E-Health-Initiative des BMG: Arbeitsergebnis der Projektgruppe Rechtliche Hemmnisse

Position zum IT-Einsatz im Gesundheitswesen am Beispiel der Wartung und Fernwartung

Beteiligte BÄK, BZÄK, DKG, KBV, Bitkom, bvitg, ZVEI

Stand 21.12.2016

Vorbemerkung

Ärzte, Zahnärzte, Krankenhäuser und sonstige medizinische Einrichtungen und Dienstleister sind auf den Einsatz von IT-Infrastruktur und Mittel zur elektronischen Datenverarbeitung angewiesen. Der Einsatz von elektronischer Datenverarbeitung erfordert die Wartung und Pflege durch qualifizierte Fachkräfte. IT-Dienstleister, die diese Aufgaben übernehmen, tragen besondere Verantwortung für die Vertraulichkeit der personenbezogenen Gesundheitsdaten der Patienten. Insbesondere im Rahmen von sog. Fehlersuchen ergibt sich regelmäßig die Situation, dass das Wartungspersonal Kenntnis von personenbezogenen Gesundheitsdaten erhalten kann. Für die Prüfung und Wartung von EDV-Systemen durch externe IT-Dienstleister gelten die Anforderungen des § 11 Bundesdatenschutzgesetz. Unabhängig von der Umsetzung der datenschutzrechtlichen Anforderung stellt sich zunehmend die Frage nach den strafrechtlichen Konsequenzen der Beauftragung externer IT-Dienstleister, die Kenntnis von personenbezogenen Daten erhalten können. Insofern besteht erhebliche Rechtsunsicherheit, inwiefern Ärzte, Zahnärzte und IT-Dienstleister einem Strafbarkeitsrisiko ausgesetzt sind.

1. Notwendigkeit der IT-Anwendung in der Gesundheitsversorgung

Moderne Gesundheitsversorgung bedient sich zunehmend informationstechnologischer Verfahren. In Kliniken und Praxen ist der IT-Einsatz in den Bereichen Dokumentation, Diagnostik und Therapie weit verbreitet. Die Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur, zuletzt durch das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) forciert, führt digitale Anwendungen ein, die der Verbesserung der Gesundheitsversorgung dienen und ermöglicht telemedizinische Verfahren. In Zeiten zunehmender Digitalisierung steigt daher die Notwendigkeit stabiler und verlässlicher IT-Systeme in der Gesundheitsversorgung.

1.1 Medizinische Notwendigkeit der Anwendung von Mitteln zur EDV im Gesundheitswesen

Der Einsatz von IT im Gesundheitswesen kann an einem einfachen Beispiel aus der täglichen Gesundheitsversorgung verdeutlicht werden – dem Ausstellen eines Rezepts. Früher genügte ein Rezeptblock und ein Arzneimittelverzeichnis in Buchform – heute erfolgt der gleiche Prozess in einem komplexen Zusammenspiel verschiedener Software-Module: Der verschreibende Arzt kann aus seinem Praxisverwaltungs-System (PVS) heraus ein Rezept erstellen. Im Hintergrund wird dafür eine regelmäßig aktualisierte Arzneimitteldatenbank eingesetzt, die in der Regel von einem anderen Hersteller als dem des PVS angeboten wird. Häufig wird ein Arzneimittel-Interaktions-Check mit anderen Medikamenten oder tiefergehende AMTS-Prüfungen für den Patienten durchgeführt – dies erfolgt wiederum in einem anderen Software-Tool. Zuletzt wird neben dem Rezeptdruck das verordnete Medikament auch an das Software-Modul übergeben, welches einen bundeseinheitlichen Medikationsplan für den Patienten ausdruckt.

Hier lässt sich an einem einfach erscheinenden Prozess der Gesundheitsversorgung verdeutlichen, dass zur wirtschaftlichen und sicheren Patientenversorgung komplexe IT-Prozesse genutzt werden, die von verschiedener Seite Wartungsprozesse benötigen. Bei dem sehr breiten Einsatz von moderner Informations- und Kommunikationstechnologie in Diagnostik, Therapie und bei Dokumentationsprozessen im Gesundheitswesen ließen sich an dieser Stelle Beispiele in beliebiger Anzahl aufzeigen.

1.2 Gesetzlich bedingte Anforderungen zur Nutzung von Mitteln zur EDV im Gesundheitswesen

Die folgenden Beispiele belegen das breite Spektrum gesetzlicher Verpflichtungen und Optionen zum Einsatz von EDV durch Ärzte und Krankenhäuser:

Durch das Krebsfrüherkennungs- und -registergesetz (KFRG) aus dem Jahr 2013 wurden die Bundesländer zur Einrichtung von klinischen Krebsregistern verpflichtet (vgl. § 65c SGB V). Die mittlerweile erlassenen Landeskrebsregistergesetze verpflichten Ärzte und Krankenhäuser zu jedem Krebserkrankungsfall einen bundesweit einheitlichen Meldedatensatz an das jeweilige Landeskrebsregister zu übermitteln (vgl. z.B. § 12 Abs. 2 LKRG NRW). Hierbei fordern die Krebsregistergesetze der Länder ausdrücklich die elektronische Übermittlung der Meldedaten (vgl.z.B. § 15 Abs. 1 LKRG NRW).

Im Rahmen der aktuellen Novellierung des Infektionsschutzgesetzes ist die Errichtung eines elektronischen Melde- und Informationssystems vorgesehen. Die meldepflichtigen Ärzte und Krankenhäuser sollen durch Rechtsverordnung des Bundesministerium für Gesundheit zur Nutzung des elektronischen Meldesystems verpflichtet werden (vgl. § 14 Abs. 8 S. 1 Nr. 2 IfSG-E).

Ärzte oder Zahnärzte, die Medizinprodukte zur Eigenanwendung an ihre Patienten abgeben, sind zudem verpflichtet, ihnen mitgeteilte Vorkommnisse den zuständigen Bundesoberbehörden wie dem Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM, zu melden. Diese Meldungen erfolgen elektronisch und maschinenlesbar im Sinne von § 12 des E-Government-Gesetzes (vgl. §§ 3 i.V.m. 7 Abs. 2 Medizinprodukte-Sicherheitsplanverordnung, MPSV).

Das Patientenrechtegesetz eröffnet in § 630f BGB den Ärzten und Krankenhäusern ausdrücklich die Möglichkeit, die Patientendokumentation elektronisch zu führen.

§ 295 Abs. 4 SGB V schreibt vor, dass die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, Einrichtungen und medizinischen Versorgungszentren die für die Abrechnung der Leistungen notwendigen Angaben der Kassenärztlichen Vereinigung im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern zu übermitteln haben. Beide Varianten setzen den Einsatz von EDV in der Arztpraxis zwingend voraus, wobei durch die Richtlinien der KBV diese Vorgabe dahingehend konkretisiert wurde, dass die Abrechnung im Wege der elektronischen Datenübertragung zu erfolgen hat. Der Einsatz von EDV in der Arztpraxis wird auch durch weitere, durch das E-Health-Gesetz eingeführte Vorgaben eingefordert. So sollen Regelungen zur Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung (§ 291f SGB V) sowie zu technischen Verfahren zur konsiliarischen Befundbeurteilung und zur Videosprechstunde (§ 291g SGB V) getroffen werden. Ebenso wird im Zusammenhang mit der elektronischen Gesundheitskarte und der dazugehörigen Anwendungen gemäß § 291a SGB V zwingend eine EDV in der Arztpraxis benötigt.

Krankenhäuser sind gem. § 301 SGB V verpflichtet, den Krankenkassen detailliert ihre Abrechnungsdaten (Versichertendaten, institutionelle Daten, Diagnosen und Prozeduren sowie berechnete Entgelte) im Wege elektronischer Datenübermittlung oder maschinell verwertbar auf Datenträgern zu übermitteln. Vergleichbares gilt gem. § 17c Abs. 5 KHG für die Abrechnung gegenüber privaten Krankenversicherungen bei selbstzahlenden Patienten. Korrespondierend dazu besteht die Verpflichtung zur Übermittlung der DRG-Daten an das DRG-Institut auf Bundesebene (InEK) gem. § 21 KHEntgG. Hinzu kommen umfassende Datenübermittlungsverpflichtungen an die Vertrauens- und Datenaufbereitungsstelle im Rahmen der Datentransparenz gem. §§ 303a ff. SGB V bzw. im Rahmen der Krankenhausstatistik (sachliche und personelle Ausstattung, wie Betten, medizinische Großgeräte, ärztliches und nichtärztliches Personal der Krankenhäuser und Vorsorge- oder Rehabilitationseinrichtungen sowie ihrer organisatorischen Einheiten (Fachabteilungen), Kostennachweise und Diagnosedaten) nach Maßgabe der Krankenhausstatistikverordnung an die empfangsberechtigten Stellen. Flankiert wird dies durch Datenübermittlungsverpflichtungen im Rahmen von Modellvorhaben gem. §§ 63 ff. SGB V, bei der Erbringung ambulanter Institutsleistungen gem. §§ 115b ff. SGB V, der einrichtungsübergreifenden Qualitätssicherung gem. §§ 137 ff. SGB V, gegenüber den Medizinischen Diensten gem. §§ 275 ff. SGB V und künftig im Rahmen der Nutzung der Telematikinfrastruktur gem. §§ 291a ff. SGB V und der Sicherung kritischer Infrastrukturen im Rahmen des IT-SiG. Diese – hier nur auszugsweise genannten – gesetzlichen Verpflichtungen werden faktisch ergänzt durch die notwendige Datenübermittlung bei der Nutzung der gesamten Medizintechnik und der krankenhausinternen IT-Infrastruktur.

2. Der Einsatz von Mitteln zur EDV bedingt eine (Fern-)Wartung

Ohne (Fern)Wartung dieser IT-Systeme ist deren Funktionsfähigkeit nicht zu gewährleisten. Dabei ist eine Kenntnisnahme patientenbezogener Daten durch den mit der (Fern)Wartung beauftragten Dienstleister nicht immer auszuschließen. Theoretisch könnte zur vollständigen Absicherung eine Einwilligung aller Patienten eingeholt werden, deren Daten in den Systemen gespeichert sind. Dieses Vorgehen erscheint jedoch in der Praxis unrealistisch.

Auch wenn die Hersteller der IT-Systeme und Geräte vieles ohne den Zugriff auf Patientendaten lösen können, gibt es in Ausnahmesituationen immer wieder die Notwendigkeit, dass auch Mitarbeiter des Herstellers auf die in einem IT-System oder Gerät gespeicherten Daten zugreifen müssen.

Oft entsteht aus der Kombination der verschiedenen IT-Systeme verschiedener Hersteller eine einzigartige Konstellation. Liegt der Fehler nicht primär in den Komponenten eines Herstellers, kann der Fehler nur beim Kunden analysiert werden. Für die Fehleranalyse werden teilweise sehr spezielle Werkzeuge eingesetzt, die entweder vor Ort in der medizinischen Einrichtung nicht zur Verfügung stehen oder für die die Mitarbeiter der Einrichtung eine umfangreiche Schulung erhalten müssten.
Daraus ergibt sich, dass in seltenen Fällen Experten der Hersteller zur Wiederaufnahme des Betriebs hinzugezogen werden müssen. Aus wirtschaftlichen Gründen wird dies oft über Fernwartung geschehen, technisch kann die Fernwartung sehr gut abgesichert werden.

Grundsätzlich ist es üblich, dass Anbieter von IT-Anwendungen für das Gesundheitswesen mit anonymisierten Testdatensätzen arbeiten, wo immer dies praktikabel ist. Beispielsweise gibt es Testsysteme für das Testen neuer Versionen von Applikationen, die nur Testdaten oder anonymisierte Daten enthalten.

Für das Replizieren von Softwarefehlern seitens des Supportteams des Anbieters stößt dieses Verfahren an seine Grenzen. Um einen konkreten Anwendungsfehler beispielsweise in einem Entlassbrief nachvollziehen zu können, kann es erforderlich sein, die Sicht des den Brief verfassenden Arztes innerhalb der Applikation einzunehmen, z.B. durch Aufschalten auf dessen Arbeitsplatz, während der Arzt den Fehler vorführt. Dabei sieht der Support-Mitarbeiter Gesundheitsdaten eines konkreten Patienten.

Ursächlich hierfür sind insbesondere folgende Aspekte: Ein Fehler ergibt sich unter Umständen nicht nur aus einer einzelnen Applikation heraus, in welcher der Fehler für den Anwender offenkundig wird, sondern durch das Zusammenspiel mehrerer über Schnittstellen miteinander verbundener Applikationen. Im genannten Beispiel des fehlerhaften Entlassbriefs könnten Laborwerte in der Schnittstelle zwischen Laborsystem und Krankenhausinformationssystem fehlerhaft verändert werden oder sogar verloren gehen. Um ohne Kenntnisnahme von Gesundheitsdaten einen solchen Fehler zu analysieren, wäre eine komplett anonymisierte Anwendungslandschaft aus Krankenhausinformationssystem und Laborsystem notwendig. Typischerweise besteht die Anwendungslandschaft in mittelständischen Krankenhäusern aus mehr als 30 Applikationen. Eine solche anonymisierte Testlandschaft ist mit dem heute üblichen Stand der Krankenhaus-IT nicht oder nicht wirtschaftlich zu realisieren.

IT-Systeme erreichen insbesondere in Kliniken oft eine Komplexität, die es nicht zulässt das System einfach abzuschalten und durch ein anderes zu ersetzen (wie dies bei kleineren medizinischen Geräten möglich wäre). Da der Betrieb des Krankenhauses nicht unterbrochen werden kann, spielen bei der Entscheidung Experten vom Hersteller zur Lösung hinzuzuziehen nicht nur finanzielle Aspekte eine Rolle.

3. Rechtsunsicherheit im Kontext der Wartung

3.1. Strafbarkeitsrisiken bei der Einschaltung externer Dienstleister

Gemäß § 203 Abs. 1 StGB macht sich wegen Verletzung von Privatgeheimnissen (z. B. gesundheitsbezogene Informationen) strafbar, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Arzt, Zahnarzt oder sonstiger Berufsgeheimnisträger anvertraut worden oder auf andere Weise bekannt geworden ist. Von einer Offenbarung ist unter anderem dann auszugehen, wenn einem Dritten der Zugang zu den Geheimnissen verschafft wird, wobei ein ungesichertes Überlassen mit der Möglichkeit der Kenntnisnahme bereits genügt. Auf eine tatsächliche Kenntnisnahme kommt es daher nicht an.

Der Strafvorschrift liegt der Gedanke zugrunde, dass grundsätzlich nur Berufsgeheimnisträger von Privatgeheimnissen Kenntnis erlangen dürfen. § 203 Abs. 3 S. 2 StGB stellt den Geheimnisträgern allerdings weitere Personen gleich. Danach sind auch berufsmäßig tätigen Gehilfen von Ärzten, Zahnärzten und sonstigen Berufsgeheimnisträgern zum Schweigen verpflichtet.
"Externe IT-Dienstleister", die anlässlich ihrer Tätigkeit Kenntnis von Patientengeheimnissen erhalten könnten, gehören nach überwiegender Auffassung nicht zum Kreis der berufsmäßig tätigen Gehilfen. Von einer konkludenten Einwilligung kann ebenfalls nicht ausgegangen werden, da der Patient von der Einbeziehung der externen "IT-Dienstleister" zum Zweck der Wartung von EDV-Systemen in der Regel keine konkrete Vorstellung entwickelt. Selbst wenn man IT-Dienstleister zu den berufsmäßigen Gehilfen im Sinne des § 203 Abs. 3 S. 2 StGB zählen würde, ergibt sich aus den oben dargelegten Gründen noch keine Befugnis des Arztes zur Offenbarung der Patientengeheimnisse. Anders kann es sich dann verhalten, wenn das IT-Personal in der Arztpraxis oder in dem Krankenhaus angestellt ist. Eine Rechtsprechung, die den Einsatz von externen IT-Dienstleistern durch Ärzte, Zahnärzte und andere Berufsgeheimnisträger als Straftat im Sinne des § 203 StGB beurteilt, liegt bislang nicht vor. Das Landgericht Flensburg hat allerdings in einem zivilrechtlichen Schadensersatzprozess die Beauftragung einer externen Hilfsperson zu Wartungsarbeiten durch einen Arzt als Verstoß gegen § 203 StGB beurteilt, da dieser ungehinderten Zugriff auf die in seiner EDV-Anlage gespeicherten Patientendaten eingeräumt hatte (LG Flensburg, 05.07.2013, Az.: 4 O 54/11).
Nicht zuletzt aufgrund dieser Rechtsprechung ist von einem Strafbarkeitsrisiko für Ärzte, Zahnärzte oder sonstigen Berufsgeheimnisträgern auszugehen. Daneben kommt eine Strafbarkeit des IT-Dienstleisters wegen Teilnahme an der Verletzung von Privatgeheimnissen in Betracht.

3.2. Sicht der Aufsichtsbehörden für den Datenschutz

Datenschutz und Schweigepflicht sind grundsätzlich zwei unterschiedliche Rechtsgebiete. Gleichwohl war diese Thematik immer wieder im Fokus der nationalen Datenschutzbehörden.

So forderte die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung Nachbesserungen beim E-Health-Gesetz, insbesondere klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern:

> „Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem E-Health-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. Die notwendige rechtliche Regelung muss (z.B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.“

Fazit

Die Initiative und Zielrichtung des zwischenzeitlich vorgelegten Entwurfs eines *Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen* ist grundsätzlich zu begrüßen. Eine bundeseinheitliche Lösung, die das Strafbarkeitsrisiko möglichst ausschließt, wird begrüßt.