Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Datenschutz und Digitalisierung im Krankenhaus“

bei der Digitalen Veranstaltung

15. Berliner Tag

der Patientenfürsprecherinnen und – fürsprecher

der Bundesregierung

19. April 2021

Es gilt das gesprochene Wort

Sehr geehrte Frau Prof. Schmidtke,

sehr geehrte Damen und Herren,

I. Einleitung

Gerade im Bereich der Krankenhäuser sind die anzuwendenden Datenschutzregelungen unübersichtlich.

In allererster Linie ist natürlich die Datenschutz-Grundverordnung anzuwenden. Dort ist zunächst auf das ausdrückliche Verbot des Umgangs mit Gesundheitsdaten in Artikel 9 Absatz 1 Datenschutz-Grundverordnung hinzuweisen. Dass die Verarbeitung von Gesundheitsdaten im Krankenhaus durch Artikel 9 Absatz 2 Buchstabe h) Datenschutz-Grundverordnung in Verbindung insbesondere mit den Landeskrankenhausgesetzen erlaubt ist, bedarf an dieser Stelle keiner näheren Vertiefung. Denn schließlich ist es notwendig, in einem Krankenhaus personenbezogene Daten zu verarbeiten. Dies wird natürlich von der Datenschutz-Grundverordnung nicht verboten.

Damit ist bereits eine weitere Rechtsgrundlage genannt. Da die allermeisten Krankenhäuser in der Trägerschaft im Landesbereich liegen, dies gilt etwa für die Universitätskliniken, die Landes- und Kommunalkrankenhäuser, oder die privaten Krankenhausgesellschaften, gelten für diese die jeweiligen Landeskrankenhausgesetze, die teilweise eigene Datenschutzregelungen beinhalten, soweit sie nicht auf die Datenschutz-Grundverordnung verweisen.

Hinzu kommen noch die kirchlichen Krankenhäuser, für die das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland bzw. das Katholische Gesetz über den kirchlichen Datenschutz gilt.

Für die wenigen Krankenhäuser des Bundes, dies sind die fünf Bundeswehrkrankenhäuser sowie die Kliniken der DRV Bund, der DRV Knappschaft Bahn See und die Kliniken der Berufsgenossenschaften, gelten neben der Datenschutz-Grundverordnung noch § 22 Bundesdatenschutzgesetz und zum Teil die jeweiligen Sozialgesetzbücher.

II. Das Krankenhausinformationssystem und die weitere Digitalisierung im Krankenhausbereich

Demgegenüber sind die Herausforderungen der Digitalisierung für alle Krankenhäuser weitgehend gleich. Es wir kaum mehr ein Krankenhaus geben, dass nicht ein Krankenhausinformationssystem betreibt. Dabei verstehe ich unter einem Krankenhausinformationssystem nicht ein spezielles Software-Produkt, sondern die Gesamtheit aller in einem Krankenhaus eingesetzten IT-Systeme, die der Verwaltung und Dokumentation der Patientendaten dienen.

Neben den bisherigen Terminals, an denen die Patientendaten in das Krankenhausinformationssystem eingepflegt wurden, sind seit einigen Jahren bereits auch mobile Geräte wie Tablets getreten. Auch sind viele medizinische Geräte an das Krankenhausinformationssystem angeschlossen und die von ihnen erhobenen Messwerte werden

automatisiert in das Krankenhausinformationssystem eingepflegt und dort bereitgestellt, wo sie gebraucht werden.

Neu hinzukommen weitere digitale Anwendungen. So werden seit einigen Jahren bereits sogenannte Tumorboards nicht nur mit den Onkologen innerhalb des Krankenhauses, sondern auch via Videokonferenz mit Spezialisten im In- und Ausland geführt.

Mit dem Krankenhauszukunftsgesetz vom 23. Oktober 2020[1] stellt der Bund für die Digitalisierung von Krankenhäusern ab dem 1. Januar 2021 3 Milliarden Euro bereit, damit Krankenhäuser in moderne Notfallkapazitäten, in die Digitalisierung und in ihre IT-Sicherheit investieren können. Hinzu sollen noch ca. 1,3 Milliarden Euro von den Ländern kommen, die durch den beim Bundesamt für Soziale Sicherheit verwalteten Krankenhauszukunftsfond verwaltet werden. Gefördert werden sollen Investitionen in moderne Notfallkapazitäten und eine bessere digitale Infrastruktur, z.B. Patientenportale, elektronische Dokumentation von Pflege- und Behandlungsleistungen, digitales Medikationsmanagement, Maßnahmen zur IT-Sicherheit sowie sektorenübergreifende telemedizinische Netzwerkstrukturen. Auch erforderliche personelle Maßnahmen sollen durch den Krankenhaus-zukunftsfond finanziert werden.

Ich komme später noch darauf zurück, dass dies auch erforderlich ist.

[1] Gesetz für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz -KHZG) vom 23. Oktober 2020, BGBl. I S. 2208.

III. Die Orientierungshilfe Krankenhausinformationssysteme (OH KIS) der Datenschutzkonferenz

Zunächst einmal zurück zum Krankenhausinformationssystem, in dem sich die sensiblen Patientendaten befinden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[2], kurz Datenschutzkonferenz, war sich schon sehr früh der besonderen Bedeutung der Gesundheitsdaten und auch der Chancen und Risiken der Digitalisierung im Gesundheitswesen bewusst. So beauftragte sie bereits im Jahr 2008 ihren Arbeitskreis Gesundheit und Soziales sowie ihren Arbeitskreis Technik mit der Entwicklung einer „Orientierungshilfe Krankenhausinformationssysteme“ oder kurz: der OH KIS. Im Frühjahr 2011 wurde die OH KIS herausgegeben, die es Betreibern und Herstellern von Krankenhausinformationssystemen erleichtern sollte, den gesetzlichen Anforderungen und den gerechtfertigten Erwartungen der Patienten im komplexen System Krankenhaus gerecht zu werden, aufgrund einer entsprechenden Entschließung der Datenschutzbeauftragten des Bundes und der Länder sowie kirchliche Datenschutzbeauftragter. Die OH KIS stellt einen Leitfaden dar, der aus den gesetzlichen Vorgaben, Empfehlungen und Best-Practice-Ansätzen erarbeitet wurde.

[2] Die hieß damals noch so. Erst vor wenigen Jahren wurde sie nach stärker Berücksichtigung des privaten Sektors und der Beauftragung der Landesdatenschutzbeauftragten mit den bisher bei der Innenverwaltung der Länder liegenden Datenschutzaufsicht im nicht-öffentlichen Sektor aufgrund des EuGH-Urteils von 2010 wurde die DSK in „Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder“ umbenannt.

Die OH KIS traf bei den betroffenen Krankenhausverbänden zwar durchweg auf Interesse, aber bei einigen Krankenhausbetreibern und Herstellern von Krankenhausinformationssystemen auch auf deutliche Kritik. Hierauf hat die Datenschutzkonferenz reagiert. Die Kritik wurde von ihren Arbeitskreisen ausgewertet, Pilotprojekte zur Umsetzung der technischen Anforderungen aus der Orientierungshilfe wurden begleitet und in verschiedenen Foren ein reger Austausch mit Vertretern der Hersteller und Betreiber geführt.

In der Folgezeit wurde auch nach Auswertung der Erfahrungen aus der Kontroll- und Beratungstätigkeit der Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe zur Klarstellung einiger der fixierten Anforderungen und im Sinne einer besseren Lesbarkeit und Übersichtlichkeit überarbeitet. Die OH KIS liegt nunmehr auch schon seit einigen Jahren in einer Neufassung vor, deren Teil I (Rechtliche Rahmenbedingungen) präzisiert und in deren Teil II (Technische Anforderungen) der durchgehende Bezug zu den rechtlichen Rahmenbedingungen besser verdeutlicht wurde.

Durch das Inkrafttreten der Datenschutz-Grundverordnung wurde die OH KIS nicht obsolet. Im Gegenteil: durch das ausdrückliche Verbot des Umgangs mit Gesundheitsdaten in Artikel 9 Absatz 1 Datenschutz-Grundverordnung wurde die Bedeutung der besonderen Sensibilität der Gesundheitsdaten noch einmal deutlich unterstrichen.

Allerdings wird von den Datenschutzaufsichtsbehörden zu prüfen sein, ob die OH KIS nicht aufgrund der fortschreitenden technischen Entwicklung einer Revision bedarf.

IV. Cyberangriffe auf Krankenhäuser

Ich komme nun auf den Krankenhauszukunftsfonds zurück, mit dem erklärtermaßen eine bessere digitale Infrastruktur, u.a. Maßnahmen zur IT-Sicherheit, gefördert werden sollen. Dies halte ich auch für dringend erforderlich.

So berichtete die Ärztezeitung und weitere regionale Zeitungen am 31. März diesen Jahres, vor noch nicht einmal drei Wochen, unter der Überschrift: „Hackerangriff auf Klinik in Lippstadt“, dass es in den meisten Bereichen dieses Krankenhauses nach einem Hackerangriff zu einem Aufnahmestopp gekommen war und nur noch Notfälle erstversorgt wurden. Erst sechs Wochen vorher, am 15. Februar 2021, wurde in süddeutschen Medien über einen Hackerangriff auf die Urologische Klinik München Planegg berichtet.

Ich könnte meinen ganzen Vortrag mit Beispielen füllen, in denen Krankenhäuser und Kliniken einem Cyberangriff zum Opfer gefallen sind. Bundesweit ins Rampenlicht gerückt sind diese Angriffe auf die IT von Krankenhäusern und Kliniken erstmals im Frühjahr 2016 mit dem Cyberangriff auf das Lukaskrankenhaus in Neuss, wo ebenfalls Operationen verschoben und bei lebensnotwendigen Operationen Patienten in andere Krankenhäuser gebracht werden mussten.

Damals gab das Lukaskrankenhaus Neuss den Gesamtschaden durch die Cyberattacke laut einer Pressemitteilung mit 900.000 Euro an. Immerhin kam damals und bei den meisten weiteren Cyberattacken kein Mensch zu Schaden.

Dass dies nicht so bleiben muss, zeigt der Fall der Cyberattacke auf das Uniklinikum Düsseldorf im September letzten Jahres, bei dem eine lebensbedrohlich erkrankte Patientin starb, nachdem der Rettungswagen, der sie in das Uniklinikum Düsseldorf bringen sollte, wegen des Cyberangriffs in ein Krankenhaus nach Wuppertal umgeleitet wurde. Die lebensrettende Behandlung konnte erst mit einstündiger Verspätung beginnen, so dass die Patientin kurze Zeit nach ihrer Ankunft in der Wuppertaler Klinik starb.

Auch außerhalb von Cyberangriffen, die in der Regel von außen die IT-Systeme von Krankenhäusern und Kliniken bedrohen, möchte ich an dieser Stelle auch Angriffe auf Patientenrechte von innerhalb des Systems – ich möchte dies hier bewusst offen formulieren – nicht vergessen. Ich erinnere hier beispielsweise an den Fall der damals 22-jährige Lehramtsstudentin Tugce, die im November 2014 nach einem Schlag gegen den Kopf auf dem Boden aufgeschlagen und mit schwersten Kopfverletzungen ins Offenbacher Klinikum gebracht worden, wo sie wenige Tage später starb.

Damals gab es ein reges Medieninteresse und Teile der Patientenakte fanden sich in der Presse wieder. Eine Untersuchung der Klinikleitung ergab, dass 94 Mitarbeiterinnen und Mitarbeiter der Klinik die

elektronische Patientenakte im Krankenhausinformationssystem aufgerufen haben, aber nur 31 von ihnen waren direkt in die Behandlung der jungen Frau involviert.

63 Klinikmitarbeiterinnen und –mitarbeiter hatten also die elektronische Patientenakte unter Verstoß gegen die Ärztliche Schweigepflicht, die auch für die Pflegerinnen und Pfleger gilt, illegal eingesehen. An die Fälle von aufgegebenen Kliniken, in denen man noch nach Jahren auf den Schreibtischen offen liegende Patientenakten gefunden hat, weise ich hin.

Skurril fand ich den Fall über den heise.de im Jahr 2016 berichtete und mit dem sich mein Kollege aus Thüringen befassen musste: Beim Straßenkarneval in einem Ort im Wartburgkreis wurden zerschredderte Patientenakten als Konfetti unters Volk gebracht, wobei auf den nicht fachgerecht zerkleinerten Papierschnipseln personenbezogene Daten wie Namen, Adressen und Telefonnummern der Patienten des Klinikums Bad Salzungen zu lesen waren.

V. Die IT-Sicherheitsgesetze und die Kritis-Verordnung

Während sich die OH KIS der Datenschutzaufsichtsbehörden mit der Frage befasst, wie man mit Patientendaten im Krankenhaus umgehen darf, insbesondere wenn diese sich in einem Krankenhausinformationssystem befinden, geben die Regelungen aufgrund der IT-Sicherheitsgesetze und der Kritis-Verordnung vor, was zu tun ist, wenn es zu einem Sicherheitsvorfall gekommen ist.

Bevor ich darauf zurückkomme, möchte ich kurz etwas zu einer entscheidenden Frage sagen, die ich auch für einen großen Schwachpunkt der IT-Sicherheitsgesetze und der Kritis-Verordnung halte. Die Frage ist hier nämlich zunächst: sind diese rechtlichen Vorgaben für das konkrete Krankenhaus oder die konkrete Klinik anwendbar?

Mit dem IT-Sicherheitsgesetz vom 17. Juli 2015[3] wurden für sogenannte Kritische Infrastrukturen durch Ergänzungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) insbesondere Meldepflichten bei Störungen in den IT-Systemen, aber auch eine Pflicht die Betreiber von IT-Systemen eingeführt, um ein Mindestniveau an Sicherheit für ihre IT Systeme zu schaffen. Was Kritische Infrastrukturen im Sinne des BSI-Gesetzes sind, sollte erst später in einer Rechtsverordnung geregelt werden.
So wurden durch Kritis-Verordnung vom 22. April 2016[4] zunächst bestimmt, was Kritische Infrastrukturen in den Bereichen, Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation sind. Ein weiteres Jahr später wurde mit der ersten Änderungsverordnung zur Kritis-Verordnung vom 21. Juni 2017[5] auch die Kritischen Infrastrukturen für die Bereiche Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr bestimmt.

[3] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 15. Juli 2015, BGBl. I S. 1324.

[4] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) vom 22. April 2016, BGBl. I S. 958.

[5] Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017, BGBl. I S. 1903.

Seit dieser Zeit bestimmt § 6 der Kritis-Verordnung, was im Bereich Gesundheit „Kritische Infrastruktur“ ist. Während es im ersten Absatz dieser Regelung noch heißt:

„Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Gesundheit kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. *die stationäre medizinische Versorgung;“*

wird dies in Absatz 6 deutlich eingeschränkt. Dort heißt es nämlich:

„Im Sektor Gesundheit sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. *den in Anhang 5 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für die stationäre medizinische Versorgung, … und*
2. *den Schwellenwert nach Anhang 5 Teil 3 Spalte D erreichen oder überschreiten.“*

Und hier liegt das Problem. Nach Anhang 5 Teil 3 Spalte D beträgt der Schwellenwert 30.000 vollstationäre Fallzahlen pro Jahr, damit ein Krankenhaus eine Kritische Infrastruktur mit den entsprechenden gesetzlichen Pflichten hinsichtlich der IT-Sicherheit ist. Das federführende Bundesinnenministerium wollte aus Akzeptanzgründen nur eine begrenzte Anzahl von Unternehmen und öffentlichen Stellen mit kostenauslösenden Verpflichtungen belasten. Aber ebenso wie es dem Corona-Virus völlig egal ist, ob es sich im Körper einer Frau oder eines Mannes oder eines Deutschen, Chinesen, Japaners, Neuseeländers, Amerikaners, Togolesen, Australiers oder Chilenen vermehrt, ist es einem Angreifer egal, ob er die Patientendaten aus einem Krankenhaus

abgreift, das mehr oder weniger als 30.000 vollstationäre Fallzahlen pro Jahr hat.

Von den Stand 2018 in Deutschland noch existierenden 1.914 Krankenhäusern unterlagen nach Angaben des BSI im Jahr 2019 ganze 96 Krankenhäuser als sogenannte Kritische Infrastruktur den Vorgaben des BSI-Gesetzes.

Die vollstationäre Fallzahl pro Jahr ist zwar grundsätzlich geeignet, die Anzahl der Krankenhäuser zu reduzieren, die gesetzlich nach dem BSI-Gesetz verpflichtet sind, ein Mindestniveau an IT-Sicherheit aufgrund Gesetzes zu garantieren und bei Angriffe auf die IT-Infrastruktur dem BSI zu melden. Sie ist aber gänzlich ungeeignet, die sensiblen Gesundheitsdaten von Patientinnen und Patienten auch in kleineren und mittleren Krankenhäusern zu schützen.

Ich unterstütze nachdrücklich die Forderung des Marburger Bundes, die dieser vor anderthalb Jahren nach den Hacker-Angriffen auf die DRK-Kliniken in Rheinland-Pfalz und dem Saarland formuliert hat[6]: ALLE Kliniken sind Kritische Infrastrukturen – Es darf hinsichtlich der Bereitstellung ausreichender Schutzvorkehrungen für die IT-Systeme keine Unterschiede zwischen Großkliniken und Kliniken der Regel- und Grundversorgung gemacht werden.

[6] Ärztezeitung vom 30.08.2019

Die Nennung eines solchen Schwellenwertes ist auch deshalb schädlich, weil sie die Verpflichtung auch der Krankenhäuser außer Acht lässt, die weniger als 30.000 vollstationäre Fallzahlen pro Jahr haben, für ein angemessenes Sicherheitsniveau zu sorgen. Diese Verpflichtung ergibt sich aus Artikel 32 Datenschutz-Grundverordnung.

Zudem ergibt sich aus Artikel 33 Datenschutz-Grundverordnung eine Pflicht gegenüber der für das Krankenhaus zuständigen Datenschutzaufsichtsbehörde zu melden, wenn sich im Krankenhaus eine Datenschutzverletzung ereignet hat. Dies kann beispielsweise auch ein Cyberangriff sein. Auch Krankenhäuser, die über diesem Schwellenwert liegen, müssen Störungen ihrer IT-Systeme nicht nur nach § 8b Absatz 4 BSI-Gesetz dem BSI melden, sondern – soweit personenbezogene Daten gefährdet sind – auch zusätzlich nach Artikel 33 Datenschutz-Grundverordnung ihrer zuständigen Datenschutzaufsichtsbehörde.

VI. Neue Regelungen durch das 2. IT-Sicherheitsgesetz ?

Zurzeit befindet sich das 2. IT-Sicherheitsgesetz in den Beratungen des Deutschen Bundestages. Im Zusammenhang mit der Sicherheit in den Krankenhäusern muss allerdings gesagt werden, dass der Entwurf eines 2. IT-Sicherheitsgesetzes keine Regelung enthält. Für den Gesundheits-bereich sind lediglich für das Bundesgesundheitsministerium einschließlich seines Geschäftsbereichs für Zwecke des Gesetzes fünf Planstellen vorgesehen.

Dies ist erstaunlich, da das BSI anlässlich eines Runden Tisches, zudem im August 2019 die rheinland-pfälzische Gesundheitsministerin Sabine Bätzing-Lichtenthäler aufgrund der erwähnten Cyberangriffen auf Krankenhäuser und andere Einrichtungen des Deutschen Roten Kreuzes (DRK) in Rheinland-Pfalz und im Saarland eingeladen hatte, erklärte, nach seinen Vorstellungen solle bei einer Novelle des 1. IT-Sicherheitsgesetzes von 2015 auch Klinikverbünde zu verschärften IT-Sicherheitsmaßnahmen verpflichtet werden. Damit hätten nicht nur die bundesweit 96 Kliniken, die mehr als 30.000 vollstationäre Fälle pro Jahr versorgen, den erhöhten Sicherheitsanforderungen nach dem BSI-Gesetz und der BSI-KRITIS-Verordnung genügen müssen.

In der Folge des Cyberangriffs auf die DRK-Kliniken forderte die rheinland-pfälzische Landesregierung ein Sofortprogramm Bund zur IT-Sicherheit in Krankenhäusern, das besonders kleinere Kliniken dabei unterstützen soll, verstärkt in die Sicherheit der Krankenhaus-IT zu investieren. Mit diesem Sofortprogramm Bund zur IT-Sicherheit in Krankenhäusern sollten die Mittel des Krankenhausstrukturfonds für Investitionen in die IT-Sicherheit auf alle Krankenhäuser ausgeweitet werden. Bislang ist Voraussetzung für eine Förderung entsprechender Investitionen für die IT-Sicherheit in Krankenhäusern allerdings, dass die Krankenhäuser als „Kritische Infrastruktur“ (KRITIS) jährlich mehr als 30.000 Behandlungsfälle – entsprechend der „BSI-Kritisverordnung“ – aufweisen.

Nicht nur die letzten Fälle von Cyberangriffen auf Krankenhäuser aus diesem Jahr zeugen davon, wie berechtigt diese Forderung ist.

Immerhin haben im Fall einer Cyberattacke **alle** Krankenhäuser und Kliniken Anspruch auf Hilfe der Mobile Incident Response Teams (MIRT) des BSI, da alle Krankenhäuser per se zum Gesundheitssektor und damit zu einem der sieben definierten kritischen Infrastruktur-Bereiche gehören. Die Leistungen eines MIRT des BSI sind für Kliniken kostenlos.[7]

Gleichwohl bedauere ich es sehr, dass der Gesundheitsbereich bei der Novellierung des IT-Sicherheitsgesetzes zumindest zunächst ausgespart bleibt. Ich hoffe, dass der Gesetzgeber diesem wichtigen Bereich in der kommenden Legislaturperiode nach den Wahlen im September mehr Aufmerksamkeit zukommen lässt. Auch wenn mehr IT-Sicherheit ein nicht zu vernachlässigender Kostenfaktor ist, sind die Schäden, die eintreten können, ein noch weitaus größerer Kostenfaktor.

VII. Nutzung von Patientendaten für Forschungszwecke

Am Ende meines Vortrages möchte ich nur kurz das Thema Nutzung von Patientendaten für Forschungszwecke ansprechen. Vorausschicken möchte ich, dass die Datenschutz-Grundverordnung grundsätzlich forschungsfreundlich ausgestaltet wurde. Insbesondere wird durch Artikel 5 Absatz 1 Buchstabe b) Datenschutz-Grundverordnung klargestellt, dass die Weiterverwendung von personenbezogenen Daten für Forschungszwecke keine unzulässige Zweckänderung darstellt.

[7] Siehe ÄrzteZeitung vom 16.08.2019 - https://www.aerztezeitung.de/Wirtschaft/Mainz-versus-Cybercrime-314410.html.

Allerdings stellt Artikel 89 Absatz 1 Datenschutz-Grundverordnung auch klar, dass die Nutzung personenbezogener Daten für Forschungszwecke der Datenschutz-Grundverordnung unterliegen und es Maßnahmen – die Datenschutz-Grundverordnung spricht von Garantien – bedarf, um die Rechte der Personen zu schützen, mit deren Daten Forschung betrieben werden soll. Hinzu kommt, dass mit besonderen Kategorien von personenbezogenen Daten, zu denen Gesundheitsdaten gehören, nur dann geforscht werden darf, wenn entweder eine Einwilligung nach Artikel 9 Absatz 2 Buchstabe a) Datenschutz-Grundverordnung der betroffenen Person – im Krankenhaus also des Patienten – oder aber eine gesetzliche Grundlage entweder aus dem europäischen Recht oder aus dem nationalen Recht vorliegt.

Dabei gilt allerdings auch der Grundsatz, dass, soweit eine gesetzliche Regelung vorliegt, diese einer Einwilligung vorgeht. Es ist also nicht möglich, gesetzlich vorgegebene Einschränkungen durch die Einholung einer Einwilligung auszuhebeln.

Für die Krankenhäuser sind in aller Regel die Vorgaben der Landeskrankenhausgesetze maßgeblich, die Möglichkeiten der Forschung mit Patientendaten ganz unterschiedlich regeln. Es reicht von der Möglichkeit nach Artikel 27 Bayerisches Krankenhausgesetz auch außerhalb des Krankenhauses Forschenden die Möglichkeit zu eröffnen, mit Patientendaten ohne deren Einwilligung zu forschen, wenn die Patientendaten im Gewahrsam des Krankenhauses bleiben.[8] § 12 Hamburgisches Krankenhausgesetzes erlaubt auch die Forschung mit

[8] Artikel 27 Absatz 4 Satz 2 BayKrG

den Patientendaten außerhalb des Krankenhauses. In anderen Bundesländern ist Forschung nur mit anonymisierten oder pseudonymisierten Daten erlaubt.[9]

In einigen Landeskrankenhausgesetzen fehlt überhaupt eine Forschungsregelung.[10] § 43 Absatz 3 Baden-Württemberg erklärt die im Gesetz vorhandenen Regelungen zum Datenschutz für Zwecke wissenschaftlicher Lehre und Forschung gar für nicht anwendbar und das Gesetz erlaubt gleichzeitig nach § 46 Absatz 1 Nr. 2a die Übermittlung zur Durchführung medizinischer Forschungsvorhaben des Krankenhauses auch an Stellen und Personen außerhalb des Krankenhauses.

Die gesetzlichen Regelung sind – wie in einem föderalen Staatverbund wie Deutschland nicht unüblich – außerordentlich unterschiedlich. Hieran – und nicht am Datenschutz – scheitern häufig Forschungsvorhaben mit Patientendaten aus Krankenhäusern. Mir ist ein Fall bekannt, wo ein Forscher in einem Länderdreieck in drei Kliniken, die demselben privaten Krankenhausträger gehören, das Forschungsvorhaben schließlich aufgab, weil es nicht möglich war, es aufgrund der unterschiedlichen Landeskrankenhausgesetze durchzuführen. Bekanntgeworden ist das Forschungsvorhaben meiner Dienststelle allerdings wegen der zunächst erhobenen Behauptung, das Forschungsprojekt sei am Datenschutz gescheitert.

[9] Z.B. § 12 Abs. 2 Nr. 9 Hessisches Krankenhausgesetz

[10] Z.B. in Nordrhein-Westfalen

Beschrieben habe ich hier zunächst die Möglichkeit der Bereitstellung von Patientendaten aus dem Krankenhausbereich für die wissenschaftliche Forschung, wie sie bisher die Regel war. Künftig werden weitere Möglichkeiten hinzukommen. § 363 Fünftes Buch Sozialgesetzbuch sieht beispielsweise vor, dass Versicherte es erlauben können, dass aus ihrer von ihre Krankenkasse angebotenen elektronischen Patientenakte Daten für Forschungszwecke zur Verfügung gestellt werden.

Sie werden fragen, was hat dies mit den Krankenhäusern zu tun. Nun, es gibt Überlegungen, künftig die Patienten bei der Aufnahme ins Krankenhaus zu fragen, ob sie bereit sind, zusätzlich zu den Daten, die im Krankenhaus über sie erhoben werden, auch die Daten, die sie in ihrer elektronischen Patientenakte speichern, für wissenschaftliche Forschungsvorhaben zur Verfügung zu stellen. Die Daten aus der elektronischen Patientenakte würden dann über den Zugang des Krankenhauses zur Telematikinfrastruktur einem oder einer Forschenden zur Verfügung gestellt werden. Es gibt allerdings hier noch eine Reihe von schwierigen Fragen zu klären.

Am Ende meines Vortrages möchte ich in diesem Zusammenhang noch ansprechen, dass auf Initiative Deutschlands im letzten Herbst die Europäische Kommission beschlossen hat, einen Europäischen Gesundheitsdatenraum zu schaffen. Ziel des Europäischen Gesundheitsdatenraumes ist es, die nationalen Gesundheitssysteme durch den sicheren und effizienten Austausch von Gesundheitsdaten stärker miteinander zu verknüpfen.

Letztlich soll dies die Versorgung, die Forschung und die Infrastruktur der einzelnen Gesundheitssysteme insgesamt verbessern.

Eine große Herausforderung für den Europäischen Gesundheits-datenraum ist sicherlich die Interoperabilität der Daten. Die Daten aus Italien müssen auch in Deutschland oder Frankreich genutzt werden können. Dies ist beispielsweise auch eine Herausforderung für die elektronische Patientenkurzakte, die derzeit über das in diesen Wochen im Bundestag in der Beratung befindliche Digitale Versorgung- und Pflege-Modernisierungs-Gesetz eingeführt werden soll.

Eine der Funktionen dieser elektronischen Patientenkurzakte soll sein, dass sich Ärzte und Krankenhäuser im Ausland grundlegende Daten etwa über Blutgruppe, Allergien etc. für einen aus Deutschland stammenden Patienten herunterladen können.

Auch hier kommen viele Neuerungen auf die Krankenhäuser und Kliniken zu. Dazu wird auch gehören, dass sich im Rahmen des Europäischen Gesundheitsdatenraumes künftig viele ausländische Forschende an deutsche Krankenhäuser und Kliniken mit der Bitte um Datenlieferungen wenden werden. Für die Datenschutzaufsichts-behörden wird die große Herausforderung sein, dafür zu sorgen, dass hierbei die Vorgaben der Europäischen Datenschutz-Verordnung gewahrt bleiben.

Ich danke Ihnen für Ihre Aufmerksamkeit.