www.jusletter.ch

Sarah Winkler

Ausführungsrecht zum elektronischen Patientendossier

Kommentierung der Zertifizierungsvoraussetzungen der Gemeinschaften und Stammgemeinschaften

Zukünftig sollen die behandelnden Ärzte die relevanten medizinischen Daten ihrer Patienten über ein elektronisches Patientendossier beziehen können. Den Patienten wird dabei die Möglichkeit gegeben, die Zugriffsrechte auf ihre Patientendaten selber zu verwalten. Bis allerdings das erste Mal Daten über das elektronische Patientendossier bereitgestellt und bezogen werden können, müssen noch einige rechtliche Fragen geklärt werden, insbesondere im Bereich der gesetzlich vorgeschriebenen Zertifizierungen.

Beitragsarten: Beiträge
Rechtsgebiete: Gesundheitsrecht; Sozialversicherungsrecht; Patientenrechte, Persönlichkeitsrechte; Datenschutz

Zitiervorschlag: Sarah Winkler, Ausführungsrecht zum elektronischen Patientendossier, in: Jusletter 29. August 2016

Inhaltsübersicht

1. Einleitung

[Rz 1] Jeder Mensch generiert im Laufe seines Lebens eine grosse Menge an Gesundheitsdaten. Da die einzelnen medizinischen Handlungen jedoch eher selten an einem Ort durchgeführt werden können, sind diese Daten häufig auf eine Vielzahl von behandelnden Gesundheitspersonen und -organisationen verstreut. Innerhalb einer Gesundheitsorganisation wie einem Spital wird der bereichsübergreifende Zugriff auf Patientendaten durch Krankenhausinformationssysteme (KIS) sichergestellt.[1] Eine vertrauliche elektronische Weitergabe von Patientendaten zwischen einzelnen Gesundheitsorganisationen, wie beispielsweise zwischen einem Hausarzt und dem behandelnden Spital, kann bisher in der Regel nicht mit Sicherheit gewährleistet werden. Häufig werden die medizinischen Informationen auf einem Datenträger dem Patienten mitgegeben oder, mit Zustimmung des Patienten, über nur unzureichend geschützte Kanäle, wie E-Mail, versandt.

[Rz 2] Der Bund möchte dieser Problematik durch die Einführung eines elektronischen Patientendossiers entgegenwirken. Dieses stellt einen wichtigen Teil der vom Bund und den Kantonen gemeinsam erarbeiteten «Strategie eHealth Schweiz» aus dem Jahr 2007[2] dar. Ziel des elektronischen Patientendossiers ist es, alle behandlungsrelevanten Informationen allen an einer Behandlung beteiligten Gesundheitsfachpersonen unabhängig von Ort und Zeit zugänglich zu machen,[3] um so die Effizienz im Gesundheitssystem zu steigern.[4] Dem Patienten[5] soll ermöglicht werden, auf seine eigenen Daten zuzugreifen und die Zugriffsrechte von Dritten selber zu verwalten.[6] Das Bundesgesetz über das elektronische Patientendossier (EPDG) wurde am 19. Juni 2015 von der

1 Für ausführliche Informationen betreffend die interne Weitergabe von Patientendaten siehe: Yves Gogniat, Datenschutz in Spitälern, in: Jusletter 20. Juni 2016, N 36 ff.

2 Bundesamt für Gesundheit (BAG), Strategie «eHealth» Schweiz vom 27. Juni 2007.

3 Botschaft zum Bundesgesetz über das elektronische Patientendossier, BBl 2013 5321, 5329.

4 BBl 5321, 5323.

5 Aus Gründen der Lesbarkeit wird im Folgenden ausschliesslich der Begriff «Patient» verwendet, womit sowohl die männliche wie auch die weibliche Form eingeschlossen sind.

6 BBl 2013 5321, 5329.

Bundesversammlung als Rahmengesetz[7] verabschiedet und am 22. März 2016 wurde das entsprechende Ausführungsrecht veröffentlicht.[8] Dieses besteht aus der Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV) sowie die Verordnung über das elektronische Patientendossier (EPDV) und die darauf basierende Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI).

[Rz 3] Einer der wichtigsten Bestandteile der Umsetzung dieser gesetzlichen Grundlagen ist die Zertifizierung mehrerer beteiligter Systeme und Akteure.[9] Damit bezweckt der Gesetzgeber einerseits, das Funktionieren des systemübergreifenden Datenaustauschs sicherzustellen (Interoperabilität).[10] Da medizinische Daten aus datenschutzrechtlicher Sicht als besonders schützenswert[11] gelten, soll andererseits das Vertrauen der Patienten in das elektronische Patientendossier gestärkt werden, indem über die Kontrolle durch eine externe Zertifizierungsstelle der korrekte und sichere Umgang mit den Daten bestätigt wird.[12]

[Rz 4] Die Kompetenz zur Regelung der Zertifizierungsvoraussetzungen delegierte der Bundesrat an das Eidgenössische Departement des Inneren (EDI). Dieses erliess unter anderem Anhang 2 der EPDV-EDI, in welchem die «Technischen und organisatorischen Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften» (TOZ) geregelt werden. Die zukünftigen Betreiber der Systeme für das elektronische Patientendossier (sogenannte Gemeinschaften und Stammgemeinschaften) müssen die darin enthaltenen Anforderungen einhalten, was von einer akkreditierten Zertifizierungsstelle bestätigt werden muss.

[Rz 5] Unglücklicherweise zeichnen sich die TOZ vorwiegend durch ihre hohe Komplexität und teilweise nicht praxisorientierten Regelungen aus. Ziel dieses Artikels ist es aufzuzeigen, dass bei der Ausarbeitung der Zertifizierungsvoraussetzungen von einem Verständnis der Zertifizierungen und der Rolle der Zertifizierungsstellen ausgegangen wurde, welches sich nicht mit den bereits gängigen Zertifizierungsnormen deckt. Hierfür wird zunächst eine kurze Einführung in das elektronische Patientendossier gegeben und werden die Grundlagen der Zertifizierungen erläutert. Danach wird erklärt, welche Zertifizierungen im Rahmen des elektronischen Patientendossiers notwendig sein werden, wobei insbesondere auf die Gemeinschaften und Stammgemeinschaften eingegangen wird. In einem letzten Schritt wird der Artikel aufzeigen, weshalb die Zertifizierungen der Gemeinschaften und Stammgemeinschaften nach der aktuell vorliegenden Version der Zertifizierungsvoraussetzungen nicht praktikabel sind und Schwierigkeiten bei der Umsetzung machen werden.

2. Das elektronische Patientendossier

[Rz 6] Die Entscheidung, am System des elektronischen Patientendossiers teilzunehmen, ist sowohl für die Patienten als auch für die Gesundheitsfachpersonen freiwillig (doppelte Freiwillig-

7 BBl 2013 5321, 5322.

8 Die Anhörung dauerte bis am 29. Juni 2016, siehe: Bundesamt für Gesundheit, Medienmitteilung – Eröffnung Anhörung Ausführungsrecht zum EPDG vom 23. März 2016, zu finden unter http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/16000/index.html?lang=de (Website zuletzt besucht am 14. Juli 2016).

9 Art. 11 EPDG.

10 BBl 2013 5321, 5331.

11 Art. 3 lit. c Ziff. 2 Bundesgesetz über den Datenschutz (DSG, SR 235.1).

12 BBl 2013 5321, 5351.

keit).[13] Ausgenommen von dieser freiwilligen Teilnahme sind ausschliesslich die Spitäler, Geburtshäuser und Pflegeheime, welche Leistungen auf Kosten der obligatorischen Krankenpflegeversicherung (OKP) erbringen. Diese haben nach Ablauf der Übergangsfrist die gesetzliche Verpflichtung, sich einer zertifizierten Gemeinschaft oder Stammgemeinschaft anzuschliessen.[14]

[Rz 7] Der Anschluss an eine solche Gemeinschaft oder Stammgemeinschaft ist die Voraussetzung dafür, dass Gesundheitsfachpersonen die Daten ihrer Patienten in einem elektronischen Patientendossier bereitstellen und selber darüber Patientendaten beziehen dürfen. In der Botschaft zum EPDG werden Gemeinschaften und Stammgemeinschaften als Zusammenschlüsse von Gesundheitsfachpersonen und -institutionen definiert, welche die für die Datenbearbeitung im elektronischen Patientendossier notwendige Informatikinfrastruktur gemeinsam nutzen.[15] Nach der Legaldefinition von Art. 2 lit. d EPDG müssen Gemeinschaften sicherstellen, dass die medizinischen Daten über das elektronische Patientendossier zugänglich sind sowie dass jede Bearbeitung von Daten protokolliert wird.[16] Stammgemeinschaften wiederum sind Gemeinschaften, die zusätzlich zur Datenbereitstellung weitere Aufgaben erfüllen, wie unter anderem das Anbieten von Funktionen, mit denen die Patienten die Zugriffrechte verwalten können.[17]

[Rz 8] Eröffnet ein Patient ein elektronisches Patientendossier, werden seine Daten weiterhin in den Praxis- und Klinikinformationssystemen der Gesundheitsfachpersonen gespeichert.[18] Diese werden als «Primärsysteme» bezeichnet.[19] Die Daten werden allerdings nun über das elektronische Patientendossier anderen Gesundheitsfachpersonen zur Verfügung gestellt («Sekundärsystem»). Hierfür werden die Daten nicht auf einer zentralen Datenablage gespeichert, auf welche die einzelnen Gesundheitsfachpersonen Zugriff erlangen. Vielmehr geben Dokumentenregister Auskunft über den dezentralen Ablageort der Daten und Dokumente bei den Gesundheitsfachpersonen bzw. Gemeinschaften und Stammgemeinschaften.[20] Die über das elektronische Patientendossier zur Verfügung gestellten Dokumente werden mit einer dem Patienten eindeutig zugewiesenen Identifikationsnummer versehen, um so die korrekte Zusammenführung sicherzustellen.[21] Aufgrund der dezentralen und verteilten Datenspeicherung spricht der Gesetzgeber von einem «virtuellen Patientendossier».[22]

[Rz 9] Die Zugriffe von Gesundheitsfachpersonen und Patienten erfolgen über sogenannte Zugangsportale. Den Patienten wird darüber ermöglicht, entweder über das (interne) Zugangsportal der Stammgemeinschaft oder über ein (externes) Zugangsportal eines zertifizierten Drittanbieters[23] orts- und zeitunabhängig auf ihre medizinischen Daten zuzugreifen sowie die Zugriffsrechte der Gesundheitsfachpersonen selber zu verwalten. Über das interne Zugangsportal der

13 BBl 2013 5321, 5323; Jurius, Elektronisches Patientendossier, Jusletter 23. März 2015, N 1.

14 Art. 39 Abs. 1 lit. f, Änderung gemäss Schlussbestimmungen Art. 25 EPDG.

15 BBl 2013 5321, 5333.

16 Art. 10 Abs. 1 EPDG.

17 Art. 2 lit. e EPDG; BBl 2013 5321, 5338.

18 Bianka S. Dörr, ePatientendossier – Ausgewählte Aspekte zur Sicherung von behandlungsrelevanten Patientendaten, in: Sicherheit & Recht 2/2012 S. 128, 130.

19 BBl 2013 5321, 5333.

20 BBl 2013 5321, 5334.

21 BBl 2013 5321, 5335; Jurius, Elektronische Patientendossiers: Behandlungen verbessern, in: Jusletter 3. Juni 2013, N 3.

22 BBl 2013 5321, 5334.

23 BBl 2013 5321, 5336.

Stammgemeinschaft muss es dem Patienten zudem ermöglicht werden, selbständig Daten, wie beispielsweise Blutdruck- und Blutzuckerwerte, zu erfassen und diese den Gesundheitsfachpersonen zugänglich zu machen.[24] Verfügt das Primärsystem einer Gesundheitsfachperson nicht über die Funktionalität, mit den übergeordneten Systemen der Gemeinschaft oder Stammgemeinschaft zu kommunizieren, so kann die Gesundheitsfachperson die Daten und Dokumente auch über das interne Zugangsportal einsehen oder bereitstellen.[25]

[Rz 10] Die folgende Grafik gibt eine Übersicht, welche Funktionen die internen Zugangsportale der Gemeinschaften und Stammgemeinschaften bzw. die externen Zugangsportale von zertifizierten Drittanbietern zu erfüllen haben.

Tabelle 1

Funktionalitäten der Zugangsportale

Funktion	Interne Zugangsportale der Stammgemeinschaften	Interne Zugangsportale der übrigen Gemeinschaften	Externe Zugangsportale
Dateneinsicht durch Patientinnen und Patienten	Ja	Ja	Ja
Datenbereitstellung durch Patientinnen und Patienten	Ja	Nein	Nein
Anpassung Zugriffsrechte durch Patientinnen und Patienten	Ja	Nein	Nein
Datenbereitstellung durch Gesundheitsfachpersonen[1]	Ja[2]	Ja[2]	Nein
Dateneinsicht durch Gesundheitsfachpersonen[1]	Ja	Ja	Nein

1 Gilt nur für Gesundheitsfachpersonen, die Mitglied der entsprechenden Gemeinschaft sind und über eine elektronische Identität verfügen – alle übrigen Gesundheitsfachpersonen haben keine Möglichkeit auf Daten und Dokumente im elektronischen Patientendossier zuzugreifen.

2 Gilt für Gesundheitsfachpersonen, die Mitglied der entsprechenden Gemeinschaft sind, aber die Informatikintegration noch nicht vollzogen haben.

Quelle: BBl 2013 5321, *5339*, *Tabelle 1 «Funktionalitäten der Zugangsportale».*

[Rz 11] Der Zugriff auf die Daten darf nicht nur gemeinschaftsintern erfolgen, ansonsten die Effizienz des elektronischen Patientendossiers erheblich beeinträchtigt wird. Aus diesem Grund führt das Bundesamt für Gesundheit (BAG) Abfragedienste, welche die für die Kommunikation zwischen Gemeinschaften, Stammgemeinschaften und Zugangsportalen notwendigen Referenzdaten liefern.[26]

[Rz 12] Für den sicheren Identitätsnachweis beim gemeinschaftsinternen wie auch gemeinschaftsübergreifenden Zugriff auf das elektronische Patientendossier müssen sowohl die Patienten als

24 BBl 2013 5321, 5336.

25 BBl 2013 5321, 5339.

26 Art. 14 Abs. 1 EPDG.

auch die Gesundheitsfachpersonen über eine elektronische Identität verfügen. Diese wird durch zertifizierte Hersteller erstellt und auf Identifikationsmitteln wie einer SmartCard oder auch einem Mobiltelefon gespeichert.[27]

[Rz 13] Das Funktionieren des elektronischen Patientendossiers bedingt, dass der Austausch zwischen den unabhängigen Systemen, Gemeinschaften, Stammgemeinschaften, Leistungserbringern und Patienten sowie allen weiteren Akteuren funktioniert (Interoperabilität). Dies wiederum erfordert eine hoheitliche Koordination und Steuerung durch die Einführung von technischen und organisatorischen Mindestanforderungen.[28] Das EPDG sieht vor, dass diese Mindestanforderungen durch eine Reihe von gesetzlich vorgeschriebenen Zertifizierungen überprüft werden, um so eine schweizweite Normierung sicherzustellen und eine sichere Datenbereitstellung und einen sicheren Datenabruf zu ermöglichen.[29] Gemäss Art. 11 EPDG müssen die Gemeinschaften und Stammgemeinschaften (lit. a), die (externen) Zugangsportale[30] (lit. b) und die Herausgeber von Identifikationsmitteln (lit. c) durch eine anerkannte Stelle zertifiziert sein.

[Rz 14] In den Ausführungsverordnungen wurden die Einführung und die Zertifizierung von externen Zugangsportalen nicht umgesetzt und auch auf den Erlass von Zertifizierungsvoraussetzungen für die Herausgeber von Identifikationsmitteln[31] wurde verzichtet, wobei der Bundesrat bzw. das EDI keine Begründung für dieses Vorgehen geben. Aus diesem Grund werden die Zertifizierungen von Zugangsportalen und von Herausgebern von Identifikationsmitteln hier nicht behandelt. Der Artikel wird sich vielmehr auf die technischen und organisatorischen Zertifizierungsvoraussetzungen für die Gemeinschaften und Stammgemeinschaften konzentrieren.

3. Zertifizierungen und akkreditierte Zertifizierungsstellen

3.1. Grundlagen

[Rz 15] Eine Zertifizierung ist ein Verfahren, nach dem eine unabhängige Stelle bestätigt, dass Produkte, Prozesse, Systeme oder Personen mit festgelegten Anforderungen konform sind[32] und dessen Ziel die Ausstellung eines Zeugnisses bzw. Zertifikats ist.[33]

[Rz 16] Zertifizierungen können sowohl auf gesetzlichen wie auch privaten Zertifizierungssystemen basieren.[34] Gesetzliche Zertifizierungen können einerseits freiwillig sein, wie beispielsweise die Zertifizierung nach der Verordnung über die Datenschutzzertifizierungen (VDSZ)[35]. Ande-

27 BBl 2013 5321, 5335.

28 BBl 2013 5321, 5331.

29 BBl 2013 5321, 5351.

30 BBl 2013 5321, 5386.

31 Delegationsnorm an das EDI in Art. 30 Abs. 3 EPDV.

32 Siehe FAQ der Schweizerischen Akkreditierungsstelle, zu finden unter https://www.sas.admin.ch/sas/de/home/akkreditierung/faq.html#-863295946 (Website zuletzt besucht am 6. August 2016).

33 Lucie von Büren, Akkreditierte Zertifizierung im gesetzlich geregelten Bereich, Systeme, Einordnung und Rechtsschutz, Bern 2014, S. 5.; Patrick Kos, Rechtliche Anforderungen an die elektronische Schriftgutverwaltung in der Privatwirtschaft und Zertifizierungen nach ISO 15489-1 und ISO/IEC 27001.

34 von Büren, S. 10.

35 Verordnung über die Datenschutzzertifizierungen vom 27. September 2007 (VDSZ; SR 235.13); Ausnahme bilden hier die Datenannahmestellen derjenigen Krankenversicherer, welche SwissDRG-Rechnungen empfangen und

rerseits können Zertifizierungen gesetzlich verpflichtend sein, wie dies beispielsweise häufig im Rahmen der Produktsicherheit der Fall ist.

[Rz 17] Private Zertifizierungsnormen im Gegensatz dazu werden von privaten Organisationen erlassen und haben daher keinen Gesetzescharakter. Eine der grössten privaten Organisationen ist die «International Organization for Standardization» (ISO)[36], welche vorwiegend Standards für den Aufbau und die Zertifizierung von Managementsystemen erlässt.

[Rz 18] Um die entsprechenden Zertifikate vergeben zu können, benötigt die unabhängige Zertifizierungsstelle ebenfalls eine Erlaubnis, die sogenannte Akkreditierung. In der Schweiz werden Akkreditierungen durch die Schweizerische Akkreditierungsstelle (SAS) durchgeführt[37], die sich in ihrer Tätigkeit nach der Akkreditierungs- und Bezeichnungsverordnung (AkkBV)[38] bzw. nach den in Anhang 2 der AkkBV genannten Akkreditierungsnormen richtet. Mit der Akkreditierung wird formell die Kompetenz einer Stelle anerkannt, nach international massgebenden Anforderungen bestimmte Prüfungen oder Konformitätsbewertungen durchzuführen.[39] Dadurch wird bestätigt, dass die Zertifizierungsstelle über die notwendigen Kompetenzen und das erforderliche Fachwissen verfügt, um Produkte, Managementsysteme oder Personen auf der Basis einer bestimmten Zertifizierungsnorm zu zertifizieren. Akkreditierungen können sowohl für die Vergabe von gesetzlichen als auch privaten Zertifikaten notwendig sein. Die ISO beispielsweise erlässt eigene Anforderungen an die Akkreditierung von Zertifizierungsstellen.[40]

3.2. Zertifizierung von Managementsystemen

[Rz 19] Managementsysteme können in vielen unterschiedlichen Bereichen einer Organisation aufgebaut werden. Zu denken ist unter anderem an Qualitäts-,[41] Umwelt-,[42] Informationssicherheits-[43] und Datenschutzmanagementsysteme[44], um nur einige zu nennen. Der Aufbau und die Ausgestaltung eines Managementsystems hängen jeweils vom Tätigkeits- und Aufgabengebiet einer Organisation und der dadurch entstehenden Risiken ab.

[Rz 20] Eine vereinheitlichte Definition eines Managementsystems lässt sich im Anhang 2 der ISO/IEC Directive Part 1 finden. Gemäss dieser ist ein Managementsystem ein «*set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives*».[45] Ein Managementsystem bezweckt somit die operationelle und strategische Pla-

bearbeiten wollen. Seit dem 1. Januar 2013 müssen diese Datenannahmestellen gesetzlich vorgeschrieben nach VDSZ zertifiziert sein (Art. 59a Abs. 6 Verordnung über die Krankenversicherung, KVV).

36 Zu finden unter http://www.iso.org/iso/home.html (Website zuletzt besucht am 6. August 2016).

37 Zu finden unter https://www.sas.admin.ch/sas/de/home.html (Website zuletzt besucht am 6. August 2016).

38 Verordnung über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen vom 17. Juni 1996 (AkkBV, SR 946.512).

39 Art. 2 AkkBV.

40 Siehe hier vorwiegend ISO/IEC 17021.

41 ISO/IEC 9000.

42 ISO/IEC 14000.

43 ISO/IEC 27001.

44 Art. 4 Abs. 2 VDSZ.

45 ISO/IEC Directive Part 1, 2015, Annex 2 (High Level Structure, identical core text, common terms and core definitions), Ziff. 3.4.

nung von unternehmensinternen Risiken durch die Bestimmung der Verantwortlichkeiten sowie die Einführung und Anwendung von Policies und Prozessen.

[Rz 21] Im Rahmen der Zertifizierung von Managementsystemen wird geprüft, ob die durch die entsprechende Norm vorgegebenen Elemente des Managementsystems vorhanden sind und systematisch aufrechterhalten und betrieben werden. Ein wichtiger Prüfpunkt ist dabei in der Regel auch die systematische Sicherstellung der Einhaltung der relevanten rechtlichen Vorgaben.[46] Dabei wird beispielsweise geprüft, ob das Unternehmen die für die jeweilige Norm und den Tätigkeitsbereich des Unternehmens relevanten gesetzlichen Bestimmungen erhoben hat, ob auf dieser Basis Risiken evaluiert, Weisungen erlassen und Mitarbeitende geschult sowie Prozesse geprüft wurden. Die Zertifizierung eines Managementsystems umfasst jedoch nicht die Prüfung, ob eine bestimmte gesetzliche Anforderung im Einzelfall zu jeder Zeit eingehalten wird. Oder anders ausgedrückt kann dennoch ein funktionierendes Managementsystem vorliegen, auch wenn gegen eine relevante gesetzliche Bestimmung verstossen wurde, solange die Prozesse, die das Vorgehen bei einem solchen Verstoss regeln, angemessen sind und eingehalten werden.[47] Bei der Zertifizierung von Managementsystemen geht es daher um die Kontrolle von Prozessen und Systemen, wobei diese auf die organisationsspezifischen Aufgaben und Risiken anzupassen sind.[48] Ein Prozess kann für eine Organisation passen, für eine andere aufgrund ihrer internen Struktur jedoch nicht umsetzbar sein. Auf solche Differenzierungen muss im Rahmen von Zertifizierungen eingegangen werden.

3.3. Technische Richtlinien und Zertifizierung von Produkten

[Rz 22] Grundsätzlich geht das Schweizer Produktesicherheitsrecht von der Eigenverantwortung des Inverkehrbringers eines Produktes aus.[49] Weisen Produkte ein grosses Schädigungs- oder Gefahrenpotential auf, so können sie allerdings einer gesetzlichen Zertifizierungspflicht unterliegen.[50] Die entsprechende Konformitätsbestätigung ist eine gesetzliche Voraussetzung für die Zulassung auf dem Markt.[51] Beispielsweise müssen Druckgeräte[52] oder Medizinprodukte[53] zuerst zertifiziert werden, bevor sie auf dem Markt angeboten werden dürfen.

[Rz 23] Systeme und Programme können technischen Anforderungen unterliegen, wenn sie eine bestimmte Funktionalität erbringen müssen. Als Beispiel kann hier die Zertifizierung von Lohnbuchhaltungsprogrammen durch den Verein Swissdec[54] genannt werden. Software für Lohn-

46 Interview mit einer Vertreterin einer akkreditierten Zertifizierungsstelle für Managementsysteme vom 25. Juli 2016.

47 Siehe Fn 43.

48 Siehe Fn 43.

49 von Büren, S. 66.

50 von Büren, S. 66.

51 von Büren, S. 65 f.

52 Art. 9 ff. i.V.m. Anhang 3 Verordnung über die Sicherheit von Druckgeräten (Druckgeräteverordnung, SR 819.121).

53 Art. 45 Abs. 1, Art. 46 Abs. 1 und Abs. 2 lit. b Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG, SR 812.21) i.V.m. Art. 5 und Art. 10 Abs. 1 und Anhang 3 Ziff. 2 Medizinprodukteverordnung (MepV, SR 812.213).

54 Zu finden unter http://www.swissdec.ch (Website zuletzt besucht am 6. August 2016).

buchhaltung können nach dem Lohnstandard-CH (ELM)[55] aufgebaut werden, welcher die fachlichen und technischen Anforderungen an die Übermittlung der Lohndaten von den Arbeitgebern an die Sozialversicherungen und Steuerbehörden festlegt. Im Rahmen der Zertifizierung prüft der Verein Swissdec beispielsweise die Eingabemasken, führt Systemtests und Testfälle durch und kontrolliert die Übermittlung der Lohndaten[56] anhand eines festgelegten Prüfsystems. Resultieren die Tests in einem positiven Ergebnis, wird dem Lohnbuchhaltungsprogramm durch die Vergabe eines Zertifikats bescheinigt, dass die Software nach dem Lohnstandard-CH (ELM) konform ist, den technischen Anforderungen entspricht und von den Unternehmen für die elektronische Übermittlung der Lohndaten eingesetzt werden darf.

[Rz 24] Ein weiteres anschauliches Beispiel für die Zertifizierung von Produkten und Systemen nach technischen Anforderungen findet sich zudem in Deutschland. Das Deutsche Bundesamt für Sicherheit in der Informationstechnik hat beispielsweise technische Richtlinien erlassen, welche Anforderungen an den Betrieb von IT-Produkten und -Systeme stellen, die für den Einsatz in hoheitlichen und daher sicherheitskritischen Bereichen der Bundesrepublik Deutschland vorgesehen sind.[57]

3.4. Audits und Grenzen der Zertifizierung

[Rz 25] Die Überprüfung der relevanten Zertifizierungsvoraussetzungen führen die Zertifizierungsstellen im Rahmen von Audits durch. Während dieser können Vertreter von Zertifizierungsstellen beispielsweise Dokumente sichten, Personen befragen, Räumlichkeiten inspizieren, Verfahren und Prozesse kontrollieren und die Einhaltung von Normen und Regulierungen stichprobenartig überprüfen. Ein Audit beschränkt sich allerdings auf eine Momentaufnahme: Es wird überprüft, ob die relevanten Voraussetzungen zu einem bestimmten Zeitpunkt eingehalten werden. In einer jährlichen summarischen Prüfung wird kontrolliert, ob die Zertifizierungsvoraussetzungen immer noch gegeben sind, wobei allfällige Änderungen der Prozesse und Systeme sowie relevante Vorfälle berücksichtigt werden. Werden relevante Änderungen festgestellt, dann muss die Zertifizierung in der Regel wiederholt werden. Vor Ablauf der Gültigkeitsdauer des Zertifikats muss das gesamte Managementsystem wieder geprüft werden (vergleiche Art. 6 Abs. 2 VDSZ, der die Gültigkeit der Zertifizierung eines Datenschutzmanagementsystems auf drei Jahre beschränkt).

[Rz 26] Es ist folglich nicht die Aufgabe der Zertifizierungsstellen, im Gegensatz beispielsweise zu einer Revisionsgesellschaft, im Rahmen der Zertifizierung von Managementsystemen die korrekte Einhaltung von gesetzlichen Vorgaben detailliert zu überprüfen. Insbesondere können die Zertifizierungsstellen in der Regel ausserhalb der periodischen Überprüfung keine Informationen verlangen. Meldeplichten bestehen ausserhalb der Audits nur indirekt: Vor dem erstmaligen Audit muss festgelegt werden, welcher Geltungsbereich (Scope) des Managementsystems überprüft

55 Mehr Informationen zu finden unter http://www.bfs.admin.ch/bfs/portal/de/index/news/00/14.html(Website zuletzt besucht am 6. August 2016).

56 Zu finden unter http://www.swissdec.ch/de/software-hersteller/software-zertifizieren/ (Website zuletzt besucht am 6. August 2016).

57 Zu finden unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/zertifizierungnachtr_node.html (Website zuletzt besucht am 6. August 2016).

und zertifiziert werden soll.[58] Ergeben sich nach der Vergabe des Zertifikats erhebliche Änderungen des Geltungsbereichs, beispielsweise wenn sich die zertifizierten Datenbearbeitungsprozess oder die Organisation wesentlich verändert haben, so umfasst das Zertifikat nicht mehr alle relevanten Bereiche. Die Organisation verwendet in diesem Fall ein nicht korrektes Zertifikat, was allenfalls gar wettbewerbsrechtliche Relevanz haben kann.[59] Die zertifizierten Organisationen haben daher ein grosses Interesse daran, erhebliche Änderungen des Scopes der Zertifizierungsstelle zu melden, damit eine erneute Zertifizierung durchgeführt werden kann.[60]

[Rz 27] Zusammengefasst kann daher folgende Aussage gemacht werden: Zertifizierte Managementsysteme beinhalten keine dauernde Überprüfung der Rechtskonformität durch die Zertifizierungsstelle. Vielmehr wird durch periodische Prüfungen sichergestellt, dass die Voraussetzungen einer bestimmten Zertifizierungsnorm, welche die systematische Gewährleistung der Einhaltung der Rechtsnormen sicherstellen, dauerhaft erfüllt werden.

4. Die technischen und organisatorischen Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (TOZ)

4.1. Die TOZ als neue Zertifizierungsnorm

[Rz 28] Nach dem Wortlaut von Art. 12 Abs. 1 EPDG hat der Bundesrat die Kompetenz, unter Berücksichtigung der entsprechenden internationalen Normen sowie des aktuellen Stands der Technik die Anforderungen für die Zertifizierung der Gemeinschaften und Stammgemeinschaften, der Herausgeber von Identifikationsmitteln sowie der Zugangsportale festzulegen. Insbesondere legt er fest:

a. welche Normen, Standards und Integrationsprofile anzuwenden sind;
b. wie der Datenschutz und die Datensicherheit zu gewährleisten sind;
c. welche organisatorischen Voraussetzungen zu erfüllen sind.

[Rz 29] Gemäss der Botschaft zum EPDG sind in Art. 12 Abs. 1 lit. a EPDV die anzuwendenden technischen und semantischen Normen und Standards sowie die für die Gewährleistung der Interoperabilität notwendigen Integrationsprofile gemeint.[61] Sie betreffen insbesondere die Sicherstellung der korrekten Identifikation von Patienten, Patientinnen und Gesundheitsfachpersonen, die Organisation und Verwaltung der Dokumentenregister und der internen Zugangsportale der Gemeinschaften und Stammgemeinschaften wie auch der Abfragedienste und die gemeinschaftsübergreifenden Abfragen.[62] Zudem sind allgemeine technische Voraussetzungen aufzustellen.[63] Die Ausarbeitung der TOZ, welche die Voraussetzung an die Zertifizierung der Gemeinschaften

58 Maria Winkler, Implementierung, Auditierung und Zertifizierung von Datenschutz-Managementsystemen, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Datenschutz-Managementsysteme im Aufwind?, Zürich/Basel/Genf 2016, S. 107.

59 Art. 3 lit. c Bundesgesetz über den unlauteren Wettbewerb (UWG, SR 241).

60 Siehe Fn 43.

61 BBl 2013 5321, 5386.

62 BBl 2013 5321, 5386.

63 BBl 2013 5321, 5386.

und Stammgemeinschaften enthalten, oblag somit dem Bundesrat, welcher die Kompetenz wiederum an das EDI delegierte.[64]

[Rz 30] Gemäss Art. 13 Abs. 1 lit. d EPDG hatte der Bundesrat dabei die Möglichkeit, die Anerkennung von Zertifizierungsverfahren nach anderen Gesetzen zu regeln. Von dieser Kompetenz hat er allerdings weder Gebrauch gemacht, noch diese an das EDI delegiert. Die TOZ verweisen zwar verschiedentlich auf bestimmte ISO/IEC Normen, eine Zertifizierung der Systeme der Gemeinschaften und Stammgemeinschaften nach einer ISO/IEC Norm oder einer anderen bestehenden Zertifizierungsnorm ist allerdings nicht vorgesehen. Vielmehr ist davon auszugehen, dass die TOZ eine eigenständige und neue Norm darstellen sollen, welche zwar punktuell auf bestehende Normen und Standards Bezug nimmt, aber ansonsten unabhängig die erforderlichen Zertifizierungsvoraussetzungen festlegt. Damit wurde nach der hier vertretenen Auffassung eine Chance zur Vereinfachung und Beschleunigung des Zertifizierungsprozesses nicht genutzt.

[Rz 31] Die Anforderungen der Zertifizierung, welche sich auf die technischen und semantischen Normen und Standards gemäss Art. 12 Abs. 1 lit. a EPDG beziehen, sind klarerweise auf die spezifische Funktionsweise des elektronischen Patientendossiers und die notwendige Interoperabilität zugeschnitten. Eine Ausarbeitung von entsprechend spezifischen Voraussetzungen war daher notwendig und eine Anerkennung von allenfalls bestehenden Normen nicht möglich. Auf die Frage, ob diese Voraussetzungen allerdings überhaupt durch eine Zertifizierung überprüft werden können, wird später eingegangen.[65]

[Rz 32] Eine andere Beurteilung ergibt sich bezüglich den Voraussetzungen an den Datenschutz und die Datensicherheit. Die TOZ sehen hier mehrheitlich allgemeine Anforderungen an die Gewährleistung des Datenschutzes und der Datensicherheit vor, mit nur wenigen spezifischen Voraussetzungen, wie beispielsweise die Verpflichtung zur Einsetzung eines Datenschutz- und Datensicherheitsverantwortlichen.[66] Viele der Zertifizierungsvoraussetzungen wurden gar von der ISO/IEC 27001 übernommen,[67] welche eine internationale Norm zur Zertifizierung von sogenannten Informationssicherheitsmanagementsystemen (ISMS) darstellt. Gemäss ISO/IEC 27001:2013 Ziff. 0.1 bewahrt ein Informationssicherheitsmanagementsystem die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, indem Risikomanagementprozesse angewendet werden, und vermittelt interessierten Dritten auf diese Weise Vertrauen, dass Risiken angemessen berücksichtigt werden.[68] In der Schweiz ist eine Zertifizierung nach dieser Norm recht häufig, sodass eine Anerkennung von bereits bestehenden ISO/IEC 27001 Zertifizierungen allenfalls Vorteile bei der Zertifizierung hätte bringen können.

[Rz 33] Eine weitere bekannte und verbreitete Norm ist die Verordnung über die Datenschutzzertifizierungen (VDSZ), welche im Gegensatz zur ISO/IEC 27001 keine internationale sondern eine Schweizer Norm darstellt. Private Personen oder Bundesorgane, die Personendaten bear-

64 Art. 29 Abs. 2 EPDV.

65 Siehe Kapitel 4.3.

66 Ziff. 4.3 TOZ.

67 So beispielsweise die Einführung eines «Incident Managements» (Ziffer 4.4 ff. TOZ und Control A.16 ISO/IEC 27001:2013), die Verwaltung kryptographischer Schlüssel (Ziffer 1.8 TOZ und Control A.10.1.2 ISO/IEC 27001:2013) oder die Durchführung eines jährlichen Management Reviews (Ziffer 4.2.4 TOZ und Ziffer 9.2 ISO/IEC 27001:2013).

68 Freie Übersetzung aus dem Englischen: «*The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed*».

beiten, können ihre Systeme, Verfahren und ihre Organisation (sogenannte Datenschutzmanagementsysteme oder DSMS) einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.[69] Der Kanton Zürich beispielsweise anerkennt die freiwillige Zertifizierung seiner öffentlichen Organe nach der VDSZ und verspricht sich dadurch eine Qualitätssicherung.[70] Seit dem 1. Januar 2013 sind die sozialen Krankenversicherer gar gesetzlich verpflichtet, ihre Datenannahmestellen für den Empfang und die Verarbeitung von SwissDRG-Rechnungen nach der VDSZ zertifizieren zu lassen.[71] Die VDSZ übernimmt in weiten Teilen die Zertifizierungsvoraussetzungen der ISO/IEC 27001[72], auch wenn die Begriffe der Informationssicherheit und des Datenschutzes nicht identisch sind. Gemäss den Richtlinien des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten muss bei der Anwendung der VDSZ der Begriff Informationssicherheit durch den Begriff Datenschutz ersetzt werden.[73] Das bedeutet, dass die Voraussetzungen an ein ISMS nach der ISO/IEC 27001 (fast) unverändert auch für die Zertifizierung eines DSMS nach der VDSZ anwendbar sind.[74]

[Rz 34] Sowohl die ISO/IEC 27001 als auch die VDSZ sind branchenneutral formuliert[75], was bedeutet, dass jedes ISMS bzw. DSMS einer beliebigen Organisation damit zertifiziert werden kann. Es wäre daher möglich und allenfalls sogar von Vorteil gewesen, im Ausführungsrecht zum EPDG eine Zertifizierung der Gemeinschaften und Stammgemeinschaften bzw. ihrer entsprechenden Managementsysteme nach einer der zwei etablierten und geprüften Zertifizierungsnormen vorzusehen. Insbesondere hätte auf die (nur teilweise und lückenhafte) Übernahme von ISO/IEC 27001 Anforderungen in die TOZ verzichtet werden können. Zudem bestehen bereits für diese Normen akkreditierte Zertifizierungsstellen[76], was einer Beschleunigung des Zertifizierungsvorgangs wohl zuträglich wäre.

4.2. Die Zertifizierungsvoraussetzungen

4.2.1. «Datenschutz- und Datensicherheitsmanagementsystem»

[Rz 35] Da auf eine Anerkennung einer bestehenden Zertifizierungsnorm verzichtet wurde, stellen die TOZ eigene Zertifizierungsvoraussetzungen auf, auch in Bezug auf die Gewährleistung des Datenschutzes und der Datensicherheit. Gemäss Art. 11 Abs. 1 EPDV müssen Gemeinschaf-

69 Art. 11 Abs. 1 DSG, genauere Informationen zu der Zertifizierung nach VDSZ lassen sich finden unter: David Rosenthal, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 11; Gabor P. Blechta, in: Urs Maurer-Lambrou/Gabor-Paul Blechta, Balser Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Auflage, Basel 2014, Art. 11 DSG.

70 Zu finden unter https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/weitere_themen/datenschutzmanagementsystem_und_zertifizierung/_jcr_content/contentPar/downloadlist_1/downloaditems/1_1380089283046.spooler.download.1380089109140.pdf/Merkblatt_Zertifizierung.pdf (Website zuletzt besucht am 6. August 2016).

71 Art. 59a Abs. 6 KVV.

72 Siehe Art. 3 Richtlinie über die Mindestanforderungen an ein Datenschutzmanagementsystem vom 16. Juli 2008.

73 Ziffer 3 der Richtlinien über die Mindestanforderungen an ein Managementsystem vom 19. März 2014 (Richtlinien über die Zertifizierung von Organisation und Verfahren), zu finden unter https://www.edoeb.admin.ch/datenschutz/00756/00974/index.html (Website zuletzt besucht am 6. August 2016).

74 Blechta, BSK DSG, Art. 11 DSG N 10.

75 Siehe Fn 53.

76 Die akkreditierten Stellen können über die Suchmaske der SAS aufgerufen werden unter https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas.html (Website zuletzt besucht am 6. August 2016).

ten und Stammgemeinschaften ein Datenschutz- und Datensicherheitsmanagementsystem betreiben, welches insbesondere folgende Elemente umfasst:

a. die Benennung eines oder einer Datenschutz- und Datensicherheitsverantwortlichen;
b. ein System zur Erkennung von und zum Umgang mit Sicherheitsvorfällen;
c. ein Verzeichnis der Datenablagen;
d. ein Verzeichnis der angeschlossenen Primärsysteme;
e. die Datenschutz- und Datensicherheitsvorgaben für die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen;
f. die Datenschutz- und Datensicherheitsanforderungen an das Personal und Dritte.

[Rz 36] Die TOZ wiederholen diese Anforderungen, indem sie vorschreiben, dass ein Datenschutz- und Datensicherheitsmanagementsystem betrieben werden muss, wie es in der ISO/IEC 27001:2013 definiert wird.[77] Zudem wird definiert, dass dieses Managementsystem mindestens einen Risikokatalog, einen Risikobehandlungsplan und ein aktuell gehaltenes Inventar einiger definierter Betriebsmittel enthalten muss.

[Rz 37] Diese Regelung kann in der praktischen Umsetzung zu Problemen führen, da mit der ISO/IEC 27001:2013 Informationssicherheitsmanagementsysteme zertifiziert werden und die Norm dementsprechend keine Definition eines «Datenschutz- und Datensicherheitsmanagementsystems» enthält. Zwar können Datenschutzmanagementsysteme nach der VDSZ zertifiziert werden, gemäss derer die Anforderungen der ISO/IEC 27001 ja eingehalten werden müssen, allerdings stellt ein DSMS nur eine Teilmenge eines ISMS dar.[78]

[Rz 38] Weitere Unklarheiten ergeben sich zudem aus den Anforderungen der EPDV und der TOZ an ein «Datenschutz- und Datensicherheitsmanagementsystem», denn nach dem heutigen Verständnis eines DSMS ist diese Auflistung der Anforderungen unvollständig. Unter anderem fehlt die Verpflichtung der Gemeinschaften und Stammgemeinschaften, eine Datenschutzpolitik[79], welche die Grundlage eines DSMS[80] bildet, zu führen und diese umzusetzen.

[Rz 39] Diese missverständlichen Anforderungen an ein «Datenschutz- und Datenschutzmanagementsystem» nach Art. 11 Abs. 1 EPDV und Ziffer 4.2.1 TOZ wurde auch in der Vernehmlassung kritisiert und werden wohl bei der Überarbeitung des Ausführungsrechts zu verbessern sein.[81] Sollte der Bundesrat bzw. das EDI sich für die Anerkennung der VDSZ oder der ISO/IEC 27001 entscheiden, so müssten die Gemeinschaften und Stammgemeinschaften ohnehin ein DSMS bzw. ein ISMS gemäss der entsprechenden Norm aufbauen, da diese die Grundlage für eine Zertifizie-

77 Ziffer 4.2.1 TOZ.

78 Schweizerische Vereinigung für Qualitäts- und Managementsysteme (SQS), Formular für Stellungnahme zur Anhörung Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG vom 28. Juni 2016, S. 16, zu finden unter http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/16000/16135/index.html?lang=de (Website zuletzt besucht am 6. August 2016); Diese Aussage ist so zu verstehen, dass der Geltungsbereich eines DSMS, welcher ausschliesslich die Personendaten gemäss Art. 3 lit. a DSG umfasst, kleiner ist als derjenige eines ISMS, welcher sich auf alle Informationen und Daten einer Organisation bezieht.

79 Art. 4 Abs. 2 lit. a VDSZ.

80 Blechta, BSK DSG, Art. 11 DSG N 8.

81 Schweizerische Vereinigung für Qualitäts- und Managementsysteme, Grundsätzliche Überlegungen der Stellungnahme zu Zertifizierung, Zertifizierungsverfahren und Akkreditierung als Zertifizierungsstelle im Ausführungsrecht zum EPDG, S. 1, zu finden unter http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/16000/16135/index.html?lang=de (Website zuletzt besucht am 6. August 2016).

rung sind.[82]Auch ohne Anerkennung einer der beiden Normen wäre es allerdings nach der hier vertretenen Meinung vorteilhaft, die Gemeinschaften und Stammgemeinschaften entweder zum Aufbau eines DSMS nach der VDSZ oder eines ISMS nach der ISO/IEC 27001 zu verpflichten und bezüglich der Anforderungen auf die entsprechende Norm zu verweisen.

[Rz 40] Dies würde zu einer Verschlankung der TOZ führen, da einerseits die Definition der Mindestanforderungen an das Datenschutz- und Datensicherheitsmanagementsystem wegfallen würde. Andererseits enthalten die TOZ weitere Zertifizierungsvoraussetzungen, wie beispielsweise das Führen eines «Security Information and Event Management Systems» (SIEM)[83], welche als integrale Bestandteile eines DSMS bzw. eines ISMS ohnehin erfüllt werden müssen.

4.2.2. Technische Anforderungen

[Rz 41] Neben den Anforderungen an den Datenschutz und die Datensicherheit enthalten die TOZ unter anderem Regelungen über die technische Umsetzung des elektronischen Patientendossiers. So bestimmen beispielsweise die Ziffern 3.4 und 3.5 der TOZ (i.V.m. Anhang 3 der EPDV-EDI über die Metadaten), welche Dateiformate das Zugangsportal für Gesundheitsfachpersonen für den Abruf und die Bereitstellung von Daten zulassen muss, während Ziffer 2.9 TOZ die anzuwendenden Integrationsprofile für den Datenaustausch festlegt. In dieser Hinsicht gleichen die TOZ eher einer Swissdec-Zertifizierung von Lohnbuchhaltungen.[84]Im Gegensatz zur Zertifizierung eines DSMS wird hier nicht kontrolliert, ob die notwendigen Prozesse und Systeme aufgesetzt sind und umgesetzt werden, um die relevanten gesetzlichen Verpflichtungen einzuhalten, sondern es wird konkret überprüft, ob das elektronische Patientendossier bestimmte Eigenschaften besitzt und Funktionen aufweist, um den gemeinschaftsinternen und gemeinschaftsübergreifenden Datenaustausch zu garantieren. Bei der Überprüfung der technischen Voraussetzungen wird somit faktisch getestet, ob die Systeme der Gemeinschaften und Stammgemeinschaften zu der notwendigen Interoperabilität fähig sind und insbesondere ob die gemeinschaftsübergreifende Kommunikation ermöglicht wird.

[Rz 42] Der Bundesrat sah hierfür in der Botschaft ein Testsystem vor, mit welchem hätte überprüft werden können, ob eine Gemeinschaft oder Stammgemeinschaft die Zertifizierungsvoraussetzungen in Art. 12 Abs. 1 lit. a EPDG erfüllt.[85] Damit sollten die technischen Schnittstellen der Gemeinschaften und Stammgemeinschaften und die Kommunikation mit den Abfragediensten geprüft werden.[86] Das Ausführungsrecht hat diese Idee allerdings nicht aufgenommen, sodass zumindest in der aktuell vorliegenden Version der TOZ kein Testsystem für die Zertifizierung vorgesehen ist. Dies ist zu bedauern, da dadurch die Überprüfung und allfällige Zertifizierung hätte erheblich erleichtert werden können.

[Rz 43] In der Vernehmlassung wurde von unterschiedlichen Stellen die Kritik geäussert, dass insbesondere die technischen Anforderungen zu detailliert sind und so die Möglichkeit von innova-

82 Nicole Beranek Zanon, Eckpunkte von Datenschutz-Managementsystemen (DSMS), in: Rolf H. Weber/Florent Thouvenin, Datenschutz-Managementsysteme im Aufwind?, Zürich/Basel/Genf 2016, S. 52.

83 Siehe ISO/IEC 27001:2013 A.16.

84 Siehe Kapitel 3.3.

85 BBl 2013 5321, 5386.

86 BBl 2013 5321, 5386.

tiven Entwicklungen unterdrückt wird.[87] Dieser Meinung wird hier gefolgt. Gemeinschaften und Stammgemeinschaften sind auf den funktionierenden Datenaustausch, sowohl gemeinschaftsintern wie auch gemeinschaftsübergreifend, angewiesen, weshalb eine grundsätzliche Normierung notwendig ist. Allerdings besteht auch gerade aufgrund der notwendigen Interoperabilität ein grosses Potenzial an innovativen Entwicklungen und Lösungen, da sich die einzelnen Gemeinschaften und Stammgemeinschaften von den Konkurrenten abheben können müssen. Werden potentielle Innovationen durch enge gesetzliche Regelungen und Normierungen verhindert, wird auch das Entstehen eines Wettbewerbs auf dem Markt verunmöglicht.

[Rz 44] Auch in dieser Hinsicht wäre allenfalls die Einführung eines Testsystems von Vorteil. Die notwendige Interoperabilität könnte technisch wohl über mehrere Wege erreicht werden. Die Konformität der technischen Umsetzung der einzelnen Gemeinschaften und Stammgemeinschaften könnte in diesem Fall durch ein übergeordnetes Testsystem sichergestellt werden. Nach der hier vertretenen Auffassung wäre es vorteilhaft, solche oder andere Alternativen unter Beizug von Experten zu prüfen. Es ist auf jeden Fall zu hoffen, dass bei der Überarbeitung des Ausführungsrechts auf diese Kritik eingegangen wird und die TOZ entsprechend reduziert werden.

4.2.3. Kontrolle der Rechtskonformität

[Rz 45] In weiten Teilen verpflichten die TOZ die Gemeinschaften und Stammgemeinschaften indirekt zur Einhaltung ihrer gesetzlichen Pflichten, indem Anforderungen an die Umsetzung gegeben werden. Dies lässt sich an Art. 8 lit. a EPDV veranschaulichen. Während die Gemeinschaften und Stammgemeinschaften darin zur Regelung des Eintritts und des Austritts der Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen verpflichtet werden, wiederholt Ziffer 1.1.1 TOZ diese Pflicht folgendermassen: «*Die Prozesse für den Eintritt und den Austritt von Gesundheitseinrichtungen müssen definiert, dokumentiert, umgesetzt und eingehalten werden.*» Die beiden Bestimmungen sind inhaltlich (fast) identisch. Während Art. 8 lit. a EPDV die Gemeinschaften und Stammgemeinschaften jedoch direkt zur Regelung des Ein- und Austritts verpflichtet, ist diese Pflicht in den TOZ nur eine indirekte, indem im Rahmen der Zertifizierungen überprüft werden muss, ob die entsprechenden Prozesse aufgesetzt sind und umgesetzt werden.

[Rz 46] Auf den ersten Blick fällt beim genannten Beispiel zudem auf, dass während die EPDV noch von «Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen» spricht, die TOZ nur noch den Begriff der «Gesundheitseinrichtung» verwenden. Es kann wohl davon ausgegangen werden, dass diese Inkongruenz ein Versehen auf Seiten des EDI war und die Gemeinschaften und Stammgemeinschaften entgegen dem Wortlaut der TOZ auch für den Eintritt und den Austritt der Gesundheitsfachpersonen und der Gruppen von Gesundheitsfachpersonen Prozesse aufstellen müssen. Solche begriffliche Ungenauigkeiten erschweren aber das Verständnis der TOZ und würden wohl in der Umsetzung viele Fragen aufwerfen.

---

87 Unter mehreren: Kanton Zürich in seiner Stellungnahme zum Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier vom 22. Juni 2016, S. 4 zu finden unter http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/16000/16130/index.html?lang=de (Website zuletzt besucht am 6. August 2016); Die Schweizerische Post AG in ihrer Stellungnahme zum Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier vom 28. Juni 2016, S. 1 f., zu finden unter http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/16000/16135/index.html?lang=de (Website zuletzt besucht am 6. August 2016).

[Rz 47] Indem die TOZ die Gemeinschaften und Stammgemeinschaften in solcher Weise dazu verpflichten, Prozesse und Systeme zu definieren und umzusetzen, könnte der Schluss gezogen werden, dass auch hier ein Managementsystem auditiert und zertifiziert werden soll. Die gesetzliche Pflicht, entsprechende Prozesse aufzusetzen, ergibt sich allerdings bereits aus den direkten Normen der EPDV. Nach der hier vertretenen Meinung ist es unnötig, die Gemeinschaften und Stammgemeinschaften in den TOZ zur Implementierung von Prozessen und Systemen zu verpflichten, um die Umsetzung der EPDG und der EPDV sicherzustellen. Oder anders formuliert: Es ist nicht nachvollziehbar, wieso die TOZ den Gemeinschaften und Stammgemeinschaften vorschreibt, Prozesse für den Eintritt und Austritt von Gesundheitseinrichtungen (sowie Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen) zu definieren, wenn die EPDV ihnen diese Pflicht bereits auferlegt. Dadurch werden die Zertifizierungsstellen faktisch zu einer vorgezogenen Überprüfung der Rechtskonformität des Handelns der Gemeinschaften und Stammgemeinschaften verpflichtet. Zertifizierungsstellen kann nicht zugemutet werden, alle relevanten rechtlichen Anforderungen zu kennen und beurteilen zu können, ob diese gesetzeskonform umgesetzt werden. Hinzu kommt, dass eine rechtliche Beurteilung und entsprechende Weisung durch einen Vertreter einer Zertifizierungsstelle einer beratenden Tätigkeit gleichkommt, was in den Akkreditierungsvoraussetzungen teilweise als «Selbstbewertung» und daher als Gefährdung der Unparteilichkeit der Zertifizierungsstelle betrachtet wird.[88]

[Rz 48] Eine Überprüfung, ob die Gemeinschaften und Stammgemeinschaften alle relevanten gesetzlichen Grundlagen einhalten, geht somit über die Kompetenzen der Zertifizierungsstelle bzw. ihrer Vertreter hinaus.[89]

[Rz 49] Durch die Wiederholungen der Pflichten in der EPDV werden die TOZ unnötig umfangreich und unübersichtlich, wie dies auch verschiedentlich in der Vernehmlassung kritisiert wurde.[90]Die Überprüfung, ob gesetzliche Verpflichtungen eingehalten werden, darf nicht Privaten, d.h. den Zertifizierungsstellen, übertragen werden, sondern ist allenfalls Teil der Überwachungsaufgabe des BAG. Grundsätzlich sind allfällige Verstösse gegen die gesetzlichen Grundlagen des elektronischen Patientendossiers vor Gericht zu behandeln und es ist nicht ersichtlich, wieso in diesem Fall die nachträgliche gerichtliche Kontrolle nicht möglich sein soll.

4.3. Entflechtung der Zertifizierungsvoraussetzungen

[Rz 50] Aus den vorherigen Ausführungen geht hervor, dass die TOZ somit drei unterschiedliche Arten von Voraussetzungen enthält: Solche an ein Datenschutzmanagementsystem, solche an die erforderlichen technischen Anforderungen an den Datenaustausch sowie die Verpflichtung, Prozesse und Systeme umzusetzen, anhand derer die gesetzlichen Pflichten des EPDG und der EPDV eingehalten werden. Bei einer Zertifizierung einer Gemeinschaft oder Stammgemeinschaft nach der aktuellen Version der TOZ müssten daher drei unterschiedliche Arten von Zertifizierungen gleichzeitig erfolgen.

[Rz 51] Die EPDV und die EPDV-EDI lassen allerdings darauf schliessen, dass bei der Ausarbeitung der Zertifizierungsvoraussetzungen von einer reinen Zertifizierung von Managementsyste-

88 Siehe unter anderem Ziffer 4.2.4.c ISO/IEC 17021-1; siehe Fn 43.

89 Kanton Zürich in seiner Stellungnahme zum Ausführungsrecht EPDG, S. 3.

90 Unter mehreren: Kanton Zürich in seiner Stellungnahme zum Ausführungsrecht EPDG, S. 3.

men ausgegangen wurde. So verlangt Anhang 7 der EPDV-EDI[91], dass das Zertifizierungspersonal über Kenntnisse der Medizininformatik, des Datenschutzrechts und im Bereich der Informatiksicherheit verfügen muss, wobei dieses Fachwissen auf eine Mehrzahl von Personen aufgeteilt werden kann.[92] Die Auditoren müssen zudem Ausbildungen nach ISO/IEC 17021 und ISO/IEC 27006 nachweisen können. Diese beiden ISO-Normen bilden die Akkreditierungsvoraussetzungen für die Stellen, die Managementsysteme bzw. Informationssicherheitsmanagementsysteme zertifizieren.

[Rz 52] Dabei wird verkannt, dass ein Auditorenteam mit Kenntnissen in den Bereichen Medizininformatik, Datenschutzrecht und Informatiksicherheit zwar kompetent ist, ein DSMS bzw. ein ISMS zu überprüfen und allenfalls zu kontrollieren, ob die notwendigen Integrationsprofile verwendet werden. Jedoch fehlt ihm vermutlich dennoch das notwendige Wissen, um eine EPDG-spezifische Normenkontrolle vornehmen zu können. Durch eine Zertifizierung eines Managementsystems kann ausschliesslich bestätigt werden, dass eine Organisation über die notwendigen Prozesse und Systeme verfügt, um Risiken zu erkennen sowie angemessen und systematisch zu managen.

[Rz 53] Nach der hier vertretenen Meinung müssen daher die unterschiedlichen Voraussetzungen an die Gemeinschaften und Stammgemeinschaften in den TOZ entflochten werden. Einerseits würde bereits die Anerkennung eines VDSZ oder ISO/IEC 27001 Zertifikats in der EPDV das Zertifizierungsverfahren erheblich erleichtern. Dadurch würden in einem ersten Schritt jegliche Voraussetzungen der TOZ, die sich auf den Datenschutz und die Datensicherheit beziehen, wegfallen.

[Rz 54] Ausserdem wäre es möglich, Bestimmungen der TOZ, die ausschliesslich Wiederholungen der Pflichten in den Art. 8–20 EPDV sind, ebenfalls zu entfernen bzw. diese als direkte Verpflichtungen in die EPDV aufzunehmen. Die tatsächlich notwendigen technischen Voraussetzungen werden in diesem Fall weiterhin in den TOZ definiert, allerdings ist hier der Meinung der Schweizerischen Vereinigung für Qualitäts- und Managementsysteme zu folgen, die in der Vernehmlassung den Antrag stellte, die TOZ in «Technische und organisatorische Voraussetzungen an die Gemeinschaften und Stammgemeinschaften» umzubenennen.[93] Zudem wird darauf verwiesen, dass die Einhaltung der technischen Vorgaben und die Interoperabilität allenfalls durch ein allgemein gültiges Testsystem überprüft werden können, wie dies bereits in der Botschaft vorgeschlagen wurde.[94]

4.4. Überwachung durch die akkreditierte Zertifizierungsstelle

[Rz 55] Gemeinschaften und Stammgemeinschaften müssen die im Datenschutz- und Datensicherheitsmanagementsystem als sicherheitsrelevant eingestuften Vorfälle der Zertifizierungsstelle und dem BAG melden[95], womit die Zertifizierungsstelle somit neben dem BAG als Überwachungsbehörde eingesetzt wird. Dabei wird verkannt, dass eine Zertifizierungsstelle nach dem

91 Ziffer 1.1.4 und 1.1.5 Anhang 7 EPDV-EDI (Mindestanforderungen an die Qualifikation der Angestellten der Zertifizierungsstellen).

92 Ziffer 1.1.1-1.1.3 Anhang 7 EPDV-EDI.

93 SQS, Grundsätzliche Überlegungen der Stellungnahe, S. 3.

94 Siehe Kapitel 4.2.2.

95 Art. 11 Abs. 2 EPDV.

heutigen Verständnis gerade keine Überwachungstätigkeit ausübt, sondern im Rahmen von periodischen Überprüfungen, wiederum als Momentaufnahme, feststellt, ob die Zertifizierungsvoraussetzungen weiterhin gegeben sind. Allfällige sicherheitsrelevante Vorfälle müssen während der nächsten periodischen Überprüfung besprochen werden. Meldepflichten bestehen hier allerdings grundsätzlich keine.

[Rz 56] Die EPDV räumt den Zertifizierungsstellen das Recht ein, Zertifikate zu sistieren oder zu entziehen, falls im Rahmen der jährlichen Überprüfung schwere Mängel festgestellt werden.[96] Eine entsprechende Handlungsmöglichkeit kommt ihr nach der aktuellen Fassung der EPDV allerdings nicht zu, wenn sicherheitsrelevante Vorfälle gemeldet werden. Die Entscheidungskompetenz wird hier allein dem BAG überlassen, welches die Zertifizierungsstelle über eine allfällige Sistierung oder einen Entzug des Zertifikats wohl zu informieren hat. Die Zertifizierungsstelle erfährt somit in jedem Fall, wenn auch meist nachträglich, von sicherheitsrelevanten Vorfällen, wobei eine zeitnahe Meldung allein an das BAG als tatsächliche Aufsichtsbehörde erfolgen muss. Eine Meldung an die Zertifizierungsstelle, wie sie in Art. 11 Abs. 2 EPDV vorgesehen ist, wird aufgrund der Überwachungstätigkeit des BAG daher redundant und würde für die Zertifizierungsstellen nur einen unnötigen administrativen Aufwand bedeuten.

5. Weitere offene Fragen

[Rz 57] Obwohl das Ausführungsrecht zum EPDG sehr umfangreich ist, werden einige essentielle Fragen nicht thematisiert. Aus Sicht der Zertifizierungen stellt sich unter anderem die Frage der Kompetenzaufteilung zwischen dem BAG als Überwachungsbehörde und den Zertifizierungsstellen und hier insbesondere, inwiefern das BAG in das privatrechtliche Verhältnis[97] zwischen den zertifizierten Gemeinschaften und Stammgemeinschaften und der Zertifizierungsstelle eingreifen darf. Die Zertifizierungsstelle entscheidet grundsätzlich über die Vergabe der Zertifikate sowie deren Sistierung und Entzug, falls sie im Rahmen der jährlichen Überprüfung schwere Mängel feststellt.[98] Zudem kann sie (ausserordentliche) Rezertifizierungen anordnen, wenn die Gemeinschaft oder Stammgemeinschaft ihr wesentliche technische oder organisatorische Änderungen meldet.

[Rz 58] Das BAG wiederum darf unter anderem eine ausserordentliche Rezertifizierung anordnen, wenn eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vorliegt.[99] Besteht der begründete Verdacht, dass eine zertifizierte Gemeinschaft oder Stammgemeinschaft die Zertifizierungsvoraussetzungen nicht einhält, kann das BAG zudem eine Überprüfung durch die Zertifizierungsstelle anordnen, die Gültigkeit des Zertifikats aussetzen oder das Zertifikat entziehen.

[Rz 59] Zertifizierungsstellen sind somit zum Entzug bzw. zur Sistierung von Zertifikaten berechtigt, wenn bei der jährlichen Überprüfung Mängel festgestellt werden, während dem BAG diese Kompetenz unter gewissen Voraussetzungen immer zukommt. Rezertifizierungen dürfen durch die Zertifizierungsstelle vorgenommen werden, wenn die zertifizierte Gemeinschaft oder Stamm-

96 Art. 37 Abs. 1 EPDV.

97 Art. 37 Abs. 2 EPDV.

98 Art. 37 Abs. 1 EPDV.

99 Art. 36 lit. c EPDV.

gemeinschaft Änderungen vorgenommen hat, die eine erneute und ausserplanmässige Überprüfung rechtfertigen. Dem BAG kommt diese Kompetenz erst zu, wenn eine konkrete Gefahrensituation für die Integrität und Verbrauchlichkeit der medizinischen Daten besteht.

[Rz 60] Problematisch ist hier, dass der Zertifizierungsvertrag zwischen den Gemeinschaften und Stammgemeinschaften und den Zertifizierungsstellen privatrechtlicher Natur ist. Das BAG benötigt eine genügende gesetzliche Grundlage, um in dieses Vertragsverhältnis einzugreifen, andernfalls das Legalitätsprinzip[100] verletzt wird. Das EPDG sieht ausschliesslich vor, dass der Bundesrat die Voraussetzungen für den Entzug der Zertifikate regelt[101], ermächtigt ihn jedoch nicht zur Regelung der entsprechenden Kompetenzen. Nach der hier vertretenen Meinung müsste daher überprüft werden, ob das BAG eine genügende gesetzliche Grundlage besitzt, um bestehende Zertifikate zu sistieren oder zu entziehen bzw. um Rezertifizierungen anzuordnen.[102]

[Rz 61] Nicht nur die Kompetenz für die Sistierung und den Entzug der Zertifikate ist ungenau geregelt. Das Ausführungsrecht zum EPDG lässt zudem die wichtige Frage offen, welche Folgen eine Suspendierung oder der Entzug für die angeschlossenen Gesundheitsfachpersonen bzw. Gesundheitseinrichtungen hat. Diese Frage ist insbesondere für die Spitäler und Geburtshäuser von grosser Bedeutung, da sie sich zwingendermassen einer zertifizierten Gemeinschaft oder Stammgemeinschaft anschliessen müssen, wenn sie zu Lasten der obligatorischen Krankenpflegeversicherung Leistungen erbringen wollen. Nach der «Taschenstatistik der Kranken- und Unfallversicherung» aus dem Jahr 2015 des Bundesamtes für Gesundheit rechneten die Spitäler im Jahr 2014 ambulante und stationäre Leistungen zu Lasten der OKP im Bruttoumfang von CHF 10'853 Mio. ab.[103] Aus dieser Zahl geht bereits hervor, welche gravierenden finanziellen Folgen ein Spital zu tragen hat, sollte ihm die Kostenvergütung durch die OKP verwehrt bleiben. Insbesondere sind die Spitäler und Geburtshäuser von der Zertifizierung eines Dritten, d.h. der Gemeinschaft oder Stammgemeinschaft, abhängig, für deren Handeln sie nicht verantwortlich sind. Eine gesetzliche Regelung der Folgen einer Suspendierung oder des Entzugs eines Zertifikats ist daher nach der hier vertretenen Meinung dringend zu treffen.

6. Zusammenfassende Würdigung

[Rz 62] Der Gesetzgeber verspricht sich von der Einführung des elektronischen Patientendossiers eine Steigerung der Effizienz im Gesundheitswesen, indem die behandelnden und berechtigten Gesundheitsfachpersonen orts- und zeitunabhängig auf die relevanten medizinischen Daten ihrer Patienten zugreifen können. Um das Vertrauen der Patienten in das elektronische Patientendossier zu steigern sowie um eine notwendige Interoperabilität zwischen allen Systemen und Akteuren sicherzustellen, sieht das EPDG eine Zertifizierung unter anderem für die Gemeinschaften und Stammgemeinschaften vor. Die entsprechenden Voraussetzungen wurden im Anhang 2 zur EPDV-EDI («Technische und organisatorische Zertifizierungsvoraussetzungen an die Gemeinschaften und Stammgemeinschaften» oder «TOZ») festgelegt.

---

100 Art. 5 Abs. 1 Bundesverfassung der Schweizerischen Eidgenossenschaft.

101 Art. 13 Abs. 1 lit. c EPDG.

102 Siehe auch SQS, Grundsätzliche Überlegungen der Stellungnahme zum Ausführungsrecht zum EPDG, S. 5.

103 Zu finden unter http://www.bag.admin.ch/themen/krankenversicherung/01156/index.html?lang=de (Website zuletzt besucht am 6. August 2016).

[Rz 63] Die TOZ sind darauf ausgerichtet, dass die Gemeinschaften und Stammgemeinschaften im Rahmen einer Auditierung eines Managementsystems zertifiziert werden. Nach dem gängigen Verständnis wird dabei geprüft, ob die durch die entsprechende Zertifizierungsnorm vorgegebenen Elemente vorhanden sind und durch die Einführung von Prozessen systematisch aufrechterhalten und betrieben werden. Eine Überprüfung, ob gesetzliche Bestimmungen im Einzelfall eingehalten werden, wird dabei nicht vorgenommen. Die TOZ enthalten jedoch unglücklicherweise nicht nur Anforderungen an ein Managementsystem sondern auch technische Voraussetzungen an das elektronische Patientendossier und verpflichten die Zertifizierungsstellen zudem in weiten Teilen zu einer Kontrolle der Rechtskonformität der Gemeinschaften und Stammgemeinschaften. Dies führt nicht nur dazu, dass die TOZ sehr umfangreich sind, sondern wirft für die akkreditierten Zertifizierungsstellen insbesondere die Frage auf, wie sie Zertifizierungsvoraussetzungen auditieren müssen, deren Prüfung über ihre eigentlichen Kompetenzbereich hinausgeht.

[Rz 64] Da im Rahmen des elektronischen Patientendossiers sensitive medizinische Daten bearbeitet werden, kommt der Gewährleistung des Datenschutzes und der Datensicherheit eine hohe Bedeutung zu, weshalb ein gewichtiger Teil der TOZ diesem Bereich gewidmet ist. Hier hätte der Bundesrat gemäss Art. 13 Abs. 1 lit. d EPDG die Möglichkeit gehabt, bereits bestehende Zertifizierungsnormen, wie die Verordnung über die Datenschutzzertifizierung (VDSZ) oder die ISO/IEC 27001, mit welcher Datenschutzmanagementsysteme bzw. Informationssicherheitsmanagementsysteme zertifiziert werden, als anwendbar zu erklären. Bedauerlicherweise wurde von dieser Möglichkeit nicht Gebrauch gemacht. Die TOZ verweist zwar auf die ISO/IEC 27001, indem sie vorschreibt, dass Gemeinschaften und Stammgemeinschaften ein Datenschutz- und Datensicherheitsmanagementsystem nach der ISO/IEC 27001 betreiben müssen. Allerdings enthält diese Norm keine entsprechende Begriffsdefinition, was in der Umsetzung daher wohl zu mehr Problemen als Klarheit führen wird.

[Rz 65] Entsprechend umfangreich fiel auch die Kritik in der Vernehmlassung aus. Es ist zu hoffen, dass bei der Überarbeitung des Ausführungsrechts zum EPDG auf diese Kritik eingegangen und insbesondere auch darauf geachtet wird, die Voraussetzungen an die Akkreditierung und die Zertifizierung zu vereinfachen und an bereits bestehende nationale und internationale Normen anzupassen sowie noch bestehende offene Fragen zu behandeln. Nach der hier vertretenen Meinung sollte im Rahmen der Überarbeitung des Ausführungsrechts zum EPDG unter anderem unbedingt erhoben werden, welche Voraussetzungen der TOZ tatsächlich als Zertifizierungsvoraussetzungen taugen und welche Voraussetzungen ausschliesslich im Rahmen einer technischen Prüfung kontrolliert werden können. Anderweitige Elemente der TOZ sind gar als direkte gesetzliche Pflichten in der EPDV aufzunehmen und deren Prüfung im Falle einer Widerhandlung den Gerichten zu überlassen.

[Rz 66] Aufgrund der erschwerten Umsetzbarkeit der EPDV und der TOZ ist es zweifelhaft, ob die bezweckte Effizienzsteigerung im Gesundheitswesen auch tatsächlich erreicht werden kann. Das elektronische Patientendossier bringt tatsächlich ein enormes Verbesserungspotential in der medizinischen Versorgung, was allerdings nicht durch unnötig enge und komplizierte gesetzliche Regelungen verhindert werden darf. Die Akkreditierung der Zertifizierungsstellen und die darauffolgenden Zertifizierung der Gemeinschaften und Stammgemeinschaften sind die ersten Schritte in der Umsetzung des elektronischen Patientendossiers. Eine Vereinfachung dieser Etappen könnte einen positiven Einfluss auf die darauffolgende Verwendung und Verbreitung des elektronischen Patientendossiers haben.

Sarah Winkler, MLaw, schloss ihr Rechtsstudium an der Universität Zürich im Jahr 2016 ab und bearbeitet seit Februar 2016 im Rahmen einer Dissertation das Thema des elektronischen Patientendossiers. Bereits seit 2010 arbeitet sie bei der IT&Law Consulting GmbH in Zug und ist seit August 2016 als Dozentin an der Fernfachhochschule Schweiz angestellt.