nachdem Branche für Branche und nahezu sämtliche Lebensbereiche von der digitalen Revolution erfasst wurden, wird auch unser Gesundheitssystem in den kommenden Jahren durchgreifende Veränderungen erfahren. Und diese werden auch vor der Zahnmedizin nicht haltmachen. Der Markt für Gesundheits-Apps - auch zum Thema Mundgesundheit - boomt bereits und die Stichworte eHealth und Telemedizin sind in aller Munde. Informations- und Beratungsportale über Krankheiten aller Art gehören zu den meist genutzten Webseiten überhaupt. In der Gesamtzahl hoch frequentiert sind auch die zahlreichen Foren, in denen sich Betroffene über Beschwerden oder Therapieerfahrungen austauschen, oft zu seltenen Erkrankungen. Mit den Gesundheits- und Lifestyle-Apps wächst auch die Zahl der mit ihnen verknüpften „Wearables“ unaufhaltsam. Gerade bei diesen erheben die Nutzer unbedarft eigene, persönlichste (Gesundheits)Daten (Stichwort Self-Tracking) und geben diese preis, ohne genau zu wissen, was der App-Hersteller damit macht.

Der Vorstand der Bundeszahnärztekammer hat sich auf seiner diesjährigen Klausurtagung intensiv mit den gesellschaftlichen und politischen Herausforderungen der Digitalisierung und Vernetzung im Gesundheitswesen auseinandergesetzt. Ausgehend von der Prämisse, dass die Digitalisierung des Gesundheitswesens tiefgreifend und unumkehrbar ist, gilt es, den Berufsstand und die Kammern zukunftsgerichtet aufzustellen und klar zu positionieren. Denn bei aller Begeisterung für die digitale Vernetzung dürfen wir ihre Gefahren nicht außer Acht lassen. Es steht viel auf dem Spiel. Folgt man dem Weg der Daten werden die einzelnen Herausforderungen deutlicher:

Patientenorientierung gilt auch digital

Aus gutem Grund gelten Gesundheitsdaten als besonders sensible, personenbezogene Daten. Deutschland war eines der ersten Länder, in dem das Recht auf informationelle Selbstbestimmung seit dem Jahr 1983 als ein Grundrecht der Bürger anerkannt ist. Noch viel älter, nämlich mehr als 2.000 Jahre, ist der Eid des Hippokrates, mit dem sich jeder (Zahn) Arzt auch heute noch in abgewandelter Form zur Verschwiegenheit verpflichtet: „Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.“

Durch die Digitalisierung droht der seit jeher geschützte Vertrauensbereich zwischen Patient und (Zahn)Arzt zu erodieren. Und dies liegt nicht daran, dass die (Zahn)Ärzte in zunehmendem Maß Daten digital erheben, speichern und austauschen, sondern dass unsere Patienten ihre Gesundheitsdaten freiwillig gegenüber Dritten preisgeben. In den geschützten Wirkkreis von (Zahn)Arzt und Patienten drängen immer mehr „Mitwisser“: Gesetzliche Krankenkassen und private Krankenversicherungen, die bislang überwiegend über reine Abrechnungsdaten verfügten und ihre Mitglieder inzwischen für gesundheitsbewusstes Verhalten mit Zuschüssen für Fitnessarmbänder oder „smarte“ Uhren belohnen, um im Gegenzug zusätzliche Daten von Ihnen aus erster Quelle zu erhalten. Oder IT-Konzerne aus Übersee, die die Gesundheitsdaten für eigene oder fremde Forschungszwecke verwenden.

Die Versprechen, welche Vorteile gesammelte und strukturiert ausgewertete Daten (Big Data) im Gesundheitsbereich jedem Einzelnen bringen, sind groß: In Zukunft kommt der Patient nicht mehr wegen Beschwerden zum Arzt, sondern weil seine Erkrankung bereits vor ihrem Entstehen bzw. ihrem Ausbruch erkannt wurde – durch Daten, die er täglich mittels App oder Wearable sammelt. Durch ein gezieltes Sportprogramm, eine Ernährungsumstellung oder bestimmte Medikamente werden die Beschwerden so sofort im Keim erstickt. Ärzte müssen in diesem Szenario Daten nicht mehr selbst erheben, sondern werten nur noch die vom Patienten selbst gesammelten Daten aus. Zugleich helfen die mittels neuer Algorithmen und enormer Rechenkraft ausgewerteten Daten, Krankheiten schneller und besser zu heilen und damit die Versorgung insgesamt zu verbessern.

Soweit so gut. Doch bei aller Euphorie sind auch vorsichtige Zweifel angesagt.

- Droht mit der durch Big Data versprochenen „personalisierten Medizin“ womöglich eine Entsolidarisierung unserer Gesellschaft, in dem Gesunde bevorzugt und Kranke benachteiligt werden und

Jürgen Herbert,
Mitglied des Vorstandes der Bundeszahnärztekammer, Präsident der Landeszahnärztekammer Brandenburg

dies womöglich generationenübergreifend, sofern genetisch bedingte Dispositionen bekannt werden? Denn sowohl unsere sozialen Sicherungssysteme, aber auch die Tarife der privaten Krankenversicherung funktionieren auf der Basis einer Quersubventionierung der „schlechten“ durch die „guten“ Risiken.

- Können wir darauf vertrauen, dass unsere Daten nur für die von uns beabsichtigten Zwecke genutzt werden, wenn wir sie in die Hände der Versicherer oder ausländischer Konzerne geben?
- Und schließlich: Was nützt uns das vermeintliche Heilversprechen, aus den gigantischen Datenbergen durch die ständig wachsende Rechenleistung und verbesserte Suchalgorithmen neue, bislang unbekannte Abhängigkeiten finden zu können, wenn diese nicht in einem Wirkzusammenhang stehen?

Korrelation ist nicht gleich Kausalität

Denn eine hohe Korrelation zwischen zwei Variablen bedeutet nicht, dass die beiden Variablen kausal miteinander zusammenhängen. Stattdessen liefern Korrelationen lediglich einen ersten Hinweis auf Ursachen und ihre mögliche Wirkung. So wurde zwar in den zwanziger Jahren des letzten Jahrhunderts in Schweden sowie in siebziger Jahren in Niedersachsen eine hohe Korrelation zwischen der Storchenpopulation und der Geburtenrate festgestellt. Dennoch hängen diese beiden Ereignisse nicht kausal miteinander zusammen. Und um ein Beispiel aus der Versorgung zu nennen: Die Verweildauer im Krankenhaus korreliert zwar mit einem schlechteren Gesundheitszustand nach dem Krankenhausaufenthalt. Maßgeblicher Grund dafür ist jedoch der Gesundheitszustand der Patienten vor der Einlieferung in das Krankenhaus. Patienten mit schweren Vorerkrankungen benötigen in der Regel eine längere Behandlung und weisen auch nach ihrer Entlassung einen schlechteren Gesundheitszustand auf, als Personen mit leichteren Erkrankungen.

Eine internationale Herausforderung

Klar ist: Wer Zugriff auf die Gesundheitsdaten der Patienten hat, wird sie auch für eigene Zwecke gebrauchen. Dabei sind die Strategien der Krankenkassen, aber auch der privaten Krankenversicherungen relativ eindeutig: Vordergründig versprechen Sie sich Chancen im Wettbewerb um junge und gesunde Mitglieder und wollen ihre Gesundheitsangebote passgenauer auf ihre Versicherten zuschneiden. Es geht Ihnen aber sicherlich auch darum, die Versorgung noch effizienter in ihrem Sinn zu steuern. Ob diese Ziele immer dem Patientenwohl entsprechen, darf vorsichtig bezweifelt werden.

Wo die Grenze zum Unerlaubten liegt, ist in Deutschland am ehesten noch für den Bereich der gesetzlichen Krankenversicherung durch die Sozialgesetzgebung definiert. Konsequent hat die Bundesdatenschutzbeauftragte Andrea Voßhoff daher im August die gesetzlichen Krankenkassen bei dem Versuch, die Daten aus Fitness-Apps für ihre Bonusprogramme zu nutzen, in ihre Schranken verwiesen.

Bei den teilweise als europäische Konzerne agierenden privaten Krankenversicherungen wird das schon schwieriger, wie auch Frau Voßhoff einräumen musste. Denn hier gilt Europäisches Datenschutzrecht, das einen möglichst freien und ungehinderten Waren- und Dienstleistungsverkehr gewährleisten soll. In Brüssel tobt derzeit eine der größten Lobbyschlachten, die die EU je erlebt hat, um die neue europäische Datengrundschutzverordnung. Diese Verordnung wird auch auf privat erhobene und verfügbare Gesundheitsdaten Anwendung finden.

Für die zumeist amerikanischen IT-Konzerne scheint es inzwischen gar keine verbindlichen Regeln mehr zu geben. Aber gerade die Geschäftsmodelle von Google, Facebook und Co. basieren darauf, die Daten ihrer Nutzer gewinnbringend zu verwenden. Der Gesundheitsbereich, wo hochsensible Daten erfasst werden, mit deren strukturierter Auswertung sich Milliarden verdienen lassen, gerät in dieser Logik ganz automatisch in den Fokus. So gab der Internetkonzern Google unlängst eine Kooperation mit dem Pharmahersteller Sanofi zur Bekämpfung von Diabetes bekannt. Dafür sammelt Google umfassende Gesundheitsdaten; nach Unternehmensangaben zum Wohle der Kranken. Datenschützer äußern jedoch ihre Bedenken. Nicht ohne Grund sprach sich der Generalanwalt beim Europäischen Gerichtshof Ende September diesen Jahres dafür aus, die 16 Jahre alte Entscheidung der EU-Kommission, dass ein Drittland wie die USA einen ausreichenden Schutz für persönliche Daten bietet, für ungültig zu erklären.

IT-Sicherheit im Griff?

Hinzu kommt der bislang noch nicht thematisierte Aspekt der IT-Sicherheit: Wie unsicher selbst vermeintlich gut geschützte Daten sind, wissen wir seit den Enthüllungen von Edward Snowden über die US-Spähprogramme. Und wie unsicher vermeintlich gut geschützte IT-Systeme sind, davon zeugt die Cyberattacke auf den Deutschen Bundestag, die es letztlich erforderlich machte, das Bundestagsnetzwerk komplett neu aufzusetzen. Aus den wenigen Beispielen wird hoffentlich deutlich: Den sicherlich in hohem Maße durch die Digitalisierung begründeten Chancen stehen auch erhebliche Risiken wie eine für Patienten nachteilige Risikoselektion gegenüber. Und auch die Grenzen zwischen einer echten Innovation und dem Missbrauch von Daten sind fließend.

Wer schützt die sensiblen Daten?

Klar ist: Wer Daten sammelt oder Zugriff auf sie hat, wird sie in den seltensten Fällen löschen oder zumindest nicht weiter benutzen. Es ist also ganz entscheidend, wer diese Daten nutzt, wer sie schützt und wer sie zum Wohl der Patienten einsetzt. Hierfür brauchen wir verbindliche Regeln und Standards auf nationaler, europäischer und internationaler Ebene. Oder können wir den Unternehmen vertrauen? Ich meine Nein, auch wenn sie einen Missbrauch der Ihnen anvertrauten Daten natürlich bestreiten.

nisses möglichen Eingriffen in die Privatsphäre der Patienten und der (kommerziellen) Auswertung und Weitergabe ihrer persönlichen Daten entgegenzutreten. Bundeszahnärztekammer und Landeszahnärztekammern haben aufgrund ihres Fachwissens und ihrer Gemeinwohlverpflichtung die Verantwortung, Patienten dahingehend aufzuklären und als „Filter" von der Datenerhebung über die Datenspeicherung bis hin zur -weitergabe zu agieren. Wir müssen möglichen Eingriffen in die Privatsphäre der Patienten und der (kommerziellen) Auswertung und Weiter-

Den sicherlich in hohem Maße durch die Digitalisierung begründeten Chancen stehen auch erhebliche Risiken wie eine für Patienten nachteilige Risikoselektion gegenüber. Und auch die Grenzen zwischen einer echten Innovation und dem Missbrauch von Daten sind fließend.

Und wie steht es mit der politischen Administration? Sie konnte weder das Ausspähen des Kanzlerinnen-Handys noch die Cyberattacke auf den Bundestag verhindern. Zudem kann der Gesetzgeber hierfür sowohl auf nationaler wie auf europäischer Ebene nur den Rahmen setzen und gegebenenfalls nachsteuern. Denn verantwortlich für seine Daten bleibt der Nutzer, ergo der Patient, selbst.

Mit dem eHealth-Gesetz will die Bundesregierung immerhin für den Bereich der sozialen Krankenversicherung eine sichere digitale Kommunikation von Gesundheitsdaten gewährleisten. Begrüßenswert ist die Absicht des Gesetzgebers, die Telematikinfrastruktur rasch aufzubauen und damit die Grundlage für eine sichere elektronische Verbindung im Gesundheitswesen zu schaffen. Das ist die Voraussetzung, um überhaupt (tele)medizinische Anwendungen einführen zu können, die elektronische Kommunikationswege nutzen. Aus Sicht der Bundeszahnärztekammer funktioniert dies allerdings nur zum Teil. Mit ursächlich hierfür sind die extrem hohen Anforderungen an die Sicherheit von Sozialdaten, die die Infrastruktur starr machen und stark verkomplizieren. Denn die Musik spielt längst woanders. Die Tendenz zur weiteren Digitalisierung und Vernetzung von Gesundheitsdaten jenseits des eHealth-Gesetzes wird weitergehen – vor allem in mehr oder weniger unregulierten Bereichen.

Die Selbstverwaltung ist gefragt

Wer kann dann die Gesundheitsdaten schützen und darauf hinwirken, dass sie zum Wohl der Patienten eingesetzt werden? Hier sind meines Erachtens die Heilberufekammern gefragt, im Sinne des auf Vertrauen basierenden (Zahn)Arzt-Patienten-Verhältgabe ihrer persönlichen Daten entgegentreten. Zugleich müssen wir praktische Anregungen und Hilfestellungen geben.
Ein erster Schritt könnten z.B. von den Kammern zusammen mit der Politik und Industrie erarbeitete ethische Standards sein. Gerade wegen unserer Verantwortung gegenüber dem einzelnen Patienten und unserer Verpflichtung gegenüber der Gesellschaft als Ganzes können wir praktische Anregungen und Hilfestellungen zum Schutz und zur „fachgerechten" Verwertung von persönlichen Daten geben.

Doch auch die Kammern selbst müssen sich auf die zunehmende Digitalisierung einstellen. Die Kammer der Zukunft, die Kammer 2.0, wird (zumindest auch) eine digitale Kammer sein, die ihrer Dienstleistungspflicht gegenüber den Kollegen und gegebenenfalls Patienten auch online nachkommt. Zudem sind die Kammern durch die Heilberufsgesetze der Länder auch Player bei der Digitalisierung, da sie Heilberufsausweise ausgeben, deren digitale Zertifikate für einen sicheren Austausch sensibler (Gesundheits)Daten unerlässlich sind.

Letztlich müssen sich alle vertrauensgebundenen und verkammerten Berufe und ihre Berufsvertretungen Gedanken machen, wie wir im Zeitalter der Digitalisierung agieren können und sollten. Es geht darum, nationale, europäische und internationale Vorgaben und Richtlinien für den digitalen Wandel mitzugestalten, ethische Standards einzufordern und umzusetzen und eigene Prioritäten zu setzen. Wenn wir hier als glaubwürdiges Regulativ wirken, werden wir auch in Zukunft unserer Bestimmung nachkommen: gemeinwohlorientiert, patientenorientiert und kollegenorientiert.

Franz-Joseph Bartmann

Chancen, Risiken und Nebenwirkungen

Die Telematikinfrastruktur im deutschen Gesundheitswesen

Dr. Franz-Joseph Bartmann,
Vorsitzender des Ausschusses Telematik der Bundesärztekammer,
Präsident der Ärztekammer Schleswig-Holstein

Als im Jahr 2004 der Gesetzgeber unter dem Eindruck des sogenannten Lipobay-Skandals das Thema „Telematikinfrastruktur im Gesundheitswesen" in Gesetzesform goss, hatten die Parlamentarier eine Reihe von gutgemeinten Anwendungsszenarien der elektronischen Gesundheitskarte (eGK) vor Augen: das elektronische Rezept, Arzneimitteltherapiesicherheitsprüfung, Notfalldaten, Aktualisierung von Versichertenstammdaten auf der eGK und einiges mehr. Insgesamt ein bunter Strauß von Ideen, der sich im Laufe der Jahre dann zusehends noch vergrößert hat. So kam die Anwendung elektronische Fallakte und die Speicherung der Organspendeerklärung auf der eGK hinzu. Manches davon, wie z. B. die Notfalldaten und das Versichertenstammdatenmanagement haben sich weiter konkretisiert und sollen bald eingeführt werden. Andere Anwendungen, wie z. B. das elektronische Rezept, sind wieder in den Hintergrund getreten. Leitend für die jeweils aktuelle Umsetzungspriorität waren in der Vergangenheit oftmals aktuelle Themen, die angetrieben von einem aktuellen Problem in den politischen Raum getragen wurden und sich dann letztlich in Gesetzestexten wiederfanden. Eine systematische, ernsthaft medizinisch-fachliche Analyse, wo und wie genau eine Telematikinfrastruktur (TI) einen Beitrag zur Verbesserung der Patientenversorgung leisten kann, ist eher selten erfolgt. Das erklärt auch zu einem großen Teil die Vorbehalte der Ärzteschaft gegenüber dem Gesamtvorhaben. Aus Sicht der Ärzteschaft ist der Nutzenbeitrag neuer Technologien der Schlüssel für deren Akzeptanz. Technik um der Technik willen, ohne Bezug zu konkreten Herausforderungen in der täglichen Versorgungswirklichkeit, erscheint daher eher als unnötig, bürokratisch und oktroyiert. Wo und wie lassen sich nun solche nutzbringenden Anwendungen finden?

Einen Hinweis geben die hinlänglich beklagten „Insellösungen". Aus Mangel an einer bundesweit verfügbaren technischen Kommunikationsinfrastruktur sind in den vergangenen Jahren eigene, oftmals proprietäre Netzwerke entstanden, die ein konkretes Versorgungsszenario adressieren. Sie sind mit viel Einzelengagement geschaffen worden, weil der Wunsch und Zwang zu einer vernetzten Zusammenarbeit größer sind, als die jeweiligen juristischen und technischen Hürden. Einen guten Überblick zu solchen Projekten im Bereich der Telemedizin gibt das deutsche Telemedizinportal (www.telemedizin.fokus.fraunhofer.de). Andere individuelle Lösungsansätze zu sektorübergreifenden Versorgungsmodellen (elektronische Patientenakten etc.) lassen sich bundesweit finden. Für diese Netzwerke muss zukünftig die TI integrative Lösungen anbieten, um zumindest die technischen Einstiegsbarrieren zu senken.

Ein weiterer Hinweis ergibt sich aus einer repräsentativen Allensbach-Befragung „Der Einsatz von Telematik und Telemedizin im Gesundheitswesen" aus dem Jahr 2010 . In der im Auftrag der Bundesärztekammer durchgeführten Befragung haben Krankenhaus- und niedergelassene Ärzte den Nutzen verschiedener Anwendungsfelder der Telematik eingeschätzt. Weit vorn in der Einstufung liegen der Notfalldatensatz, der elektronische Arztbrief und die elektronische Arzneimitteltherapiesicherheitsprüfung. Zurückhaltender wird eine elektronische Patientenakte bewertet. Gegenüber dem elektronischen Rezept herrscht eher Skepsis. Die Befragung zeigt, dass bei der Ärzteschaft auch hier das Einsatzgebiet einer TI primär für die Verbesserung in der Patientenversorgung gesehen wird, weniger in der Beseitigung oder Verringerung administrativen Aufwands.

Der Gesetzgeber setzt nun, zehn Jahre nach der ersten gesetzlichen Festschreibung der eGK und der TI, im Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) durch die Förderung medizinischer Anwendungen in der TI begrüßenswerte Impulse in diese Richtung. Das Anlegen und Aktualisieren von Notfalldatensätzen, der Versand elektronischer Arztbriefe, die Erstellung eines elektronischen Medikationsplans als Vorstufe einer Arzneimitteltherapiesicherheitsprüfung sowie Vorgaben zur konsiliarischen Befundbeurteilung von Röntgenaufnahmen mittels Telemedizin sind Ausdruck des Gedankens, dass eine TI ihre Stärken in der konkreten Verbesserung der medizinischen Versorgung ausspielen soll.

Mit diesen positiven Wirkungen des E-Health-Gesetzes gehen aber leider auch unerwünschte Nebenwirkungen einher. So sieht das Gesetz für die Einführung dieser Anwendungen verbindliche Fristen

teilweise in Verbindung mit Sanktionen vor. Wenn gesetzte Termine nicht eingehalten werden, drohen dem GKV-Spitzenverband, der Kassenärztlichen Bundesvereinigung und der Kassenzahnärztlichen Bundesvereinigung in ihrer Rolle als Gesellschafter der gematik massive Haushaltskürzungen. Die Sanktionen kommen zu einem Zeitpunkt, an dem der Einfluss der Betroffenen, den Sanktionen aus dem Weg zu gehen, nicht mehr gegeben ist. Denn längst sind die Verträge mit Industriekonsortien zur Testung der ersten Anwendungen der eGK und der TI geschlossen. Ob Termine eingehalten werden können, liegt nun überwiegend in der Hand dieser Konsortien. Die Sanktionsdrohung des E-Health-Gesetzes, die sich in einer Haushaltskürzung der genannten Körperschaften in Höhe von ca. 10 bis 15 Prozent niederschlägt, verführt dazu, dass Aspekte der Wirtschaftlichkeit und der Qualität der zu testenden Anwendungen in den Hintergrund rücken. Aber auch die Industrie benötigt ihre Zeit, um qualitativ hochwertige Produkte zu liefern. Diese sind wiederum unabdingbare Voraussetzungen, dass die TI und deren Anwendungen nicht nur funktionieren, sondern Patienten und Ärzte auch überzeugen.

Dieser gesetzgeberische Druck kann eine stringente „Telematikstrategie“ nicht ersetzen, an der man sich auf dem weiteren Gestaltungsweg orientieren könnte. An ihr mangelt es nach wie vor. Vieles bleibt auch nach einem geplanten E-Health-Gesetz unscharf und klärungsbedürftig. Eine stringente Ausrichtung der gesetzlichen Rahmenbedingungen für die TI auf medizinische Versorgungsziele ist leider nur unzureichend erkennbar. Unter einer solchen Zielausrichtung kann man alle Vorhaben fassen, die ein direkt benanntes Defizit oder eine Schwäche in der Patientenversorgung benennen und dazu auf eine klar messbare Verbesserung abzielen. Leider sind im aktuellen gesetzgeberischen Verfahren Vorschläge, die in die dargestellte Richtung zielen, z. B. in den kommenden fünf Jahren die Hälfte aller chronisch erkrankten Patienten mit einer elektronischen Patientenakte auszustatten, nicht durchgedrungen.

Letztlich wird man aber nicht um eine Analyse herumkommen, mit der die erfolgversprechenden Anwendungsbereiche für eine Vernetzung im Gesundheitswesen aus dem Blickwinkel von Versorgungsnotwendigkeiten herausgearbeitet werden.
Die Politik ist also weithin aufgerufen, mit Weitblick und Sachverstand zu agieren. Um dies zu unterstützen, bleiben die Selbstverwaltungspartner dabei ebenfalls in der Verantwortung. Eine gemeinsame Vereinbarung und ein Konsens zu einer konzeptionellen Ausrichtung der TI an konkret bestimmten Versorgungszielen ist ein erstrebenswertes Ziel.

Eine systematische, ernsthaft medizinisch-fachliche Analyse, wo und wie genau eine Telematikinfrastruktur (TI) einen Beitrag zur Verbesserung der Patientenversorgung leisten kann, ist eher selten erfolgt. Das erklärt auch zu einem großen Teil die Vorbehalte der Ärzteschaft gegenüber dem Gesamtvorhaben. Aus Sicht der Ärzteschaft ist der Nutzenbeitrag neuer Technologien der Schlüssel für deren Akzeptanz. Technik um der Technik willen, ohne Bezug zu konkreten Herausforderungen in der täglichen Versorgungswirklichkeit, erscheint daher eher als unnötig, bürokratisch und oktroyiert.

Alexander Beyer

Ein sicheres Netz für Gesundheitsdaten: Die Telematikinfrastruktur

Alexander Beyer,
Geschäftsführer der gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Um die Patientenversorgung zu verbessern, wird das deutsche Gesundheitswesen digital und sektorenübergreifend vernetzt. Als eine Art Datenautobahn können mit der Telematikinfrastruktur künftig medizinische Daten zwischen den informationstechnischen Systemen von Praxen und Krankenhäusern schnell und vor allem sicher ausgetauscht werden. Das bietet die enorme Chance, nicht nur den Verwaltungsaufwand zu minimieren und bestehende Behandlungsabläufe zu optimieren, sondern zugleich die Patientenversorgung sowie Datenschutz und Datensicherheit im Gesundheitswesen deutlich zu verbessern.

Moderne Informations- und Kommunikationstechnologien sind längst nicht mehr aus dem gesellschaftlichen Alltag wegzudenken. Und auch in Industrie und Handel ist der Umgang mit solchen Technologien selbstverständlich. Nur dem Gesundheitswesen fällt es bislang schwer, diese flächendeckend als entsprechenden Ersatz für eine papiergebundene Kommunikation und lückenhafte Dokumentation anzunehmen und umzusetzen. Per Post oder Fax versandte Arztbriefe oder Laborbefunde sowie Patienten, die ihre Röntgenbefunde von einem Heilberufler zum anderen transportieren, sind nach wie vor keine Seltenheit. Dabei bieten Informations- und Kommunikationstechnologien ein großes Potenzial, um Prozessabläufe effizienter sowie die Arbeitsteilung und Zusammenarbeit aller Beteiligten effektiver zu gestalten.

Für qualitativ hochwertige, an den Bedürfnissen der Patientinnen und Patienten orientierte und zugleich wirtschaftliche Gesundheitsversorgung bedarf es zweifelsohne der Kunstfertigkeit von Heilberuflern im Zusammenspiel mit dem medizinischen und technischen Fortschritt. Doch auch die für die Behandlung erforderlichen Informationen müssen zuverlässig und sicher vorliegen. Das aber erweist sich im Praxisalltag als immer schwieriger umsetzbar. Denn dieser ist geprägt von einem fortschreitenden Fachkräftemangel, einer steigenden Zahl älterer, multimorbider und chronisch kranker Menschen sowie einem zunehmenden Verwaltungsaufwand, der die Kosten im Gesundheitswesen in die Höhe schnellen lässt. Aktuellen Schätzungen des Nationalen Normenkontrollrates zufolge entstehen durch sogenannte Informationspflichten im ambulanten Sektor jährliche Ausgaben in Höhe von insgesamt 4,33 Milliarden Euro[1]. Auf den zahnärztlichen Bereich entfallen davon 1,13 Milliarden Euro.[2] Große Aufwände aus Informationspflichten entstehen für eine Zahnarztpraxis beispielsweise bei der Versorgung mit Zahnersatz und Zahnkronen.

Zu dem Kostenfaktor kommt der zeitliche Aufwand hinzu: Viele Heilberufler klagen seit Jahren darüber, im Arbeitsalltag immer weniger Zeit für ihre Patientinnen und Patienten zu haben.[3] Darüber hinaus haben Ärzte und medizinisches Personal fortwährend mit einer Fülle von Unterlagen wie Laborberichten oder Untersuchungsergebnissen zu tun, die standardisiert verwaltet werden und schnell abrufbar sein müssen. Mitunter liegen diese jedoch nur in Papierform vor und müssen erst zeitaufwendig digitalisiert werden, damit sie in der Praxissoftware zur Verfügung stehen. Anschließend werden sie im Bedarfsfall entweder in Papierform an Kollegen gefaxt, per Post versendet oder aber unverschlüsselt über das Internet verschickt.

Ferner wächst die Bedeutung einer sektorenübergreifenden Gesundheitsversorgung kontinuierlich.[4] Viele Patienten werden heute von Ärztinnen und Ärzten verschiedener Fachrichtungen, in Krankenhäusern, von Physio- und Psychotherapeuten sowie anderen Heilberuflern betreut. Dabei kommt es immer wieder zu Informationsbrüchen an den Schnittstellen zwischen ambulanter und stationärer Versorgung oder zwischen den unterschiedlichen Institutionen: Wichtige, für die medizinische Behandlung notwendige Informationen liegen dadurch oftmals gar nicht oder nur lückenhaft vor.

Um dem steigenden Bedarf an Gesundheitsversorgung gerecht zu werden, entstehen vielerorts seit Jahren telemedizinische Netzwerke. Dabei handelt

1 *Nationaler Normenkontrollrat: Mehr Zeit für Behandlung. Vereinfachung von Verfahren und Prozessen in Arzt- und Zahnarztpraxen, herausgegeben vom Statistischen Bundesamt, Wiesbaden 2015, S.42.*
2 *ebenda*
3 *Vgl. www.kbv.de (Ärztemonitor 2014), Stand: 13.11.2014*
4 *Vgl. Geiger B, Wolf T. IT-Strategien für sektorenübergreifende Versorgungskonzepte, in: Hrsg. Innovatives Versorgungsmanagement, hrsg. von Amelung VE et al, Berlin 2011. S. 341–345, hier: 341.*

Moderne Informations- und Kommunikationstechnologien sind längst nicht mehr aus dem gesellschaftlichen Alltag wegzudenken. Nur dem Gesundheitswesen fällt es bislang schwer, diese flächendeckend als entsprechenden Ersatz für eine papiergebundene Kommunikation und lückenhafte Dokumentation anzunehmen und umzusetzen.

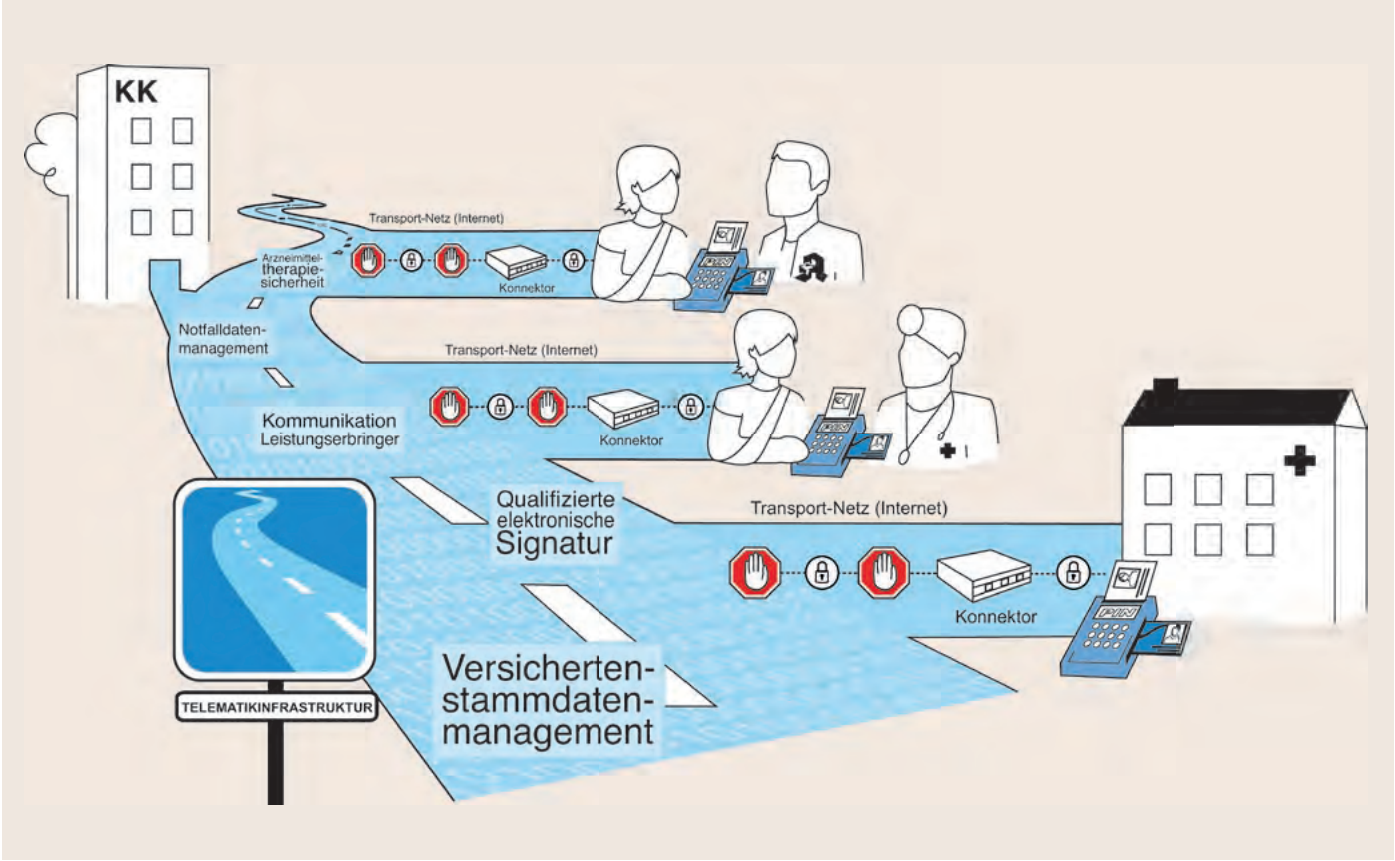
es sich oftmals um Pilotprojekte mit regionalen Ansätzen. Viele dieser Projekte sind – mangels fortwährender Anpassungen an die Fortschritte im informationstechnischen Bereich – technisch nicht darauf vorbereitet, sich mit anderen Systemen zusammenzuschließen. Nicht selten scheitern diese Netzwerke dann an dem Übergang von der Projektphase in einen Regelbetrieb[5] – obwohl sie ihre Praxistauglichkeit bereits unter Beweis gestellt haben.

Telematikinfrastruktur sichert wohnortnahe Patientenversorgung

Mit dem in §291a Sozialgesetzbuch V festgeschriebenen Aufbau der Telematikinfrastruktur (TI) soll schließlich durch die gematik eine interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur für das gesamte Gesundheitswesen geschaffen werden. Gesellschafter der gematik sind die Bundesärztekammer, die Bundeszahnärztekammer, der Deutsche Apothekerverband, die Deutsche Krankenhausgesellschaft, der GKV-Spitzenverband, die Kassenärztliche Bundesvereinigung sowie die Kassenzahnärztliche Bundesvereinigung. Gemeinsam mit diesen und in Kooperation mit den beauftragten Industrieunternehmen arbeitet die gematik mit Hochdruck daran, die Telematikinfrastruktur mit den dazugehörigen Anwendungen aufzubauen. Diese werden dazu beitragen, den Verwaltungsaufwand zu minimieren, bestehende Behandlungsabläufe zu optimieren sowie bereits vorhandene, nicht-interoperabel agierende telemedizinischen Einzelprojekte in die TI zu integrieren und flächendeckend zur Verfügung zu stellen.

Zugleich stellt die TI sicher, dass alle für eine medizinische Behandlung relevanten Informationen schnell

5 *Veronika Strotbaum: Europa wächst zusammen?! Aktuelle Entwicklungen und Perspektiven der Telemedizin in Europa, in: e-Health 2015, hrsg. von Frank Duesberg, Solingen 2014, S. 48-51, hier: 48.*



Telematikinfrastruktur
Quelle: gematik

und zuverlässig vorliegen, wenn sie tatsächlich benötigt werden. „Sind strukturierte und digital erfasste Informationen sektorenübergreifend verfügbar, ist von [...] positiven Effekten auszugehen“[6], bewertet der Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen die Telematikinfrastruktur in seinem Sondergutachten 2012 zum Wettbewerb an der Schnittstelle zwischen ambulanter und stationärer Gesundheitsversorgung. Für Patienten bedeute dies unter anderem, dass Doppeluntersuchungen vermieden werden.[7]

sollen daher im [einheitlichen Bewertungsmaßstab] ausgebaut und mit Zuschlägen gefördert werden.“ Auch wird darin bekräftigt, dass die Telematikinfrastruktur mit ihren Sicherheitsmerkmalen als die zentrale Infrastruktur für eine sichere Kommunikation im Gesundheitswesen etabliert werden soll. Basierend darauf, erarbeitet die gematik technische und datenschutzrechtliche Standards, damit „neue digitale Anwendungen vorhandene Standards und Profile nutzen können und weitere ‚Insellösungen‘ vermieden werden“[9].

Die Telematikinfrastruktur setzt sich aus einer Vielzahl verschiedener technischer Elemente zusammen, die die informationstechnischen Systeme aller Beteiligten im Gesundheitswesen miteinander vernetzen. Dabei hat der Schutz der medizinischen Daten oberste Priorität.

Der sektorenübergreifende Informationsaustausch mittels Telematikinfrastruktur kann insbesondere in ländlichen und strukturschwachen Regionen die medizinische Versorgung sicherstellen. Durch Telematik und Telemedizin lassen sich unnötige Arztkontakte vermeiden und Patienten können trotz großer Entfernungen auch in Zukunft qualitativ hochwertig, wohnortnah und kosteneffizient betreut werden. Die Versorgung durch den Arzt soll nicht ersetzt, sondern vielmehr ergänzt werden, um Heilberufler zu entlasten und ihnen wieder mehr Zeit für ihre Patientinnen und Patienten zu geben.

Das Potenzial der Telematikinfrastruktur für eine wohnortnahe Patientenversorgung auch in strukturschwachen Regionen hat die Gesundheitsministerkonferenz erkannt: „Eine flächendeckende, qualitativ hochwertige, effiziente, aber auch finanzierbare medizinische Versorgung kann nur dann sachgerecht unterstützt werden, wenn baldmöglichst umfassende nutzerorientierte Telematikanwendungen auch den ländlichen Raum anbinden. Hierzu bedarf es des Aufbaus einer bundesweiten, sektorenübergreifenden Infrastruktur, die den Anforderungen des Datenschutzes genügt“[8], heißt es in einem aktuellen Beschluss der Gesundheitsminister.
Auch die Bundesregierung hat darauf reagiert und im Gesetzentwurf des sogenannten E-Health-Gesetzes hervorgehoben: „Telemedizinische Leistungen

Datenschutz hat bei medizinischen Daten oberste Priorität

Die Telematikinfrastruktur setzt sich aus einer Vielzahl verschiedener technischer Elemente zusammen, die die informationstechnischen Systeme aller Beteiligten im Gesundheitswesen miteinander vernetzen. Sie dient als eine Art Datenautobahn, auf der medizinische Daten zwischen den informationstechnischen Systemen von Arzt- und Zahnarztpraxen sowie Krankenhäusern schnell und vor allem sicher transportiert werden können. Vor dem Transport werden die Daten in der (Zahn)Arztpraxis verschlüsselt. Nur der Empfänger kann die Daten entschlüsseln und darauf zugreifen. Denn der Datenschutz spielt eine entscheidende Rolle.

Um die Patientenrechte und -souveränität zu wahren, entscheidet der Versicherte eigenverantwortlich, ob überhaupt und welche medizinischen Daten gespeichert oder gelöscht sowie von wem diese gelesen und genutzt werden dürfen. Die Datenhoheit liegt also stets in der Hand des Versicherten.

Den Zugriff auf Daten auf der elektronischen Gesundheitskarte oder bei medizinischen Anwendungen über die Telematikinfrastruktur hat der Gesetzgeber im §291a Sozialgesetzbuch V geregelt. Die auf der eGK gespeicherten Versichertenstammdaten sind, wie bei der bisherigen Krankenversichertenkarte, frei zugänglich.
Auf medizinische Daten können ausschließlich Ärzte, Zahnärzte, Therapeuten und andere Heilberufler zugreifen, die einen elektronischen Heilberufsausweis besitzen. Das heißt: Heilberufsausweis und

6 *Sondergutachten 2012 des Sachverständigenrates zur Begutachtung der Entwicklung im Gesundheitswesen „Wettbewerb an der Schnittstelle zwischen ambulanter und stationärer Gesundheitsversorgung“ vom 10.07.2012, BT-Drucksache 17/10323, S. 141.*
7 *Ebenda.*
8 *Beschluss der 88. Gesundheitsministerkonferenz der Länder vom 01.07.2015, TOP 5.1 „Beteiligung der Länder am Aufbau einer Telematikinfrastruktur im Rahmen der Digitalisierung des Gesundheitswesens.*
9 *E-Health-Gesetz. Gesetzentwurf der Bundesregierung eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen. Stand: 22.06.2015.*

eGK müssen gleichzeitig in das Lesegerät gesteckt sein. Außerdem muss der Patient dem Zugriff auf seine Daten mit der Eingabe seiner PIN zustimmen. Jeder Zugriff auf die Daten der elektronischen Gesundheitskarte wird auf der Karte protokolliert. So lässt sich jederzeit nachvollziehen, wer die Daten eingesehen hat. Datenschützer wie beispielsweise der ehemalige schleswig-holsteinische Landesdatenschutzbeauftragte Thilo Weichert halten deshalb das Konzept der Telematikinfrastruktur aus Datenschutzsicht für vorbildlich.[10]

Aus Datenschutzgründen werden beim Abgleich der Versichertenstammdaten sämtliche Informationen zur Praxis anonymisiert. Dazu gehört unter anderem die Auskunft darüber, bei welchem Arzt oder Zahnarzt die eGK eingelesen wurde. Die Krankenkasse erfährt lediglich, dass für eine von ihr herausgebene Gesundheitskarte angefragt wurde, ob die darauf abgelegten Versichertenstammdaten noch aktuell sind ...

Umfangreiche Tests gewährleisten Sicherheit der TI

Um zu gewährleisten, dass die technischen Elemente der Telematikinfrastruktur sicher, interoperabel und kompatibel funktionieren, erarbeitet die gematik Konzepte und Spezifikationen für jedes einzelne Element. Anhand dieser Spezifikationen entwickelt die Industrie dann die Produkte der Telematikinfrastruktur, die anschließend von der gematik umfangreich getestet und vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert werden. Erst wenn die technischen Elemente ihre Funktionalität und die vorgeschriebenen Sicherheitseigenschaften nachweisen können und von der gematik zugelassen wurden, dürfen sie in der Telematikinfrastruktur eingesetzt werden. Bei diesem Prozess arbeitet die gematik im Interesse der Patientinnen und Patienten intensiv mit dem Bundesgesundheitsministerium, der Bundesdatenschutzbeauftragten, den Landesdatenschutzbeauftragten und Patientenvertretern zusammen.

Die meisten gesetzlich Versicherten nutzen bei einem Arztbesuch mittlerweile ganz selbstverständlich ihre elektronische Gesundheitskarte (eGK). Auch in Arzt- und Zahnarztpraxen sowie Krankenhäusern gehört der Umgang mit den entsprechenden Lesegeräten zum Alltag. Damit ist die Basis geschaffen, um Praxen und Krankenhäuser über die Telematikinfrastruktur miteinander zu vernetzen und zu testen, ob der Betrieb im Alltag störungsfrei funktioniert. Als erste Anwendungen und Funktionen werden der Online-Abgleich von Versichertenstammdaten auf der elektronischen Gesundheitskarte, die qualifizierte elektronische Signatur, der sichere Informationsaustausch zwischen Heilberuflern, ein sicherer Internetzugang für Praxen und Krankenhäuser sowie die Anbindung von bestehenden Netzen wie dem Sicheren Netz der KVen oder dem Portal der Kassenzahnärztlichen Vereinigung Westfalen-Lippe an die Telematikinfrastruktur erprobt. Die Tests finden in den Testregionen Nordwest (Schleswig-Holstein, Nordrhein-Westfalen, Rheinland-Pfalz) und Südost (Sachsen und Bayern) statt.

Der Online-Abgleich: Aktuelle Versichertenstammdaten künftig auf Knopfdruck

Auf der elektronischen Gesundheitskarte sind aktuell ausschließlich die Versichertenstammdaten des Patienten gespeichert. Durch die Vernetzung des Gesundheitswesens können Ärzte, Zahnärzte und Psychotherapeuten künftig beim Einlesen der eGK online überprüfen, ob ein gültiges Versicherungsverhältnis vorliegt und die Versichertenstammdaten noch aktuell sind. Liegt kein gültiges Versicherungsverhältnis vor, wird die Karte gesperrt und im Praxis- oder Krankenhaussystem erscheint ein entsprechender Hinweis. Der Online-Abgleich ist bei jeder ersten Behandlung im Quartal verpflichtend.

Sind die Versichertenstammdaten nicht mehr aktuell, erfragt das System bei der jeweiligen Krankenkasse, ob ein Aktualisierungsauftrag vorliegt. Das heißt: Zieht der Versicherte beispielsweise um, meldet er dies wie bisher seiner Krankenkasse, die die Adressänderung in ihr System eingibt. Sobald die Gesundheitskarte das nächste Mal in der Arztpraxis eingelesen wird, werden die Versichertenstammdaten auf der Karte mit dem aktuellen Datensatz überschrieben. Damit entfällt der aufwendige Kartenaustausch. Für Praxen und Krankenhäuser hat der Online-Abgleich den Vorteil, dass sie ihre administrativen Patientendaten auf Wunsch einfach aktualisieren können. Damit sind diese in jedem Quartal aktuell und Abrechnungsfehler können vermieden werden.

10 Schlingensiepen I, Krüger A. Nicht für fremde Augen: In: Financial Times Deutschland, Dossier IT-Sicherheit vom 6.11.2012, S. 3- 5, hier: 4

Alternativ kann der Versichertenstammdaten-Abgleich auch offline durchgeführt werden. Beim sogenannten Standalone-Szenario wird die Gesundheitskarte mit den aktualisierten Versichertenstammdaten noch einmal in ein separat installiertes Kartenterminal eingelesen, um die Daten in das Praxissystem zu übernehmen.

Aus Datenschutzgründen werden beim Abgleich der Versichertenstammdaten sämtliche Informationen zur Praxis anonymisiert. Dazu gehört unter anderem die Auskunft darüber, bei welchem Arzt oder Zahnarzt die eGK eingelesen wurde. Die Krankenkasse erfährt lediglich, dass für eine von ihr herausgebene Gesundheitskarte angefragt wurde, ob die darauf abgelegten Versichertenstammdaten noch aktuell sind oder gegebenenfalls aktualisiert werden müssen.

Eindeutig zu erkennen: die qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur ist das digitale Pendant zur Unterschrift von Hand. Mit der Signatur können Heilberufler medizinische Dokumente elektronisch unterschreiben. Damit geben sich diese als Absender zu erkennen und bestätigen die rechtsgültige Echtheit des Dokuments. Falls diese nachträglich verändert oder ergänzt werden, ist das durch die Prüfung der Signatur erkennbar. Um Dokumente qualifiziert elektronisch signieren zu können, ist eine Signaturkarte erforderlich. Für Heilberufler ist dies der elektronische Heilberufsausweis.

Um zu vermeiden, dass beim Signieren mehrerer Dokumente für jedes einzelne Dokument die PIN eingegeben werden muss, wird es eine sogenannte Stapelsignaturfunktion geben. Das heißt, Praxis- und Krankenhausmitarbeiter können mehrere Arztbriefe vorbereiten, die dann vom Heilberufler zusammen freigegeben und mit dessen qualifizierter elektronischer Signatur unterzeichnet werden können.

Für eine vertrauliche Kommunikation unter Kollegen

Über die Telematikinfrastruktur können Heilberufler zudem künftig Befunde oder andere Dokumente sicher und schnell austauschen. Es werden nur verschlüsselte Daten versendet. Unbefugte können die Daten nicht einsehen. Um Dokumente vertraulich versenden zu können, müssen sich Ärzte, Zahnärzte und Psychotherapeuten sowie Krankenhäuser bei einem entsprechenden, dafür zugelassenen Fachdienstanbieter registrieren. Dafür benötigen Heilberufler lediglich ihren gültigen Heilberufsausweis.

Die qualifizierte elektronische Signatur ist das digitale Pendant zur Unterschrift von Hand. Mit der Signatur können Heilberufler medizinische Dokumente elektronisch unterschreiben. Damit geben sich diese als Absender zu erkennen und bestätigen die rechtsgültige Echtheit des Dokuments.

Medizinische Einrichtungen brauchen ihre gültige Institutionskarte. Nur registrierte Nutzer können untereinander kommunizieren.

Die neue technische Funktion fügt sich nahtlos in das vorhandene Praxis- und Krankenhaussystem ein. Das erleichtert Heilberuflern den sicheren und schnellen Austausch von sensiblen Patientendaten. Das heißt: Die Funktion ist so eingerichtet, dass die Nutzer sie direkt über ihr technisches System nutzen oder weiter ihre bisherigen E-Mail-Programme wie Outlook oder Thunderbird verwenden können. Die Funktion arbeitet unbemerkt im Hintergrund. Arbeitsprozesse in den Praxen laufen unverändert weiter. Die Anwendung verschlüsselt die zu versendenden Daten und signiert diese auf Wunsch. Auch empfangene Daten entschlüsselt diese automatisch, überprüft die Signatur und stellt anschließend die Daten wie gewohnt im E-Mail-Programm zur Verfügung.

Ohne Medienbrüche: Medizinische Anwendungen verbessern Patientenversorgung

Nur mit zuverlässigen und sicheren Informationen lassen sich Patienten auch zukünftig adäquat versorgen. Sind der Online-Abgleich von Versichertenstammdaten und der sichere Informationsaustausch zwischen Heilberuflern flächendeckend verfügbar, werden weitere Funktionen folgen:

So können Patienten künftig Informationen etwa über Allergien, Arzneimittelunverträglichkeiten oder Implantate, die im Notfall wichtig sein können, auf der Gesundheitskarte speichern lassen. Im Notfall

Wie kein anderes Netzwerk in Deutschland bietet die Telematikinfrastruktur die enorme Chance, Qualität und Wirtschaftlichkeit im Gesundheitswesen zu verbessern sowie den Datenschutz und die Informationssicherheit zu erhöhen.

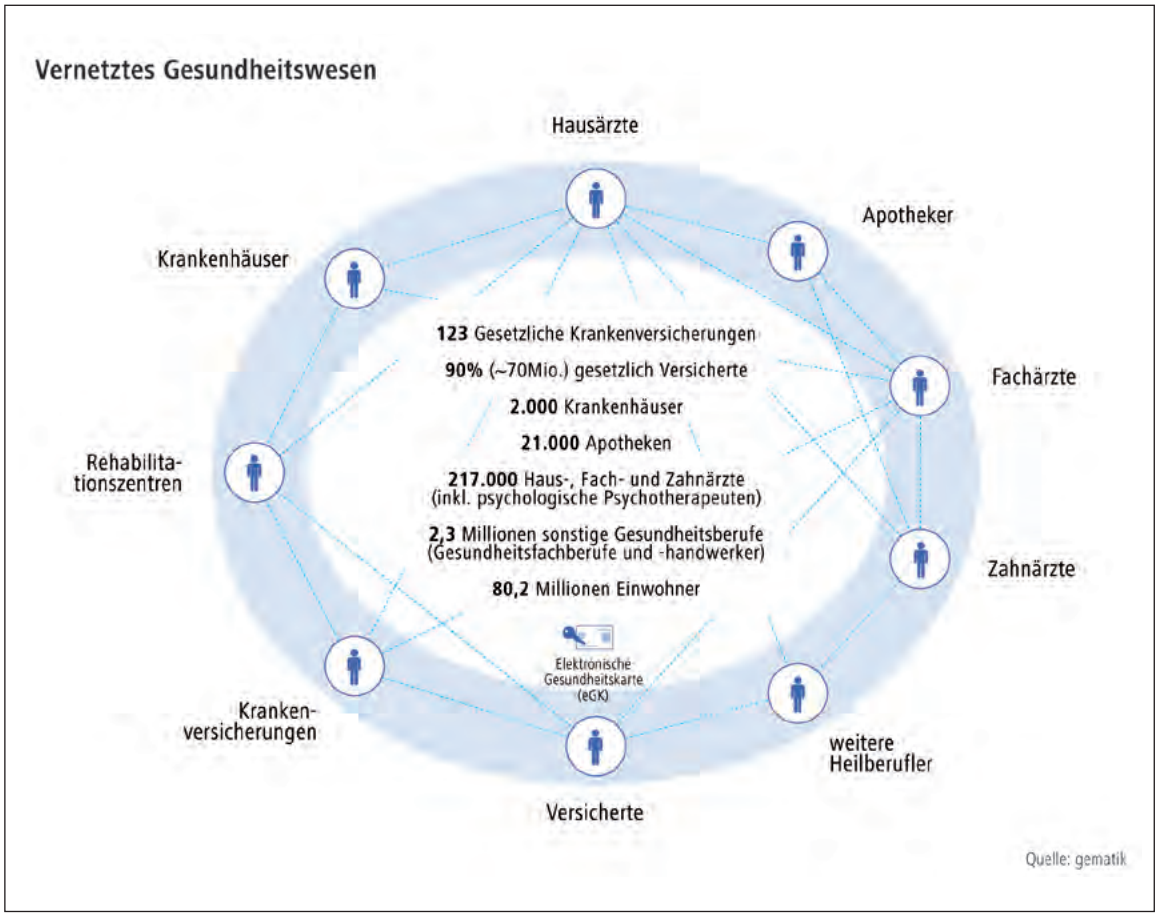
können Ärzte oder Notfallsanitäter dann die Daten ohne PIN-Eingabe des Patienten mit einem mobilen Lesegerät abrufen. Denn der Versicherte ist im Notfall mitunter gar nicht zur Eingabe einer PIN in der Lage. Allerdings hat der Versicherte hier bereits zuvor in die Nutzung seiner Notfalldaten eingewilligt, indem er gemeinsam mit seinem Arzt und dessen Heilberufsausweis sowie durch Eingabe seiner PIN die Notfalldaten auf seiner elektronischen Gesundheitskarte angelegt hat.

Mit dem Datenmanagement zur Prüfung der Arzneimitteltherapiesicherheit werden Ärzte und Apotheker in Zukunft detaillierte Informationen darüber erhalten, welche Medikamente der Patient aktuell einnimmt. So können Fehl- und Doppelverordnungen und unerwünschte Wechselwirkungen einfacher vermieden werden.

Mittels elektronischer Fallakten sollen medizinische Daten eines Patienten zu einem bestimmten Fall über die Telematikinfrastruktur ohne Medienbrüche sektorenübergreifend ausgetauscht werden können. Das verbessert beispielsweise die Betreuung von herzkranken Patienten in versorgungsschwachen Regionen oder erleichtert den Versorgungsübergang von Krebspatienten vom Krankenhaus zu ambulanten Einrichtungen.

Fazit

Wie kein anderes Netzwerk in Deutschland bietet die Telematikinfrastruktur die enorme Chance, die Patientenversorgung auch in strukturschwachen, ländlichen Regionen qualitativ hochwertig und wohnortnah auch in Zukunft aufrechtzuerhalten. Zudem wird die Qualität und Wirtschaftlichkeit im Gesundheitswesen verbessert sowie Datenschutz und Informationssicherheit erhöht.



Holm Diening

Sicherheitsmechanismen der Telematikinfrastruktur

Holm Diening,
Abteilungsleiter Datenschutz und Informationssicherheit, gematik GmbH

Die Telematikinfrastruktur – zusammen mit der elektronischen Gesundheitskarte – gehört europaweit zu einem der größten IT-Projekte. Die Anforderungen an Datenschutz und Sicherheit sind dabei enorm hoch.

Als Geburtsstunde der elektronischen Gesundheitskarte (eGK) gilt der sogenannte „Lipobay"-Skandal. Bei diesem starben weltweit Menschen an Wechselwirkungen zwischen dem Cholesterinsenker Lipobay und anderen Arzneimitteln. Aus der ursprünglich als digitale „Verschreibungsliste" geplanten eGK wurde schließlich das Konzept für ein umfassendes, vernetztes Gesundheitssystem: die Telematikinfrastruktur (TI).
Der Umgang mit sensiblen medizinischen Daten ruft jedoch auch Sorgen und Ängste hervor, denen nur mit besonders vertrauenswürdigen Lösungen begegnet werden kann. Genau dies ist der Auftrag der gematik nach §291b SGB V. Dieser umfasst: „die Interessen von Patientinnen und Patienten zu wahren", „die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen" und „das notwendige Sicherheitsniveau der Telematikinfrastruktur zu gewährleisten". Die Vertrauenswürdigkeit der TI hängt in starkem Maße davon ab, wie wirksam die Sicherheitsmaßnahmen sind und wie konsequent diese in der Praxis tatsächlich umgesetzt und nachgewiesen werden.

Grundlegende Sicherheitsparadigmen

Die Sicherheit der Telematikinfrastruktur wird maßgeblich durch die kontinuierliche Begleitung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei der Entwicklung von fachspezifischen Sicherheitskonzepten sowie verbindlichen Zertifizierungsanforderungen für die sicherheitsrelevanten TI-Bestandteile durch das BSI erreicht. Alle technischen Spezifikationen, Schutzprofile und technischen Richtlinien sind auf der Internetseite der gematik und des BSI veröffentlicht.

Zwei-Schlüssel-Prinzip

Durch das Zwei-Schlüssel- Prinzip ist sichergestellt, dass auf medizinische Daten nur mit der eGK des Versicherten zusammen mit einem berechtigten Heilberufsausweis (HBA) zugegriffen werden kann. Erst wenn die eGK durch eine erfolgreiche Card-2-Card-Authentifizierung festgestellt hat, dass sie sich einem gültigen HBA nach PIN-Eingabe gegenübersieht und auch der Versicherte seine PIN eingegeben hat, ist der Zugriff auf die medizinischen Daten möglich.
Eine Ausnahme bildet der Zugriff auf freiwillig auf der Karte abgelegte medizinische Notfalldaten: Ärzte, Notfallsanitäter und Rettungsassistenten können die auf der Karte gespeicherten Notfalldaten auch ohne PIN–Eingabe durch den Versicherten abrufen – falls der Versicherte nicht mehr in der Lage ist diese einzugeben. Denn der Versicherte hat dem Zugriff im Notfall zuvor bei der Anlage des Datensatzes schriftlich zugestimmt. Die Autorisierung für den Zugriff auf die Daten wird auf der Gesundheitskarte dokumentiert.
Allerdings ist der Zugriff auf die Notfalldaten durch einen HBA ohne PIN-Eingabe des Patienten auf bestimmte Typen von Heilberufsausweisen beschränkt. Maßgeblich sind hier bestimmte Inhalte der Zertifikate des HBA, die nur bei Ärzten, Notfallsanitätern und Rettungsassistenten gesetzt sind. Die technische Durchsetzung des Zugriffsschutzes erfolgt dabei direkt durch das Kartenbetriebssystem der eGK, das damit die Rechte der Versicherten umsetzt.
Die Definition der Zugriffsprinzipien auf medizinische Daten leitet sich im Übrigen immer aus den Vorgaben für die jeweiligen Zugriffsrechte ab, die im §291a SGB V geregelt sind.

Dezentrale und verschlüsselte Speicherung schützt Daten

Derzeit gibt es keine medizinische Fachanwendung in der Telematikinfrastruktur, die einen zentralen Speicherdienst betreibt. Alle bisher spezifizierten Anwendungen verwenden für die Speicherung von medizinischen Daten einzig die eGK, sofern sie nicht gänzlich in der Praxis oder im Krankenhaus verbleiben.
Für Anwendungen wie etwa das „Datenmanagement zur Prüfung der Arzneimitteltherapiesicherheit", die auch eine Online-Speicherung in einem Fachdienst vorsehen, gilt der unabdingbare Grundsatz der patientenindividuellen Datenverschlüsselung mit der eGK. Die Daten können dadurch nur in einer Praxis oder im Krankenhaus über den Konnektor entschlüsselt werden. Konnektoren können nur eingesetzt werden, wenn diese die hohen BSI-Sicherheitskriterien erfül-

len, von der gematik zugelassen sind und durch eine berechtigte Praxis oder ein Krankenhaus freigeschaltet wurden. Auf diese Weise sind medizinische Daten auch bei einer Online-Speicherung nur dezentral im Klartext vorhanden. Eine solche Fachanwendung könnte außerdem nur nach einem gesetzlichen Auftrag des Bundesgesundheitsministeriums, nach gemeinsamer Entscheidung der gematik-Gesellschafter sowie unter notwendiger Einbeziehung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und des BSI etabliert werden.

Geschlossenes Netz

Das zentrale Netz der TI ist ein in sich geschlossenes Netz: Zugang zu diesem bestehen nur über sichere zentrale Zugangspunkte, die entsprechend der konkreten Anforderungen der Fachdienste durch den Gesamtbetriebsverantwortlichen – die gematik – freigeschaltet werden. Eine Anbindung an die TI-Plattform setzt voraus, dass der jeweilige Dienst ein Zulassungs- oder Bestätigungsverfahren bei der gematik durchläuft. Medizinische Institutionen werden nur über einen vom BSI zertifizierten Konnektor und einen VPN-Zugangsdienst an die TI angeschlossen.

Verschlüsselte Datenübertragung

Wie bereits ausgeführt, werden medizinische Daten oder andere personenbezogene Daten des Versicherten vor einem etwaigen Transport aus der geschützten Umgebung einer Praxis oder eines Krankenhauses heraus verschlüsselt. Darüber hinaus sind alle Kommunikationsverbindungen in der TI zusätzlich verschlüsselt. Auch der Betreiber des zentralen Netzes der TI kommt in keinem Fall mit den Daten der Fachdienste im Klartext in Berührung.

Intermediär: Medizinische Einrichtungen bleiben anonym

Aus Datenschutzgründen werden beim Online-Abgleich der Versichertenstammdaten durch den „Intermediär“ die Identität der Arztpraxis aus den übermittelten Daten an die Krankenkassen entfernt. Damit wird sichergestellt, dass die Krankenkassen lediglich erfahren, dass für die eGK eines ihrer Versicherten der Datenabgleich angefragt wurde, nicht jedoch, woher die Anfrage kommt. Selbstverständlich wird der Intermediär nicht durch die Fachdienste der Krankenkassen betrieben: Er ist ein Dienst der zentralen TI und liegt somit in der Verantwortung der gematik.

Sicherheit der TI-Bestandteile durch Evaluierung und Zertifizierung nachweisen

Grundsätzlich sind sämtliche kryptografischen Verfahren, die in der Telematikinfrastruktur zur Anwendung kommen dürfen, in der Technischen Richtlinie „Kryptographische Vorgaben für Projekte der Bundesregierung (TR-03116-1) verankert und für die gematik verbindlich. Die dort aufgeführten Verfahren und Mindest-Schlüssellängen gelten international als sicher und umfassen ausschließlich offengelegte und standardisierte Algorithmen. Die Verschlüsselungsverfahren werden jedes Jahr vom BSI überprüft. Dabei erstellt das BSI Prognosen darüber, wie wirksam die Verschlüsselungen in den kommenden sieben Jahren sein werden.

Die Bestandteile der TI-Plattform mit den höchsten Sicherheitsanforderungen wie beispielsweise die Chipkarten, die Kartenterminals oder der Konnektor müssen zusätzlich durch eine Zertifizierung bestätigen, dass sie die notwendige Kryptografie und die restlichen Sicherheitsanforderungen der zugrunde liegenden Schutzprofile erfüllen. Um ihre Geräte zertifizieren zu lassen, beauftragen die Hersteller vom BSI akkreditierte Prüfstellen mit der Evaluierung ihrer Geräte und lassen diese anschließend vom BSI zertifizieren. Diese Zertifizierung ist, neben den technischen Prüfungen durch die gematik, Voraussetzung für eine Zulassung vieler TI-Bestandteile.

Die Sicherheit der wichtigsten TI-Bestandteile wird durch eine Zertifizierung nachgewiesen. Durch Zwei-Schlüssel-Prinzip, dezentrale Speicherung und Verschlüsselung wird die Sicherheit der Patientendaten auch im laufenden Betrieb auf höchstem Niveau aufrechterhalten.

Sicherheit im operativen Betrieb

Der Aufbau und Betrieb eines Informationsicherheitsmanagement-Systems (ISMS) nach der internationalen Norm ISO 27001, mit speziellen Ausprägungen für die Telematikinfrastruktur, ist für alle Betreiber von zentralen Diensten der TI verbindlich. Für die Zulassung müssen diese alle drei Jahre durch unabhängige Sicherheitsgutachten nachweisen, dass die Anforderungen umgesetzt sind. Darüber hinaus werden alle Betreiber von Diensten der Telematikinfrastruktur in das koordinierende Informationssicherheits- und Datenschutzmanagementsystem der gematik eingebunden.

Nicht zuletzt wird die Telematikinfrastruktur als Kritische Infrastruktur in Deutschland geführt. Damit gehört die gematik zur öffentlich-privaten Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen – dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem BSI (UP KRITIS).

Durch die Gesamtheit der Maßnahmen kann die gematik das angestrebte Sicherheitsniveau auch im laufenden Betrieb sicherstellen.

Katja Leikert

Digitalisierung als Chance für eine bessere medizinische Versorgung

Dr. Katja Leikert, MdB
Mitglied der CDU/CSU-Fraktion im Deutschen Bundestag, Mitglied im Gesundheitsausschuss des Deutschen Bundestages

Was die Zukunftsfähigkeit unseres Gesundheitswesens angeht, zeichnen sich bereits heute Konfliktlinien ab, die sich in den kommenden Jahren verstärken werden. Absehbar ist, dass der Anteil älterer und kranker Menschen in Relation zur jüngeren und gesunden Bevölkerung wachsen wird. So sehr es zu begrüßen ist, dass wir nicht zuletzt aufgrund des medizinischen Fortschritts unsere durchschnittliche Lebenserwartung ständig steigern können, so deutlich ist als Konsequenz daraus eine finanzielle Mehrbelastung für unsere sozialen Sicherungssysteme zu erwarten. Gleichzeitig wird sich niemand dagegen aussprechen, möglichst vielen Menschen eine möglichst gute ärztliche Versorgung zuteilwerden zu lassen. Ebenfalls absehbar ist, dass es in bestimmten Regionen Deutschlands einen Mangel an niedergelassenen (Fach-)Ärzten geben wird, wohingegen in anderen Teilen mit einer Ballung zu rechnen ist, was die Frage nach einer ausgewogenen medizinischen Versorgung auch künftig regelmäßig aufwerfen wird.
Im stationären Bereich finden wir eine Gemengelage wieder, die vielen Stimmen eine Vorlage zur Einforderung von mehr Qualität und Effizienz liefert – gekoppelt an die Mechanismen von Unterfinanzierung und der Bereithaltung von Kapazitäten.
Moderiert werden sollen diese Entwicklungen in einem hochkomplexen Gesundheitssystem, das nicht nur eine relativ große Abschottung der Sektoren kennt, sondern auch die Interessen der darin agierenden Institutionen und Akteure, systemimmanente Hürden und Vorbehalte und nicht zuletzt die heterogene Gruppe von Patienten und Versicherten. Dabei bietet mehr sichere digitale Kommunikation im Gesundheitswesen einen großen Vorteil, gerade für die Überwindung der Sektorengrenzen und die schnelle und sichere Verfügbarkeit von Gesundheitsdaten.

Informationen verfügbar machen, wo sie benötigt werden

Wenn von Digitalisierung im Gesundheitswesen die Rede ist, wird oft von extremen Positionen aus diskutiert. Dabei bedeutet der Einsatz moderner Informations- und Kommunikationstechnologie (IKT) konkret die Möglichkeit, Daten dort verfügbar zu machen, wo sie benötigt werden – einige Beispiele: In einem Krankenhaus können Stationsarzt und das Pflegepersonal Befunde per Mouse-Klick abrufen und erhalten somit eine weitaus aussagekräftigere Krankenhistorie, als wenn Papierumschläge in Regalen nicht gefunden oder erst mühselig besorgt werden müssten. Auch der niedergelassene Arzt könnte dank einer flächendeckend verfügbaren elektronischen Patientenakte die Gesundheitsdaten seiner Patienten nach deren Zustimmung einsehen. In einer immer mobiler werdenden Gesellschaft gehen beim Wechsel des Wohnortes – und dem damit einhergehenden Wechsel der Ärzte – nicht automatisch Daten verloren, sondern können einfach digital übermittelt werden. Und genauso einfach erlaubt es der elektronische Medikationsplan, einen aktuellen Stand der Medikation einzusehen, fortzuschreiben und nicht zuletzt zu überprüfen, wo es zu nicht vertretbaren Interaktionen zwischen den einzunehmenden Medikamenten kommt.
Der Mehrwert des Einsatzes von IKT geht natürlich über das reine Versenden und zur Verfügung stellen von bereits generierten Gesundheitsdaten hinaus. Digitalisierung ermöglicht Telemedizin und unterstützt somit bereits bestehende Methoden der Prävention, Diagnose und Therapie. War es bislang üblich, dass beispielsweise Patienten mit Herz-Kreislaufbeschwerden in zeitlich festgesetzten Abständen den Hausarzt aufsuchten, ungeachtet dessen, dass sich ihr gesundheitlicher Zustand auch zwischen den Visiten merklich verschlechtert haben könnte, ermöglicht das tägliche Übersenden von Vitaldaten an ein telemedizinisches Zentrum ein engmaschiges Monitoring des Patienten. Stellen sich relevante Veränderungen in Gewicht oder Blutdruck ein, so wird der Arzt umgehend tätig, kann frühzeitig eine Anpassung der Medikation verordnen und somit der weiteren Verschlechterung des Gesundheitszustandes zuvorkommen. Die Praxis zeigt: Auf diese Art und Weise kann nicht nur das Wohlbefinden von Patienten verbessert, sondern (Re-)Hospitalisierungen können verringert und Kosten reduziert werden. Dabei ist Telemedizin sicher nicht für sämtliche Patienten gleich empfehlenswert. Doch bietet die Möglichkeit der Überwindung von Distanzen sowie der regelmäßigen Erhebung und Auswertung von Gesundheitsdaten Chancen, die wir nicht unge-

nutzt lassen sollten – und das nicht nur im Bereich der Herzinsuffizienz.

Digitale Technik in der Forschung

Der Einsatz digitaler Technik ermöglicht nicht zuletzt neue Ansätze und Wege in der Forschung. Medizinische Daten können dank steigender Rechnerkapazitäten im größeren Umfang ermittelt und miteinander abgeglichen werden. „Big Data" birgt die Chance, gezielt Fragen an strukturierte Datensammlungen zu stellen und zu Erkenntnissen zu kommen, die in der analogen Welt noch nicht erkennbar waren. Große Hoffnungen werden in die Individualisierung von Therapien gesetzt, und obgleich hier sicherlich noch viele offene Fragen zu beantworten sind, zeigen bereits erfolgreiche Forschungsprojekte, dass es sich lohnt, diesen Weg weiter zu bestreiten. Patienten und Mediziner haben hier gleichermaßen ein großes Interesse, neue Therapieansätze voranzubringen. Für den Wissenschaftsstandort Deutschland wiederum bedeutet dies eine große Chance, im internationalen Vergleich in Führung zu gehen. Diese sollten wir nicht ungenutzt lassen.

Neben der Grundlagenforschung und der klinischen Forschung eröffnet der Einsatz digitaler Technik gerade in der Versorgungsforschung neue Möglichkeiten. Hier gilt es zu erfassen und zu bewerten, wie Therapien tatsächlich wirken – im echten Leben, und eben nicht unter klinischen Bedingungen, wie das bereits in etablierten Krebsregistern geschieht. Meiner Einschätzung nach haben wir auf diesem Gebiet in Deutschland noch Defizite, die in Teilen auch auf die Frage zurückzuführen sind, wer unter welchen Bedingungen auf mehr oder minder aussagekräftige und versorgungsrelevante Daten zugreifen und diese zu welchem Zweck verarbeiten kann. Dies zu klären erscheint als ein eher politischer Prozess, der auch unter dem Aspekt der Datensicherheit zu führen ist. Das Potenzial zur Erfassung und Auswertung von Versorgungsdaten wird durch den Einsatz digitaler Technik erhöht – dessen bin ich mir sicher – und damit auch die Chance, aussagekräftige Rückschlüsse zu ziehen und möglichst passgenaue Verbesserungen vorzunehmen.

Datensicherheit und Praktikabilität gewährleisten

Persönliche Gesundheitsdaten sind besonders schützenswert und die Politik hat mit darauf zu achten, dass keine Einfallstore für Datenmissbrauch geschaffen werden. Gleichzeitig ist es fair, sich vor Augen zu halten, dass es eine absolute Datensicherheit nicht geben wird – und auch nicht gab, nicht in der analogen und nicht in der digitalen Welt. Es ist anzunehmen, dass IT-Spezialisten die Sicherheitsanforderungen nach dem neuesten Stand der Technik immens hochschrauben können. Es stellt sich aber auch die Frage, ob wir damit etwas gewinnen, wenn am Ende beträchtliche Abstriche bei der Praktikabilität gemacht werden müssen. Dies ist ein fortwährender Abwägungsprozess, den alle Beteiligten gewissenhaft durchlaufen müssen. Sicher ist, dass niemandem gegen seinen Willen Daten „entnommen" werden dürfen, das bedeutet: Freiwilligkeit lautet hier die oberste Devise. Das Einverständnis vorausgesetzt, bestehen dann wiederum Möglichkeiten der Pseudonymisierung und Verschlüsselung, die eine Rückführung der Daten auf eine einzelne Person erheblich erschweren. Schließlich darf auch die Frage gestellt werden, wem die Daten gehören und wo sie liegen. Hier brauchen wir einen Perspektivwechsel, denn die Gesundheitsdaten gehören zuerst dem Versicherten selbst. Er soll dann entscheiden, wer Zugriff auf seine Daten hat.

Absolute Datensicherheit gibt es nicht - weder in der analogen noch in der digitalen Welt. Hohe Sicherheit hat meist Abstriche bei der Praktikabilität zur Folge. Hier ergibt sich ein fortwährender Abwägungsprozess, den alle Beteiligten gewissenhaft durchlaufen müssen.

Ausblick

Anhand ausgewählter Beispiele habe ich versucht darzulegen, dass im gezielten Einsatz digitaler Technik im Gesundheitswesen viel gewonnen werden kann – und zwar auf unterschiedlichen Ebenen: bei Prozessabläufen verwaltungstechnischer Natur, in der Telemedizin wie auch in der Forschung. Im Vergleich zum Status Quo bietet der Einsatz moderner IKT die Möglichkeit, die medizinische Versorgung zu verbessern sowie mittel- und langfristig Kosten zu sparen. Die vergangenen Jahre haben gezeigt, dass es andere Industriestaaten als Deutschland sind, die beim Thema Digitalisierung vorangehen. Gleichzeitig entwickelt sich der Consumer-orientierte Gesundheitsmarkt sehr rasch. Fundierte Aussagen über die Qualität dieses Angebots sind nur schwer zu treffen. Politik muss hier eine ordnende Rolle einnehmen, um Risiken und Chancen der Digitalisierung in ein gesundes Verhältnis zu bringen. Das im Kabinettsentwurf vorliegende „eHealth-Gesetz" bietet dazu sehr gute Ansatzpunkte.

Walter Ernestus

Die Gesundheitskarte ist sicher, aber ...

***RD Dipl.Inf. Walter Ernestus**, Referent im Referat VI, Technologischer Datenschutz, bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*

Das Jahr 2016 kommt gewiss und die Gesundheitskarte geht ONLINE. Dies stellt zumindest in der Geschichte der Technik und des Gesundheitswesens in Deutschland einen Meilenstein dar. Zehn Jahre nach dem gesetzlich vorgesehenen Start der Karte geht es also los. Die Karte steht flächendeckend in Deutschland zur Verfügung und soll im nächsten Jahr zumindest in ausgewählten Regionen online gehen. Viel wurde bislang geschrieben über diese Karte, Ängste und Befürchtungen wurden verbreitet. Das Hauptthema war die „Sicherheit". Viele (vermeintliche) Unsicherheiten wurden gefunden – die dann doch keine waren - und viele Schreckensszenarien verbreitet, die jeder Grundlage entbehrten. Nach den Enthüllungen des Whistleblowers Snowden haben viele schon das Ende der Karte kommen sehen. Doch weit gefehlt, sie lebt und geht also ONLINE.

Besorgte Bürger und Ärzte, ja sogar verschiedene Verbände haben Bedenken und lehnen die Karte und die Telematik-Infrastruktur (TI) ab. Immerhin sollen mit der Karte sehr sensible Daten – medizinische Daten, die der ärztlichen Schweigepflicht unterliegen und damit zu den sensibelsten Daten überhaupt gehören - verarbeitet werden. Kaum jemand möchte seine Daten einer Datenwolke im Internet anvertrauen, dort wo sie den ständigen Angriffen von Hackern weltweit ausgesetzt sind. Datenpannen wie die jüngste Affäre um das infiltrierte Netz des Deutschen Bundestages nähren zusätzlich Misstrauen. Ein so umfassendes Projekt wie die TI wird jedoch nicht erfolgreich sein können, wenn diejenigen, die es nutzen sollen, kein Vertrauen dazu haben. Darum stellt sich die Frage nach der Sicherheit der Gesundheitskarte und der dazugehörigen Telematikinfrastruktur zurecht!

Wie sieht es nun mit der Sicherheit aus. Betrachtet man die Karte selbst, wird man feststellen, dass die Konzeption stimmt. Die Daten auf der Karte sind sicher! Nach dem heutigen Stand der Technik wurde eine Karte entwickelt, die den höchsten Sicherheitsansprüchen genügt und seine Geheimnisse (Daten des Versicherten, Notfalldaten, Berechtigungsschlüssel und Verschlüsselungsschlüssel) sicher vor Unbefugten schützt. Dies gilt natürlich nur, wenn der Benutzer sich an die Bedienungsregeln der Karte hält (beispielsweise das PIN-Geheimnis wahrt) und seiner Sorgfaltspflicht nachkommt. Eine 100%-ige Sicherheit gibt es nicht und wird es nicht geben. Erfahrungen aus dem Bankenbereich und beim Einsatz der Kreditkarten zeigen, dass die Gefahren im Umfeld bei der Bedienung der Karte lauern und nicht bei der Karte selbst.

Zum Umfeld der Gesundheitskarte gehören die Telematikinfrastruktur und die Nutzer (Versicherte, Ärzte, Leistungserbringer) und auf die kommt es an. Um die Sicherheit rund um die Karte und in und aus der TI zu garantieren, gelten die folgenden Grundsätze: Für Zugriffe auf die schützenswerten Daten der eGk gilt das 2 Karten Prinzip: Es muss die eGk vorliegen und es muss eine 2. Karte vorhanden sein, ein Heilberufsausweis und/oder eine Signaturkarte mit einer qualifizierten Signatur. Ferner stellt ein Konnektor sicher, dass alle Daten die über die TI übertragen werden, nur kryptografisch verschlüsselt übertragen werden und dass nur mit „zertifizierten" Stellen kommuniziert wird. Die derzeitigen Konzepte setzen diese Grundsätze konsequent in die Technik um und garantieren damit höchste Sicherheit. Der Versicherte soll jederzeit die Datenhoheit über seine Daten haben. Dies ist das Ziel dieser Grundsätze.

Doch der Teufel steckt im Detail. Einige dieser Fragen werden nur gelöst werden können, wenn alle Beteiligten an einem Strang ziehen. Ein Problem wird bereits ab 2016 auf viele Beteiligte zukommen. Die Frage nämlich nach dem Umgang mit den „Bestandsnetzen". Viele Praxen, Leistungserbringer sowie Krankenhäuser sind heute schon in internetbasierte Netzwerke eingebunden, beispielsweise zum Zweck der Abrechnung. Mit der Einführung des Konnektors als Sicherheitsanker der TI stellt sich die Frage, wie diese Netze sicher integriert werden. Der Betrieb von zwei oder mehreren separaten Netzen in einer Arztpraxis verbietet sich schon aus ökonomischen Gründen. Also müssen diese „Bestandsnetze" über den Konnektor geleitet werden.

Der Konnektor als zentraler Sicherheitsanker ist quasi der „Internet-Pförtner" jedes Leistungserbringers und muss deshalb wissen, wer in die Praxis rein und

raus darf/muss. Er muss also sehr viel Information über den Datenverkehr der Bestandsnetze besitzen, um seiner Aufgabe, die Sicherheit der Kommunikation zu gewährleisten, nachkommen zu können. Unterschiedliche Sicherheitspolitiken über den Konnektor zu leiten ist eigentlich nicht geplant und stellt ein erhebliches Risiko dar. Langfristig müssen alle Bestandsnetze in die TI integriert werden und sich den Sicherheitsvorgaben der TI unterwerfen. Dies muss Ziel der Sicherheitspolitik der TI sein. Doch schon jetzt zeigen sich Probleme bei der Umsetzung der Vorgaben. Die Betreiber der Bestandsnetze verweisen auf Ihre Sicherheitsmaßnahmen und auf die Kosten, die mit den höheren Sicherheitsanforderungen der TI verbunden wären. Eine Integration in die TI wird von etlichen Betreibern abgelehnt. Der Konnektor als Sicherheitsanker kann aber damit seine Aufgabe nur bedingt wahrnehmen und stellt damit selbst einen Angriffspunkt dar. Ein Konflikt, der zwar eigentlich aufgelöst werden könnte, wenn alle Beteiligten dies wollten. Aber leider ist dies nicht so. Tendenz in diesem Konflikt: ein eher unsicheres Übergangsstadium. Der Konnektor wird als Angriffspunkt auf die TI ins Zentrum rücken. Er wird ständig Ziel von Angriffen sein, deren Absicht es sein wird, auf die Daten der TI zugreifen zu können.

Berücksichtigt werden muss auch folgendes: Sicherheit ist nicht statisch, sondern immer dynamisch, d.h. eine ständige Fortschreibung der Sicherheitskonzeption ist Pflicht, nicht Kür - ja geradezu Voraussetzung für Sicherheit, sowohl in der TI als auch in den Bestandsnetzen. Integriert man aber die Bestandsnetze nicht in die TI, werden sich unterschiedliche Sicherheitsniveaus quasi über Jahre festschreiben und vertiefen, mit der Folge, dass das Bestandsnetz mit den schwächsten Schutzmechanismen zum Einfallstor für erfolgreiche Angriffe auf die Daten werden kann. Deshalb muss das Ziel sein, alle Bestandsnetze in die TI zu integrieren, eine einheitliche Sicherheitsarchitektur zu entwerfen und dynamisch fortzuschreiben - und das so schnell wie möglich. Wer dies nicht akzeptiert, wird „Schiffbruch“ erleiden und die Karte mitsamt der TI untergehen. Leider läuft die Entwicklung nicht in diese Richtung. Im Gegenteil, die 10jährige Verzögerung der Einführung der eGk und der TI zeigt bereits jetzt, wie langsam alle Beteiligten im Gesundheitswesen agieren. Setzt sich diese Behäbigkeit fort, ist es nicht gut bestellt um die Sicherheit der TI.

Die schnelle technologische Entwicklung macht es zwingend erforderlich, sich bereits heute schon Gedanken darüber zu machen, wie die TI und die eGK sich weiterentwickeln sollen. So ist bereits jetzt absehbar, dass sich in den nächsten 5 bis 8 Jahren die Verschlüsselungsalgorithmen und Schlüssellängen ändern werden, die Chipkartentechnologie sich ändern wird, aber eben auch sich die Angriffsmethoden verbessern werden. Wer hier sich nicht ständig den Herausforderungen stellt, wird den Anschluss an die Technik verlieren und Sicherheitslücken produzieren. Was heute noch als sicher gelten darf, wird morgen bereits unsicher sein. Die Schaffung von Sicherheit ist kein statisches Konstrukt, sondern ein beständiger hochinnovativer Prozess, der - einmal installiert - allen Beteiligten auf Dauer einen erheblichen Aufwand mit den entsprechenden „Betriebskosten“ abverlangen wird. Doch bereits heute zeichnet sich ab, dass zwar alle von der Karte und der TI profitieren wollen, aber niemand dafür bezahlen möchte. Es ist immer noch der Glaube verbreitet, bei der TI handele es sich um eine im wesentlichen einmalige Investition ohne nennenswerte Erhaltungskosten. Ein gedankliches Dilemma, dass den Erfolg des Projektes gefährden wird.

Neben diesen, bereits jetzt in Fachkreisen diskutierten Problemen, werden sich aber noch weitere dazugesellen. Ein Beispiel dafür ist das Problem mit der PIN. Die Konzeption und die gesetzlichen Regelungen sehen vor, dass der Versicherte seine Karte und auch die darauf befindlichen Anwendungen mit einer PIN sichert. Dies kann dazu führen, dass bei einem Arztbesuch bis zu 10 PIN's eingegeben werden müssen, wenn ein Versicherter alle Anwendungen nutzt. Ein Unding und vor allem nicht jedem Versicherten zuzumuten. Zwar gibt es bereits jetzt schon techni-

Die Schaffung von Sicherheit ist kein statisches Konstrukt, sondern ein beständiger hochinnovativer Prozess, der - einmal installiert - allen Beteiligten auf Dauer einen erheblichen Aufwand mit den entsprechenden „Betriebskosten“ abverlangen wird. Doch bereits heute zeichnet sich ab, dass zwar alle von der Karte und der TI profitieren wollen, aber niemand dafür bezahlen möchte.

sche Lösungen dieses Problems, beispielsweise durch den Einsatz von biometrischen Merkmalen auf der Karte – hier Fingerabdrücke – doch deren Einsatz ist sowohl bei den Versicherten selbst, wie bei der Datenschutzgemeinde sehr umstritten. Werden allerdings zur Lösung des Problems wiederum 10 Jahre benötigt, wird kaum jemand die Anwendungen (also Notfalldaten, elektronische Patientenakte etc.) nutzen, weil die Eingabe der PIN's in der Praxis oder im Krankenhaus nur lästig ist. Die Effektivität der eGk schlechthin ist damit gefährdet.

sie werden „ewig" gespeichert! Oder doch nicht? Ein schlüssiges Konzept fehlt auch hier. Da sind kritische Fragen durchaus berechtigt, wie beispielsweise die eines Versicherten, der anlässlich einer Diskussion zu diesem Punkt folgendes feststellte: „Wenn meine medizinische Daten 100-200 Jahre im Netz gespeichert werden, kann mir das persönlich zwar ziemlich gleichgültig sein, aber trifft dies auch für meine Nachfahren zu? Offenbaren nicht diese Daten eventuell Erbkrankheiten, Gesundheitsschwächen meiner Blutsverwandten und werden damit zum Brandmahl

Es ist immer noch der Glaube verbreitet, bei der TI handele es sich um eine im wesentlichen einmalige Investition ohne nennenswerte Erhaltungskosten. Ein gedankliches Dilemma, dass den Erfolg des Projektes gefährden wird.
Die eGK und die TI werden nur dann ein Erfolg, wenn sich alle Beteiligten umgehend mit den vielen unbeantworteten Fragen auseinandersetzen. [...] Nur so wird das Vertrauen in die eGK und in die TI gestärkt, nur so werden die eGK und die TI eine Erfolgsgeschichte.

Weitere noch nicht gelöste Probleme sind: Sperrung von Heilberufsausweisen! Einführung von Berufsregistern von nicht-verkammerten Berufen (Hebammen, Optiker, Akustiker, etc.). Welche Berufsgruppen werden noch als Leistungserbringer im Gesundheitswesen betrachtet und mit einem Berufsausweis ausgestattet und welche nicht? Ist der Taxifahrer, der einen Erkrankten in die Klinik oder zur Praxis fährt noch Leistungserbringer und benötigt er einen Heilberufsausweis oder nicht? Wie wird mit Medienbrüchen im Umfeld der TI umgegangen und wo liegen die Grenzen der TI. Fragen über Fragen, die zwar alle bereits hätten beantwortet werden müssen, zu denen es aber keine Entscheidungen gibt.

Viele offene Fragen werden unzureichend oder gar nicht diskutiert. So beispielsweise die Frage, wer die Daten des Versicherten in den Anwendungen nach dessen Tod eigentlich löschen soll? Der Versicherte selbst kann es begreiflicherweise nicht. Da die Daten nach den Grundsätzen der IT-Sicherheit alle verschlüsselt und pseudonymisiert abgelegt wurden, sind sie auch nicht einfach auffindbar oder gar lesbar, d.h.

meiner Familie und meiner Nachfahren. Möchte ich dies? Wer schützt meine Familie davor, wenn diese Daten irgendwann einmal ausgewertet werden?"

Die eGk und die TI werden nur dann ein Erfolg, wenn sich alle Beteiligten zentral mit diesen Fragen auseinandersetzen und zwar umgehend und nicht erst in 10 bis 20 Jahren. Wenn dies nicht geschieht, werden, wie bei der Organspende bereits gesehen, Akzeptanzprobleme auftreten - im Falle der TI werden die Folgen jedoch ungleich weitreichender sein. Der erste Sicherheitsvorfall, das Hacking der TI wird das Misstrauen in die Karte und die TI nähren und der Versicherte wird sich abwenden. Die Karte degeneriert dann zum reinen Kassenausweis, ein Misserfolg auf der ganzen Linie. Lassen wir es nicht soweit kommen. Packen wir die Probleme an und suchen nach den besten Lösungen. Nur so wird das Vertrauen in die eGK und in die TI gestärkt, nur so werden die eGK und die TI eine Erfolgsgeschichte.

Sandro Gaycken im Gespräch

Die Zeit ist reif für eine neue IT.

Gesundheitskarte und Telematikinfrastruktur können davon profitieren.

Die Diskussion um die elektronische Gesundheitskarte und die Telematikinfrastruktur ist zentral verknüpft mit der Frage nach der Sicherheit der IT-Systeme, mit denen dieses Projekt umgesetzt werden soll. Viele Experten sehen Sicherheitsfunktionen, wie sie mit den heute am Markt verfügbaren Ressourcen machbar sind, vorbildlich implementiert. Das Problem liegt jedoch darin, dass die Hard- und Software, auf der diese Sicherheitsfunktionen aufsetzen, als inhärent unsicher gelten müssen. Zu diesem Thema sprachen wir mit dem Berliner IT-Sicherheitsforscher Dr. Sandro Gaycken.

IGZ:
Herr Dr. Gaycken, Sie forschen seit Jahren intensiv zu den Themen Cybercrime und Cyberwar und haben vor einiger Zeit Aufsehen in der Öffentlichkeit erregt mit Ihrer Aussage, Sicherheit für die heutigen computerbasierten Infrastrukturen sei mit den vorhandenen Systemen nicht mehr machbar. In einem Interview mit der FAZ haben Sie das zugespitzt auf die Formel „Werft Eure Computer weg." Warum ist Sicherheit aus Ihrer Sicht mit den heutigen Mitteln nicht mehr herstellbar?

Gaycken:
Computer sind über 40 Jahre unsicher entwickelt worden. In den Anfangszeiten der Computerentwicklung waren die technischen Möglichkeiten der allumfassenden Vernetzung, wie wir sie heute kennen, noch weitgehend außerhalb der Vorstellungskraft. Computer galten als fortschrittliches Hilfsmittel in Spezialbereichen. Rechnersicherheit konnte hergestellt werden, indem man Geräte und Netzwerke isoliert von der Außenwelt betrieb. Für die Einbindung in größere Netze glaubte man, Sicherheit durch Einziehung von Schutzwällen rund um die zu schützende Infrastruktur schaffen zu können. Da Sicherheit als Design-Eigenschaft von IT den Bedienkomfort schwächt, teuer ist und Merkmalen wie Geschwindigkeit, Volumen, Multifunktionalität entgegenwirkt, hat man sie im Verlaufe der Entwicklung immer wieder zugunsten der Performancefaktoren geschwächt. Funktionalität und Komfort waren wichtiger. Sicherheit wurde als „Zusatzaufgabe" externalisiert.

Dieser Prozess hat inzwischen eine so hohe Komplexität in die Maschinen getrieben, dass Computer heute hunderttausende Schwachstellen beinhalten, dass die Programmiersprachen nicht sicher sind, dass Sicherheitsfunktionen nicht mit hoher Zuverlässigkeit arbeiten können. In vielen Situationen wie mit meinen Consumer Electronics kann ich damit arbeiten. In vielen anderen Situationen mit höheren Sicherheitsanforderungen aber inzwischen nicht mehr.

IGZ:
Wie würden Sie die heutige Situation beschreiben - die unsicheren Computer sind im Gegensatz zu den Anfangstagen der IT inzwischen weltweit vernetzt?

Gaycken:
Es wurde schnell klar, dass die Vernetzung der Computer die Arbeitswelt revolutionieren und einen ungeheuren Produktivitätsschub bringen würde. Deshalb hat sich diese Entwicklung auch in einem so rasanten Tempo vollzogen. Es ist - um ein einfaches Beispiel zu nennen - eben viel effizienter, einen Brief als eMail zu versenden als ihn auszudrucken und in die Post zu geben. Die Vernetzung schafft völlig neue Möglichkeiten, Prozesse auf allen Ebenen der Arbeits- und Lebenswelt effizienter zu organisieren und das macht sie so attraktiv.

Die Folge ist allerdings, dass wir heute in hochkritische Abhängigkeiten von IT-Systemen hineingewachsen sind. Ohne IT sind viele Prozesse in der Wirtschaft inzwischen nicht mehr durchführbar. Die Grundannahmen über Rechnersicherheit aus den Anfangstagen haben sich ins Gegenteil verkehrt. Computersysteme sind nicht mehr isolierbar, Schutzwälle arbeiten nicht mehr effektiv. Die Systeme sind inzwischen so komplex geworden, dass es selbst Experten unmöglich ist, ihr Verhalten vollständig zu modellieren und vorauszusagen. IT-Systeme produzieren Effekte, die von ihren Entwicklern nicht antizipiert werden können. Wenn man so will, haben sie sich - zumindest teilweise - der menschlichen Kontrolle entzogen, sind von einem technischen Konstrukt zu einem Naturgegenstand geworden.

Dr. Sandro Gaycken,
Senior Researcher für Cybersecurity und Cyberstrategy an der European School of Management and Technology (ESMT), Dr. Gaycken berät zahlreiche politische Institutionen im In- und Ausland zu Themen der IT-Sicherheit.

IGZ:
Wie kann ein von Menschenhand erschaffenes technisches System zu einem Naturgegenstand mutieren? Haben wir tatsächlich so wenig Kontrolle über die selbstgeschaffenen Produkte, dass wir ihr Verhalten erst erforschen müssen?

Gaycken:
Seriöse Schätzungen besagen, dass selbst bei umfangreich geprüftem Programmcode, beispielsweise in gehärteten und nie veränderten Open Source Kernmodulen, 0,004% der Codezeilen Sicherheitslücken sind, die persistenten Systemzugang ermöglichen. Bei schlecht programmierter Software kann dieser Anteil auf 1% ansteigen - potentiell ermöglicht also jede hundertste Codezeile ein Eindringen ins System. Die allermeisten dieser Sicherheitslücken werden nie entdeckt, aber starke Angreifer beforschen diesen „Naturgegenstand“, suchen gezielt nach Sicherheitslücken und werden auch fündig.

IGZ:
Welche Akteure treten denn heute als Angreifer auf und welche Interessen verfolgen sie?

Gaycken:
Man kann Angreifer nach den Ressourcen, die ihnen zur Verfügung stehen, grob in starke und schwache Angreifer unterscheiden. Schwache Akteure sind digitale Taschendiebe, die mit im Netz verfügbarem Schadcode operieren und damit versuchen, beispielsweise Kreditkartendaten zu erbeuten. Zu den starken Akteuren gehören Geheimdienste und Militärs, aber auch große, organisierte Hackergruppen. Diese Gruppen können alle Teile der Informationstechnik inklusive der implementierten Sicherheitsfunktionen angreifen. Dabei werden spezielle, selbstentwickelte Angriffsmethoden zum Einsatz gebracht, die auf bislang unentdeckten Sicherheitslücken basieren. Der dazugehörige Aufwand ist natürlich nur gerechtfertigt, wenn damit ein adäquater Informationsgewinn bzw. Nutzen verbunden ist. Bei Geheimdiensten und Militärs liegen die Interessen vor allem in der Überwachung, der gezielten Spionage, aber auch in offensiven Aktionen, wie der Fall Stuxnet nahelegt. Hier wurden Leitsysteme des iranischen Atomprogramms angegriffen. Die für Deutschland größte Gefahr geht von der Industriespionage aus. Kriminelle Hackergruppen wollen dagegen Geld und erhalten das durch den Verkauf von Daten, durch Erpressung oder durch Betrugsmodelle mit digitalen Identitäten. Erpessung hat beispielsweise in den letzten Jahren stark zugenommen. Haben sich Kriminelle Zugang zu einem Firmennetzwerk verschafft, können sie den Betriebsablauf empfindlich stören, woraus sich dann das Erpressungspotenzial ergibt.

IGZ:
Unter solchen Bedingungen scheint die Vertraulichkeit der Kommunikation - immerhin ein Grundrecht - schon heute schlicht abhanden gekommen zu sein. Welche Möglichkeiten haben wir, eine sichere Kommunikation wiederherzustellen?

> Neben graduellen Sicherheitsverbesserungen mit den heutigen Mitteln müssen wir aber eine komplette Neuentwicklung sicherer IT ins Auge fassen. [...] Es gibt kein Sicherheitskonzept, das sich irgendwie ausgezeichnet und länger als eine Woche gehalten hätte.

Gaycken:
Man kann sehr viele sehr gute Dinge tun. Neben graduellen Sicherheitsverbesserungen mit den heutigen Mitteln müssen wir aber eine komplette Neuentwicklung sicherer IT ins Auge fassen. Es gibt den unangreifbaren Computer. Das ist nur einfach ein neuer Computer, daher gibt es da viele Hürden in der Akzeptanz und auch viel Gegenwind aus der IT-Lobby. Aber meiner Meinung nach ist die Zeit reif dafür. Einen Markt würde es da allemal geben - das Interesse an sicheren Systemen ist riesengroß. Andere zuverlässige Wege sehe ich nicht. Es gibt kein Sicherheitskonzept, das sich irgendwie ausgezeichnet und länger als eine Woche gehalten hätte. Technisch sind die Konzepte zwar oft durchaus sauber, aber in den Rahmenbedingungen oder unter anderen Ausgangslagen versagen die Sicherheitsfunktionen leicht.

IGZ:
Eine komplette Neuentwicklung der IT klingt nach einem Jahrhundertprojekt. Dazu kommt, dass in Europa kaum noch nennenswerte Hardware und wenig bedeutende Software produziert wird. Sind das nicht denkbar schlechte Voraussetzungen?

Gaycken:
Das ist auch eine Gelegenheit. So ganz weg vom Fenster sind wir auch nicht. Wir haben schon noch Kapazitäten in Hardware- und Softwareproduktion. Es gibt eine Reihe von Strategien, die man hier nutzen kann. Ich habe unlängst eine entwickelt, die jetzt umgesetzt wird.

IGZ:
In welcher Zeitspanne könnte so ein Projekt realisiert werden?

Gaycken:
Wir rechnen mit zwei bis fünf Jahren.

IGZ:
Die elektronische Gesundheitskarte und die geplante Telematikinfrastruktur im Gesundheitswesen bauen letztlich auf der aktuellen unsicheren Infrastruktur auf. Da Patientendaten äußerst sensibel und damit auch in besonderem Maße schutzwürdig sind, läge es doch nahe, gerade bei diesem Projekt - es gilt als das weltweit ambitionierteste seiner Art - eine komplette Neuentwicklung der IT ins Auge zu fassen?

Gaycken:
Das wäre wünschenswert, aber die Kartenhersteller stemmen sich gegen neue Infrastrukturen. Dann bräuchte ja keiner mehr ihre Karten, respektive deren Sicherheitsfunktionen, in denen der Hauptteil der Innovation geparkt ist. Vielleicht gibt es da nochmal ein Umdenken, aber bisher kam aus dieser Ecke eher Gegenwind. Gerade für Patientendaten halte ich es aber für unverantwortlich, auf einer nachgewiesenermaßen unsicheren Struktur aufzubauen.

IGZ:
Die elektronische Gesundheitskarte / Telematikinfrastruktur soll neben den auf der Gesundheitskarte gespeicherten Daten zunächst kommunikative Funktionen wie das Stammdatenmanagement und den elektronischen Arztbrief erfüllen. Dabei geht es schlicht darum, Informationen geschützt zwischen den Ärzten, Kassen und IT-Dienstleistern zu transportieren. Wäre eine solche Funktionalität aus Ihrer Sicht mit den vorhandenen Techniken vernünftig absicherbar?

Gaycken:
Das müsste man im Detail prüfen. Vor allem bräuchte man dazu aber noch ein Bedrohungsmodell. Sicherheit ist immer relativ. Gegen starke Angreifer wie NSA & Co kann sich im Moment absolut niemand absichern. Wenn es nur um digitale Taschendiebe geht, reichen hochwertige und gut implementierte Lösungen vermutlich für 90 Prozent der Fälle.

IGZ:
Sinnvolle künftige Anwendungen der Telematik-Infrastruktur wären absehbar auch mit einer zentralen Datenverwaltung bzw. -speicherung verbunden. Anwendungen wie beispielsweise die elektronische Patientenakte wären nicht sinnvoll umsetzbar, wenn Unterlagen, die in der Arzt- oder Zahnarztpraxis abgelegt sind, von anderen Ärzten nur zu den Praxisöffnungszeiten eingesehen werden können. Diese Unterlagen müssten, um sinnvoll genutzt werden zu können, jederzeit für die Einsicht zur Verfügung stehen, was notwendigerweise eine elektronische Kopie in einer zentral verwalteten Infrastruktur voraussetzt.
Würden nicht solche Datensammlungen sensibler Patientendaten durch die Menge hochwertiger Information ein lohnendes Angriffsziel für Internetangriffe abgeben? Gibt es ggf. technische Alternativen, um den angestrebten Nutzen zu erhalten, ohne die Risiken einer zentralen Speicherung eingehen zu müssen?

Gerade für Patientendaten halte ich es aber für unverantwortlich, auf einer nachgewiesenermaßen unsicheren Struktur aufzubauen. [...]
Zentrale Datensammlungen sind automatisch attraktive Ziele, die oft sehr hochwertige Angreifer anziehen, weil der Return on Invest ausreichend hoch ist.

Gaycken:
Zentralisierungen von Daten sind immer eine gefährliche Idee. Das sind automatisch attraktive Ziele, die auch oft sehr hochwertige Angreifer anziehen, weil der Return on Invest ausreichend hoch ist. Besser wäre ein Peer-To-Peer-System, bei dem die Daten dezentral gehalten werden, aber trotzdem verfügbar gemacht werden können. Das erhöht die Angriffskosten.

IGZ:
Gestohlene Gesundheitsdaten werden Berichten zufolge heute schon in anonymen Online-Marktplätzen gehandelt - u.a. neben illegal erlangten Kreditkarten-/Kontoinformationen, Drogen und Waffen. Welche Rolle könnten Gesundheitsdaten im Schwarzmarkthandel künftig spielen?

Gaycken:
Patientendaten haben ein hohes Potential für Erpressungen. Man hat einen solchen Fall bei der Dating-Plattform Ashley Madison gesehen - in Folge der Veröffentlichung persönlicher Daten im Internet kam es sogar zu Selbsttötungen. Sehr private Informationen haben da einen hohen inhärenten Wert. Auch als Anreicherung von bestehenden Datensätzen für bessere Betrugsoptionen sind solche Daten interessant. Ethische Barrieren gibt es hier in keinster Weise.

Das Gespräch führte Benn Roolf.

Thilo Weichert

Electronic Health und Datenschutz

Dr. Thilo Weichert,
Von 2004 bis 2015 Landesbeauftragter für Datenschutz des Landes Schleswig-Holstein und Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD), Kiel

Anfang Juli 2015 behandelte der Deutsche Bundestag den Regierungsentwurf eines „Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen", kurz „E-Health-Gesetz". Den Ankündigungen gemäß soll damit ein Durchbruch für electronic Health, also für die Einführung der Informationstechnik (IT) im Gesundheitswesen, erreicht werden. Dies ist in zweierlei Hinsicht etwas großspurig: Die IT hat das Gesundheitswesen zum einen schon voll im Griff. Zum anderen ist der Vorschlag kein großer Wurf, sondern nicht viel mehr als der gesetzgeberische Versuch, die elektronische Gesundheitskarte (eGK) und die Telematik-Infrastruktur (TI), die eigentlich schon Anfang 2006 „zur Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz" eingeführt sein sollten, endlich zum realen Leben zu erwecken.

Bis Ende 2014 wurden für das Projekt eGK/TI über eine Milliarde Euro ausgegeben, doch ist es bis heute nur begrenzt startklar. Schuld hieran war ausnahmsweise weniger die Politik, die im Sozialgesetzbuch (SGB) V valide rechtliche Grundlagen geschaffen hatte. Auch hinsichtlich der Technik gibt es nur begrenzte Probleme; wohl muss noch einiges spezifiziert werden, um konkret programmiert, installiert und ausgerollt werden zu können.

Professioneller Widerstand

Es war (zahn-)ärztlicher Widerstand mit teilweise falschen Argumenten, der die Bevölkerung, die Medien und letztlich die Politik irritierte und dadurch das Gelingen des äußerst ambitionierten, und zugleich im Prinzip dringend nötigen und sinnvollen Projektes hinauszuzögern. Gewarnt wurde vor dem „gläsernen Patienten". Die Vertrauensbeziehung des (Zahn)Arztes zu seinen Patienten würde zusammenbrechen, weil medizinische Daten in riesigen Datenzentren ungenügend geschützt zentral abgespeichert würden, wo sich dann so mancher Nichtberechtigte bedienen könnte. Diese Behauptungen haben zwar nichts mit dem Projektdesign gemein, doch schürten sie bei vielen Menschen Angst und Vorbehalte.

Die gesetzlichen Regelungen zu eGK und TI sind aus Datenschutzsicht fast vorbildlich. Die digitale Datenspeicherung erfolgt, wie bisher, dezentral bei den Leistungserbringern, nicht wie behauptet zentral. Umfassende Transparenz und ein Bestimmungsrecht der Betroffenen sind vorgesehen. Zunächst ist die TI nicht viel mehr als eine Netzstruktur, deren wichtigstes Ziel eine abgeschottete verschlüsselte Übermittlung zwischen medizinischen Leistungserbringern ist. Die dafür vorgesehene Technik ist ausgereift. 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.

Reale Gefahren

Berechtigten Grund zur Kritik hat die (Zahn)Ärzteschaft, wenn sie Gängelung und übermäßige Kontrolle durch die Krankenkassen befürchtet, die aus Gründen der Kosteneinsparung die Behandlungs- und Verschreibungspraxis noch stärker überwachen und die Therapiefreiheit beeinträchtigen wollen. Dies tun die Kassen aber nicht über die eGK oder die TI. Diese technische Infrastruktur ist hierfür nur begrenzt geeignet und darf so nicht genutzt werden. Außer beim Stammdatenmanagement fallen bei den Kassen überhaupt keine Daten über die TI an. Die Kontrolle des Gesundheitswesens durch die Kassen erfolgt raffinierter durch verborgene Big-Data-Auswertungen der Abrechnungen und über die Beschaffung weiterer medizinischer Daten mit verführerischen Versprechen zu Prävention, Qualitätssicherung und Patientenberatung. Dieser schon lange anhaltende Trend wurde von der (Zahn) Ärzteschaft bisher viel zu wenig kritisiert. Das Präventionsgesetz vom Juli 2015 und das kurz danach in Kraft getretene Gesundheitsversorgungsstärkungsgesetz blieben insofern bisher weitgehend unkommentiert.

Die Informatisierung des Gesundheitswesens schreitet derweil weiter voran. Google, Microsoft und andere Anbieter breiten sich aus, ohne dass ein effektiver Datenschutz besteht. Bei den meisten der weltweit 400.000 Medizin-, Gesundheits- und Lifestyle-Apps mangelt es an inhaltlicher oder technischer Qualität. Dessen ungeachtet werden Daten von sogenannten Wearables, also elektronischen Messgeräten, die Gesundheits- und sonstige Körpermerkmale erfassen, auf Geheiß von Versicherungen, Krankenkassen und sogar von Ärzten an IT-Dienstleister, evtl. mit Sitz in den USA, übermittelt, deren Vertraulichkeit nicht an-

satzweise gewährleistet ist. Elektronische medizinische Kommunikation erfolgt bisher oft unzureichend gesichert, sogar unverschlüsselt und über offene Netze. Platzhirsche 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.

Die möglichen Konsequenzen einer unkontrollierten Auslagerung der Gesundheitsdatenverarbeitung auf kommerzielle Dienstleister und offene Netze sind evident und werden dennoch ignoriert: Datenlecks können nicht nur die Vertrauenswürdigkeit der Gesundheitsversorgung beeinträchtigen, sondern zu gewaltigen persönlichen Schäden führen, etwa wenn Daten im Internet veröffentlicht oder an Versicherungen oder Arbeitgeber durchgestochen werden. Gar nicht zu reden von der möglichen Sabotage lebenswichtiger IT-Systeme, die Leben und Gesundheit direkt gefährdet.

Anreize und Sanktionen

Angesichts dessen ist es zu begrüßen, wenn die Bundesregierung versucht, der eGK sowie der TI Leben einzuhauchen. Das E-Health-Gesetz will mit finanziellen Anreizen, etwa Vergütungen für die Erstellung und Aktualisierung der Notfalldatensätze oder für die Übermittlung von elektronischen Entlass- und Arztbriefen, und Sanktionen, etwa für die Nichtnutzung von IT-Angeboten oder das Nichteinhalten von Fristen, die sicherere Digitalisierung voranbringen.
Durch eine Öffnung für sonstige Leistungserbringer, etwa nicht-approbierte Gesundheitsberufe im Bereich der Pflege, soll die TI-Kommunikation auf eine breitere Basis gestellt werden. Um eine multifunktionale Nutzung der TI zu ermöglichen, sollen für die vertrags(zahn)ärztliche Versorgung und für Krankenhäuser offene und standardisierte Schnittstellen für den Datenaustausch integriert werden. Ein über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ soll Anreize geben für die Entwicklung vertrauenswürdiger Applikationen.

Patientenschaft kommt zu kurz

Das E-Health-Gesetz ist so äußerst industrielastig geworden. Datenschutz und Verbraucherschutz kommen zu kurz, ebenso wie beim sonstigen Ausrollen der TI.
Patientenbelange fallen zunehmend unter den Tisch. Insofern ist es nicht gerade beruhigend, dass bei der Vergabe für den Aufbau der TI der Zuschlag u. a. an Arvato Systems und die CompuGroup Medical AG erfolgte. Arvato ist ein großer Player im Geschäft mit personenbezogenen Daten; die CompuGroup ist Marktführer bei Arztinformationssystemen mit einem kommerziellen Interesse an Patientendaten.
Im Gesetz ist vorgesehen, dass die Versicherten ihre Daten selbst verwalten können sollen. Doch ist bisher nicht absehbar, dass über sogenannte Kioske hierfür eine Infrastruktur geschaffen wird, ganz zu schweigen von dem ehrgeizigen Ansatz, den Versicherten am heimischen Computer die Administration der eigenen Daten zu eröffnen.
Unklar bleibt weiterhin, wie der Übergang von den bisher genutzten ärztlichen Netzwerken, etwa des Safe-Net der Kassenärztlichen Vereinigungen oder DALE, organisiert werden soll. Weitere Fragen sind bisher unbeantwortet: Lässt sich die Authentisierung der eGK mit Hilfe biometrischer Verfahren vereinfachen? Wie soll die Verwaltung der Health Professional Card bei nicht verkammerten Berufen erfolgen? Wie kann ein wirksames Löschkonzept etabliert werden? ...

Datenlecks können nicht nur die Vertrauenswürdigkeit der Gesundheitsversorgung beeinträchtigen, sondern zu gewaltigen persönlichen Schäden führen, etwa wenn Daten im Internet veröffentlicht oder an Versicherungen oder Arbeitgeber durchgestochen werden.

Externe IT-Dienstleister sind derzeit unzulässig

Das größte Problem des E-Health-Gesetzes ist das, was darin nicht geregelt wird. Deshalb forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 19.03.2015 „klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern“: Deren Einschaltung ist „oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden. Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen.“
Hinsichtlich dieses Aspektes, der das aktuell größte Hindernis für eine digitale Effektivierung des Gesundheitswesens ist, besteht Einigkeit zwischen allen Stakeholdern. Es ist nicht nachvollziehbar, weshalb der Gesetzgeber hier seit Jahren untätig bleibt. Und es gibt viele weitere Baustellen, bei denen der Gesetzgeber gefordert ist: medizinische Forschung, Einsatz von Big-Data, kommerzielle Verwertung von Patientendaten... Der Ball liegt weiterhin im Feld der Bundespolitik.

Silke Lüder

Praxisfern, gefährlich, teuer

Warum eGK und Telematikinfrastruktur keine Lösung, sondern ein Problem sind.

Dr. med. Silke Lüder
Fachärztin für Allgemeinmedizin, Hamburg
Stellvertretende Vorsitzende der VV der KV Hamburg,
Stellvertretende Vorsitzende des Freie Ärzteschaft e.V.,
Sprecherin der Aktion „Stoppt-die-e-Card“

Datensicherheit, Schweigepflicht, Therapiefreiheit – das alles könnte bald Schnee von gestern sein, denn längst ist das E-Health-Gesetz beschlossen. Damit will Bundesgesundheitsminister Hermann Gröhe (CDU) die Medizinlandschaft in Deutschland umpflügen und dem stockenden Mammutprojekt Telematik-Infrastruktur mit der elektronischen Gesundheitskarte (eGK) Beine machen. In der Tat: Seit Jahren jagt eine Panne die nächste, es werden weiter Abermillionen Euro versenkt und eine erfolgreiche Einführung der eGK ist nicht in Sicht. Das Projekt muss sich wahrlich nicht hinter anderen Großpannen wie dem Berliner Flughafen oder der Hamburger Elbphilharmonie verstecken.
Nur: Das eGK-System „handelt“ nicht etwa mit Flugtickets oder Konzertkarten, sondern mit hochsensiblen Gesundheitsdaten von etwa 70 Millionen Bürgern. Und diese kann niemand schützen. Die digitale Vernetzung der Arztpraxen mit den Krankenkassen und die zentrale Datenspeicherung - um die man letztlich nicht herumkommen wird - gefährden die Vertraulichkeit ganz persönlicher Informationen. Durch den Online-Datentransfer entstehen weitere Daten. Die geplanten Datensammelstellen sind ein lohnendes Ziel für Hacker – und dass Datenklau kein Hexenwerk ist, haben in der jüngsten Vergangenheit zahlreiche Datenskandale bewiesen.

Industrie scheitert an Sicherheitsanforderungen

Mangelnde Datensicherheit torpediert auch immer wieder den Fahrplan für Online-Tests. Diese wurden nun zum x-ten Mal verschoben. Denn offenbar beißt sich die Industrie an den Sicherheitsanforderungen die Zähne aus und konnte daher die sogenannten Konnektoren nicht pünktlich liefern. Als eine Art Router sollen sie die Praxen mit der Datenautobahn der gematik, der Betreiberorganisation der eGK, verbinden. Aufgebaut hat diese Datenautobahn die Arvato AG, eine Tochter des Bertelsmann-Konzerns. Obwohl unabhängige Patientenvertreter, Datenschützer und Ärzte seit vielen Jahren das eGK-Projekt kritisieren und den mangelnden Datenschutz anprangern, bleibt der Wille von Politik, gesetzlichen Krankenkassen und IT-Industrie ungebrochen, an der eGK festzuhalten. Warum?

Medizindaten sollen zu einem lukrativen Geschäftsfeld werden und die Wirtschaft ankurbeln. Sie werden jetzt schon als „Gold unseres Jahrhunderts“ bezeichnet. Die Gesundheitswirtschaft etwa könnte mit individuellen Patientendaten gezielt Therapien „verkaufen“. Im April 2015 forderte BIO Deutschland, der Verband deutscher Biotechnologie-Unternehmen, die auf der eGK gespeicherten Patientendaten nutzen zu dürfen. Die Unternehmen bräuchten eine möglichst breite Datenbasis, um den Forschungsstandort Deutschland zu stärken.

Kassen bestimmen Therapie

Auch die gesetzlichen Krankenkassen wollen die Patientendaten auf der Karte nutzen. So locken die ersten Kassen ihre Versicherten bereits mit Bonuszahlungen für Datenspeicherungen. Ziel ist dabei wohl weniger die Verbesserung der medizinischen Versorgung der Versicherten, womit das Bundesgesundheitsministerium immer wieder die Notwendigkeit der eGK begründet. Vielmehr geht es um Rationierung der Medizin und durch Kassen-gesteuerte Versorgung im Sinne von „managed care“. Zentral gespeicherte und überwachte Patientendaten möglichst der gesamten Bevölkerung sollen helfen, derlei Pläne zu realisieren.

Im Juni ließ der Spitzenverband der Gesetzlichen Krankenversicherungen in einer Pressekonferenz erstmals die Katze aus dem Sack. Wie der Ärztenachrichtendienst änd berichtete, stellen sich die Kassen die künftige Arzneimitteltherapie etwa so vor: Der Medizinische Dienst der Krankenversicherungen könnte mit Hilfe von auf der eGK gespeicherten genetischen Patientendaten entscheiden, welcher Patient ein bestimmtes Medikament bekommen soll und welcher nicht. Es geht dabei um teure Medikamente für die Behandlung schwerer Erkrankungen wie Hepatitis C und Krebserkrankungen. Die Therapie bestimmen also die Kassen – das ist ein Angriff auf die Therapiefreiheit der Ärzte.

Die Kassen wollen ihre Arzneimittelausgaben drosseln und dafür ein schärferes Amnog-Verfahren (Arzneimittelmarktneuordnungsgesetz) durchdrücken. In der Umsetzung hieße das: Bestimmte Medikamente werden nur noch jenen Patientengruppen erstattet, bei denen ein Zusatznutzen feststellbar ist. Bisher werden Medikamente, bei denen für mindestens eine Patienten-Subgruppe im Amnog-Verfahren ein

Zusatznutzen festgestellt wurde, generell allen Patienten erstattet. Ob jemand zu einer Subgruppe gehört oder nicht, entscheiden dann Faktoren wie Alter oder Geschlecht – oder eben der Genotyp. Eine Anwendung auf der elektronischen Gesundheitskarte könnte den Vorstellungen der Kassen zufolge dem Austausch zwischen Kassen und Ärzten dienen.

Pseudosicherheit durch digitale Notfalldaten

Eine bereits geplante Anwendung auf der eGK ist der Notfalldatensatz. Sofern der Patient das wünscht, sollen die Notfalldaten ab Mitte 2018 auf der eGK gespeichert werden. Seit zehn Jahren sind sie das wichtigste Werbeargument der Protagonisten der Totalvernetzung. Ihre Begründung: Die Blutgruppe sei dort gespeichert und der Notarzt könne sofort sehen, welche Medikamente ein Patient einnähme. Kurzum: Die Notfalldaten retteten Leben, weiß zumindest das Bundesgesundheitsministerium. Die Notärzte allerdings wissen das nicht so genau. Viele notfallmedizinische Fachgesellschaften, Verbände und Arbeitsgemeinschaften haben sich noch gar keine Meinung zum Notfalldatensatz gebildet. Fakt ist aber: Notfalldaten müssen schnell, zuverlässig und sicher zur Verfügung stehen. Es ist mehr als fraglich, ob die eGK das leisten kann. Denn die Daten sind ohne Lesegerät und Datenverbindung nicht lesbar, ihre Durchsicht kostet Zeit, sie sind möglicherweise nicht vollständig oder aktuell und die Blutgruppe wird im Fall einer Transfusion sowieso neu bestimmt. Hier wird Sicherheit vorgegaukelt, die es nicht gibt.

Und wer glaubt, der Notfalldatensatz enthielte nur Notfalldaten, der irrt. Vielmehr handelt es sich um eine elektronische Patientenakte, in die etwa manche Krankenkassen, Klinikkonzerne oder künftige Arbeitgeber gern einmal einen Blick werfen würden. Das „Lastenheft“ für das Notfalldatenmanagement listet auf 123 Seiten auf, welche Daten zu speichern sind: beispielsweise alle Diagnosen und wer diese wann gestellt hat, alle Medikamenteneinnahmen, Allergien, Implantate, Schwangerschaften mit voraussichtlichem Entbindungstermin und Komplikationen, Patientenbetreuer mit persönlichen Daten, bestehende Weglaufgefährdung, Patientenverfügung und Organspendeerklärung mit Ablageort.

Verschlüsselung schützt nicht vor Zugriff

War der Notfalldatensatz einst dafür gedacht, die Behandlung eines Patienten durch verschiedene Ärzte zu unterstützen, so steht inzwischen ein ganz anderes Ziel im Fokus. Mehr als ein Dutzend weiterer Berufsgruppen im Gesundheitswesen sollen auf die kleine elektronische Patientenakte zugreifen können. Deshalb müsste der Notfalldatensatz wiederum durch eine 6- bis 8-stellige Patienten-PIN geschützt werden. Bei früheren eGK-Tests scheiterten allerdings drei Viertel aller Patienten und genauso viele Ärzte an dem angeblichen „Sicherheitsmerkmal“ PIN – sie hatten die Nummer vergessen. Die bessere Alternative zum digitalen Notfalldatensatz auf der eGK ist der Europäische Notfall-Ausweis in neun Sprachen – vor allem für Reisefreudige, denn die eGK ist im Ausland nicht lesbar. Der kleine Papierausweis kostet nur wenige Cent und bleibt in der Hand des Versicherten.

Für das den Leistungsträgern in der Medizin aufgezwungene Mammutprojekt scheint es nur eine Lösung zu geben: die weiteren Anwendungen möglichst schnell beerdigen und künftig die Versichertengelder dort investieren, wo sie hingehören – in eine gute medizinische Versorgung.

Dort sind die Patientendaten ohnehin am besten aufgehoben. Jede zentrale Haltung großer Datenmengen ist ein Risiko für den Datenschutz. Daran ändern auch Verschlüsselungen nichts, da viele Verfahren Datenschutzexperten zufolge unwirksam sind. Auch Anonymisierung und Pseudonymisierung würden wenig helfen: In den Datenstrukturen ließe sich die Verwendung sogenannter Objektidentifikationsnummern nachweisen, dadurch könnten Daten stets einem Patienten zugeordnet werden. Metadaten lieferten weitere Informationen, durch Kombinieren von Suchanfragen würden neue Metadaten generiert. Für den Schutz der Patientendaten brauchen wir eine datensparsame sowie dezentrale Datenhaltung und Kommunikation.

Nicht zuletzt ist das eGK-Projekt mit der zentralen Totalvernetzung völlig abgehoben von der ärztlichen und zahnärztlichen Praxis. Das verdeutlichen aktuelle Planungen: Der Patient soll jede der insgesamt 7 bis 8 unterschiedlichen Anwendungen auf der Karte mit einer anderen mindestens 6-stelligen „Sicherheits-PIN“ freischalten. Das ist absurd. Für dieses den Leistungsträgern in der Medizin aufgezwungene Mammutprojekt scheint es nur eine Lösung zu geben: die weiteren Anwendungen möglichst schnell beerdigen und künftig die Versichertengelder dort investieren, wo sie hingehören – in eine gute medizinische Versorgung.

Bertram Raum

Neue Herausforderungen für den Gesundheitsdatenschutz im digitalen Zeitalter

MR Bertram Raum,
Referatsleiter des Referates III - Sozial- und Gesundheitswesen, Beschäftigtendatenschutz - bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ende des ausgehenden 20. Jahrhunderts sprach man von der „digitalen Revolution", dessen Ergebnis die „Digitalisierung der Gesellschaft" ist. Sie brachte einen radikalen Umbruch in der Art der Kommunikation. Während über Jahrhunderte hinweg Informationen in Schriftform ausgetauscht wurden, werden sie heute überwiegend auf digitalem Wege übermittelt. Die Diskussion, ob die Auswirkungen der Digitalisierung auf das Leben des Einzelnen positiv oder negativ zu bewerten sind, ist müßig. Die „Digitalisierung der Gesellschaft" ist ein Faktum. Diese Feststellung ist jedoch kein Grund zur Resignation, sondern zur Überprüfung, welche Konsequenzen sich hieraus ergeben, und die Aufforderung, diese auch zu ziehen.

Die obligatorische Ersetzung der früheren Versichertenkarte durch die elektronische Gesundheitskarte (eGK) zum 1.1.2015 hat einen Zustand herbeigeführt, den der Gesetzgeber durch das GKV-Modernisierungsgesetz vom 14.11.2003 bereits zum 1.1.2006 erreichen wollte. Zum weiteren Ausbau der hiermit zusammenhängenden Telematikinfrastruktur hat die Bundesregierung am 27.5.2015 den „Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen" („E-Health-Gesetz") beschlossen, der noch im Jahr 2015 Gesetz werden soll. Nach der amtlichen Begründung zielt der Entwurf „insbesondere darauf ab,

- die zügige Einführung nutzbringender Anwendungen der elektronischen Gesundheitskarte zu unterstützen,
- die Telematikinfrastruktur mit ihren Sicherheitsmerkmalen als die zentrale Infrastruktur für eine sichere Kommunikation im Gesundheitswesen zu etablieren und sie für weitere Anwendungen im Gesundheitswesen und für weitere Leistungserbringer zu öffnen,
- die Strukturen der Gesellschaft für Telematik zu verbessern und ihre Kompetenzen zu erweitern
- die Interoperabilität der informationstechnischen Systeme im Gesundheitswesen zu verbessern,
- und telemedizinische Leistungen zu fördern"[1].

An gleicher Stelle betont die Bundesregierung: „Datenschutz hat dabei höchste Priorität und wird durch rechtliche und technische Maßnahmen sichergestellt". Zuvor war das mittlerweile vom Deutschen Bundestag beschlossene IT-Sicherheitsgesetz[2] auf den Weg gebracht worden, das in § 2 BSI-Gesetz einen neuen Absatz einführte. Danach gehört der Bereich Gesundheit zu den „kritischen Infrastrukturen" (§ 2 Abs. 10 Nr. 2 BSI-Gesetz). Eine genauere Definition, was zu den „kritischen Infrastrukturen" im Sinne des IT-Sicherheitsgesetzes gehört, bleibt allerdings einer künftigen Rechtsverordnung vorbehalten, die noch nicht im Entwurf vorliegt. Das sogenannte E-Health-Gesetz und das IT-Sicherheitsgesetz sind nicht isoliert voneinander zu betrachten, sondern ergänzen sich. Immerhin zeigt sich durch diese beiden Gesetzgebungsvorhaben, dass der Gesetzgeber sich der Gefahren und Unwägbarkeiten der modernen Technik bewusst ist.

Die technische Entwicklung hat unzweifelhaft die Medizin vorangebracht und für die Patienten erheblichen Nutzen gestiftet. Andererseits sind die Gefahren für deren Persönlichkeitsrechte nicht zu leugnen. Sicherlich gibt es bei der analogen Übermittlung durch Brief und Fax sowie bei der Speicherung von Patientendaten auf Papier nicht zu leugnende Gefahren. Briefe und Faxe erreichen den falschen Empfänger – dies lässt sich bei aller Umsicht nicht vermeiden. Dass Patientenakten gestohlen werden oder anderweitig abhandenkommen, ist zwar selten, aber nicht ausgeschlossen.[3]

Allerdings bestehen bei der Übermittlung oder Speicherung digitaler Daten spezifische Gefahren. So können digitale Informationen – falls keine Sicherheitsmaßnahmen ergriffen wurden – verändert oder kopiert und an Dritte übermittelt werden, ohne dass dies überhaupt bemerkt wird. Viele Nutzer von sogenannten Fitness-, Gesundheits- und Lifestyle-Apps wissen nicht, dass ihre (Gesundheits-)Daten nicht unmittelbar zu einem medizinischen Leistungserbringer (dem Haus- oder Facharzt) oder zur gesetzlichen oder privaten Krankenversicherung übermittelt werden. Häufig werden diese Daten, bevor sie ihren vom Benutzer adressierten Empfänger erreichen, zu kommerziellen Zwecken von weiteren Dienstleistern – etwa dem App-Entwickler, aber auch von anderen kommerziell Interessierten, die sich zudem häufig im Ausland befinden – ausgewertet, ohne dass der Nutzer der Apps dies auch nur erahnt. Die App verschafft sich zusätzliche Informationen des Smartphones oder Handys, etwa Kontakt-, Standort- oder Nachrichten-

daten, ohne dass zu erkennen ist, warum sie diese Zugriffe benötigt. Zudem übermittelt ein Großteil der Apps selbst hochsensible Daten unverschlüsselt, so dass diese abgefangen werden können.[4] Soweit öffentliche Stellen, wie etwa gesetzliche Krankenkassen, Fitness- oder Gesundheits-Apps anbieten, sollte dies nur erlaubt sein, wenn die Anbieter Sicherheitsvorkehrungen garantieren können. Dazu gehört nicht nur, dass (Gesundheits-)Daten ausschließlich verschlüsselt übertragen werden dürfen. Die Anbieter müssen auch transparent machen, wer die Daten für welchen Zweck erhält.

Ein weiteres Stichwort ist „Big Data". Hierunter wird eine Form der Datenanalyse verstanden, die es erlaubt, mit einer hohen Verarbeitungsgeschwindigkeit große Datenmengen aus vielfältigen Quellen (Texte, Audio- bzw. Videodateien, Sensor- oder Geolokationsdaten), unabhängig davon, ob die Daten strukturiert oder unstrukturiert vorliegen, auszuwerten und hieraus wissenschaftlichen oder wirtschaftlichen Nutzen zu generieren.[5] Um die Ergebnisse zu verbessern sollen hierbei möglichst viele Daten ausgewertet werden.[6] Das Gesundheitswesen gehört zu den Branchen mit dem größten Potenzial für Big Data-Anwendungen.[7] Welche Potenziale hierin gesehen werden, kann man auch darin erkennen, dass von einer Big Data-Revolution gesprochen wird. Big-Data ermöglicht aber auch eine Totalerfassung der Daten des Betroffenen[8] und damit eine vom Grundgesetz verbotene Profilbildung. Wissenschaftliche Auswertungen von medizinischen Daten bedürfen einer strengen Regulierung.

Nicht vernachlässigt werden darf, dass es nach Angaben des Bundesamtes für die Sicherheit in der Informationstechnik mehr als 250 Millionen Schadprogramme gibt, zu denen täglich ca. 300 000 neue hinzukommen.[9] Der Ausfall informationstechnischer Systeme kann das gesellschaftliche Leben in zentralen Bereichen bedrohen und dramatische Folgen haben. Durch Schadprogramme besteht dabei nicht nur Gefahr für die in den IT-Systemen gespeicherten Gesundheitsdaten, sondern auch für den Ausfall medizinischer Geräte. Bestimmte sogenannte Kritische Infrastrukturen, etwa Krankenhäuser, sind durch das IT-Sicherheitsgesetz besonders verpflichtet, Maßnahmen zur Datensicherheit zu ergreifen. Allerdings besteht die Verpflichtung, technisch-organisatorische Maßnahmen zu ergreifen auch für die niedergelassene Ärzte und Zahnärzte aus § 9 Bundesdatenschutzgesetz. Wer diese unterlässt, macht sich schadensersatzpflichtig.

Die Nutzung moderner Informationstechnik im Gesundheitsbereich hat der Medizin zum Nutzen des Patienten erhebliche Fortschritte gebracht. Allerdings dürfen die damit verbundenen Gefahren nicht aus dem Blick geraten. Die Schaffung und Einhaltung geeigneter datenschutzrechtlicher Standards hat das Ziel, Missbrauchsszenarien und Gefährdungspotenziale der neuen Technologien zu minimieren und ist damit eine Grundvoraussetzung dafür, die Chancen und Möglichkeiten der digitalen Welt in verantwortlicher Weise ausschöpfen zu können. Datenschutz ist ein zentrales Qualitätsmerkmal von eGK und Telematikinfrastruktur und entscheidet letztlich auch über die Akzeptanz bei den Patienten.

Datenschutz hat das Ziel, Missbrauchsszenarien und Gefährdungspotenziale der neuen Technologien zu minimieren und ist damit eine Grundvoraussetzung dafür, die Chancen und Möglichkeiten der digitalen Welt in verantwortlicher Weise ausschöpfen zu können.

Die Veröffentlichung sensibler Gesundheitsdaten im Internet, genetisches Scoring von Versichertengruppen, Big-Data-Profiling können teils drastische Konsequenzen für den Einzelnen nach sich ziehen - angefangen von kriminellen Erpressungsversuchen bis hin zu handfesten Nachteilen in der Arbeits- und Lebenswelt. Die jüngsten Datenskandale in Amerika haben das deutlich vor Augen geführt.

Wir brauchen deshalb einerseits mehr Aufklärung der Patienten selbst über den verantwortlichen Umgang mit ihren Daten. Der Patient ist aufgerufen, genau hinzusehen, wem er seine Daten anvertraut - gerade im Hinblick auf die Tendenzen zur Datenerhebung mit Smartphone-Apps. Andererseits müssen neben dem Datenschutz auch die Patientenrechte gestärkt werden. Dazu sollten schnellstmöglich Regelungen getroffen werden, in welcher Weise Patienten Einblick in die über sie gespeicherten Gesundheitsdaten nehmen und nach welchem Procedere sie ihre Daten löschen können.

Absolute Sicherheit wird es in der digitalen Welt nicht geben. Deshalb sollten für Patienten, die durch die Nutzung der Technik Nachteile erleiden, auch effektive, lebensnahe Schadensersatzansprüche geschaffen werden. Auch in diesem Bereich gibt es noch etlichen Regelungsbedarf.

1 Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, BT-Drs. 18/5293.

2 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.7.2015, BGBl. I S.1324.

3 Haufe Online-Redaktion (2012): Patientendaten aus Klinikum Mittelbaden verschwunden. http://www.haufe.de/recht/datenschutz/patientendaten-aus-klinikum-mittelbaden-verschwunden_224_141910.html. Zugegriffen: 14.8.2015 ; Mand, Datenschutz in Medizinnetzen, MedR 2003,395 (Fn. 18).

4 Heinzelmann, Fitness-Apps, Datenschutz-Berater 2015,168.

5 Vgl. statt vieler Becker/Schwab: Big Data im Gesundheitswesen - Datenschutzrechtliche Zulässigkeit und Lösungsansätze, ZD 2015,151; Zieger/Smirra: Fallstricke bei Big Data-Anwendungen - Rechtliche Gesichtspunkte bei der Analyse fremder Datenbestände, MMR 2013,418.

6 Roßnagel, Big Data – Small Privacy? - Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013,564.

7 McKinsey (April 2013) The Big Data revolution in US healthcare. http://healthcare.mckinsey.com/bigdata-revolution-us-healthcare. Zugegriffen: 09.09.2015; Rüping, Big Data in Medizin und Gesundheitswesen, Bundesgesundheitsbl 2015,794.

8 Koch, Big Data und der Schutz der Daten, ITRB 2013,14

9 Krüger-Brand, Gesundheitstelematik: Zwei Gesetze, viele offene Fragen, Dtsch Ärztebl. 2015; (Heft 18): A-807.

Wolfgang Linder

Die elektronische Patientenakte - mit welchen Zielen, in wessen Interesse?

Wolfgang Linder,
Jurist, bis 2004 stellvertretender Datenschutzbeauftragter des Landes Bremen, Mitglied des Komitees für Grundrechte und Demokratie

§ 291a SGB V, die für die eGK grundlegende Norm, führt die elektronische Patientenakte (ePA) als eine der Anwendungen auf, die die eGK unterstützen soll. Dies darf man als die wichtigste Funktion der eGK – jedenfalls soweit es deren Wirkung auf Qualität und Aufwand der medizinischen Behandlung betrifft – betrachten. Um so verwunderlicher mag es erscheinen, dass es ausgerechnet unter Ärzten und Zahnärzten, die laut BMG Nutznießer sein sollen, so viel Widerstand gegen die eGK/TI gibt. Die Argumente sind vielfältig und hinlänglich bekannt. Als weitere Nutznießer gelten dem BMG auch die Versicherten, deren Gesundheitsversorgung sich durch die eGK/TI verbessern soll. Amerikanische Studien haben jedoch zum einen die Bedeutung der Arzt-Patienten-Kommunikation für die Qualität der Behandlung, zum anderen die negativen Auswirkungen der Nutzung elektronischer Patienteninformationen darauf belegt.[1]

Mögliche Profiteure könnten auch die Krankenkassen sein. Bereits seit 2004 – zeitgleich mit der Einfügung des § 291a SGB V – erhalten die Kassen die Abrechnungsdaten der ambulanten Ärzte und Zahnärzte versichertenbezogen, ohne dass ihnen untersagt wäre, die Daten für andere Zwecke als die Überprüfung der Richtigkeit der Abrechnung bzw. in anonymisierter Form auszuwerten.[2] Da die Daten digitalisiert zu liefern sind, erhalten die Kassen ein lückenloses Krankheitsprofil ihrer Mitglieder, das sie mit ihren data-warehouse-Systemen umfassend auswerten können. Seitdem können sie in einzelne Behandlungsprozesse eingreifen. Daher bezweifle ich, dass die Krankenkassen aus eigenem Interesse das Projekt „eGK“ vorantreiben. Ein Motiv könnte allenfalls das nachträglich eingefügte Versichertenstammdatenmanagement sein.

Da offensichtlich weder Ärzte noch Versicherte oder Kassen zu denjenigen gehören, die das Projekt „eGK“ vorantreiben, muss die Frage erlaubt sein, ob die Verbesserung der Qualität und die Minderung des Aufwandes medizinischer Behandlung die eigentlichen Triebfedern des Projektes sind, oder ob nicht zumindest auch andere Interessen durchgesetzt werden sollen.
In 2005 ordnete das BMG an, dass die gematik eine zentristische Telematikinfrastruktur (TI) zu entwickeln habe. Auf der eGK selbst sollen nur die Stammdaten und der Notfalldatensatz gespeichert werden, im übrigen soll die eGK dazu dienen, per Freigabe durch den Inhaber den Zugriff auf zentral auf Servern gespeicherte medizinische Daten, etwa der ePA zu eröffnen. Hingegen hat man nicht den Weg der Punkt-zu-Punkt-Kommunikation der einzelnen an der medizinischen Behandlung Beteiligten gewählt. Andernfalls wären Behandlungsdokumentationen dort geblieben, wo sie hingehören, in den Arztpraxen. Aber man hat sich dafür entschieden, mit immensem Aufwand die zentristische TI aufzubauen, nicht etwa in die bessere Sicherung der Patientendaten in den Praxen und des elektronischen Austauschs unter diesen zu investieren. Welche Konsequenzen zieht das nach sich und wessen Interessen dient das?

Die erste Konsequenz ist, dass die auf den Servern gespeicherte Datenmenge von geschätzt mehreren Dutzend Terabyte (1 TB – 1024 GB) die Versuchung unerlaubter Zugriffe auf Gesundheitsdaten in enormem Maße steigern dürfte. Dabei dürfte bei ca. 2 Mio. zugriffsberechtigten Angehörigen von Heilberufen und bei ca. 70 Mio. gesetzlich Versicherten die Gefährdung durch „Insider“ nicht geringer sein als die durch „Outsider“.

Die zentristische TI bietet hingegen - dies ist die zweite Konsequenz - eine optionale Grundlage für umfassende Auswertungen der Gesundheitsdaten aller Versicherten. Erklärtes Ziel des Entwurfs für ein E-Health-Gesetz ist es, die TI für weitere Anwendungen und auch für weitere Nutzer zu öffnen.[3] Es ist vorhersehbar, dass die ePA's zu einer Fundgrube für Mehrwertdienste und Auswertungen werden. Prompt hat sich die forschende Biotech-Industrie zu Wort gemeldet. Die Arbeitsgruppe „Bio-IT und Big Data“ der BIO Deutschland[4] fordert, entgegen geltender Gesetzeslage Zugriff auf die im Rahmen der E-Health generierten Daten zu erhalten.[5] „Big Data“ ist ohnehin das Zauberwort der Stunde. Nicht ohne Grund machte der Deutsche Ethikrat „Die Vermessung des Menschen – Big Data und Gesundheit“ zum Thema seiner Jahrestagung 2015.

In die Zusicherung der gematik, die Gesundheitsdaten seien wirkungsvoll verschlüsselt bzw. sollten nur

1 www.forum-gesundheitspolitik.de/artikel/artikel.pl?artikel=2023 bzw. 2330, abgerufen am 16.09.2015
2 Dies wurde „in letzter Minute“ in § 295 SGB V eingefügt. Beschlüsse des zuständigen Bundestagsausschusses, die Daten dürften nur für Abrechnungs- und Prüfzwecke genutzt werden, und des Plenums, 2008 solle das BMG berichten, wie Fehlentwicklungen vermieden würden, wurden konsequent missachtet.
3 Referentenentwurf für das E-Health-Gesetz vom 13.01.2015 sowie §§ 291d und f, SGB V
4 Lobby-Organisation der Biotech-Industrie incl. der Deutschen Bank
5 www. biodeutschland.org/nachricht-anzeigen/items/ag-bio-it-und-big-data-befasst-sich-mit-e-health.html, abgerufen am 16.09.2015

anonymisiert ausgewertet werden, darf man kein allzu großes Vertrauen setzen. Die Datendichte, die sich rasant entwickelnden Auswertungstechniken und das Zusatzwissen der miteinander vernetzten Nutzer dürften diesen die Identifizierung der Betroffenen ermöglichen. Die Versicherten haben es noch in der Hand, die ePA für sich selbst abzulehnen und die zentrale Speicherung ihrer Behandlungsdokumentationen zu verhindern. Da sie ihre Entscheidung ihren Ärzten gegenüber äußern sollen, wird es wesentlich auf deren Beratung ankommen. Zudem darf nach geltender und auch durch den Entwurf für ein E-Health-Gesetz bislang nicht geänderter Regelung auf in der TI gespeicherte medizinische Daten nur mit Zustimmung der Versicherten, d.h. nach Autorisierung mittels eGK, durch Inhaber von Heilberufsausweisen und nur zwecks Abrechnung und zur Versorgung des Betroffenen zugegriffen werden. Ob aber diese strikten Regelungen Bestand haben werden, steht angesichts der Lobbyarbeit der Nutzungsinteressenten und der vielen Änderungen des § 291a SGB V in der Vergangenheit doch sehr in Frage. Dabei muss man nicht einmal auf die starken industriellen Interessen abheben. So könnten etwa die Patientenrechte den ärztlichen Nutzen der ePA mindern. Darf der behandelnde Arzt einer Dokumentation vertrauen, von der er nicht weiß, ob sie vollständig und/oder aktuell ist? Denken wir weiter: Angenommen, nur ein geringer Teil der Patienten entscheidet sich dafür, die Daten überhaupt zentral speichern zu lassen, etwa weil allein das Procedere zu kompliziert und zeitraubend ist. Der behandelnde Arzt wird Patienten nicht dazu drängen, er hat die eigenen Diagnosen ohnehin in seinem Praxissystem - alles weitere verzögert seinen Praxisablauf. Weder Patient noch Arzt dürften übermäßig motiviert sein, nach der Konsultation sensible Daten an zentrale Server zu versenden.

Wird es nun die Politik wirklich hinnehmen, eine milliardenschwere Investition einfach abzuschreiben, weil die Versicherten nicht mitmachen wollen? Die Erfahrungen mit der Einführung der eGK sehen anders aus: Das System eGK kann seinen Zweck nur sinnvoll erfüllen, wenn ALLE Versicherten mitmachen. Schon diese Voraussetzung allein schließt Freiwilligkeit von vornherein aus - es geht also nur mit Zwang und Sanktionierung und genau für diesen Weg hat sich die Politik entschieden - mit der Einführung der eGK und nun mit dem Entwurf für das E-Health-Gesetz. Es gehört wenig Phantasie dazu, sich vorzustellen, wie sich die Politik entscheiden wird, wenn sie in den nächsten Jahren zwischen gelebten Patientenrechten und einer „funktionstüchtigen“ ePA wählen muss.

Wie aber wird es sich auf das Bewusstsein und Verhalten der Versicherten auswirken, falls in Zukunft ihre Behandlungsdokumentationen auf Dauer zentral gespeichert, abrufbar und nutzbar sein werden? Der Versicherte wird sich dessen bewusst sein müssen, dass seine Behandlungsdokumentationen nicht länger nur dezentral bei seinen Ärzten, sondern auch zentral gespeichert und auswertbar sind. Dies dürfte ihm vor Augen führen, dass seine Gesundheit nicht mehr nur seine Privatangelegenheit ist, sondern einer für ihn anonymen Überwachung unterliegt. Das wiederum wird Rückwirkungen auf sein Verhalten haben und die Neigung zur Anpassung an als Norm empfundene Verhaltensanforderungen stärken.

Das System eGK kann seinen Zweck nur sinnvoll erfüllen, wenn ALLE Versicherten mitmachen. Schon diese Voraussetzung allein schließt Freiwilligkeit von vornherein aus - es geht also nur mit Zwang und Sanktionierung.

All diejenigen, zumeist jungen Versicherten, die heute bereits - im Rahmen von Präventions- und Bonusprogrammen - ihre täglich zurückgelegten Schritte, eingenommenen Mahlzeiten, Puls- und sonstige Gesundheitsdaten Krankenversicherungen bzw. deren Dienstleistern über Smartphoneapps übermitteln, lassen erahnen, wie die idealtypischen Versicherten der neuen Welt funktionieren. Im Zentrum steht ein Bewertungssystem, an dessen Skala sich ablesen lässt, wie gesundheitsförderlich sich der Betreffende verhält. Der ganze Ehrgeiz der Fitnessjünger zielt darauf, möglichst hohe Punktwerte zu erreichen. Wird das „wissenschaftliche“ Bewertungssystem irgendwann geändert, joggt die Herde dem neuen Ziel entgegen.

Was beim Blick auf diese kleine Gruppe eifriger Zeitgenossen noch amüsant wirken mag, ist jedoch strukturell bereits in eGK und Telematik angelegt. Es handelt sich letztlich um eine Fremdsteuerung mittels Selbstkonditionierung, ein Aspekt der von Michel Foucault entwickelten „gouvernementalité“.[6] Gegenstand dieser Steuerung ist hier der gleichgerichtet handelnde Versicherte, der das Richtige isst, zur richtigen Zeit schläft und der seinen Körper auf die richtige Weise fit hält. Und natürlich wird der Versicherte allzeit richtig untersucht, erhält die richtigen Medikamente und wird ausschließlich mit den richtigen Therapien behandelt. Das Richtige wird selbstverständlich wissenschaftlich ermittelt und sollte - mit Blick auf die begrenzten Mittel - nicht zu teuer sein.

Vielfalt, Individualität, Freiheit kommen in dieser Welt nicht mehr vor. Wollen wir das wirklich?

6 vgl. Oliver Decker. „Alles auf eine Karte setzen: elektronisches Regieren und die Gesundheitskarte“, Psychotherapeutenjornal, 4/2005, S. 338ff

Maria Klein-Schmeink

Die Patientinnen und Patienten sind Zaungäste der Entwicklung

Maria Klein-Schmeink, MdB
Mitglied der Fraktion Bündnis 90 / Die Grünen im Deutschen Bundestag, Sprecherin für Gesundheitspolitik, Mitglied des Gesundheitsausschusses im Deutschen Bundestag

Seit mehr als zehn Jahren wird über die elektronische Gesundheitskarte und die Telematik im Gesundheitswesen gestritten. Passiert ist wenig. Jetzt legt die Bundesregierung ein reines Telematik-Infrastruktur-Sicherstellungsgesetz vor. Erst wenn die Infrastruktur steht, sollen weitere, längst überfällige Schritte folgen. Die Patientinnen und Patienten spielen dabei die Randrolle. Entgegen der Gesetzeslage ist eine Erprobung des Patientenzugriffs auf die eigenen Daten noch lange Zukunftsmusik und ihre Mitwirkungsmöglichkeiten in der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) sind gering.

Mit der elektronischen Gesundheitskarte (eGK) sollten die Patientinnen und Patienten ihr Recht auf informationelle Selbstbestimmung wirksam ausüben können. Sie sollten insbesondere umfassende Rechte auf Einsichtnahme ihrer Patientendaten jederzeit wahrnehmen können. Das Zugriffsrecht der Versicherten auf ihre Daten ist für die Wahrung der Transparenz und für die Akzeptanz der elektronischen Gesundheitskarte und der geplanten freiwilligen medizinischen Anwendungen von entscheidender Bedeutung. Die Zugriffsrechte der Versicherten sind zwar gesetzlich normiert, befinden sich aber noch nicht einmal in der Entwicklung. Zu Beginn der Telematikentwicklung definierte Lösungen wie das Patientenfach auf der eGK und der eKiosk wurden nicht umgesetzt und alternative Lösungen auch nicht diskutiert. Bislang existierte hierfür noch nicht einmal eine Projektgruppe in der gematik. Auch der Entwurf der Bundesregierung für ein Gesetz zur sicheren digitalen Kommunikation im Gesundheitswesen enthält keinerlei wirksame Vorgaben, klare Fristen oder Anstöße wie Sanktionen bei Verzögerungen, wodurch die Patientinnen und Patienten rasch Zugang zu ihren Daten bekommen können.

Klar ist auch: Nur durch die Einbeziehung von Patientenorganisationen und ihr Mitberatungsrecht innerhalb der Gesellschaft für Telematik lässt sich die Patientenorientierung bei allen Projekten gewährleisten. Zwar sieht der erwähnte Gesetzentwurf vor, Patientenvertreterinnen und -vertreter in den geplanten Beirat der gematik aufzunehmen, dies wird allerdings angesichts der erheblichen Defizite als nicht ausreichend angesehen. Eine stärkere Orientierung an den Bedürfnissen der Patientinnen und Patienten sollte beispielsweise durch eine Querschnittsarbeitsgruppe zu den Belangen der Patientinnen und Patienten innerhalb der gematik ermöglicht werden, wie sie vom Verbraucherzentrale Bundesverband vorgeschlagen wurde. Auch ein Mitberatungsrecht von Vertreterinnen oder Vertretern der für die Wahrnehmung der Interessen der Patienten und der Selbsthilfe chronisch Kranker und behinderter Menschen maßgeblichen Organisationen in der Gesellschafterversammlung der gematik wäre denkbar.

Voraussetzung für die notwendige breite Akzeptanz und das Vertrauen in die digitale Vernetzung des Gesundheitssektors sind darüber hinaus vor allem höchstmögliche Datenschutz- und Datensicherheitsstandards. Hier muss die Bundesregierung beim geplanten E-Health-Gesetz noch nachbessern, damit die Patientinnen und Patienten die geplanten medizinischen Anwendungen auf der elektronischen Gesundheitskarte bedenkenlos nutzen können. Sie muss sicherstellen, dass auch bei der Einschaltung externer Dienstleister durch Berufsgeheimnisträger der Vertraulichkeitsschutz und deren Schweigepflicht sichergestellt wird und die Patientendaten auch bei diesen durch einen Beschlagnahmeschutz abgesichert sind. Die Einschaltung externer Dienstleister ist für Berufsgeheimnisträger oft alternativlos, wenn sie moderne Informationstechnik nutzen wollen. Hierfür muss die Bundesregierung Rechtssicherheit schaffen und klarstellen, unter welchen Voraussetzungen diese eingeschaltet werden dürfen.

Zur Herstellung von Transparenz über verwendete technische und semantische Standards, Profile und Leitfäden im Gesundheitswesen plant die Bundesregierung, die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) damit zu beauftragen, ein Interoperabilitätsverzeichnis aufzubauen. Neue digitale Anwendungen sollen hierdurch vorhandene Standards und Profile nutzen können. Neben wissenschaftlichen Fachleuten und IT-Experten sollten hierbei auch zwingend Datenschutzexperten in zentralen Fragen der Weiterentwicklung der IT-Systeme beratend herangezogen werden.

Darüber hinaus müssen für alle künftigen in der Telematik zu nutzenden, insbesondere medizinischen Anwendungen geeignete Qualitätsstandards entwickelt werden und die Patientinnen und Patienten eine bessere Unterstützung bei der Auswahl für sie sinnvoller Anwendungen erhalten. Der Entwurf der Bundesregierung für ein Gesetz zur sicheren digitalen Kommunikation im Gesundheitswesen schweigt sich hierzu aus. Bei der Entwicklung geeigneter Qualitätsstandards und Konzepte sind im Übrigen auch die Patientinnen und Patienten einzubeziehen.

Die Zugriffsrechte der Versicherten [auf ihre Daten] sind zwar gesetzlich normiert, befinden sich aber noch nicht einmal in der Entwicklung. Zu Beginn der Telematikentwicklung definierte Lösungen wie das Patientenfach auf der eGK und der eKiosk wurden nicht umgesetzt und alternative Lösungen auch nicht diskutiert.

Außerhalb der Telematik existiert bereits eine nahezu unüberschaubare Anzahl unterschiedlicher mobiler Gesundheits- und Medizin-Apps. Sie richten sich an Patientinnen und Patienten wie auch an Angehörige der Gesundheitsberufe. Die wenigsten Apps sind evidenz- oder leitlinienbasiert und mit Beteiligung von Gesundheitsexperten entwickelt. Auch beim Datenschutz sind zahlreiche dieser Apps fragwürdig. Nur ein kleiner Teil der Apps wird wegen der medizinischen Zweckbestimmung als Medizinprodukt reguliert und besitzt eine CE-Kennzeichnung – noch dazu wird diese Zweckbestimmung allein durch den Hersteller definiert. Es sind für Gesundheits-Apps etliche sinnvolle Anwendungsmöglichkeiten denkbar. So bietet beispielsweise die Barmer GEK ihren Versicherten schon heute eine App zum internetbasierten Sehtraining für Kinder mit funktionaler Sehschwäche und hat hierzu einen Vertrag mit einem bundesweiten Netz von Augenärzten abgeschlossen. Im besten Fall sind solche Apps damit Teil eines umfassenderen, telemedizinischen Versorgungskonzeptes und können die Interaktion zwischen Patientin bzw. Patient und Behandlerin bzw. Behandler verbessern.

Jedoch wünschen sich nicht ohne Grund viele zur Unterstützung ihrer Entscheidung bei der Auswahl einer App mehr staatliche Kontrolle der Angebote und ein verpflichtendes Prüf-Siegel für Gesundheits-Apps. Die Bundesregierung kennt den wachsenden Markt mit Angeboten von Google, Apple und Co. Dennoch wird auch dieser Bereich von der Bundesregierung derzeit ignoriert und wahrscheinlich frühestens in der nächsten Legislaturperiode genauer betrachtet und auf etwaige Regelungsbedarfe überprüft. Der Markt wird weiter wachsen. Und während viele Patientinnen und Patienten noch kritisch überlegen, welche individuellen Daten sie auf ihrer eigenen elektronischen Gesundheitskarte gespeichert haben wollen, werden zugleich im Rahmen ihrer individuellen Vorsorge und Behandlung mehr und mehr sensible Gesundheitsdaten wie beispielsweise Puls- oder Blutzuckerwerte regelmäßig in vollkommen ungeschützte Apps eintragen.

An der Zeit ist auch eine bessere Einbeziehung der Pflege und anderer Gesundheitsberufe. Seit langem wird über die notwendige Neuverteilung der Aufgaben in der Gesundheitsversorgung, eine bessere Zusammenarbeit der Gesundheitsberufe und die Stärkung der intersektoralen Versorgung diskutiert. Passiert ist bislang jedoch recht wenig. Auch der geplante Gesetzentwurf der Bundesregierung leistet hierzu keinen hinreichenden Beitrag. So fehlt beispielsweise eine stärkere Öffnung der Telematikinfrastruktur für Hebammen, Pflegekräfte, Pflegeeinrichtungen und andere Therapieberufe. Hier besteht also noch Nachbesserungsbedarf, um die Pflege als „komplementäres Anwendungsfeld“ für telemedizinische Leistungen zu stärken, wie dies die Bundesregierung zuletzt noch in ihrer E-Health-Initiative 2012 bekräftigte. Innerhalb der Gesellschaft für Telematikanwendungen (gematik) sind bislang keine geeigneten Verbände aus der Pflege eingebunden, um pflegerische Aspekte einfließen zu lassen. Deswegen muss dafür gesorgt werden, dass der Deutsche Pflegerat insbesondere im geplanten Beirat der gematik vertreten ist und hier die pflegerische Perspektive einbringen kann.

Insgesamt brauchen wir somit eine grundlegendere Regelung, die überfällige Schritte in die Wege leitet, um die Chancen der Digitalisierung im Dienste der Patientinnen und Patienten zu nutzen.

Hardy Müller, Frank Verheyen

Chancen und Risiken der Digitalisierung im Gesundheitswesen:

Eine Herausforderung für die Versorgung

Hardy Müller M.A.
Gesundheitswissenschaftler, Anthropologe, Referent am Wissenschaftlichen Institut der TK für Nutzen und Effizienz im Gesundheitswesen (WINEG)

Dr. Frank Verheyen,
Direktor des Wissenschaftlichen Instituts der TK für Nutzen und Effizienz im Gesundheitswesen (WINEG)

Im Jahr 2007 wurde die Internetseite quantifiedself.com gegründet, um Daten zur Quantifizierung der eigenen Person zu sammeln. Je mehr Zahlen gewonnen werden, desto besser, so lautet die Devise der Bewegung. Als Programm der ursprünglich amerikanischen Bewegung gilt „self knowledge through numbers". Das Ziel ist die Verbesserung des eigenen Lebens. Die notwendigen Technologien - Sensoren, Cloud computing, Smartphones, Wearables, Internet der Dinge - sind mittlerweile allgegenwärtig. Die Methode des Big Data soll uns in die Lage versetzen, aus der Vielzahl von Daten Informationen und am Ende Wissen zu generieren. Doch werden wir sicher die Chancen realisieren?

Mit dem Begriff des Big Data werden Technologien bezeichnet, mit denen die Analyse von Daten möglich wird, die vor kurzem aufgrund ihrer Menge (volume), ihrer Veränderlichkeit (velocitiy) oder ihrer Heterogenität (variety) nicht auswertbar waren. Eine Herausforderung ist die Qualität der Daten (veracity). Wir wissen, dass alle Daten nie präzise sein können und immer Fehler und Unsicherheiten enthalten (1). Die Daten werden nicht zum Selbstzweck erhoben, sondern diese werden ausgewertet, um damit Werte zu schaffen (value): Big Data ist auch Big Business. Ein Prinzip des Big Data besteht in der Analyse von Korrelationen. Aus historischen Entwicklungen werden Prognosen extrapoliert. Die Verfahren werden jedoch wenig zur Hypothesengenerierung und Theoriebildung in den Wissenschaften beitragen (2).

Chancen: Effizienzsteigerung des Gesundheitswesens durch Digitalisierung

Erste Entwicklungen zeigen, dass gesundheitsbezogene Daten eingesetzt werden, um Personengruppen zu charakterisieren. Beispielsweise möchte ein Schweizer Unternehmen mit einer einzigen Kennzahl aus einer Gesundheits-App das Wohlbefinden jedes einzelnen Menschen messen und empfiehlt Krankenkassen zur finanziellen Sanierung den Einsatz seiner Verfahren (3). Haben Versicherte günstige Werte, sind sie zu bonifizieren. Das Gesundheitssystem insgesamt würde dann insgesamt gerechter und effizienter - so die Argumentation der Initiatoren.
Zur Effizienzsteigerung des Gesundheitssystems und um das System überhaupt finanzierbar zu halten werden Versicherungstarife vorgeschlagen, die sich nach dem individuellen Verhalten des Versicherten richten. Diese Tarifierungen werden unter dem Begriff des „Pay-As-You Live - PAYL" diskutiert. Auf der Basis individueller Tracking-Daten werden Prämien kalkuliert. „Meist wird der Patient für eine ‚gesunde Lebensführung' belohnt, die er mittels mobil erhobener Daten nachweist".(4) Die KFZ-Versicherung bietet seit langem bereits sogenannte Telematik-Tarife an. Demnach bezahlen Fahrer, die Ihr Fahrverhalten dokumentieren, weniger als solche, die unüberwacht fahren.

Einzelne Krankenversicherungen setzen bereits Apps zur Dokumentation des eigenen Gesundheitsverhaltens ein oder künden den baldigen Start derartiger Anwendungen an. Die Apps dienen zur Gesundheitsoptimierung. Letztlich entscheidet jeder individuell, ob eine Nutzung der App für ihn sinnvoll ist. Die Chancen werden von den Anbietern der neuen Technologien im Allgemeinen betont - obschon immer darauf hingewiesen wird, dass auch mit dieser Technologie Gefahren verbunden sind. Die Bundesregierung anerkennt die Relevanz des Themas, betont die Verantwortung der Verbraucher und erklärt selbst aber keinen Regulierungsbedarf. „Die Bundesregierung geht davon aus, dass Versicherte sich der besonderen Bedeutung ihrer Daten zum persönlichen Lebenswandel und ihrem Gesundheitsverhalten bewusst sind und daher sorgsam und zurückhaltend mit der Weitergabe entsprechender Informationen umgehen." (5)

Risiken: Edward Snowden markiert das Ausmaß

Welche Risiken bestehen? Gefährlich sind nicht allein etwa Datenschutz-Verletzungen oder das Problem der Validität und Reliabilität der Messungen.
Die amerikanische Wirtschaftswissenschaftlerin Shoshana Zuboff vertritt die Auffassung (6), dass „Big Data" als euphemistischer Begriff eigentlich „großer Schmuggel" bedeutet. Denn die von den Nutzern erzeugten Daten („Daten-Abgase") werden oft ohne unser Wissen und ohne unser Einverständnis abgeschöpft und für andere Zwecke ge- bzw. missbraucht.(7)
Diese neuen Daten entstammen einer Überwachungspraxis und werden als Güter gehandelt. Wie die Geschäftsmodelle des Silicon Valley zeigen, ziehen diese Überwachungs-Güter viel Kapital an. Zuboff bezeich-

Literatur:
(1) Marquart W (2015): Was ist Big Data? In: Deutscher Ethikrat, Jahrestagung 2015.
(2) Pigeot I, Jacobs S, Koch-Gromus U (2015): Große Datensammlungen im Gesund-heitswesen - Chancen oder Risiko? Editorial zum Leitthema Big Data contra große Datensammlungen. Chancen und Risiken für die Gesundheitsforschung. Bundesgesundheitsbl 58:785-787

net diese Marktform mit dem Begriff des „Überwachungskapitalismus“ (6).
Diese neue Marktform birgt in Folge Schwierigkeiten auch für die Anwendung von sogenannten Gesundheits-Apps und deren Einsatz durch die Krankenkassen. Der mittlerweile offenkundige massenhafte Missbrauch von Daten (8) erodiert zwangsläufig und verständlicherweise auch die Bereitschaft von Versicherten, ihre Daten für Analyse- und Forschungszwecke (weiter) zur Verfügung zu stellen. Der Legitimationsdruck wird für die Forschung an Daten erhöht, die Auswertungen damit erschwert. Die sozialkritischen Diskussionen um die von Edward Snowden offenbarten Vorgänge sind damit unmittelbar von Bedeutung für Datenanalysen. Daher ist gerade auch eine Befassung in den Krankenkassen mit dem Thema notwendig. Die Krankenkassen sind nicht nur verpflichtet, umfassende Sicherungsmaßnahmen zum Datenschutz zu gewährleisten, sondern dies auch als sensibles Thema umfassend zu diskutieren. Ein entscheidendes Kriterium für Datenauswertungen ist dabei sicherlich auch die informierte Einwilligung der Versicherten.

Quantified Self und die Digitalisierung des Gesundheitswesens ist dabei, unser Gesundheits- und Krankheitsverständnis zu verändern, mit Konsequenzen für das gesamte Gesundheitssystem.
Die Quantified Self-Bewegung folgt einer Mensch-Maschinen Philosophie (9). Wer den Menschen für etwas Machbares, Formbares hält, überträgt ihm dadurch die alleinige Verantwortung für seine Existenz, seine Gesundheit. Wer, wie die Self-Tracker sich selbst bis in den letzten Winkel vermisst, wer nicht nur sprichwörtlich, sondern wortwörtlich tägliche Nabelschau betreibt, übernimmt diese Verantwortung auch in vollem Bewusstsein. Die logische Folge dessen ist aber, dass Krankheit als Versäumnis, als Fehlmanagement und damit als Schuld begriffen wird: Man hätte sie durch genaues Beobachten, Dokumentieren und Auswerten rechtzeitig erkennen und verhindern können (10). Dies führt in letzter Konsequenz zur Entsolidarisierung: Wer an seinem (pathologischen) körperlichen Zustand selbst schuld ist, der hat auch keinen Anspruch auf solidarische Hilfe.

„Pay-As-You Live“-Tarife unterstellen, dass aus einem dokumentierten Verhalten individuelle Risiken zu errechnen sind und konterkarieren damit das Versicherungs-Prinzip. Die Versicherungsidee fußt auf der Erfahrung, wonach das Leben Risiken bereit hält, die der einzelne nicht kalkulieren oder absichern kann. Erst durch den solidarischen Zusammenschluss eines Kollektives können sehr seltene, aber existentielle Bedrohungen von Individuen abgesichert werden. „Pay-As-You Live“-Tarife sind keine Versicherungstarife, sondern Rücklagen um einen individuellen „Bedarf“ zu decken. Falls sie überhaupt funktionieren - wirken sie jedenfalls entsolidarisierend. *Quantified Self* kann eine Überversorgung befördern. Schon heute berichten Ärzte, dass nach sogenannten Gesundheits-Messungen nicht behandlungsbedürftige Menschen die Praxen verstopfen und damit Behandlungsressourcen für kranke Menschen vergeuden.

„Pay-As-You Live“-Tarife unterstellen, dass aus einem dokumentierten Verhalten individuelle Risiken zu errechnen sind und konterkarieren damit das Versicherungs-Prinzip. [...] Falls sie überhaupt funktionieren, wirken sie jedenfalls entsolidarisierend.

Fazit: Risiken verwirklichen sich von allein, Chancen müssen erarbeitet werden

Die Digitalisierung des Gesundheitswesens hält viele offene Fragen bereit. Die Jahrestagung des Deutschen Ethikrates 2015 oder der 3. Zukunftskongress der Techniker Krankenkasse 2015 zur Digitalen Gesundheit thematisiert das Spektrum von offenen Fragen, Fragen, die beantwortet werden müssen, um die Digitalisierung des Gesundheitswesens voranzubringen. Die vorhandenen Datenschutz-Einrichtungen in Deutschland sind dazu angesichts der Geschwindigkeit, mit der Big Data Anwendungen umgesetzt werden immer weniger in der Lage. „Die Datenschützer sind ihrer Aufgabe nicht gewachsen. Während Google, Facebook und andere Internetkonzerne aufrüsten, spart der Staat“ (11).
Über den Datenschutz hinaus müssen wir uns grundsätzlich mit sozial-rechtlichen, ethischen und sozialen Konsequenzen beschäftigen. Eine Diskussion, die bislang vornehmlich in den Feuilletons geführt wird. In Deutschland ist u.a. Frank Schirrmacher für die Initialisierung dieser Debatte zu danken. Die Digitale Debatte muss sich auch im Versorgungsmanagement widerspiegeln.

Damit sich Chancen der Digitalisierung zum Ausbau einer humanen Krankenversorgung realisieren, bedarf es einer aktiven Auseinandersetzung der Akteure im Gesundheitswesen mit dem Thema. Notwendig sind nun Stellungnahmen von Leistungserbringern und Krankenkassen (-verbände), in der auch Antworten auf die zentralen Fragen im Zusammenhang mit der digitalen Gesundheit gegeben werden. Eine aktive Förderung des Themas - hoffentlich auch über den Innovationsfonds - ist notwendig, damit sich die Chancen der Digitalisierung im Gesundheitswesen realisieren lassen.

(3) Gernert B (2015): Wie weit gehen Sie für Ihre Gesundheit? TAZ am Wochenende, 18.04.2015, 18ff
(4) Schoss M (2015): Interviewleitfaden zum Thema „Pay-As-You-Live“. unveröffentlichtes Manuskript der Uni Hamburg.
(5) BT-Drucksache 18/3849 (2015): Datensammlungen über Versicherte in der privaten Krankenversicherung (Zitierdatum 20.04.2015), abrufbar unter http://dip21.bundestag.de/dip21/btd/18/038/1803849.pdf
(6) Zuboff S (2014) Unsere Zukunft mit „Big Data“: Lasst euch nicht enteignen. FAZ 14.03.2014 (Zitierdatum 19.04.2015) abrufbar unter http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/unsere-zukunft-mit-big-data-lasst-euch-nicht-enteignen-13152809.html?printPagedArticle=true#pageIndex_2
(7) Der Spiegel 10/2015 (2015): Die Weltregierung. Wie das Silicon Valley unsere Zukunft steuert. 28.02.2015.
(8) Greenwald G (2014) Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München
(9) Müller H (2012) „Individualisierte Medizin“ und „Quantified Self“ als Herausforderung für die medizinische Versorgung. IGZ 2/2012: 20-23
(10) Eberbach WH (2014): Personalisierte Prävention: Wirkungen und Auswirkungen. – Zugleich ein Plädoyer für die Solidarität mit dem Selbstbestimmungsrecht – MedR (2014) 32: 449–464 449
(11) Büschemann K-H (2015): Digitaler Sisyphos. SZ vom 19./20.09.2015, 25.

Tobias Wenhart

Datendiebstahl in der Praxis: Haftungsrisiken für Ärzte

Die eGK als Einfallstor für Cyberkriminelle

Tobias Wenhart,
Manager Products & Underwriting, Hiscox

Sie erleichtert die Kommunikation zwischen Ärzten und Patienten und kann im Notfall Leben retten: 2011 löste die elektronische Gesundheitskarte stufenweise die klassische Krankenversicherungskarte ab und ist seit Beginn dieses Jahres der ausschließliche Berechtigungsnachweis für die Inanspruchnahme ärztlicher Leistungen. Bislang sind neben der Krankenversichertennummer nur ein Foto des Karteninhabers sowie der Nachweis einer länderübergreifenden europäischen Krankenversicherung darauf gespeichert. Zukünftig sollen jedoch mit dem Einverständnis des Patienten auch notfallrelevante Informationen wie der Notfalldatensatz, Arzneimittelunverträglichkeiten oder Patientenverfügungen gespeichert werden. Die elektronische Gesundheitskarte steht sinnbildlich für die zunehmende Digitalisierung der gesamten Gesundheitsbranche, die Ärzten und Patienten die Behandlung erleichtern soll.

Lukrative Patientendaten

Datenschützer warnen seit Jahren vor den Risiken, die insbesondere mit einer digitalisierten Patientenakte verbunden sind und zweifeln die Datensicherheit der elektronischen Gesundheitskarte an. Die Karte enthält einen Mikroprozessor, über den die medizinischen Informationen nur verschlüsselt übermittelt und für Dritte unlesbar gemacht werden. Angesichts ständig geschickter agierender Cyberkrimineller bleibt allerdings fraglich, ob und wie lange dieser Schutz für die Patienten ausreichend ist. Technische Schutzmaßnahmen sind bereits in der Vergangenheit immer wieder überwunden worden und selbst bei vermeintlich gut gerüsteten Großunternehmen wie beispielsweise bei der US-amerikanischen Krankenkasse Anthem erbeuteten Hacker erfolgreich Daten. Im Ernstfall haftet die betroffene Krankenkasse oder Praxis und Kleinunternehmer wie Ärzte sehen sich mit hohen Schadensforderungen konfrontiert, die ihre finanziellen Mittel schnell um ein Vielfaches übersteigen und auf diese Weise die berufliche Existenz bedrohen.

Bei den Informationen rund um die Gesundheit eines Karteninhabers handelt es sich um äußerst sensible Daten, die für Kriminelle besonders lukrativ sind. Die detaillierten Einblicke in die Krankheitsgeschichte eines Patienten lassen sich für Werbezwecke nutzen und bieten Raum für kriminelle Handlungen wie Erpressung und Versicherungsbetrug. Medienberichten zufolge werden Gesundheitsdaten in den USA aufgrund dieser vielfältigen Nutzungsmöglichkeiten unter Kriminellen mittlerweile vielfach teurer gehandelt als Kreditkarteninformationen. Die rund 72 Millionen elektronischen Gesundheitskarten, die in Deutschland im Umlauf sind, bieten auch hierzulande ein riesiges Angriffsziel für Hacker.

Tatort Praxis

Besonders wenn den Cyberkriminellen der Zugriff auf die Patientendaten über eine Praxis oder Klinik gelingt, ist der Schaden für die betroffenen Ärzte oft groß, wie folgende Beispiele verdeutlichen.

Im Fall eines niedergelassenen Arztes gelang es Hackern, Zugriff auf das Kartenleseterminal der Praxis zu bekommen. Die Kriminellen waren als vermeintliche Patienten in der Praxis und manipulierten das Kartenlesegerät in einem Moment, als die Arzthelferin den Empfang kurz unbesetzt zurückließ. Als die Sicherheitslücke nach einem Monat im Zuge von Wartungsarbeiten am IT-System der Praxis bemerkt wurde, waren bereits die Daten von über hundert Patienten gestohlen worden. Die Betroffenen machten aus der Persönlichkeitsverletzung resultierende Schadensersatzansprüche gegenüber dem Arzt geltend und zudem musste die Praxis für drei Werktage geschlossen werden, um die Sicherheit des IT-Systems wiederherzustellen. Der Schaden des Arztes belief sich auf eine Summe im mittleren fünfstelligen Bereich.

Gefährlich kann auch die Kommunikation zwischen verschiedenen Nutzern der Patientendaten werden, wie das Beispiel einer Gemeinschaftspraxis zeigt. Einer der beteiligten Ärzte erhielt die Mail eines vermeintlichen Pharmavertreters, der im Anhang seine aktuelle Preisliste mitschickte. Anstelle der Liste lud der betroffene Arzt jedoch unwissentlich Malware auf den Server der Praxis herunter, die sich mit dem Mailprogramm der Ärzte verband. Die Attacke blieb über mehrere Tage hinweg unentdeckt und die Zahnärzte kommunizierten weiterhin per Mail mit Krankenkassen der Patienten. Nichtsahnend transferierten sie die Malware auf das IT-System einer Krankenkasse, wo die Cyberkriminellen kurzfristigen Zugriff auf die Informationen von tausenden Versicherten hat-

Anmerkung der Redaktion:
Hiscox ist ein internationaler Spezialversicherer, der neben zahlreichen anderen Versicherungsprodukten auch Cyberversicherungen in Deutschland anbietet.
Der Markt für Cyberversicherungen gilt als Wachstumsmarkt. Seit im Jahre 2011 die erste Cyberversicherungspolice offeriert wurde, hat die Zahl der Angebote und Anbieter beständig zugenommen. Aktuell bieten 13 Versicherungsunternehmen Cyberversicherungen in Deutschland an (Quelle: ix, 9/2015).

ten. Die Krankenkasse machte die Zahnärzte und deren fahrlässiges Handeln für den Schaden verantwortlich, der sich auch durch den erlittenen öffentlichen Imageverlust auf einen einstelligen Millionenbetrag summierte.

Existenzbedrohende Schadensforderungen

Die finanziellen Forderungen, mit denen Ärzte nach Datenverlusten oder Schäden Dritter konfrontiert werden, erreichen innerhalb kürzester Zeit existenzbedrohende Höhen. Allein die meist hohe Zahl betroffener Dateninhaber schlägt mit der Entschädigung für die Verletzung der Persönlichkeitsrechte zu Buche und zudem müssen alle Dateninhaber gemäß der gesetzlichen Informationspflicht benachrichtigt werden, was einen hohen zeitlichen Aufwand darstellt. Hinzu kommen etwaige Rechtsansprüche Dritter, wie etwa im oben geschilderten Beispiel die von der Cyberattacke mitbetroffene Krankenkasse. Auch wenn das System der elektronischen Gesundheitskarte langfristig immer sicherer gestaltet wird, gibt es keine Garantie für einen vollkommen sicheren digitalen Datentransfer zwischen Ärzten, Patienten und Krankenkassen. Insbesondere das Risiko, Opfer eines Cyberangriffs zu werden, kann auch bei gewissenhaftester technischer Vorsorge durch Firewalls und Virenprogramme nicht ausgeschlossen werden.

Cyberversicherung als zusätzliche Sicherheitsmaßnahme

Als vorbeugende Maßnahme empfiehlt sich deshalb der Abschluss einer Versicherung gegen Cyberangriffe und deren weitreichende Folgen. Der Spezialversicherer Hiscox brachte als erster Anbieter Cyberversicherungen auch für kleine und mittlere Unternehmen auf den deutschen Markt. Diese eignen sich gleichermaßen für Arztpraxen, nachdem die Betriebsgröße meist vergleichbar ist und eine Cyberattacke wie beschrieben ebenfalls ernste wirtschaftliche Folgen nach sich ziehen kann.

Eine Cyberversicherung des Spezialversicherers Hiscox umfasst beispielsweise Haftpflichtansprüche, welche im Fall eines Datenverlustes etwa durch die Persönlichkeitsrechtsverletzung der betroffenen Patienten, aber auch Schadenersatzansprüche Dritter, die durch die unwissentliche Weitergabe eines Virus entstehen können. Für die sofortige Identifikation eines Cyberschadens sowie dessen Behebung arbeitet Hiscox mit den renommierten IT-Spezialisten von HiSolutions zusammen, die den Versicherten im Schadenfall rund um die Uhr zur Verfügung stehen und das unmittelbare Krisenmanagement übernehmen. HiSolutions kümmert sich im Fall eines bemerkten Cyberangriffs um dessen sofortige Abwehr und um die Wiederherstellung verlorener Daten wie etwa gespeicherter Patientenakten. Hiscox übernimmt als Versicherer ferner die Kosten für eine eventuell notwendige Aufrüstung des IT-Systems des Geschädigten und für die gesetzlich verpflichtende Information der Dateninhaber im Fall eines Datenverlusts. Sollte der Schaden nach seiner Behebung einen Rechtsstreit mit Dateninhabern oder einer beteiligten Krankenkasse nach sich ziehen, greift Hiscox seinen Versicherten mit Fachanwälten unter die Arme und berät auch bei der öffentlichen Kommunikation rund um den Cyberangriff, sofern die Reputation einer Praxis oder Klinik durch den Cyberangriff gefährdet ist. Auf Wunsch können die Unternehmen selbst den möglichen Eigenschaden, der etwa durch den Betriebsausfall als Folge einer Cyberattacke entsteht, mitversichern.

Die Details der jeweiligen Versicherung klärt Hiscox individuell mit seinen Kunden ab und bietet eine maßgeschneiderte Lösung für jede Praxis. Diese hängt unter anderem von der Größe des Unternehmens ab, aber auch vom Ausmaß und den Wegen des Datenverkehrs – wie viele Patienten und damit elektronische Gesundheitskarten sind beispielsweise mit einer Praxis verbunden und über welches Mailsystem kommuniziert der Arzt mit Krankenkassen? Zusätzlich bekommt jeder Versicherungsnehmer beim Abschluss einer Cyberversicherung einen Krisenplan zur Hand, nach dem er im Ernstfall handeln soll, um unverzüglich Schritte zur Schadensbegrenzung einleiten zu können. Mit einer Cyberversicherung als zweiter Linie der Verteidigung neben den üblichen technischen Maßnahmen sind Praxen und Ärzte gut gegen die umfangreichen finanziellen Folgen von Datendiebstählen im sensiblen Gesundheitsbereich gewappnet.

Die finanziellen Forderungen, mit denen Ärzte nach Datenverlusten oder Schäden Dritter konfrontiert werden, erreichen innerhalb kürzester Zeit existenzbedrohende Höhen. [...] Als vorbeugende Maßnahme empfiehlt sich deshalb der Abschluss einer Versicherung gegen Cyberangriffe und deren weitreichende Folgen.

Arne Schönbohm

Daten- und Patientenschutz im digitalen Zeitalter

Arne Schönbohm,
Präsident des Cyber-Sicherheitsrat Deutschland e.V.,
Vorstand der BSS AG

Die Digitalisierung von Industrie und Gesellschaft ist unaufhaltsam. Vor allem im Bereich der Medizintechnik wurden in den letzten Jahren enorme Entwicklungen vollbracht.

Connected Devices erlauben durch ihre Anbindung an das Internet den permanenten Datenaustausch zwischen Patient, Arzt und Maschine. Heutzutage gehören neben Smartphones, Smartwatches und Tablets auch Röntgengeräte und Insulinpumpen zum sogenannten Internet der Dinge. Solche telemedizinischen Anwendungen erlauben Ferndiagnosen und Therapien in abgelegenen Regionen und reduzieren somit die Distanz zwischen Arzt und Patient. Gleichzeitig reduzieren sie die Kosten für Patienten und entlasten die Krankenkassen. Letzteres stellt vor dem Hintergrund des demographischen Wandels eine notwendige Bedingung für die medizinische Versorgung der zukünftigen Generationen dar.

Neben solchen positiven Folgen beherbergt die schöne neue Welt der Digitalisierung jedoch auch Gefahren. Jedes Connected Device, also jedes mit dem Netz verbundene Gerät, stellt eine Angriffsfläche dar, die von Hackern missbraucht werden kann. Hacker nutzen die mit dem Internet verbundenen Geräte, um in die Netzwerke von Krankenhäusern, Kliniken und Forschungsstätten zu gelangen. Ihr Ziel sind Patientendaten sowie Informationen über Industriepatente und Rezepte. Die Anzahl der Geräte, die Informationen über den Gesundheitszustand ihrer Nutzer speichern, steigt hierbei rapide an. Neue Akteure mischen den Gesundheitsmarkt auf. So speichern sogenannte Wearables wie Smart-Watches und Fitnessarmbänder neben den von uns zurückgelegten Schritten und verbrannten Kalorien auch Daten über den Herzrhythmus und die Insulinwerte ihrer Nutzer. Die Produzenten solcher Wearables unterliegen meist keinen anerkannten Datenschutz- und Sicherheitsstandards. Damit bieten sie Hackern ideale Einfallstore zu hochsensiblen und wertvollen Daten.

Im Darknet, einer von den gängigen Suchmaschinen und Internetanbietern abgekapselten Form des Internets, kann eine elektronische Patientenakte - vornehmlich von US-Amerikanern - für ca. 50 US $ erworben werden. Damit kostet sie zehn Mal so viel wie eine Kreditkartennummer.[1] Hacker können die Daten weiterverkaufen, aber auch zu Erpressungszwecken nutzen. In den letzten Jahren haben die Cyberangriffe im Gesundheitssektor in ungeahntem Ausmaß zugenommen. Sie verursachen einen jährlichen Schaden von ca. 6 Milliarden US $. Dabei wurden selbst angeblich gut gesicherte Netze immer wieder desavouiert. Allein im ersten Quartal dieses Jahres wurden mehr als 90 Millionen Patientenakten in den USA gehackt.[2]

Die Angreifer nutzen hierbei oft die Sicherheitslücken der mit dem Internet verbundenen Maschinen in Kliniken und Praxen aus, um an die Daten der Patienten zu gelangen. Im Juli 2014 verübten Hacker einen Angriff auf den US-amerikanischen Krankenhausverwalter Community Health Systems (CHS) und erbeuteten 4,5 Millionen Patientenakten.[3] Im April 2015 manipulierte der Sicherheitsforscher Billy Rios eine Infusionspumpe eines österreichischen Unternehmens über das Internet. Dabei konnte er die Arzneibibliotheken austauschen und damit gezielt Über- und Unterdosierungen von Antibiotika oder Betäubungsmitteln an Patienten verabreichen. Mehr als 400.000 solcher Pumpen wurden weltweit installiert.[4] Ähnliche Sicherheitslücken wurden bereits 2008 bei Herzschrittmachern und 2012 bei Insulinpumpen für Diabetiker aufgedeckt.[5] Diese und weitere Fälle brachten die U.S. Regierung dazu, das Department of Homeland Security (DHS) mit einer Untersuchung von 24 Gesundheitsgeräten zu beauftragen.[6]

Im Vergleich zu anderen Wirtschaftssektoren wie die Finanz- und Energiebranche hat sich die Gesundheitsindustrie erst spät auf die neue Bedrohungslage eingestellt. Unternehmen, Kliniken und Praxen implementieren deshalb Mindeststandards für die Sicherheit ihrer IT-Systeme und schulen dementspre-

1 *http://www.reuters.com/article/2015/06/05/cybersecurity-usa-targets-idUSL3N0YR30R20150605*
2 *http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually*
3 *http://www.technologyreview.com/news/530411/hackers-are-homing-in-on-hospitals/*
4 *http://www.wired.com/2014/04/hospital-equipment-vulnerable/*
5 *http://www.bloomberg.com/bw/articles/2012-02-23/the-trials-of-a-diabetic-hacker*
6 *http://www.computerworld.com/article/2837413/security0/dhs-investigates-24-potentially-deadly-cyber-flaws-in-medical-devices.html*

chend ihr Personal. Sie gehen zudem intrasektorielle Allianzen ein, wie beispielsweise den Cyberhub-Health, eine Gruppe von Mitgliedern des Cyber-Sicherheitsrat Deutschland e.V., die aus staatlichen und nichtstaatlichen Unternehmen besteht und gemeinsam Strategien und Lösungen im Kampf gegen Gefahren aus dem Netz ausarbeitet.

Trotz aller Gefahren für die Datensicherheit und den Patientenschutz stellen telemedizinische Anwendungen einen florierenden Zukunftsmarkt dar. Vor allem ein technikaffiner Wirtschaftsstandort wie die Bundesrepublik Deutschland kann und sollte davon profitieren. Laut einer Studie der Techniker Krankenkasse soll der Umsatz für Telemedizin in Europa bis 2020 jedes Jahr um durchschnittlich 10% steigen. In Folge der älter werdenden Bevölkerung wird die Zahl der chronisch kranken und unter permanenter Beobachtung stehenden Patienten ebenfalls wachsen. Diesen Patienten kann mit telemedizinischen Angeboten wirkungsvoll geholfen und Kosten können gespart werden. Eine Wirtschaftslichkeitsanalyse des Telemedizin-Projektes Zertiva hat in diesem Zusammenhang gezeigt, dass durch den Einsatz von Telemedizin die Erfolgsrate bei der Behandlung von Patienten mit Herzinsuffizienz von 59% auf 75% erhöht werden konnte. Gleichzeitig konnten die Kosten um mehr als 50% verringert werden.[7]

Die Politik reagiert auf diese Herausforderungen mit dem E-Health-Gesetz. Es stellt einen ersten überfälligen Schritt zur Einführung einer anwendungsorientierten Telematikinfrastruktur im deutschen Gesundheitswesen dar. Das Gesetz soll telemedizinische Leistungen fördern und die Einführung von Anwendungen der elektronischen Gesundheitskarte (eGK) wie Notfalldatensatz, Medikationsplan, elektronische Arzt- und Entlassbriefe unterstützen. Die Telematikinfrastruktur soll dabei als zentrale Infrastruktur für eine sichere Kommunikation im Gesundheitswesen dienen. Ihr Aufbau wird von der Gesellschaft für Telematik (gematik) koordiniert.

Die Konsequenzen des Gesetzes sind für die Zukunft des E-Health-Sektors in Deutschland beachtlich. In ihm ist beispielsweise die Öffnung der Telematikinfrastruktur für zusätzliche Anwendungen, sogenannte Mehrwertdienste, vorgesehen. Die Rahmenbedingungen für die Interoperabiltät mit diesen Anwendungen müssen vom Gesetzgeber geregelt werden. Dies würde zusätzliche Anreize für langfristige technische Innovationen und moderne Versorgungsstrukturen in der Telemedizin gewährleisten. Gleichzeitig würde es zu effizienteren, schnelleren und weniger bürokratischen Verfahren im Gesundheitssektor führen.

Im E-Health-Gesetz ist die Öffnung der Telematikinfrastruktur für zusätzliche Anwendungen, sogenannte Mehrwertdienste, vorgesehen. Die Rahmenbedingungen für die Interoperabiltät mit diesen Anwendungen müssen vom Gesetzgeber geregelt werden. Dies würde zusätzliche Anreize für langfristige technische Innovationen und moderne Versorgungsstrukturen in der Telemedizin gewährleisten.

Zudem ist die sichere Handhabung mit den hochsensiblen Daten der Versicherten, die auf der elektronischen Gesundheitskarte gespeichert sind, von zentraler Bedeutung. Die Sicherheitsvorkehrungen müssen den höchsten Sicherheitsstandards entsprechen. Dies gilt nicht nur für die gematik, bei der die Daten zentral gespeichert sind, sondern auch bei allen an der Telematikinfrastruktur beteiligten Anwendern. Aus Sicht der Versicherten soll zudem der sichere Zugang zu ihren gespeicherten Daten ermöglicht werden.

Mit dem E-Health-Gesetz versucht die Politik, den Abstand Deutschlands zu den skandinavischen und baltischen Ländern, die in diesem Bereich weltweit führend sind, zu reduzieren. Dazu müssen Digitalisierung, Sicherheitsvorkehrungen und Datenschutz Hand in Hand gehen. Wenn dies konsequent umgesetzt wird, dann ist der Erfolg der Telemedizin auch in Deutschland nicht mehr aufzuhalten. Davon profieren einerseits die Wirtschaft und der Staat, vor allem aber die Patienten.

7 *Heinen-Kammerer, Tatjana; Kiencke, Peter; Motzkat, Kerstin; Liecker, Bodo; Petereit, Frank; Hecke, Torsten; Müller, Hardy; Rychlik, Reinhard: Telemedizin in der Tertiärprävention: Wirtschaftlichkeitsanalyse des Telemedizin-Projektes Zertiva bei Herzinsuffizienz-Patienten der Techniker Krankenkasse, (erhältlich unter: http://www.dsck.de/fileadmin/downloads/p002_Buchbeitrag_Telemedizin_in_der_Tertiaerpraevention_verbesserte_Abb1.pdf, letzter Aufruf am 1.10.2015)*

Impressum

Herausgeber:
Interessengemeinschaft Zahnärztlicher Verbände in Deutschland IGZ e.V.
Dr./RO Eric Banthien
Papyrusweg 8, 22117 Hamburg
Telefon: (040) 712 73 11
Telefax: (040) 712 96 24

Redaktion:
Benn Roolf
Radenzer Str. 21, 12437 Berlin
Telefon: (030) 536 99 894
Telefax: (030) 536 99 895

Verlag und Anzeigenverkauf:
DentalisVerlag Benn Roolf
Radenzer Str. 21, 12437 Berlin
Telefon: (030) 536 99 894
Telefax: (030) 536 99 895

Titelfoto:
maxsim/fotolia.com

Auflage:
2 500 Exemplare

Erscheinungsweise:
4mal im Jahr

Die Verbände der IGZ

Brandenburg:
Verband Niedergelassener Zahnärzte
Land Brandenburg e.V.
Helene-Lange-Str. 4-5, 14469 Potsdam
Tel. (0331) 297 71 04
Fax (0331) 297 71 65
www.vnzlb.de

Hamburg:
Zahnärzteverband Z-2000
Mühlendamm 92, 22087 Hamburg
Tel. (040) 22 76 180
Fax (040) 22 76 120
www.z-2000.de

Saarland:
Verband der Zahnärzte im Saarland e.V.
Puccinistr. 2, 66119 Saarbrücken
Tel. (0681) 58 49 359
Fax (0681) 58 49 363
www.vdzis.de

Westfalen-Lippe:
Wählerverband Zahnärzte Westfalen
Reichshofstr. 77, 58239 Schwerte
Tel. (02304) 671 37
Fax (02304) 632 54
www.w-z-w.de