IT-Sicherheit in der Telemedizin

Effektiv, bezahlbar, rechtssicher. Eine Illusion?

Mit dem Einzug von telemedizinischen Lösungen in den Gesundheitsmarkt verschwimmen die Grenzen zwischen den klassischen, der ärztlichen Schweigepflicht unterliegenden Akteuren und fachfremden Dienstleistern aus dem IT Sektor. Daher stellt sich die Frage, wie der Zugriff auf vertrauliche Patientendaten konkret zu sichern ist und welche Lösungen als hinreichend angesehen werden können. Da insbesondere die Schweigepflicht im Strafgesetzbuch verankert ist, erhält die Thematik eine wachsende Brisanz. Ein Überblick.

1 Die wichtigsten Grundlagen

Für jedes Bundesland gibt es unterschiedliche Regelungen, die bei der Gestaltung von Sicherheitsmaßnahmen zu beachten sind. Neben den Landesdatenschutzgesetzen können diese Vorschriften auch Krankenhausgesetze oder ähnliches umfassen. Hinzu kommen Bundesgesetze, wie das Bundesdatenschutzgesetz (BDSG), welches Gesundheitsdaten als besonders schützenswert einordnet, sowie die Artikel 203 StGB und Paragraph 35 Sozialgesetzbuch.

Auf Grund der Vielfalt dieser Regelungen ist es wenig überraschend, dass es konsistente, hinreichend konkrete und bundesweit einheitliche Vorgaben zur Zeit nicht gibt, zumal in juristischen Kreisen die Anwendbarkeit des BDSG in Frage gestellt wird. [1]

Um bei der praktischen Gestaltung von Sicherheitslösungen für telemedizinische Anwendungen dennoch voranzukommen, lohnt sich der Blick in die USA, zumal mit einer Datenschutzregulierung auf EU-Ebene wegen der gegenwärtigen Kontroversen aus unserer Sicht nicht vor 2015 zu rechnen ist.

In den USA wurde bereits 1996 - nicht zuletzt wegen des ansonsten eher schwachen Datenschutzes - der Health Insurance Portability and Accountability Act (HIPAA) für den Umgang mit Patientendaten erlassen und erhielt dann mit der Privacy und der Security Rule speziell zum Schutz von Patientendaten in den folgenden Jahren immer wieder Verschärfungen und Konkretisierungen.

Bei Verstößen gegen die Regelungen können Geld- und Haftstrafen von bis zu 10 Jahren Haft fällig werden.[2] In einem aktuellen Fall musste das Alaska Department of Health and Social Services (DHSS) dem U.S. Department of Health and Human Services (HHS) $1,7 Millionen zahlen, nachdem deutliche Schwächen in der Ausübung der HIPAA Security Rule festgestellt wurden.[3]

Die Security Rule umfasst administrative, physische und technische Maß-

[1] Vgl. Maisch, Seidl: „Cloud-Nutzung für Berufsgeheimsnisträger“, Datenschutz Berater Nr. 6/2012, S. 127ff.

[2] American Medical Association: http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page, Abgerufen am: 5.12.2012.

[3] U.S. Department of Health and Human Services: http://www.hhs.gov/news/press/2012pres/06/20120626a.html, Abgerufen am: 6.12.2012.

nahmen. Die meisten Maßnahmen werden als „required“ eingestuft, müssen also erfüllt sein. Ebenso gibt es Vorgaben, die nur „adressable“ sind, bei denen die Einhaltung flexibler gestaltet ist. Eine große Rolle spielt dabei die Verschlüsselung und die sichere Vernichtung von Patientendaten (Protected Health Information – PHI), die für einen hinreichenden Schutz als unabdingbar angesehen werden. Weitere Maßnahmen drehen sich um Zutrittsschutz, sowie Zugangs- und Zugriffskontrolle. Dabei wird meist bis ins Detail gegangen, was eine konkrete Umsetzung erleichtert. So gibt es beispielsweise Vorgaben, dass ein Bildschirm an einem öffentlichen Arbeitsplatz so ausgerichtet sein muss, dass es für Dritte unmöglich ist, auf den Bildschirminhalt zu schauen.

Technische Details werden unter Verweisen auf Normen des National Institute of Standards and Technology (NIST) geklärt. So sind die Richtlinien für die laut HIPAA zentralen Punkte, die Verschlüsselung und Löschung von Daten, genauestens erklärt. Es wird allerdings neben den Verschlüsselungs- und Löschungsalgorithmen ebenso auf die Mitarbeit weiterer Spezialisten gesetzt. So können Vorschläge für weitere Soft- und Hardware zur Einhaltung der Maßnahmen eingereicht werden.[4]

2 Der Markt für Telemedizin

Der gesamte Gesundheitsmarkt in Deutschland hat eine Größe von etwa 287 Milliarden Euro, was 11,6 % des Bruttoinlandsprodukts entspricht (2010). Diese verteilen sich auf ambulante Einrichtungen wie Arztpraxen, Apotheken und ambulante Pflege, stationäre Stellen wie Kliniken (ca. 2000), Vorsorge- und Pflegeeinrichtungen (ca. 1250), sowie Rettungsdienste. Insgesamt arbeiten im Gesundheitswesen 4,8 Millionen Beschäftigte, davon 334000 Ärzte.[5]

Um auf der einen Seite die Kosten im Rahmen zu halten und auf der anderen Seite Patienten Zugang zu ärztlicher Versorgung überhaupt erst zu ermöglichen – insbesondere z.B. im ländlichen Raum – liegt es nahe, die technischen Möglichkeiten der Informations- und Kommunikationstechnik im Rahmen der Telemedizin einzusetzen. Allerdings ist trotz vorhandenen Möglichkeiten die Telemedizin in Deutschland kaum ausgebaut. So müssen sich beispielsweise Patienten mit chronischen Leiden, immerhin ca. 20 Millionen in Deutschland, noch weitestgehend für Kontrolltermine in die Arztpraxis bemühen. Dies liegt auch an rechtlichen Bedenken, die sich in dem Berufsrecht, Standesrecht und Datenschutzrecht befinden.[6]

Laut einer Studie des Fraunhofer ISI könnten durch Telemedizin nicht nur rund 9,6 Milliarden Euro jährlich eingespart werden, ein jährlicher Wachstumsimpuls von 2,6 Milliarden Euro wäre auch noch möglich. Allein durch einen effizienteren Einsatz der elektronischen Gesundheitskarte könnten schon gut 6 Milliarden gespart werden.[7] Erst im Oktober 2011 ist das bundesweit erste flächendeckende Telemedizin-Netz am Carl-Thiem-Klinikum in Cottbus und am Städtischen Klinikum in Brandenburg/Havel gestartet. Das

[4] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 35.

[5] Vgl. Statistisches Bundesamt: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Gesundheit/Gesundheit.html, Abgerufen am: 26.11.2012.

[6] Vgl. Voigt, P.-U.: „Rechtsgutachten Telemedizin – Rechtliche Problemfelder sowie Lösungsvorschläge“, http://www.initiative-gesundheitswirtschaft.org/fileadmin/initiative-gesundheitswirtschaft.org/media/downloads/gutachten/Gutachten-Telemedizin.pdf, Initiative Gesundheitswirtschaft e.V., Stand: 15.10.2008.

[7] Vgl. Bitkom: „Intelligentes Gesundheitsnetz spart 10 Milliarden Euro jährlich“, http://www.bitkom.org/de/presse/8477_74090.aspx, Stand: 14.11.2012.

Netzwerk ist für Hoch-Risikopatienten mit chronischer Herzinsuffizienz ausgelegt, die nun auch von weitem aus medizinisch betreut werden können.[8]

Da aber gerade im medizinischen Bereich große Mengen sensibler Patientendaten erfasst, versendet und verarbeitet werden, muss sichergestellt werden, dass Missbrauch verhindert wird. Schon die Information, dass eine Person bei einem bestimmten Facharzt in Behandlung ist, wäre vertraulich zu behandeln. Im schlimmsten Fall könnten große Mengen an Patientendaten wie Befunde, Krankheitsgeschichte, Laborwerte etc. in die falschen Hände gelangen.

Es stellt sich folglich die Frage, wie Patientendaten rechtssicher, effektiv und bezahlbar geschützt werden können. Wie können die involvierten Stellen sicherstellen, dass sie ihrer gesetzlichen Schweigepflicht auch bei technischen Lösungen nachkommen, die sie vielleicht gar nicht im Detail verstehen? Wie muss ein Hersteller telemedizinscher IT-Lösungen sicherstellen, dass er bei Betrieb, Entstörung oder Wartungsarbeit erst gar nicht mit Patientendaten in Berührung kommen kann? Und nicht zuletzt: Wie können die im Datenschutz vorgesehenen Kontrollmöglichkeiten des Patienten überhaupt sichergestellt werden?

3 Relevante Akteure und Einrichtungen

In dem Bereich Telemedizin hat man es neben den „üblichen“ Akteuren, sprich Patienten, deren Angehörigen, Ärzten, Pflegern, Apothekern oder Krankenkassen, auch mit telemedizinischen Anbietern zu tun. Letztere kann man in

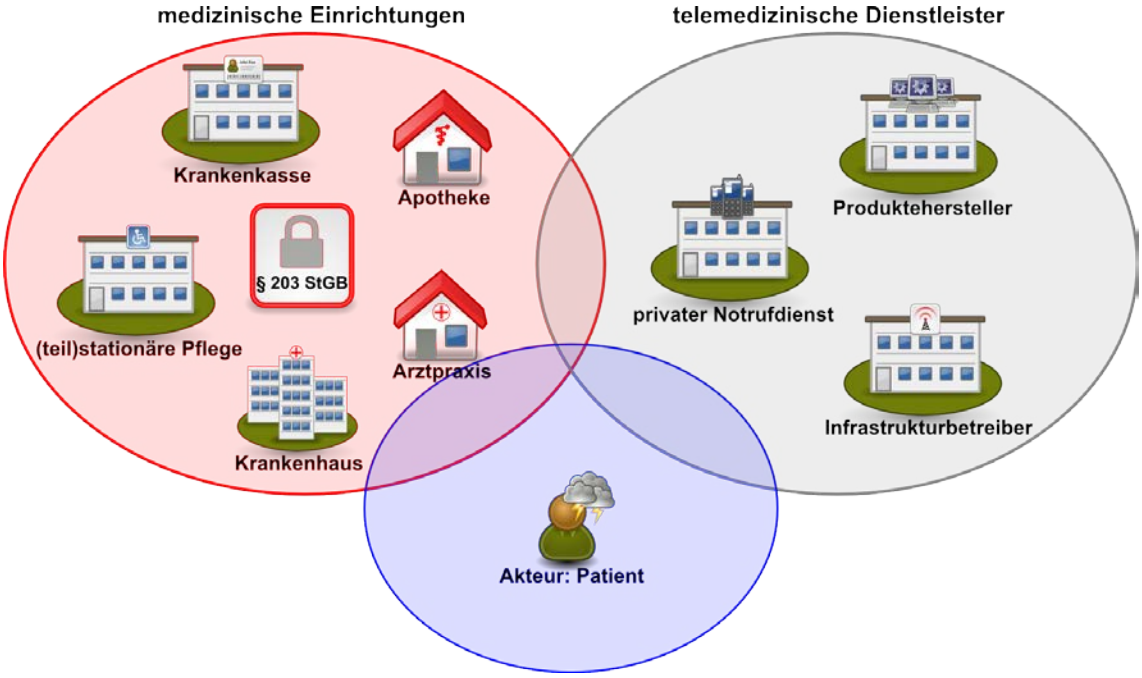

Abbildung 1: Medizinische Einrichtungen und telemedizinische Dienstleister

Dienstleister, z.B. private Notrufdienste, Produktehersteller (Hard- und Software), Infrastrukturbetreiber (Netze und System) und Integratoren aufteilen, welche schließlich alle Komponenten zusammenfügen.

Im Mittelpunkt steht aber immer der Patient, zu dem alle anderen mittelbar oder unmittelbar eine Verbindung haben. Des Weiteren sind die übrigen Akteure ebenfalls untereinander verbunden. So steht beispielsweise ein Arzt mit dem Pflegepersonal in Verbin-

[8] Vgl. Carl-Thiem-Klinikum Cottbus: „Offizieller Startschuss für brandenburgisches Telemedizin-Netz“, http://www.ctk.de/Offizieller-Startschuss-f-r-brandenburgisches.2005.0.2.html, Stand: 12.10.2011.

dung, oder Ärzte tauschen sich aus, um eine zweite Meinung zu Rate zu ziehen.

Wichtig ist bei der Einteilung der Akteure zudem, ob sie der ärztlichen Schweigepflicht (§ 203 StGB, § 9 MBO) unterliegen, da sich daraus die Pflicht der Geheimhaltung ergibt. Das heißt, auch bei den telemedizinischen Lösungen sind der Arzt, seine Helfer und alle anderen betroffenen Stellen nach wie vor in der Pflicht, Patientendaten sicher zu verwalten.

4 Anwendungsbeispiele

Im Folgenden werden einige typische Anwendungsbeispiele, sogenannte „Use Cases", der Telemedizin erläutert, um die jeweiligen Szenarien zu veranschaulichen.

Betreuung chronisch Kranker

In Deutschland gibt es ca. 20 Millionen chronisch Kranke, die regelmäßig von einem Arzt untersucht werden müssen. Um die vielen Wege zwischen Arzt und Patient zu minimieren und gleichzeitig die Qualität der Messungen zu steigern, wird der Patient beispielsweise mit einem Messgerät und einem Computer mit Webcam ausgestattet. Das Gerät erfasst die relevanten Vitaldaten und übermittelt sie automatisch an den Arzt. Der Arzt nimmt in regelmäßigen Abständen per Video Kontakt zum Patienten auf. Da ihm alle Daten bereits elektronisch vorliegen, kann die Diagnose effektiv erfolgen. Dabei unterscheiden sich die telemedizinischen Lösungen natürlich je nach Krankheitsbild.

Pflege in eigenen Räumen

Schon jetzt leben in Deutschland 1,1 Millionen Demenzkranke, deren Zahl sich bis 2050 sogar noch verdoppeln soll.[9] Dabei versucht man zu erreichen, dass ein Patient nicht zeitintensiv und teuer in einem Alters- oder Pflegeheim versorgt werden muss, sondern weiterhin zu Hause wohnen kann, was den meisten Menschen zudem auch angenehmer sein dürfte. Mit Hilfe von speziellen Sturzdetektoren können beispielsweise mögliche Unfälle erkannt und Alarme automatisch ausgelöst werden, so dass Pfleger oder Ärzte schnell zu Hilfe eilen können.

Hilfe unterwegs

Hierunter versteht man zum Beispiel den Fall, dass ein Patient unterwegs einen Unfall erleidet. Mit Hilfe einer Uhr mit eingebauter SIM-Karte schickt er, sofern er dazu noch in der Lage ist, über einen Knopfdruck einen Notruf los. Der Notruf erreicht die Notrufzentrale, die den Unfall an die entsprechenden Stellen weiterleitet. Da die Mobilnummer vorab bei der Notrufzentrale hinterlegt war, sind Identität und Krankengeschichte des Patienten bekannt, so dass vor Ort gezielter und schneller geholfen werden kann.

Themenspezifische Fachkonferenzen, Zweitmeinung

Ärzte und Fachspezialisten sind häufig räumlich getrennt und Befunde, Röntgenbilder etc. werden heute noch häufig per Post verschickt. Um Experten, die an unterschiedlichen Orten arbeiten, mit Hilfe telemedizinischer Kollaborationslösungen zusammenzubringen, bieten sich Videokonferenzen als Basis an. Neben dem Einsparen der Reisekosten, können diese auch dazu genutzt werden, die Konferenz zu dokumentieren und Patientenakten automatisch abzugleichen. Das heißt, neben Kostenvorteilen, erhöht sich auch die Qualität der Behandlung, beispielsweise durch zeitnahes Konsultieren weiterer Fachärzte.

5 Sicherheitsvorgaben für den Schutz von Patientendaten

Um die Vertraulichkeit medizinischer Daten sicherstellen und den Patienten vor Missbrauch zu schützen, sind entsprechende Sicherheitsmaßnahmen zu ergreifen. Diese leiten sich in der Regel

[9] Vgl. Briseño, C.: „Zahl der Demenzkranken wird sich bis 2050 verdoppeln", http://www.spiegel.de/wissenschaft/mensch/prognose-zahl-der-demenzkranken-wird-sich-bis-2050-verdoppeln-a-746878.html, Spiegel Online, Stand: 22.02.2011.

aus gesetzlichen Vorgaben ab, die wir hier grob skizzieren wollen.

Bundesdatenschutzgesetz, Landesdatenschutzgesetz und Krankenhausgesetze

Patientendaten sind laut Bundesdatenschutzgesetz (BDSG) „besondere Arten personenbezogener Daten" (§ 3 Abs. 1 BDSG) und werden speziell behandelt.

Laut § 9 BDSG müssen Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen, alle Maßnahmen, deren „Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht", zur Einhaltung des BDSG treffen. Bei Patientendaten liegt demnach grundsätzlich immer ein sehr hoher Schutzbedarf vor. Zu den technischen und organisatorischen Maßnahmen, die zu treffen sind, gehören nach § 9 BDSG Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Zweckbindung. Die ärztliche Schweigepflicht muss in jeder Form die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sicherstellen, da gemäß § 1 Abs. 3 S. 2 BDSG die beruflichen Regelungen unberührt bleiben.

Zwar muss nach § 4a Abs. 1 BDSG der Patient eine Einwilligungserklärung abgeben, das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten ist nach § 28 Abs. 6 BDSG allerdings auch ohne explizite Einwilligung möglich, wenn es zum Schutz lebenswichtiger Interessen des Betroffenen erforderlich ist.

Regelmäßig durchgeführte Wartungen eines verwendeten EDV-Systems müssen durch den Arzt autorisiert und überwacht werden. Im Falle der Wartung durch externe Personen ist der Arzt gemäß § 11 BDSG als Auftraggeber ebenso verantwortlich. Weiterhin sind täglich Sicherheitskopien nach § 10 MBO mit Hilfe geeigneter externer Medien zu erstellen, um die Datensicherung zu wahren.[10]

Darüber hinaus gibt es in den Ländern jeweils eigene Landesdatenschutzgesetze, sowie teilweise auch Krankenhausgesetze. Schlussendlich regelt die Sozialgesetzgebung den Austausch von Patientendaten in bestimmten Fällen.

Daher kann aus den bestehenden Vorschriften kein bundesweit gültiger, als hinreichend angesehener Schutzbedarf abgeleitet werden, der für die konkrete Umsetzung von Sicherheitsmaßnahmen geeignet wäre.

Strafgesetzbuch

Die ärztliche Schweigepflicht ist im Strafgesetzbuch verankert (§ 203 Abs. 1 StGB). Daraus leitet sich die Pflicht ab, sicherzustellen, dass Patientendaten keinem Dritten, z.B. einem technischem Telemedizindienstleister offenbart werden können, da nur der Geheimnisträger selbst für die Verschwiegenheit verantwortlich ist. So ist beispielsweise nur ein niedergelassener Arzt selbst der Geheimnisträger, nicht aber die gesamte Praxis. Für Kliniken stellt sich diese Problematik zum Beispiel im Falle des IT-Outsourcings.

Medizinproduktegesetz

In Deutschland fallen medizinische Geräte unter das Medizinproduktegesetz – was ist nun aber ein Medizinprodukt?

Ein Medizinprodukt ist gemäß einer EU-Richtlinie ein Gerät, das zur Diagnostik, Therapie und Überwachung eingesetzt werden kann.[11]

[10] Vgl. Kraska, S.: „Datenschutz in der Arztpraxis", http://www.perspektive-mittelstand.de/Bundesdatenschutzgesetz-Datenschutz-in-der-Arztpraxis-/management-wissen/3232.html, Perspektive Mittelstand, Stand: 23.02.2010.

[11] Vgl. DocCheck Flexikon: „Medizinprodukt", http://flexikon.doccheck.com/de/Medizinprodukt, Abgerufen am: 22.11.2012.

Die Inbetriebnahme von Medizinprodukten setzt die CE-Kennzeichnung durch den Hersteller oder ein zu konsultierendes unabhängiges Prüf- und Zertifizierungsinstitut voraus. Vor dem Inverkehrbringen eines Medizinproduktes muss das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) davon in Kenntnis gesetzt werden.

Falls das Gerät zur klinischen Therapie und Diagnostik verwendet wird, muss sowohl eine technische als auch eine klinische Prüfung mit Probanden durchlaufen werden.[12]

Allerdings kann auch Software unter das Medizinproduktegesetz fallen, so dass Telemedizinanbieter hier regulatorische Hindernisse erwarten könnten.

6 EU-Datenschutzgesetz

Während aktuell die Datenschutzgesetze in den 27 EU-Ländern sehr verschieden ausfallen, wurde nun eine EU-weite Regulierung vorgeschlagen, die allerdings frühestens 2014 in Kraft treten wird. Diese richtet sich sowohl an private als auch juristische Personen, wodurch es ebenso eine einheitliche Anlaufstelle für Datenschutzfragen geben soll.

Ebenso soll der Datenschutz für Gesundheitsdaten neu geregelt werden. Konkret ist eine Aufweichung des Datenschutzes für folgende Zwecke geplant:

- Krankheitsprävention, Arbeitsmedizin, Diagnosen, Krankenbetreuung, Management von Krankenversicherungen, Bekämpfung grenzübergreifender Krankheiten, Entwicklung neuer medizinischer Geräte und aus generellem öffentlichen Interesse, wie der Verbesserung der Servicequalität;
- Zu historischen, statistischen oder wissenschaftlichen Forschungszwecken, vorausgesetzt diese Zwecke können nicht ohne die Verwendung personenbezogener Daten erfüllt werden;
- Das Recht auf Löschung eigener Daten soll wegfallen, falls diese im Interesse der Öffentlichkeit stehen oder für historische, statistische oder wissenschaftliche Forschungszwecke relevant sind.[13]

Darüber hinaus sollen bestimmte Rollen, wie der „Data Controller“, „Data Processor“ und „Data Protection Officer“ in klar definierte Aufgabenbereiche unterteilt werden, um Zuständigkeiten und Verantwortlichkeiten darzustellen. So sind Data Controller beispielsweise dafür zuständig Data Protection Officers zu benennen, die wiederum in Behörden und Unternehmen ab 250 Mitarbeiten den Datenschutz regeln sollen.

Privatpersonen können gegenüber dem Data Controller der Verwendung eigener Daten zu bestimmten Zwecken zustimmen und zu einem späteren Zeitpunkt die Zustimmung wieder zurückziehen. Ebenso können Privatpersonen die Einsicht in die eigenen Daten verlangen und eine Kopie anfordern. Personenbezogene Daten werden gelöscht, sobald die Zustimmung widerlegt wird oder wenn Daten nicht weiter benötigt werden. Verstöße gegen das Datenschutzgesetz müssen innerhalb von 24 Stunden der Data Protection Authority gemeldet werden.[14]

[12] Vgl. DocCheck Flexikon: „Medizinproduktegesetz“, http://flexikon.doccheck.com/de/Medizinproduktegesetz, Abgerufen am: 22.11.2012.

[13] Vgl. Reding, V.: „Position paper on the Commission’s proposal for a General Data Protection Regulation“, http://www.encr.com.fr/DownloadFiles/Storm_ENCR2012-Cork.pdf, European Network of Cancer Registries, Abgerufen am: 23.11.2012.

[14] Vgl. Schmitt, Stahl: „How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide“, https://www.privacyassociation.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf, International Association Of Privacy Professionals, Stand: 11.10.2012.

Durch die Erneuerung und die EU-weite Regulierung des Datenschutzgesetzes wird es möglich sein, europaweite Telemedizin-Projekte aufzubauen. Eventuelle Unterschiede zwischen den Gesetzmäßigkeiten verschiedener Staaten sollte es dann nicht mehr geben.

7 USA – HIPAA

In den USA wurde der Health Insurance Portability and Accountability Act (HIPAA), der den Umgang mit Patientendaten vorschreibt, bereits 1996 erlassen. Im Jahr 2000 wurde die Privacy Rule, die eine Verschärfung des HIPAA bedeutete, veröffentlicht. 2003 wurde die Security Rule, die sich insbesondere mit digitalen Patientendaten (EPHI) befasst, veranlasst.[15]

Privacy Rule

Insbesondere nach späteren Modifikationen ist das Ziel der Privacy Rule die Sicherstellung des Datenschutzes von Patientendaten, wobei der Datenschutz die Kontrolle des Patienten über die eigenen Daten ermöglicht und dabei die Qualität der Krankenversicherung nicht beeinträchtigt werden soll. Hierbei werden Patientendaten sowohl in digitaler, als auch in Papierform betrachtet.

Die Privacy Rule limitiert den Einsatz von Patientendaten. Sie gibt den Patienten mehr Kontrolle über ihre Daten, so können sie einsehen, wie die Daten benutzt wurden und ob ihre Daten weitergeben wurden. Dies gewährleistet Transparenz und fördert das Vertrauen der Patienten.

An Krankenkassen werden bestimmte zu erfüllende Sicherheitsvorgaben gestellt, so dürfen Patientendaten ohne Erlaubnis für keinerlei Zwecke, bis auf Behandlungen, Zahlungen oder bei dem Einsatz für die Gesundheitspflege benutzt werden. Patientendaten müssen also so geschlossen wie möglich gehalten werden und dürfen nur so wenig wie nötig veröffentlich/verarbeitet werden.

Krankenkassen müssen laut der Privacy Rule ihre Patienten selbstständig über die Datenschutzrechte und die Verwendung dieser informieren. Maßnahmen zum Schutz des Datenschutzes müssen für Krankenhäuser, Behandlungen und ähnliche Situationen/Institutionen implementiert werden und Mitarbeiter müssen über diese belehrt werden. Um die Ausführung der Maßnahmen zu gewährleisten, müssen zusätzlich sogenannte Privacy Officers eingestellt werden.[16]

Security Rule

Die Security Rule beschreibt die Maßnahmen zum Schutz der elektronischen Patientendaten (EPHI). Diese können sich in den folgenden vier Zuständen befinden:

1. „Data in motion“ – die Daten werden über Netzwerke transportiert,
2. „Data at rest“ – die Daten sind auf einem Medium gespeichert,
3. „Data in use“ – die Daten werden erstellt, abgerufen, verarbeitet oder gelöscht,
4. „Data disposed“ – die Daten wurden in digitaler oder physischer Form vernichtet.[17]

Patientendaten, sogenannte Protected Health Information (PHI), beinhalten in der Regel Merkmale durch die ein direkter Personenbezug durchgeführt werden kann. Solche Merkmale sind unter anderem Namen, Anschriften, Telefon-/FAX-Nummern und so weiter. Insgesamt gibt es 18 solcher Merkmale. Patientendaten können als anonym (de-identified) klassifiziert werden, falls alle 18 Merkmale aus den Daten ent-

[15] Vgl. Wikipedia: „Health Insurance Portability and Accountability Act“, http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act, Stand: 20.11.2012.

[16] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 3ff.

[17] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 32.

fernt werden oder ein Personenbezug durch einen Experten verneint wird.[18]

Weiterhin können Daten unvollständige Datensätze, sogenannte Limited Data Sets (LDS), sein. LDS sind von den Regeln der Privacy Rule ausgenommen. Ein Limited Data Set darf 16 der 18 personenbezogener Merkmale nicht enthalten, kann aber Datumsangaben und grobe Ortsangaben (Stadt, Staat, PLZ) beinhalten.

Ein vollständige Liste der nicht erlaubten Daten kann hier gefunden werden: http://hipaa.wisc.edu/ResearchGuide/limiteddatasets.html.

LDS können beispielsweise für Forschungszwecke verwendet werden. Trotz Ausnahme von der Privacy Rule, muss vor der Benutzung eines LDS eine Nutzungsvereinbarung zwischen der medizinischen Einrichtungen und dem Empfänger der Daten unterzeichnet werden. Die Vereinbarung besagt, dass kein Personenbezug hergestellt wird und keine Kontaktaufnahme zu den Patienten erfolgt.[19]

Administrative, physische und technische Maßnahmen

Die Maßnahmen der Security Rule werden zwischen „required“ und „adressable“ unterschieden. Während Maßnahmen, die unter „required“ fallen definitiv umgesetzt werden müssen, bedeutet „adressable“, dass man einen größeren Spielraum bei der Erfüllung der Maßnahmen hat.

Maßnahmen werden außerdem weiter in drei Teile unterteilt:

„Administrative Safeguards“ sind Regeln für die Ausführung der gesetzlichen Vorgaben. So müssen zunächst generell Maßnahmen, um Sicherheitsverstöße zu verhindern, entdecken, kontrollieren und beheben implementiert werden. Weiterhin muss dafür gesorgt werden, dass Personen Ausbildungen und Belehrungen zum Thema Datenschutz durchlaufen und tatsächlich nur auf die Daten Zugriff haben, für die sie berechtigt sind. Auf Not- und andere Vorfälle im Zusammenhang mit den IT-Systemen, auf denen sich die Daten befinden, muss ebenso angemessen reagiert werden. Falls gewisse Aufgaben durch Outsourcing gelöst werden, müssen die externen Mitarbeiter vertraglich an alle Maßnahmen gebunden werden.[20] [21]

„Physical Safeguards“ regeln den physischen Zugang zu den Daten. Es muss dafür gesorgt sein, dass nur autorisierte Personen Zutritt und Zugang zu den Räumlichkeiten und IT-Systemen haben. Ebenso dürfen Arbeitsplätze nur von den vorgesehenen Mitarbeitern benutzt werden. Sich möglicherweise in der Nähe befindende Dritte oder unautorisierte Personen dürfen weder physischen noch logischen Kontakt zu dem Inhalt der Arbeitsplätze haben. Alte Hardware und Datenträger, die mit Patientendaten in Berührung kamen, müssen vor der Entsorgung entsprechen gelöscht werden (siehe „Verschlüsselung und Vernichtung von Patientendaten“).

„Technical Safeguards“ beschreiben den logischen Zugriff auf die Daten. Ein zentraler Punkt ist die Access Control (in diesem Fall: Zugriffskontrolle). Um den Zugriff auf die Daten zu schützen, muss zunächst die Ausgangslage analysiert werden. Welche Daten und Benutzer(rollen) gibt es? Wie wird auf die IT-Systeme zugegriffen? Werden die Daten gelesen, geändert oder erstellt? Es müssen Richtlinien für die Zugriffskontrolle und eindeutige Kennungen für alle Benutzer erstellt werden. Ebenso müssen die Benutzer verwaltet werden.

[18] Vgl. University of Wisconsin-Madison: „De-identification of Protected Health Information (PHI)”, Stand: 26.08.2003.

[19] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 33.

[20] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 115ff.

[21] Vgl. Wikipedia: „Health Insurance Portability and Accountability Act“, Stand: 20.11.2012.

Falls eine Person keinen Zugriff zu den Patientendaten mehr benötigt, muss dieser entsprechend beendet werden. Außerdem muss eine Ver- und Entschlüsselung der Daten stattfinden, um unberechtigten Zugriff weiter zu verhindern. Neben der Zugriffskontrolle muss zusätzlich noch die Integrität der Daten gewährleistet sein. Jegliche Aktivitäten an den IT-Systemen müssen registriert und dokumentiert werden.[22]

Verschlüsselung und Vernichtung von Patientendaten

Zusammen mit dem National Institute of Standards and Technology (NIST) hat das Department of Health and Human Services (HHS) zwei Kernmaßnahmen festgelegt, um die Daten vor unbefugtem Zugang zu schützen: Verschlüsselung und Vernichtung.

Der Erfolg der Verschlüsselung hängt dabei sowohl von der Stärke des Verschlüsselungsalgorithmus und der Sicherheit des Entschlüsselungsprozess ab, als auch von der Wahrscheinlichkeit, dass die Verschlüsselung selbst kompromittiert wird. Erlaubt sind Verschlüsselungsprozesse, die die Voraussetzungen des Federal Information Processing Standarts (FIPS) 140-2 erfüllen. Unter anderem müssen die Richtlinien zu Transport Layer Security (TLS) Implementierungen (NIST Special Publication 800-52), IPsec Virtual Private Networks (VPNs) (NIST Special Publication 800-77) und Secure Sockets Layer VPNs beachtet werden (NIST Special Publication 800-113).

Die Vernichtung von Patientendaten unterteilt sich in zwei Teile. Daten auf physischen Medien müssen so vernichtet werden, dass sie nicht mehr rekonstruierbar und lesbar sind. Elektronisch gespeicherte Daten müssen nach dem NIST Special Publication 800-88 Standard vernichtet werden. Dabei wird zwischen drei zulässigen Modi unterschieden[23]:

- „Clear“ – Überschreiben des zu löschenden Mediums mit nichtsensiblen Daten mittels Software- oder Hardware-Lösungen,
- „Purge“ – Entmagnetisieren des zu löschenden Mediums und Ausführen des Secure Erase Befehls,
- „Destroy“ – Physisches Zerstören des zu löschenden Mediums, beispielsweise durch Verbrennen.[24]

Dadurch erhalten die betroffenen Einrichtungen und Unternehmen auch hier konkrete Hinweise, wie eine Anforderung aus dem Datenschutz (hier die Löschung) hinreichend sicher durchzuführen ist.

6 Fazit

Zusammenfassend lässt sich sagen, dass wegen des Fehlens hinreichend konkreter Vorgaben in Deutschland und Europa, sich die US-amerikanischen Vorschriften als Anhaltspunkt für die Gestaltung der Sicherheitsmaßnahmen für telemedizinische Anwendungen eignen. Anders als in den Vereinigten Staaten üblich, dienen diese Maßnahmen vergleichbaren Zielen des Patientendatenschutzes und sind zudem hinreichend detailliert spezifiziert, um auch praktisch umsetzbar zu sein. Dennoch sollte zum jetzigen Zeitpunkt in jedem Fall ein komplettes Sicherheitskonzept erstellt werden, das auf die spezifischen Anforderungen zugeschnitten ist und sich auf die lokal geltenden Vorschriften bezieht.

[22] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 136ff.

[23] Vgl. Murphy, Waterfill: „The New HIPAA Guide for 2010“, Bloomington 2010, S. 32ff.

[24] Vgl. Kissel et al.: „Guidelines for Media Sanitization”, National Institute of Standarts and Technology, Special Publication 800-88, S. 7f.

7 Über Dahamoo

Die Dahamoo ist ein Team aus anerkannten Experten mit zusammen über 40 Jahren an internationaler Erfahrung.

Uns zeichnet die Leidenschaft aus, Datensicherheit als unverzichtbaren Teil des unternehmerischen Handels unserer Kunden zu begreifen. In diesem Zusammenhang gestalten und liefern wir Lösungen, die integraler Teil der Unternehmensabläufe werden.

Folglich ist unser Leitbild, Unternehmen zu helfen Ihre IT Risiken zu kontrollieren, um damit Geschäftserfolge zu sichern oder gar erst zu ermöglichen.

Mit anderen Worten: „Secure the present, enable the future!"

8 Die Autoren

Vor der Gründung der Dahamoo GmbH im Juni 2009, begleitete **Daniel Hallen** eine Reihe von Führungspositionen in der Informations- und Telekommunikationsbranche.

Er startet seine Laufbahn 1995 beim Mobilfunkbetreiber E-Plus als IT-Systemingenieur und wurde nach 3 Jahren Gruppenleiter IT Sicherheit. Im Jahre 1999 ging er ins Ausland und wurde Hauptabteilungsleiter für Sicherheit und Risikomanagement bei der Orange Schweiz.

Nach weiteren internationalen Erfahrungen bei Orange International/ France Telecom nahm er eine leitende Stelle beim US Hersteller für Sicherheitssoftware, McAfee an. Er war zuständig für die globale Produktentwicklung von Sicherheitslösungen auf mobilen Endgeräten.

Daniel Hallen spricht Deutsch, Englisch, Französisch und Italienisch und hat zwei Universitätsabschlüsse, einen in Mathematik von der Justus-Liebig Universität in Giessen und einen in Betriebswirtschaft vom International Institute of Management in Technology der Université Fribourg.

Seit 2009 studiert **Yaroslaw Medyany** an der Hochschule Bonn-Rhein-Sieg Informatik mit Schwerpunkt Informationssicherheit.

Im Rahmen des Studiums gewann er zahlreiches Wissen und viele Erfahrungen im Bereich der Informatik und Informationssicherheit und erwarb die CCNA-Zertifikate von Cisco und das Common Criteria-Zertifikat des BSI. Außerdem spricht Yaroslaw Medyany fließend Deutsch, Englisch und Russisch.

Aktuell wirkt er bei Dahamoo als freier wissenschaftlicher Mitarbeiter mit.

9 Kontakt

Bei Fragen und Anregungen stehen wir Ihnen gerne zur Verfügung:

Daniel Hallen
dhallen@dahamoo.com
www.dahamoo.com

Letzte Aktualisierung: 06.12.2012.