Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Erläuterungen zur

Verordnung über das elektronische Patientendossier (EPDV)

Fassung vom 22. März 2016

Inhaltsverzeichnis

1 Allgemeiner Teil

1.1 Ausgangslage

Das Parlament hat das Bundesgesetz über das elektronische Patientendossier (EPDG, SR 816.11, BBl 2015 4865) am 19. Juni 2015 verabschiedet. Als Rahmengesetz regelt das EPDG die Voraussetzungen für die Bearbeitung der Daten des elektronischen Patientendossiers. Damit wird eine zentrale Voraussetzung für die erfolgreiche Umsetzung der «Strategie eHealth Schweiz» erfüllt und eine wichtige Massnahme für die Weiterentwicklung des Schweizer Gesundheitssystems umgesetzt.

Gegenstand
Das EPDG legt die Rahmenbedingungen für die Bearbeitung von Daten und Dokumenten im Rahmen des elektronischen Patientendossiers fest. Dieses soll die Qualität der medizinischen Behandlung stärken, die Behandlungsprozesse verbessern, die Patientensicherheit erhöhen, die Effizienz des Gesundheitssystems steigern sowie die Gesundheitskompetenz von Patientinnen und Patienten fördern. Die als Rahmengesetz ausgestaltete Vorlage soll einerseits zu Investitionssicherheit führen und andererseits gleichzeitig ausreichend Flexibilität bei der Umsetzung in den Versorgungsregionen ermöglichen.

Mit Hilfe des elektronischen Patientendossiers können Gesundheitsfachpersonen auf behandlungsrelevante Daten ihrer Patientinnen und Patienten, die von anderen am Behandlungsprozess beteiligten Gesundheitsfachpersonen erstellt und dezentral erfasst wurden, zugreifen und diese allenfalls in ihren Praxis- und Klinikinformationssystemen ausserhalb des elektronischen Patientendossiers speichern. Sie müssen sich hierzu einer zertifizierten Gemeinschaft oder Stammgemeinschaft - einem Zusammenschluss von Gesundheitsfachpersonen und deren Einrichtungen - anschliessen, und ihre Patientinnen und Patienten müssen ihnen die notwendigen Zugriffsrechte erteilen. Zudem eröffnet das elektronische Patientendossier auch den Patientinnen und Patienten die Möglichkeit, ihre Daten einzusehen, selber eigene Daten zugänglich zu machen wie auch die Vergabe der Zugriffsrechte zu verwalten.

Der Umgang mit Patientendaten ausserhalb des elektronischen Patientendossiers, wie z. B. Dokumentations- und Haftungsregeln oder die ärztliche Schweigepflicht, sind nicht Gegenstand der Vorlage. Gleiches gilt für Regelungen zum Datenaustausch zwischen Gesundheitsfachpersonen und den Sozialversicherungen oder zur Nutzung der in den elektronischen Patientendossiers enthaltenen medizinischen Daten für den Aufbau von Krankheits- oder Qualitätsregistern sowie zu Statistik- oder Forschungszwecken.

Teilnahme am elektronischen Patientendossier
Das Führen eines elektronischen Patientendossiers ist für die Patientinnen und Patienten freiwillig. Im Sinne der informationellen Selbstbestimmung entscheidet jede Person selber, ob sie ein elektronisches Patientendossier führen will und ob sie ihren Gesundheitsfachpersonen umfassende oder eingeschränkte Zugriffsrechte erteilt.
Der Grundsatz der Freiwilligkeit gilt auch für die Gesundheitsfachpersonen und ihre Einrichtungen. Ausgenommen sind lediglich die Leistungserbringer nach den Artikeln 39 und 49a Absatz 4 des Bundesgesetzes vom 18. März 1994[1] über die Krankenversicherung. Es handelt sich dabei um die Spitäler sowie die Geburtshäuser und Pflegeheime, welche Leistungen zulasten der obligatorischen Krankenpflegeversicherung abrechnen. Spitäler müssen sich innerhalb von drei Jahren einer zertifizierten Gemeinschaft oder Stammgemeinschaft anschliessen, Geburtshäuser und Pflegeheime, innerhalb von fünf Jahren.

Den ambulant tätigen Gesundheitsfachpersonen steht es frei, ob sie ihren Patientinnen oder Patienten ein elektronisches Patientendossier anbieten wollen. Schliessen sie sich jedoch einer zertifizierten Gemeinschaft oder Stammgemeinschaft an, so sind sie verpflichtet, behandlungsrelevante Daten im elektronischen Patientendossier zugänglich zu machen.

[1] SR **832.10**

Die Bearbeitung von Daten im Rahmen des elektronischen Patientendossiers durch Gesundheitsfachpersonen ist nur mit Einwilligung der Patientin oder des Patienten möglich. Diese haben die Möglichkeit, individuelle Zugriffsrechte zu vergeben.

Elektronische Identität
Für eine sichere Datenbearbeitung braucht es eine eindeutige und sichere Identifikation und Authentisierung der Patientinnen und Patienten wie auch der Gesundheitsfachpersonen. Diese wird mittels einer elektronischen Identität eines zertifizierten Herausgebers von Identifikationsmitteln sichergestellt.

Patientenidentifikationsnummer
Um alle Daten und Dokumente korrekt und vollständig zusammenführen zu können, die zu einer Patientin oder einem Patienten im elektronischen Patientendossier erfasst sind, wird eine zufällig generierte, Nummer als zusätzliches Identifikationsmerkmal (Patientenidentifikationsnummer) verwendet. Sie ergänzt die identifizierenden Personenmerkmale wie Name, Vorname, Geschlecht oder Geburtsdatum. Die Patientenidentifikationsnummer wird von der zentralen Ausgleichsstelle der AHV (ZAS) auf Antrag vergeben.

Zertifizierungspflicht
Damit eine sichere Datenbearbeitung gewährleistet werden kann, werden für alle Beteiligten (Gemeinschaften, Stammgemeinschaften, Herausgeber von Identifikationsmitteln) Mindestanforderungen festgelegt. Die Einhaltung von technischen und organisatorischen Voraussetzungen wird mit einem Zertifizierungsverfahren sichergestellt.

Abfragedienste
Der Bund betreibt die für die Kommunikation zwischen Gemeinschaften, Stammgemeinschaften und Zugangsportalen notwendigen zentralen Abfragedienste und unterstützt die Einführung und Verbreitung des elektronischen Patientendossiers informierend und koordinierend.

Finanzhilfen
Zudem unterstützt der Bund den Aufbau und die Zertifizierung von Gemeinschaften und Stammgemeinschaften während drei Jahren durch Finanzhilfen in der Höhe von insgesamt 30 Millionen Franken. Diese sind an die Mitfinanzierung durch Kantone oder Dritte gebunden. Die Kosten, welche den Gesundheitsfachpersonen und ihren Einrichtungen durch die Anpassung ihrer Praxis- und Klinikinformationssysteme entstehen, sind durch die Finanzhilfen des Bundes nicht abgedeckt.

1.2 EU-Recht

Es bestehen zum aktuellen Zeitpunkt (März 2016) keine rechtlich verbindlichen internationalen Verpflichtungen im Bereich «eHealth». Internationale Richtlinien und Empfehlungen (z. B. der EU) wurden jedoch bei der Erarbeitung der EPDV als Orientierungshilfen beigezogen, wobei insbesondere die Empfehlung der Europäischen Kommission zur grenzübergreifenden Interoperabilität von elektronischen Patientendatensystemen von grosser Relevanz ist. Überdies bestehen folgende massgebende Richtlinien:

- Richtlinie 95/46/EG des Europäischen Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[2].
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[3].
- Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kom-

[2] ABl. L 281 vom 23.11.1995, S. 31; geändert durch Verordnung (EG) Nr. 1882/2003, ABl. L 284 vom 31.10.2003, S. 1.
[3] ABl. L 201 vom 31.7.2002, S. 37; zuletzt geändert durch Richtlinie 2009/136/EG, ABl. L 337 vom 18.12.2009, S. 11.

munikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz[4].

- Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung[5].
- Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG[6].

Weitere Informationen im Zusammenhang mit dem EU-Recht sind in der Botschaft zum EPDG, (BBl 2013 5367 ff.) aufgeführt.

1.3 Übersicht über das Ausführungsrecht zum elektronischen Patientendossier

<table>
<tr>
<td>Stufe Bundesrat</td>
<td>Verordnung über das elektronische Patientendossier (EPDV)
- 1. Kapitel: Vertraulichkeitsstufen und Zugriffsrechte
- 2. Kapitel: Patientenidentifikationsnummer
- 3. Kapitel: Gemeinschaften und Stammgemeinschaften
- 4. Kapitel: Identifikationsmittel
- 5. Kapitel: Akkreditierung
- 6. Kapitel: Zertifizierung
- 7. Kapitel Abfragedienste
- 8. Kapitel: Schlussbestimmungen</td>
<td>Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV)
- 1. Abschnitt: Allgemeine Bestimmungen
- 2. Abschnitt: Bemessung der Finanzhilfen
- 3. Abschnitt: Verfahren
- 4. Abschnitt: Inkrafttreten

- Anhang: Anrechenbare Kosten</td>
</tr>
<tr>
<td>Stufe Departement</td>
<td>Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI)
- Anhang 1: Kontrollzifferprüfung
- Anhang 2: Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften
- Anhang 3: Metadaten
- Anhang 4: Austauschformate
- Anhang 5: Integrationsprofile, Nationale Anpassungen der Integrationsprofile und Nationale Integrationsprofile
- Anhang 6: Kennzahlen für die Evaluation
- Anhang 7: Mindestanforderungen an die Qualifikation der Angestellten der Zertifizierungsstellen
- Anhang 8: Vorgaben für den Schutz der Identifikationsmittel</td>
<td></td>
</tr>
</table>

Abbildung 1 - Struktur des Ausführungsrechts zum Bundesgesetz über das elektronische Patientendossier

Das Ausführungsrecht zum elektronischen Patientendossier besteht aus der Verordnung über das elektronischen Patientendossier (EPDV), der Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI) sowie der Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV).

[4] ABl. L 337 vom 18.12.2009, S. 11.
[5] ABl. L 88 vom 4.4.2011, S. 45.
[6] ABl. L 257 vom 28.8.2014, S. 73.

1.3.1 Verordnung über das elektronische Patientendossier (EPDV)

Die EPDV regelt die Vertraulichkeitsstufen und Zugriffsrechte (1. Kapitel), die Vorgaben zu Vergabe und Verwaltung der Patientenidentifikationsnummer (2. Kapitel), die Gemeinschaften und Stammgemeinschaften (Zertifizierungsvoraussetzungen; 3. Kapitel), die Identifikationsmittel (4. Kapitel), die Akkreditierung (5. Kapitel), die Zertifizierung (6. Kapitel) sowie die Abfragedienste (7. Kapitel).

1.3.2 Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI)

Die Departementsverordnung über das elektronische Patientendossier enthält in *Anhang 1* eine detaillierte Umschreibung der Kontrollzifferlogik, welche bei der Kontrollzifferprüfung nach Artikel 4 Absatz 2 EPDV zu beachten ist und er stellt zudem den Aufbau der Patientenidentifikationsnummer für eine schriftliche Darstellung dar.

Anhang 2 regelt die Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften mittels sog. Technischer und Organisatorischer Zertifizierungsvoraussetzungen (TOZ) (vgl. Kapitel 3 « Gemeinschaften und Stammgemeinschaften» der EPDV).

Anhang 3 (vgl. Art. 9, Abs. 3, Bst. b) enthält die Liste der zu verwendenden Metadaten, die im Rahmen des elektronischen Patientendossiers zu verwenden sind, um einen interoperablen und sicheren Datenaustausch sicherzustellen.

In *Anhang 4* (vgl. Art. 9, Abs. 3, Bst. c EPDV) finden sich die zu verwendenden Austauschformate. Dabei geht es beispielsweise um Vorgaben betreffend das elektronische Impfdossier oder den elektronischen Austrittsbericht. Aktuell liegen noch keine Austauschformate vor; diese werden im Rahmen von Stakeholderprozessen erarbeitet und mittels zukünftiger Revisionen in das Ausführungsrecht aufgenommen.

In *Anhang 5* (vgl. Art. 9 Abs. 3, Bst. d EPDV) der EPDV-EDI werden die anzuwendenden Integrationsprofile, welche den gemeinschaftsübergreifenden Datenaustausch regeln sowie die nationalen Anpassungen zu diesen Integrationsprofilen spezifiziert. Zudem enthält er zwei nationale Integrationsprofile, die in Ergänzung zu den IHE-Profilen anzuwenden sind. Es ist mittel- bis langfristig geplant, die nationalen Anpassungen und die ergänzenden nationalen Integrationsprofile in den entsprechenden nationalen oder internationalen Organisationen (IHE Suisse oder IHE International) als offiziellen Standard verabschieden zu lassen. Der Erlass des Anhangs 5 stellt somit für die nationalen Anpassungen und die nationalen Integrationsprofile eine Übergangslösung dar.

Anhang 6 (vgl. Art. 21 EPDV) enthält eine Aufzählung der Daten, welche zertifizierte Gemeinschaften und Stammgemeinschaften dem Bundesamt für Gesundheit (BAG) zur Verfügung stellen, damit dieses die Evaluation nach Artikel 18 EPDG vornehmen kann.

Die Mindestanforderungen an die Qualifikation des Personal der Zertifizierungsstellen werden in *Anhang 7* detailliert aufgeführt.

Anhang 8 legt fest, welche Vorgaben für den Schutz der Identifikationsmittel gelten.

Das BAG wird zudem in Form von Datenbearbeitungsreglementen die Schnittstellen für die Kommunikation zwischen der ZAS und den Gemeinschaften und Stammgemeinschaften, sowie für die Kommunikation zwischen Gemeinschaften und Stammgemeinschaften und den Abfragediensten des Bundes festlegen.

1.3.3 Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV)

Die EPDFV regelt die Vergabe der Finanzhilfen nach den Artikeln 20–23 EPDG. Das Einreichen von Gesuchen um Finanzhilfen für den Aufbau und die Zertifizierung von Gemeinschaften und Stammgemeinschaften ist nach Artikel 27 Absatz 3 EPDG auf drei Jahre nach Inkrafttreten des Gesetzes beschränkt. Nach Artikel 26 EPDG sind die Artikel 20–23 EPDG und damit die EPDFV auf die während

ihrer Geltungsdauer eingereichten Gesuche anwendbar. Die Erläuterungen zur EPDFV finden sich in einem separaten Dokument.

1.4 Auswirkungen

In der parlamentarischen Beratung wurde das EPDG nur punktuell angepasst (insbesondere die Möglichkeit der Mitfinanzierung des Aufbaus von Gemeinschaften und Stammgemeinschaften durch Dritte zur Erlangung von Finanzhilfen des Bundes, die Vereinheitlichung des Verfahrens zur Vergabe der Finanzhilfen, die Verkürzung der Übergangsfrist für den Anschluss von Spitälern an zertifizierte Gemeinschaften und Stammgemeinschaften und die Möglichkeit der Verwendung der Versichertenkarte). Es kann somit weitgehend auf die Ausführungen zu den Auswirkungen auf die verschiedenen Akteure in der Botschaft zum EPDG verwiesen werden (vgl. BBl. 2013 5398 ff.). Nachfolgend werden nur die wichtigsten Punkte aus der Botschaft kurz aufgenommen und diejenigen Auswirkungen aufgezeigt, welche sich aus dem Ausführungsrecht ergeben.

1.4.1 Auswirkungen auf den Bund

Dem Bund wird aufgrund der nachfolgend aufgeführten Aufgaben durch die Umsetzung des EPDG ein personeller und finanzieller Zusatzaufwand erwachsen.

Das BAG wird nach Artikel 12 Absatz 2 EPDG ermächtigt, die Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften sowie Herausgeber von Identifikationsmitteln dem Stand der Technik anzupassen (siehe Art. 9 Abs. 4, Art. 29 Abs. 3 und Art. 30 Abs. 4 EPDV).

Das BAG ist zudem im Rahmen der Zertifizierung nach EPDG Besitzer des Zertifizierungsschemas («Schema-Owner»). Dies hat zur Folge, dass das BAG Ansprechpartner für Fragen der Schweizerischen Akkreditierungsstelle SAS ist. Zudem hat es einen zielgerichteten Informationsaustausch in Bezug auf die Zertifizierung unter den zu zertifizierenden Entitäten (Gemeinschaften und Stammgemeinschaften sowie Herausgeber von Identifikationsmitteln) sicherzustellen.

Um eine schweizweit einheitliche Zertifizierung im Rahmen der Vorgaben zur Interoperabilität sicherzustellen stellt das BAG zusammen mit dem Koordinationsorgan Bund-Kantone «eHealth Suisse» die den Zertifizierungsstellen eine Zertifizierungsumgebung zur Verfügung, welche als Testsystem im Rahmen der Zertifizierung die Einhaltung der Normen, Standards und Integrationsprofile überprüft, in Auftrag und kümmert sich um Betrieb und Weiterentwicklung derselben (Art. 27 Abs. 3 Bst. c EPDV).

Das BAG baut die für das Funktionieren des elektronischen Patientendossiers elementaren Abfragedienste auf und betreibt diese bzw. überwacht die mit dem Aufbau und Betrieb der Abfragedienste beauftragten Dritten (Art. 14 Abs. 1 und Art. 19 Abs. 1 EPDG).

Um den Aufbau und die Zertifizierung von Gemeinschaften und Stammgemeinschaften zu fördern, vergibt der Bund während drei Jahren ab Inkrafttreten Finanzhilfen (EPDG Art. 20-23). Das BAG prüft die Gesuche auf Finanzhilfen, holt Stellungnahmen der betroffenen Kantone ein und erarbeitet Leistungsverträge mit den Gemeinschaften oder Stammgemeinschaften, welchen Finanzhilfen gewährt werden. Die Einhaltung dieser Leistungsverträge wird laufend überprüft, um mögliche Verstösse zu erkennen und entsprechende Massnahmen zu ergreifen.

Das *Eidgenössische Departement des Innern (EDI)* evaluiert das Gesetz nach den Prinzipien von Zweckmässigkeit, Wirksamkeit und Wirtschaftlichkeit (Art. 21 EPDV).

Die Datenbearbeitung durch Private fällt in den Geltungsbereich des Bundesgesetzes über den Datenschutz (DSG; SR 235.1). Gemeinschaften und Stammgemeinschaften unterstehen aufgrund ihrer privatrechtlichen Organisation dem DSG und damit der Aufsicht des *Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)*, sofern die Spezialgesetzgebung die Aufsicht nicht anders festlegt. Gleiches gilt für alle übrigen Akteure, soweit es sich dabei um Private handelt.

Die SAS akkreditiert die Organisationen, welche Zertifizierungen nach EPDG durchzuführen gedenken. Bei der Akkreditierung wird geprüft, ob die Prüfprogramme geeignet sind, die Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften sowie für die Herausgeber von Identifikationsmitteln zu kontrollieren. Diese Prüfung umfasst sowohl organisatorische als auch technische Aspekte.

Die *Zentrale Ausgleichsstelle (ZAS)* ist zuständig für die Vergabe und die Verwaltung der Patientenidentifikationsnummer nach Artikel 5 Absatz 1. Sie stellt sicher, dass die Identifikationsdatenbank nach den Erfordernissen des EPDG und der EPDV angepasst wird.

Das *Koordinationsorgan Bund-Kantone «eHealth Suisse»* stellt sicher, dass die Normen, Standards und Integrationsprofile im Rahmen von partizipativen Prozessen weiterentwickelt werden. Das Ergebnis dieser Arbeiten fliesst direkt an das BAG, welches zuständiges Amt für die Revision von Gesetz und Ausführungsrecht ist.

«eHealth Suisse» übernimmt zudem die Aufgaben im Bereich Information (Art. 15 EPDG) und Koordination (Art. 16 EPDG).

1.4.2 Auswirkungen auf die Kantone und Gemeinden

Den Kantonen kann aus der Umsetzung des vorliegenden Entwurfs aus folgenden Gründen ein personeller und finanzieller Zusatzaufwand erwachsen:

- Prüfung und ggf. Anpassung der kantonalen Rechtsgrundlagen für die Einführung des elektronischen Patientendossiers;
- u.U. Beteiligung an den Kosten für den Aufbau, die Zertifizierung und den Betrieb der Gemeinschaften und Stammgemeinschaften;
- Erarbeitung von Stellungnahmen zu Gesuchen um Finanzhilfen des Bundes für Gemeinschaften oder Stammgemeinschaften auf dem eigenen Kantonsgebiet.

Da die Kantone für die Sicherstellung und damit die Organisation der Gesundheitsversorgung zuständig sind, fällt es auch in ihre Aufgaben- und Finanzierungsverantwortung, die Voraussetzungen zu schaffen, dass sich stationäre Einrichtungen (Listen- und Vertragsspitäler, Rehabilitationskliniken, Pflegeheime sowie Geburtshäuser; siehe Art. 39 Abs. 1 Bst. f und Art. 49a Abs. 4 erster Satz KVG) aber auch selbstständig tätige Gesundheitsfachpersonen, insbesondere Ärztinnen und Ärzte, zu Gemeinschaften oder Stammgemeinschaften zusammenschliessen und sich zertifizieren lassen.

2 Besonderer Teil

2.1 Ingress

Aufgrund der Tatsache, dass das EPDG etliche kompetenzbegründende Normen enthält, verweist der Ingress der EPDV auf das EPDG als Ganzes.

2.2 Erläuterungen zu den einzelnen Artikeln

1. Kapitel: Vertraulichkeitsstufen und Zugriffsrechte

Art. 1 Vertraulichkeitsstufen

Nach *Absatz 1* kann die Patientin oder der Patient die Daten des elektronischen Patientendossiers vier unterschiedlichen Vertraulichkeitsstufen zuordnen. Folgende Vertraulichkeitsstufen stehen zur Verfügung (*Buchstaben a bis d*). Es steht im freien Ermessen der Patientin oder des Patienten, welche Daten sie oder er welcher Stufe zuordnet, so ist beispielsweise folgende Zuteilung denkbar:

1) «nützliche Daten»: z.B. Informationen über Allergien und Unverträglichkeiten oder besondere Erkrankungen, Kostengutsprachen, Patientenverfügung, Willensäusserung zur Organspende, Kontaktdaten von im Notfall zu benachrichtigenden Personen.
2) «medizinische Daten»: behandlungsrelevante Dokumente und Daten wie z.B. Berichte, Befunde, durchgeführte Behandlungen etc.
3) «sensible Daten»: Medizinische Daten, die aus Sicht der Patientin oder des Patienten sensibel sind und nur Gesundheitsfachpersonen mit der Zugriffsstufe «erweitert» zugänglich sein sollen.
4) «geheime Daten»: Medizinische Daten, die nur durch die Patientin oder den Patienten eingesehen werden können.

Die Bezeichnungen der Vertraulichkeitsstufen sind nicht als Definitionen der in der jeweiligen Stufe beinhalteten Daten zu verstehen. Die oben aufgeführten Beispiele dienen lediglich der Anschaulichkeit. Jeder Dokumenttyp kann sich in jeder Vertraulichkeitsstufe finden. Ausschlaggebend für die Wahl ist, dass der Umfang des Zugriffsrechts je nach Vertraulichkeitsstufe unterschiedlich ist (vgl. Erläuterungen zu Art. 2).

Nimmt die Patientin oder der Patient keine Zuordnung vor, so wird neu eingestellten Daten standardmässig die Vertraulichkeitsstufe «medizinische Daten» zugewiesen (*Abs. 2*). Diese Standardeinstellung kann der Patient verändern (vgl. Erläuterungen zu Art. 3).

Gesundheitsfachpersonen können abweichend von der in Absatz 2 festgehaltenen Standardeinstellung Daten, die sie neu einstellen, der Vertraulichkeitsstufe «sensible Daten» zuweisen (*Abs. 3*). Diese Möglichkeit dient dazu, Daten, die für die Patientin oder den Patienten offensichtlich sensibel sind, von Beginn weg einer Vertraulichkeitsstufe mit restriktiverer Zugriffsmöglichkeit einzuordnen. Dies kann z.B. der Fall sein, wenn es um eine stigmatisierende Diagnose geht, oder wenn für die Gesundheitsfachperson aufgrund persönlicher Kenntnisse die Sensibilität gewisser Informationen für seine Patientin oder seinen Patienten erkennbar ist.

Art. 2 Zugriffsrechte

Artikel 2 regelt die Möglichkeiten der Erteilung von Zugriffsrechten durch die Patientin oder den Patienten. Die Stammgemeinschaften müssen die Umsetzung sicherstellen. Die Regelungen zum Notfallzugriff müssen sowohl durch die Stammgemeinschaften wie auch durch die Gemeinschaften sichergestellt werden.

Nach *Artikel 2 Absatz 1* kann die Patientin oder der Patient Gesundheitsfachpersonen oder Gruppen

von Gesundheitsfachpersonen unterschiedliche Zugriffsrechte zuweisen. Folgende Zugriffsrechte stehen zur Verfügung (*Buchstaben a bis c*):

a) «eingeschränkt»: ermöglicht Zugriff auf die Vertraulichkeitsstufe «nützliche Daten».
b) «normal»: ermöglicht Zugriff auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten».
c) «erweitert»: ermöglicht Zugriff auf die Vertraulichkeitsstufen «nützliche Daten», «medizinische Daten» und «sensible Daten».

Auf die Vertraulichkeitsstufe «Geheime Daten» hat ausschliesslich der Patient oder die Patientin Zugriff.

Nimmt der Patient oder die Patientin bei der Erteilung eines Zugriffsrechts keine spezifische Zuweisung nach Buchstabe a), b) oder c) vor, so wird nach *Absatz 2* standardmässig das Zugriffsrecht «normal» zugewiesen.

Nach *Absatz 3* gelten die Zugriffsrechte so lange, bis die Patientin oder der Patient sie wieder entzieht. Eine gesetzliche Befristung ist nicht vorgesehen. Es besteht aber die Option, Zugriffsrechte zeitlich zu beschränken (vgl. Erläuterungen zu Art. 3).

Aus Praktikabilitätsgründen können Zugriffsrechte auch summarisch an Gruppen von Gesundheitsfachpersonen erteilt werden (z.B. einem Tumorboard oder einer Abteilung im Spital). Dies bedingt, dass die Patientin oder der Patient die entsprechende Gruppe von Gesundheitsfachpersonen über den Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen (Art. 40 EPDV) suchen und ihre Zusammensetzung zur Kenntnis nehmen kann. Bei Gruppen von Gesundheitsfachpersonen sind die Zugriffsrechte abhängig von der Zugehörigkeit zur Gruppe (*Abs. 4*): Tritt eine Gesundheitsfachperson einer Gruppe von Gesundheitsfachpersonen bei, so erhält sie das mit dieser Gruppe verbundene Zugriffsrecht. Mit dieser Regelung wird sichergestellt, dass die Gesundheitsfachperson Zugriff auf die für die Behandlung notwendigen Informationen erhält. Verlässt eine Gesundheitsfachperson eine Gruppe von Gesundheitsfachpersonen, so wird ihr das mit der Gruppe verbundene Zugriffsrecht automatisch entzogen.

In medizinischen Notfallsituationen können Gesundheitsfachpersonen ohne vorgängig erteiltes Zugriffsrecht auf das elektronische Patientendossier zugreifen (*Absatz 5*). Sie erhalten in diesem Fall standardmässig Zugriff auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten». Von dieser Möglichkeit darf ausschliesslich in einer medizinischen Notfallsituation Gebrauch gemacht werden. Wann eine solche vorliegt, entscheidet sich allein nach medizinischen Kriterien. Bevor der Notfallzugriff erfolgen kann, muss die Gesundheitsfachperson eine Begründung angeben. Diese Begründung kann z.B. stichwortartig in einem Textfeld einzugeben sein, das bei der Ausführung eines Notfallzugriffs auf der Bedienoberfläche erscheint. Als Sicherungsmassnahme gegen eine missbräuchliche Verwendung des Notfallzugriffs, beispielsweise aufgrund automatisierter Angriffe auf ein Endgerät, muss der Notfallzugriff von der Gesundheitsfachperson zudem anhand einer nicht automatisiert reproduzierbaren und manuellen Interaktion zusätzlich bestätigt werden (vgl. Ziff. 9.6 der TOZ). Denkbar sind hier zusätzliche Sicherungselemente, wie beispielsweise der Erhalt eines Einmalpasswortes oder die erneute Eingabe eines sonstigen Sicherheitsmerkmals.

Aufgrund des Ausnahmecharakters des Notfallzugriffs sieht das Gesetz vor, dass die Patientin oder der Patient über einen erfolgten Notfallzugriff informiert werden muss (Art. 9 Abs. 5 2. Satz EPDG). Verantwortlich für die Einhaltung dieser Informationspflicht ist die Gemeinschaft (vgl. Ziff. 9.6 der TOZ). Die Pflicht kann an die Gesundheitseinrichtung delegiert werden, in welcher der Notfallzugriff stattgefunden hat, oder auch technisch automatisiert vollzogen werden. Wie die Informationspflicht umgesetzt wird, ob die Patientin oder der Patient z.B. per Brief, Email oder SMS über einen erfolgten Notfallzugriff informiert wird, bleibt den Gemeinschaften überlassen.

Art. 3 Optionen der Patientinnen und Patienten

Der Patientin oder dem Patienten stehen bezüglich der Anwendung der verschiedenen Vertraulichkeitsstufen und der Erteilung von Zugriffsrechten diverse Optionen offen, die in *Artikel 3* aufgelistet werden. Die Stammgemeinschaften müssen die Umsetzung sicherstellen. Die Regelungen zum Notfallzugriff müssen sowohl durch die Stammgemeinschaften wie auch durch die Gemeinschaften sichergestellt werden.

Die Patientin oder der Patient hat nach *Buchstabe a* die Möglichkeit, die erteilten Zugriffsrechte auf sechs Monate zu befristen. Damit kann sie oder er sicherstellen, dass Gesundheitsfachpersonen, die voraussichtlich nur einmal oder nur für kurze Zeit in die Behandlung involviert werden, nicht unbeschränkt lange auf das elektronische Patientendossier zugreifen können. Solche Zugriffsrechte erlöschen nach Ablauf der festgesetzten Frist von sechs Monaten ohne weiteres Zutun der Patientin oder des Patienten. Damit verringert sich die Gefahr, dass Zugriffsrechte «vergessen» werden.

Die Patientin oder der Patient hat nach *Buchstabe b* die Möglichkeit, den Notfallzugriff einzuschränken, auszuweiten oder ganz auszuschliessen. So kann sie oder er den Zugriff z.B. auf die Vertraulichkeitsstufe «nützliche Daten» einschränken oder auf die Vertraulichkeitsstufe «sensible Daten» ausweiten. Sie oder er kann die Möglichkeit des Notfallzugriffs auch vollständig ausschliessen (vgl. Art. 9 Abs. 5 EPDG).

Die Patientin oder der Patient hat nach *Buchstabe c* die Möglichkeit, die für neu eingestellte Daten standardmässig geltende Vertraulichkeitsstufe zu bestimmen. Er oder sie kann die Einstellung z.B. so anpassen, dass neu eingestellte Daten die Vertraulichkeitsstufe «sensible Daten» zugewiesen wird. Selbstverständlich kann er oder sie auch jederzeit wieder zur Standardeinstellung zurückkehren.

Die Patientin oder der Patient hat nach *Buchstabe d* die Möglichkeit, einzelne Gesundheitsfachpersonen vollständig vom Zugriff auf ihr oder sein elektronisches Patientendossier ausschliessen (vgl. Art. 9 Abs. 3 EPDG). Die entsprechenden Gesundheitsfachpersonen werden auf eine sogenannte «Ausschlussliste» gesetzt. Es können auch einzelne Gesundheitsfachpersonen aus einer definierten Gruppe auf die Ausschlussliste gesetzt werden. Die Ausschlussliste geht vor. Der Zugriff durch diese Gesundheitsfachpersonen ist immer ausgeschlossen, also selbst dann, wenn sie Mitglied einer Gruppe sind, an die ein Gruppenzugriffsrecht erteilt wird. Gesundheitsfachpersonen, die auf dieser Liste stehen, können auch keine Notfallzugriffe tätigen.

Die Patientin oder der Patient wird standardmässig benachrichtigt, wenn eine Gesundheitsfachperson in eine Gruppe eintritt, der die Patientin oder der Patient bereits ein Gruppenzugriffsrecht erteilt hat (vgl. Erläuterungen zu Art. 8 Bst. f). Nach *Buchstabe e* besteht die Möglichkeit, auf diese Benachrichtigung zu verzichten.

Hat die Patientin oder der Patient einer Gruppe von Gesundheitsfachpersonen ein Zugriffsrecht erteilt, so erhalten neu in diese Gruppe eintretende Gesundheitsfachpersonen in der Regel das entsprechende Zugriffsrecht automatisch zugewiesen. Diesen Automatismus kann die Patientin oder der Patient nach *Buchstabe f* verhindern und festlegen, dass neu in eine Gruppe eintretende Gesundheitsfachpersonen, kein Zugriffsrecht erhalten.

Die Patientin oder der Patient hat nach *Buchstabe g* die Möglichkeit, eine Stellvertretung zu benennen, die in ihrem oder seinem Namen auf das elektronische Patientendossier zugreifen und auch die Vertraulichkeitsstufen und Zugriffsrechte zuweisen kann. Die Anzahl der Stellvertretungen ist nicht limitiert. Die Stellvertretungen benötigen keine eigene Patientenidentifikationsnummer und auch kein eigenes elektronisches Patientendossier. Sie dürfen aber nur mit einem eigenen Identifikationsmittel auf das elektronische Patientendossier des oder der vertretenen Person zugreifen. Mögliche Anwendungsfälle sind beispielsweise die Vertretung eines Kindes oder betagter Menschen durch seine Angehörigen oder anderen Vertrauenspersonen.

Die Patientin oder der Patient hat nach *Buchstabe h* die Möglichkeit, Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft zu ermächtigen, das ihr erteilte Zugriffsrecht an weitere Gesundheitsfachpersonen weiterzugeben. Die ermächtigte Gesundheitsfachperson kann ein Zugriffsrecht höchstens in dem Mass weitergeben, wie sie es selber besitzt.

2. Kapitel: Patientenidentifikationsnummer

Art. 4 Format der Patientenidentifikationsnummer

Absatz 1 legt das Format und die Zusammensetzung der elfstelligen Patientenidentifikationsnummer nach *Artikel 4 EPDG* fest. Sie setzt sich aus einer zehnstelligen Nummer und einer Kontrollziffer zusammen. Sie muss eindeutig einer Person in der Identifikationsdatenbank der Zentralen Ausgleichsstelle (ZAS) zugeordnet sein, jedoch selbst keinerlei Rückschlüsse auf die Person oder deren Versichertennummer nach *Artikel 50c AHVG* («AHVN13») zulassen.

Um die Fehlerhäufigkeit bei einer manuellen Erfassung der Patientenidentifikationsnummer zu vermindern erlaubt *Absatz 2* eine solche nur, wenn eine Kontrollzifferprüfung gemäss den Vorgaben des EDI durchgeführt wird. Diese Vorgaben werden in *Anhang 1* der EPDV-EDI aufgeführt.

Art. 5 Antrag auf Zuweisung der Patientenidentifikationsnummer

Für die Erstellung eines elektronischen Patientendossiers ist die Stammgemeinschaft der Patientin oder des Patienten zuständig (*Art. 14–16*). Daher hält *Absatz 1* fest, dass die Stammgemeinschaft für die Beantragung der Patientenidentifikationsnummer bei der ZAS nach *Artikel 16 Buchstabe d* zuständig ist (vgl. *Art. 4 Abs. 1 EPDG*). Die Technischen und Organisatorischen Zertifizierungsvoraussetzungen (TOZ) in *Anhang 2* der EPDV-EDI legen fest, dass Stammgemeinschaften dafür die Angaben des Identitätsnachweises gemäss *Artikel 23 Absatz 1* verwenden müssen.

Die *Absätze 2 und 3* betreffen die Sicherstellung der Qualität bei der Zuweisung der Patientenidentifikationsnummer. Standardmässig sollten die Angaben nach *Absatz 2* ausreichen, um eine Patientin oder einen Patienten eindeutig zu identifizieren, und ihr oder ihm eine Patientenidentifikationsnummer zuzuweisen. Sollten sich aber Unsicherheiten ergeben, so kann die ZAS nach *Absatz 3* ergänzende Informationen verlangen, um die Unklarheiten auszuräumen.

Art. 6 Abfrage der Patientenidentifikationsnummer

Die Abfrage, d.h. die Vergabe (*Art. 5*), die Abfrage und die Annullierung (*Art. 7*) der Patientenidentifikationsnummer kann über ein elektronisches Abrufverfahren erfolgen.

Art. 7 Annullierung

Widerruft eine Patientin oder ein Patient ihre oder seine Einwilligung, so wird das elektronische Patientendossier nach *Artikel 20* aufgehoben. Die ZAS muss über jede Aufhebung informiert werden und die Patientenidentifikationsnummer, da sie ein Teil des elektronischen Patientendossiers ist, muss in der Folge in der Identifikationsdatenbank der ZAS annulliert werden (*Abs. 1*). Sie steht dadurch für Abfragen nach *Artikel 6* nicht mehr zur Verfügung.

Absatz 2 stellt sicher, dass annullierte Patientenidentifikationsnummern nicht erneut vergeben werden, um mögliche Verwechslungen aufgrund von Doppelvergaben zu verhindern.

3. Kapitel: Gemeinschaften und Stammgemeinschaften

1. Abschnitt: Gemeinschaften

Art. 8 Verwaltung

Gemeinschaften müssen nach *Buchstabe a* geeignete Prozesse definieren, dokumentieren, umsetzen und einhalten, um neu hinzukommende oder die Gemeinschaft verlassende Gesundheitseinrichtungen (z. B. Spitäler, Apotheken, Arztpraxen, Spitexorganisationen, Pflegeheime), Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen zu verwalten.

Die technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ) in Anhang 2 der EPDV-EDI konkretisieren in der Ziffer 1 die Anforderungen an die Verwaltung von Gesundheitseinrichtungen, Gesundheitsfachpersonen und deren Hilfspersonen sowie Gruppen von Gesundheitsfachpersonen.

Verwaltung von Gesundheitseinrichtungen
Eintrittsprozess
Dieser umfasst u. a. das Abschliessen einer Vereinbarung, in der sich die Gesundheitseinrichtung verpflichtet, die internen organisatorischen Vorgaben einer Gemeinschaft und insbesondere die Aufgaben und Pflichten im Bereich Datenschutz und Datensicherheit einzuhalten (vgl. Ziff. 1.1.2.1 sowie 4.9 der TOZ). Im Rahmen dieser Vereinbarung kann die Gemeinschaft zudem gewisse Zertifizierungsanforderungen an die ihr angeschlossenen Gesundheitseinrichtungen weiterdelegieren. Dazu zählt insbesondere die Verwaltung der Gesundheitsfachpersonen und der Gruppen von Gesundheitsfachpersonen, die in der entsprechenden Gesundheitseinrichtung arbeiten (*Bst. a–d*). Die Aufnahme, die Mutation oder der Austritt einer Gesundheitsfachperson setzt zudem voraus, dass ihre Gesundheitseinrichtung bereits in die Gemeinschaft eingetreten ist.

Austrittsprozess
Zudem müssen Gemeinschaften beim Austritt einer Gesundheitseinrichtung, die sich keiner anderen Gemeinschaft oder Stammgemeinschaft anschliesst, sicherstellen, dass diejenigen Dokumente gelöscht werden, die von der austretenden Gesundheitseinrichtung in den gemeinschaftsinternen oder eigenen Dokumentenablagen für das elektronische Patientendossier bereitgestellt wurden. Dasselbe gilt auch für die entsprechenden Einträge im Dokumentenregister (vgl. Ziff. 1.1.3 der TOZ). Patientinnen und Patienten, deren Dokumente nach einem Austritt der Gesundheitseinrichtung nicht mehr im elektronischen Patientendossier zur Verfügung stünden, müssen vorgängig entsprechend informiert werden, damit sie Gelegenheit haben, diese Dokumente zuvor abzurufen und gegebenenfalls gemäss Artikel 8 EPDG und Artikel 18 EPDV selber im elektronischen Patientendossier bereitzustellen.

Gemeinschaften müssen nach *Buchstabe c* sicherstellen, dass die Daten der ihnen angeschlossenen Gesundheitseinrichtungen im zentralen Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 aktuell sind. Da dieser Abfragedienst die Grundlage für die Vergabe der Zugriffsrechte an Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen darstellt, ist eine zeitnahe Aktualisierung der Daten notwendig. Gemeinschaften können diese Aufgabe an die Gesundheitseinrichtungen delegieren, bleiben aber für die Korrektheit und Aktualität der eingetragenen Daten verantwortlich und müssen sicherstellen, dass Veränderungen in angemessener Zeit (in den meisten Fällen heisst dies voraussichtlich täglich) nachgeführt werden (vgl. Ziff. 1.1.4 der TOZ).

Verwaltung von Gesundheitsfachpersonen
Gemeinschaften müssen nach *Buchstabe a* zudem geeignete Prozesse definieren, dokumentieren, umsetzen und einhalten, um die Gesundheitsfachpersonen, die bei den ihr angeschlossenen Gesundheitseinrichtungen arbeiten, zu verwalten. Die Prozesse müssen dabei neben den in den *Buchstaben b–d*

aufgeführten Anforderungen, weitere Vorgaben sicherstellen. Dazu gehören insbesondere die Information der Gesundheitsfachpersonen über deren Aufgaben, Rechte und Pflichten bei der Bearbeitung von Daten des elektronischen Patientendossiers (vgl. auch Ziffer 4.9.1 der TOZ). Ebenso deren Information über Risiken und Massnahmen in den Bereichen Datenschutz und Datensicherheit. Gemeinschaften müssen zudem Verfahren für die Einwilligung von Gesundheitsfachpersonen zu den spezifischen Richtlinien der Gemeinschaft oder zu spezifischen darauf aufbauenden Richtlinien der jeweiligen Gesundheitseinrichtungen umsetzen (vgl. Ziff. 1.2.2.1 der TOZ). Zudem ist das konkrete Vorgehen bei einem Austritt einer Gesundheitsfachperson aus einer Gemeinschaft (z.B. infolge Wechsel der Anstellung, Beendigung der Berufstätigkeit oder Tod) festzulegen. Die Aufnahme, die Mutation oder der Austritt einer Gesundheitsfachperson setzt zwingend voraus, dass ihre Gesundheitseinrichtung bereits in die Gemeinschaft eingetreten ist. Sie können diese Aufgaben den ihr angeschlossenen Gesundheitseinrichtungen übertragen.

Die Identifikation einer Gesundheitsfachperson nach *Buchstabe b* muss, sofern sie nicht mit einem Identifikationsmittel eines nach Artikel 30 zertifizierten Herausgebers durchgeführt werden kann, den Anforderungen nach Artikel 23 entsprechen. Zusätzlich muss die Gemeinschaft sicherstellen, dass es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG handelt (vgl. Ziff. 1.2.2.3 der TOZ). Dazu kann entweder ein Identifikationsmittel verwendet werden, dessen Herausgeber die berufliche Qualifikation im Rahmen der Herausgabe nach Artikel 23 Absatz 2 überprüft hat, oder auf den Eintrag in einem kantonalen oder eidgenössischen Berufsregister (z. B. des Registers über die universitären Medizinalberufe «MedReg», des Registers der Psychologieberufe «PsyReg» oder des Gesundheitsberuferegisters «NAREG») abgestützt werden.

Die Daten der Gesundheitsfachpersonen müssen nach *Buchstabe c* im Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 eingetragen, aktualisiert oder gegebenenfalls gelöscht werden. Sofern die Gesundheitsfachperson in einem eidgenössischen oder kantonalen Berufsregister (z. B. MedReg, NAREG, etc.) geführt wird, sind diese Angaben in den Abfragedienst zu übernehmen (vgl. Ziff. 1.2.2.5 der TOZ). Dabei ist insbesondere sicherzustellen, dass nur Gesundheitsfachpersonen im Abfragedienst geführt werden, die der Definition nach Artikel 2 Buchstabe b EPDG entsprechen, für die jeweilige Gesundheitseinrichtung tätig sind und die einen Zugang zum elektronischen Patientendossier benötigen.

Nach *Buchstabe d* darf der Zugriff von Gesundheitsfachpersonen auf das elektronische Patientendossier nur mit einem gültigen Identifikationsmittel erfolgen, welches von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurde. Dabei ist es unerheblich, ob der Zugriff über das Zugangsportal für Gesundheitsfachpersonen (Art. 10) oder andere Systeme (z. B. integrierter Zugang im Primärsystem) erfolgt. Das bedeutet, dass Systeme, die von Gesundheitsfachpersonen oder Hilfspersonen für den Zugriff auf das elektronische Patientendossier genutzt werden, ein starkes Authentifizierungsverfahren mit mindestens zwei Authentifizierungsfaktoren als Voraussetzung für die Bearbeitung von Daten des elektronischen Patientendossiers unterstützen müssen (vgl. Ziff. 1.4.3 der TOZ). Eine so erfolgte Authentifizierung anderer zertifizierter Gemeinschaften, ist als vertrauenswürdig anzuerkennen.

Gemeinschaften müssen die eindeutigen Identifikatoren der Identifikationsmittel von Gesundheitsfachpersonen und Hilfspersonen zuverlässig mit der registrierten Identität der jeweiligen Person in der Gemeinschaft verbinden (vgl. Ziff. 1.4.2 der TOZ). Der Identifikator wird in der Regel durch den Identitätsdienstleister (Herausgeber des Identifikationsmittels) im Kontext der Authentifizierung, an den Zugangspunkt des internen Zugangsportals übermittelt.

Gesundheitsfachpersonen können Hilfspersonen für die Bearbeitung von Daten des elektronischen Patientendossiers einsetzen, sofern deren Zugehörigkeit zu einer für sie verantwortlichen Gesundheitsfachperson gemeinschaftsintern verwaltet wird. Da sie nicht im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 geführt werden, können sie von Patientinnen und Patienten nicht als eigenständige Personen in der Berechtigungssteuerung verwaltet werden. Für die Identifikation und den Zugriff von Hilfspersonen sind die Bestimmungen von *Artikel 8 Buchstaben b und*

d massgeblich (vgl. Ziff. 1.3 der TOZ).

Verwaltung von Gruppen von Gesundheitsfachpersonen
Nach *Buchstabe c* müssen die Gemeinschaften auch die Verwaltung der Gruppen von Gesundheitsfachpersonen im Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 sicherstellen. Sie können diese Aufgabe den ihr angeschlossenen Gesundheitseinrichtungen übertragen. Neben der Korrektheit und Aktualität der Angaben ist dabei nach *Buchstabe e* sicherzustellen, dass die Zusammensetzung der Gruppen für Patientinnen und Patienten jederzeit nachvollziehbar ist (*Bst. e*), da diese Zugriffsrechte auch an Gruppen von Gesundheitsfachpersonen zuweisen können (*Art. 2 Abs. 1*) und die danach neu in diese Gruppe eintretende Gesundheitsfachpersonen die mit dieser Gruppe verbundenen Zugriffsrechte erhalten können (*Art. 2 Abs. 4*) (vgl. Ziff. 1.5 der TOZ). Dies jedoch nur sofern diese Funktion vom Patienten oder der Patientin nicht nach *Artikel 3 Buchstabe f* abgewählt wurde oder die Gesundheitsfachperson nicht generell durch den Patienten oder die Patientin vom Zugriff ausgeschlossen wurde (vgl. *Art. 3 Bst. d*).

Aus diesem Grund hält *Buchstabe e fest, dass* die Zusammensetzung der Gruppen von Gesundheitsfachpersonen jederzeit nachvollziehbar sein muss. Damit eine Patientin oder ein Patient beispielsweise nicht ein ganzes Spital berechtigen muss, wenn sie oder er nur die Abteilung kennt, auf der sie oder er behandelt wird, nicht aber die Namen der in die Behandlung involvierten Gesundheitsfachpersonen konkretisiert die TOZ dies durch die Vorgabe, dass die Grösse der Gruppe verhältnismässig sein muss, d. h. sie muss es dem Patienten oder der Patientin erlauben, die Zugriffsstufen, der an seiner Behandlung beteiligten Gesundheitsfachpersonen, angemessen zu verwalten, ohne dass dadurch unverhältnismässig viele Gesundheitsfachpersonen ohne Behandlungskontext mitberechtigt werden (vgl. Ziff. 1.5.2.3 der TOZ).

Buchstabe f hält fest, dass Patientinnen und Patienten über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen zu informieren sind. Damit soll den Patientinnen und Patienten die Gelegenheit gegeben werden, die Zusammensetzung der Gruppe bei Bedarf zu überprüfen, um – je nach gewählter Option nach Artikel 3 Buchstabe f – den neu eingetretenen Gesundheitsfachpersonen das fehlende Zugriffsrecht zu erteilen oder das in Folge des Eintritts in die Gruppe automatisch erhaltene Zugriffsrechte zu entziehen oder anzupassen.

Art. 9 Datenhaltung und Datenübertragung

Dieser Artikel macht in *Absatz 1 Buchstaben a und b*, sowie Absatz 2 Buchstabe c Vorgaben zur Löschung von Daten des elektronischen Patientendossiers, welche nach Absatz 1 Buchstabe c nur in ausschliesslich dafür vorgesehenen «sekundären» Ablagen, und somit als «Kopie» der Originaldokumente in den Primärsystemen gespeichert werden dürfen. In technisch begründeten Ausnahmefällen (vgl. Erläuterungen zu Art. 9 Abs. 1 Bst. c) liegen die Daten resp. Dokumente nicht in Kopie vor, sondern werden direkt aus den integrierten Ablagen der Primärsysteme abgerufen. In diesen Fällen beschränken sich die Vorgaben zum Löschen von Daten nach *Absatz 1 Buchstaben a und b* sowie nach *Absatz 2 Buchstabe c* auf den Eintrag im Dokumentenregister.

Absatz 1
Buchstabe a hält fest, dass Daten, die durch die Gesundheitsfachpersonen im elektronischen Patientendossier eingestellt worden sind, nach zehn Jahren gelöscht werden müssen. Ziel dieser Regelung ist, das elektronische Patientendossier möglichst datensparsam und für alle Beteiligten nützlich und übersichtlich zu halten. Die von der Patientin oder dem Patienten erfassten Daten unterliegen keiner Löschungsfrist.

Eine Aufhebung des elektronischen Patientendossiers nach *Artikel 20 Absatz 1*, soll nach *Buchstabe b* zur Folge haben, dass wieder der Zustand hergestellt wird, wie er vor der Erstellung des elektronischen Patientendossiers bestand. Dazu sind sämtliche Daten des jeweiligen Patienten oder der jeweiligen

Patientin aus allen abfragbaren Systemen der Gemeinschaft (Dokumentenregister, Dokumentenablagen, Patientenindex, etc.) zu löschen (vgl. Ziff. 2.1.1.2 der TOZ). Die Verantwortung zur Information einer Gemeinschaft über die Aufhebung eines elektronischen Patientendossiers liegt bei der Stammgemeinschaft des betroffenen Patienten oder der betroffenen Patientin (vgl. Art. 20 Abs. 2 Bst. a Ziff. 1). Protokolldaten und Daten in den nicht abfragbaren Primärsystemen sowie in Datensicherungen sind davon nicht betroffen.

Aus Datenschutz- und Datensicherheitsgründen dürfen die behandlungsrelevanten Daten des elektronischen Patientendossiers nach *Buchstabe c* nur in ausschliesslich für diesen Zweck vorgesehenen «sekundären» Dokumentenablagen der Gemeinschaft oder deren Gesundheitseinrichtungen gespeichert werden. In diesen Dokumentenablagen dürfen darüber hinaus nur Dokumente des elektronischen Patientendossiers gespeichert werden. Gesundheitsfachpersonen erfassen somit jeweils Kopien der in ihren Primärsystemen erstellten Daten und Dokumente. Ziel der Regelung ist es, dass die Dokumente des elektronischen Patientendossiers technisch von den Dokumenten in den «primären» Dokumentenablagen der Primärsysteme getrennt gehalten werden (vgl. Ziff. 2.2 der TOZ): Die Daten des elektronischen Patientendossiers unterliegen anderen Aufbewahrungs- und Löschpflichten als die Daten der Primärsysteme und müssen beispielsweise nach 10 Jahren (*Abs. 1 Bst. a*) oder nach einer Aufhebung des elektronischen Patientendossiers (*Abs. 1 Bst. b*) vollumfänglich respektive auf Wunsch des Patienten oder der Patientin (*Abs. 2 Bst. b und c*) selektiv gelöscht werden. Zudem würden Dokumentenablagen mit einer hybriden Nutzung oder einem über das elektronische Patientendossier hinausgehenden Datenbestand (beispielsweise ein zugleich intern genutztes «Archivsystem» eines Spitals) ein unverhältnismässiges Risiko für den Datenschutz und die Datensicherheit darstellen, da sich solche Systeme nicht genügend gut von grösseren Benutzergruppen und Netzwerkbereichen abschotten lassen und zudem das Risiko der «Diffusion» von Daten in das elektronische Patientendossier und *vice versa* bestünde. Unabhängig davon, ob die Trennung physikalisch (d. h. durch eigene Hardware) oder logisch (z. B. durch getrennte Datenbanken, virtuelle Maschine, Mandantentrennung, etc.) geschieht, muss die Isolation der «sekundären» Dokumentenablagen von den «primären» Daten der Primärsysteme eine sichere Abschottung erlauben und eine unbeabsichtigte «Durchlässigkeit» (sog. «Isolationsversagen») mit technischen Mitteln sicher verhindern.

Absatz 2

Aufgrund des informationellen Selbstbestimmungsrechts kann die Patientin oder der Patient selber über den Inhalt ihres bzw. seines elektronischen Patientendossiers entscheiden. Daraus ergeben sich für sie oder ihn die in *Absatz 2* erwähnten Möglichkeiten (vgl. Ziff. 2.3 der TOZ).

Das EPDG statuiert in Artikel 3 Absatz 2 die Vermutung, dass Gesundheitsfachpersonen davon ausgehen dürfen, dass Patientinnen und Patienten, die ein elektronisches Patientendossier erstellt haben, wünschen, dass ihre Daten dort erfasst werden. Nach *Absatz 2 Buchstabe a* EPDV kann der Patient oder die Patientin dieser Vermutung im Einzelfall widersprechen und Gesundheitsfachpersonen jederzeit anweisen, bestimmte Dokumente nicht in seinem oder ihrem elektronischen Patientendossier zu erfassen.

Der Patient oder die Patientin kann nach *Buchstabe b* verlangen, dass Dokumente, die gemäss Absatz 1 gelöscht werden sollen, weil die zehnjährige Aufbewahrungsfrist abgelaufen ist, weitere zehn Jahre im elektronischen Patientendossier verfügbar bleiben.

Buchstabe c räumt den Patientinnen und Patienten das Recht ein, zu veranlassen, dass bestimmte auf sie oder ihn bezogene Daten des elektronischen Patientendossiers gelöscht werden. Dabei müssen die entsprechenden Einträge aus den Dokumentenregistern, sowie die Dokumente aus den Dokumentenablagen des elektronischen Patientendossiers gelöscht werden. Für Dokumente, die nicht gemäss *Absatz 1 Buchstabe c* als Kopie aus den gemeinschaftsinternen Dokumentenablagen, direkt aus den «primären» Dokumentenablagen der Primärsysteme abgerufen werden, ist lediglich der Eintrag im Dokumentenregister zu löschen, damit geltende Dokumentations- und Aufbewahrungspflichten der Gesundheitsfachpersonen nicht tangiert werden.

Absatz 3
Für die Gewährleistung der Interoperabilität und einer datenschutzkonformen und sicheren Datenbereitstellung sowie eines ebensolchen Datenabrufs, müssen die Gemeinschaften die in *Absatz 3 Buchstaben a bis e* definierten Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers einhalten. Diese Vorgaben konkretisieren beispielsweise die Suche nach Patientinnen und Patienten im Patientenindex, die Kommunikation mit dem Dokumentenregister, den Dokumentenablagen und der Berechtigungssteuerung zur Abfrage oder Bereitstellung von Dokumenten, sowie die Kommunikation mit den Abfragediensten nach den Artikeln 39 und 40 und der Identifikationsdatenbank («UPI») der ZAS. Die Einhaltung dieser, für die Interoperabilität aber auch den Datenschutz und die Datensicherheit relevanten Anforderungen, wird im Rahmen des Zertifizierungsverfahrens von den Zertifizierungsstellen mit einem vom BAG zur Verfügung gestellten Zertifizierungssystems (*Art. 27 Abs. 3 Bst. c*) überprüft. Dieses überprüft beispielsweise, ob bei der Umsetzung der technischen Schnittstellen und in der Kommunikation zwischen Gemeinschaften und Stammgemeinschaften sowie mit der ZAS und den Abfragediensten die massgeblichen Spezifikationen auf der strukturellen und semantischen Ebene eingehalten werden.

Buchstabe a (Berechtigungssteuerung)
Nach *Buchstabe a* müssen Gemeinschaften und Stammgemeinschaften die Berechtigungssteuerung so umsetzen, dass die Vorgaben nach *Artikel 9 EPDG* und die Bestimmungen zur Vergabe und Weitergabe der Zugriffsrechte nach den *Artikeln 1 und 2 Absatz 5 EPDV* korrekt umgesetzt und durchgesetzt werden (vgl. Ziff. 2.4 der TOZ). Für Gemeinschaften gilt insbesondere, dass die von der Patientin oder dem Patienten über das Zugangsportal der Stammgemeinschaft vorgenommene Zuordnung von Daten des elektronischen Patientendossiers zu einer der vier Vertraulichkeitsstufen (vgl. *Art. 1*) für die bei ihr gespeicherten Dokumente übernommen werden muss (vgl. Ziff. 2.4.1.1 der TOZ).

Darüber hinaus müssen Gemeinschaften sicherstellen, dass Zugriffe auf Daten ihrer Dokumentenablagen und Dokumentenregister nur gemäss einer zuvor eingeholten Zugriffsentscheidung der Stammgemeinschaft erfolgen kann (vgl. Ziff. 2.5 der TOZ). Dies bedingt neben der Befolgung der Regelauswertungs-Entscheidung, ob z. B. die abfragende Gesundheitsfachperson Zugriff auf die Vertraulichkeitsstufe des angefragten Dokuments erhalten darf, auch die Berücksichtigung, dass z. B. ein Notfallzugriff nur auf die Vertraulichkeitsstufen «nützliche Daten» und «medizinische Daten» möglich ist und allfällige von der Patientin oder dem Patienten vorgenommene einschränkende, erweiternde oder ausschliessende Einstellungen für das Zugriffsrecht in medizinischen Notfallsituationen nach *Artikel 3 Buchstabe b* berücksichtigt werden müssen. Zur weiteren Absicherung, beispielsweise gegen sogenannte «man-in-the-client»-Angriffe, fordern die TOZ für Notfallzugriffe zudem, dass ein solcher nur nach einer nicht automatisiert reproduzierbare, manuellen Interaktion (z. B. durch die Eingabe eines Einmalpasswortes oder einer durch ein lokales Token generierten PIN) möglich sein darf (vgl. Ziff. 2.6.1.2 der TOZ).

Weitere Verpflichtungen für Gemeinschaften leitet sich aus den Optionen für Patienten nach *Artikel 3* ab. So muss für jedes neue Dokument berücksichtigt werden, welche Vertraulichkeitsstufe neu eingestellten Daten zugewiesen werden soll, denn dies kann der Patient oder die Patientin in der Stammgemeinschaft optional festlegen (vgl. *Art. 3 Bst. b*).
Weitere Erläuterungen zu den Vertraulichkeitsstufen, Zugriffsrechten und Optionen der Patientinnen und Patienten sind in den entsprechenden Erläuterungen zu den *Artikeln 1–3* aufgeführt.

Da die korrekte Umsetzung der Berechtigungssteuerung und die verlässliche Durchsetzung der Zugriffsrechte für die Gewährleistung des Datenschutzes kritisch ist, müssen die Funktionen und die korrekte Regelauswertung der Berechtigungssteuerung auch im Rahmen automatisierter Testszenarien überprüft werden können (vgl. Ziff. 2.7 der TOZ).

Buchstabe b (Metadaten)
Metadaten beschreiben die im elektronischen Patientendossier bereitgestellten Dokumente in struktu-

rierter Weise (z. B. technisches Dateiformat des Dokuments, Typ des Dokuments, Autor, Erstellungsdatum, Vertraulichkeitsstufe). Nach *Buchstabe* b sind dabei die im *Anhang 3* der EPDV-EDI definierten Metadaten-Attribute sowie deren zulässigen Werte oder Wertebereiche zu verwenden. Dabei kommen vielfach Wertelisten aus standardisierten semantischen Codierungen zum Einsatz (z. B. aus der Terminologie «Snomed CT»), die eine semantische Interoperabilität der Dokument-bezogenen Metadaten sicherstellen können. Für eine schweizweit einheitliche und technisch unterstützte Nutzung der Metadaten führt der Bund den Abfragedienst für die zugelassenen Metadaten nach *Artikel 38 Absatz 1 Buchstabe b*.

Buchstabe c (Austauschformate)
Alle durch die Metadaten klassifizierbaren Dokumenttypen können als unstrukturierte Dokumente (z. B. Bilddateien oder PDF/A) bereitgestellt werden. Für die Bereitstellung strukturierter Daten durch Gesundheitsfachpersonen gilt nach *Buchstabe c* jedoch, dass die in Anhang 4 der EPDV-EDI vorgegebenen Austauschformate für medizinische Inhalte zu verwenden sind. Für eine schweizweit einheitliche und technisch unterstützte Nutzung der Austauschformate führt der Bund den Abfragedienst für Austauschformate nach *Artikel 38 Absatz 1 Buchstabe c*.

Buchstabe d (Integrationsprofile nach IHE, nationale Anpassungen der Integrationsprofile nach IHE, nationale Integrationsprofile des EDI)
Integrationsprofile sind technische Leitfäden zur technisch interoperablen Umsetzung spezifischer Anwendungsfälle meist unter Verwendung allgemein anerkannter Normen und Standards.

Nach *Absatz 3 Buchstabe d* sind für die Informationsübertragung innerhalb der Gemeinschaften sowie zwischen Gemeinschaften und Stammgemeinschaften grundsätzlich die Transaktionen der in Anhang 5 der EPDV EDI aufgeführten Integrationsprofile von «IHE» (*Integrating the Healthcare Enterprise*) mit den entsprechenden nationalen Anpassungen («national extensions») sowie für spezifische Anwendungsfälle die Transaktionen der eigenen nationalen Integrationsprofile des EDI zu verwenden.

Im Rahmen der Zertifizierung wird die Konformität der Datenübertragung gemäss den Integrationsprofilen, den nationalen Anpassungen von Integrationsprofilen und den nationalen Integrationsprofilen mittels eines Zertifizierungssystems nach Artikel 27 Absatz 3 Buchstabe c überprüft. Die Bestimmungen zur Datenübertragung betreffen einerseits die Schnittstellen der für die Bereitstellung und Abfrage von Dokumenten verwendeten Primärsysteme und internen Zugangsportale (IHE-«Akteure» «Document Source» und «Document Consumer») und andererseits die gemeinschaftsinternen Schnittstellen zu weiteren Systemen, wie beispielsweise den Zugangspunkt der Gemeinschaften (Gateways), den Patientenindex, die Dokumentenablagen und die Dokumentenregister. Darüber hinaus muss auch die Kommunikation mit den Abfragediensten nach Artikel 38, sowie mit der ZAS den Vorgaben entsprechend auf Konformität geprüft werden. Damit soll einerseits sichergestellt werden, dass die Kommunikation zwischen allen Komponenten technisch und semantisch interoperabel funktioniert aber auch, dass in jeder Gemeinschaft die gleichen, standardisierten Schnittstellen für die anzubindenden Primärsysteme verfügbar sind. Um die konforme Anbindung von bisher nicht IHE-fähigen (Primärsystem-)Produkten zu erleichtern, steht den Herstellern ein Software-Adapter (der sogenannte eHealth-Connector) zur Verfügung, dessen Integration die Konforme Anbindung ihrer Produkte an die Schnittstellen innerhalb der Gemeinschaft erleichtern kann. Sofern die Produkte die vorgesehenen Vorgaben bereits nativ beherrschen, ist eine Verwendung des eHealth-Connectors natürlich nicht notwendig. Eine standardisierte Anbindung an die stets gleichen Schnittstellen in den Gemeinschaften, kann für Anbieter, Anwender und Gemeinschaften als Investitionsschutz angesehen werden, da einmalige Aufwände vielfach verwendet werden können.

Die unter *Ziffer 1* im *Anhang 5* der EPDV-EDI aufgeführten «IHE-Integrationsprofile» («Integrating the Healthcare Enterprise») sind international anerkannt und daher für einen universellen Einsatz konzipiert. Damit die konkreten Anforderungen des EPDG und des vorliegenden Ausführungsrechts eingehalten werden, bedürfen sie jedoch in der Regel weitergehenden spezifischen Konkretisierungen und Festlegungen (so genannte «nationale Anpassungen»). Diese legen beispielsweise fest, dass für gewisse

Abfragen ausschliesslich die Patientenidentifikationsnummer als nationaler Identifikator zu verwenden ist und nicht etwa die AHVN13. In Ziffer 2 des Anhangs 5 der EPDV-EDI werden zudem vom EDI eigene, sogenannte «nationale Integrationsprofile» erlassen, um den Besonderheiten der dem elektronischen Patientendossier zugrundeliegenden «Architektur eHealth Schweiz» wie z. B. der dezentralen Datenhaltung und Patientenverwaltung Rechnung zu tragen. So regelt das nationale Integrationsprofil CH:ADR («Authorisation Decision Request») wie berechtigungsrelevante Informationen an die über den Zugriff entscheidende Stammgemeinschaft übermittelt werden und in der Folge das Ergebnis der Regelauswertung – die Zugriffsentscheidung – der anfragenden Gemeinschaft zurückgegeben wird. Das nationale Integrationsprofil CH:PPQ («Privacy Policy Query») wiederum ermöglicht die Änderung der Konfiguration der Berechtigungssteuerung durch den Patienten oder von der Patientin sowie von dazu ermächtigten Gesundheitsfachpersonen. Teil dieses nationalen Integrationsprofils ist zudem das technische Austauschformat, welches für die Übernahme der Konfiguration der Berechtigungssteuerung bei einem Wechsel der Stammgemeinschaft zu verwenden ist.

Integrationsprofil-übergreifende Anforderungen betreffen insbesondere die Sicherstellung der Integrität und Vertraulichkeit der übermittelten Daten. So sind für die Sicherstellung der Integrität von elektronischen Nachrichten vertrauenswürdige elektronische Zertifikate zu verwenden, mit denen die Authentizität von Nachrichten verifiziert werden kann (Vgl. Ziffer 2.09.22 der TOZ). In dem Zusammenhang ist für die in der Kommunikation und die Protokollierung notwendigen Zeitstempel die gesetzliche Zeit der Schweiz, verbreitet vom eidgenössischen Institut für Metrologie (METAS), zu verwenden. Die Uhren aller relevanten informationsverarbeitenden Systeme müssen daher mit der gesetzlichen Zeit der Schweiz synchronisiert sein (vgl. Ziff. 2.09.25 der TOZ).

Buchstabe e (Protokolldaten)
Nach *Artikel 10 Absatz 1 Buchstabe a EPDG*, ist jede Bearbeitung von Daten zu protokollieren. Für die Datenschutzkontrolle, insbesondere durch die Patientinnen und Patienten, bedarf es einer angemessenen Nachvollziehbarkeit der Bearbeitung der personenbezogenen Daten des elektronischen Patientendossiers durch eine aussagekräftige und revisionsfeste Protokollierung aller datenschutzrelevanten Ereignisse. Die Protokollierungsanforderungen gemäss Artikel 9 Absatz 3 Buchstabe e EPDV beziehen sich somit auf die aus Datenschutzsicht relevanten Aspekte, die in den TOZ konkretisiert werden (vgl. Ziff. 2.11 der TOZ).

Zu den zu protokollierenden Ereignissen zählen insbesondere die Bereitstellung und der Abruf von Dokumenten, die Änderung von Metadaten (z. B. der Vertraulichkeitsstufe), die Anpassungen an der Konfiguration der Berechtigungssteuerung sowie Authentisierungs- und Autorisierungsentscheide und die Daten, aufgrund derer diese Entscheide gefällt wurden. Die für die Ereignisse protokollierten Protokolldaten müssen Informationen darüber enthalten, wer, wann und wie auf welche Daten zugegriffen oder sie erstellt hat. Bei der Protokollierung muss zudem zwischen Zugriffen, die aus der Nutzung des elektronischen Patientendossiers resultieren und technisch-administrativen Zugriffen im Rahmen des Systembetriebs differenziert werden. Die Protokollinformationen für die Einsichtnahme durch den Patienten oder die Patientin enthalten mindestens folgende Angaben (vgl. Ziff. 2.10.4 der TOZ):

- Zeitpunkt des Zugriffs;
- die Kennung des jeweiligen Benutzers;
- die Kennung des zugreifenden Systems;
- die aufgerufene Transaktion (Suche, Bereitstellung, Lesen, Schreiben, Mutieren, etc.);
- der Kontext der Transaktion (z. B. Notfallzugriff);
- das betroffene Patientendossier;
- die betroffenen Daten oder Dokumente.

Andere Protokollierungen, die im Rahmen des technischen Betriebs erfolgen, aber nicht datenschutz- oder datensicherheitsrelevant sind (z. B. Betriebsparameter erfassen), sind nicht Gegenstand dieser Anforderung.

Damit die Patientin oder der Patient die dezentral anfallenden Protokolldaten, die die Bearbeitung des

eigenen elektronischen Patientendossiers betreffen, jederzeit einsehen kann, sind die Protokolldaten von den Gemeinschaften zum Abruf über das Zugangsportal für Patientinnen und Patienten (vgl. Art. 18) bereitzustellen. Die nationalen Anpassungen für den Abruf von Protokolldaten (betreffend die IHE-Integrationsprofile ATNA, XDS.b und XCA) in Ziffer 2 des Anhangs 5 der EPDV-EDI spezifizieren die dazu notwendigen Transaktionen und das technische Austauschformat für den Abruf von Protokolldaten (vgl. Ziff. 2.10.7 der TOZ). Dadurch hat der Patient oder die Patientin über die Einsichtnahme im Zugangsportal stets die Kontrolle darüber, wer auf sein oder ihr elektronisches Patientendossier zugegriffen hat und kann bei einem allfällig unberechtigten Zugriff rechtliche Schritte einleiten (vgl. Art. 24 EPDG).

Auch die technisch-administrativen Protokolldaten im Rahmen des Systembetriebs entstehen dezentral in den Gemeinschaften. Sie dienen in erster Linie der Überprüfung der Einhaltung der Datenschutzvorschriften. Daher dürfen sie nur denjenigen Personen oder Organen zugänglich sein, welche die Umsetzung dieser Vorschriften zu überwachen haben. Sie müssen mit geeigneten technischen oder organisatorischen Mitteln gegen Veränderungen geschützt werden und für mindestens 10 Jahre aufbewahrt werden (vgl. Ziff. 2.10 der TOZ).

Art. 10 Zugangsportal für Gesundheitsfachpersonen

Das Zugangsportal für Gesundheitsfachpersonen muss den in Ziffer 3 der TOZ aufgeführten Anforderungen entsprechen. So muss z.B. die Darstellung der Daten und Dokumente des elektronischen Patientendossiers alle relevanten Informationen korrekt und vollständig präsentieren (vgl. Ziff. 3.2 der TOZ). Dies gilt insbesondere für strukturierte Daten wie beispielsweise medizinische Austauschformate nach *Artikel 9 Absatz 3 Buchstabe c*. Das Zugangsportal muss darüber hinaus beispielsweise klar erkennen lassen, ob ein Dokument durch eine Gesundheitsfachpersonen oder durch den Patienten oder die Patientin selbst bereitgestellt wurden, welche Dokumente nicht mehr gültig sind oder welche weiteren Versionen eines Dokumentes gegebenenfalls auch vorhanden sind.
Zur Förderung der hindernisfreien Zugänglichkeit für Gesundheitsfachpersonen mit Behinderungen, altersbedingten oder sprachlichen Einschränkungen müssen die Zugangsportale so ausgestaltet sein, dass sie für diese Personengruppen barrierefrei nutzbar sind, z. B. indem sie mit Vorleseprogrammen gelesen und auch ohne Maus angesteuert werden können. Massgeblich ist hierbei die Konformitätsstufe AA der Konformitätsbedingungen gemäss «Web Content Accessibility Guidelines 2.0». Da viele Anforderungen auch der allgemeinen Benutzbarkeit zuträglich sind, stellt die Einhaltung dieser Richtlinien einen Mehrwert auch für alle anderen Nutzer dar (vgl. Ziff. 3.3. der TOZ).

Aus Gründen der Interoperabilität und der Datensicherheit sind die für das elektronische Patientendossier zugelassenen Dateitypen in Ziffer 8 des Anhangs 3 der EPDV-EDI abschliessend aufgeführt (vgl. Ziff. 3.4 der TOZ). Das Zugangsportal muss die Möglichkeit bieten, diese Dateitypen bereitzustellen sowie abzurufen und darzustellen. Dateien anderer Formate (z. B. Word-Dokumente) müssen vor dem Abspeichern in einer Dokumentenablage, in ein zugelassenes Format (z. B. PDF/A) umgewandelt werden.

Damit Gesundheitsfachpersonen ihrer Dokumentationspflicht nachkommen können, muss das Zugangsportal den Abruf von Dateien zum Abspeichern auf dem lokalen System unterstützen («Download»). Aus Sicherheitsgründen sind für den Abruf und Download von Dokumenten Obergrenzen für die Anzahl an Dokumenten (sog. «rate limits») zu definieren, welche beim Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen auslösen (vgl. Ziff. 3.5.2 der TOZ). Beispielsweise könnte ein Überschreiten der Obergrenze bedingen, dass zuvor ein Captcha («Completely Automated Public Turing test to tell Computers and Humans Apart») absolviert werden muss, um unzulässige, technisch automatisierte Massen-Abrufe zu begrenzen.

Art. 11 Datenschutz und Datensicherheit

Nach *Absatz 1* müssen Gemeinschaften ein Datenschutz- und Datensicherheitsmanagementsystem, betreiben, wie in der Norm ISO/IEC 27001:2013 beschrieben. Es muss die Komplexität und Grösse der Gemeinschaft, sowie den Umfang der in der Gemeinschaft erfassten Daten und Dokumente des elektronischen Patientendossiers berücksichtigen (vgl. Ziff. 4.2 der TOZ). Ein Datenschutz- und Datensicherheitsmanagementsystem nach ISO/IEC 27001:2013 verfolgt eine ganzheitliche, koordinierte Betrachtung der Datenschutz- und Datensicherheitsrisiken der Gemeinschaft, um ein umfassendes Paket von geeigneten Sicherheitsmassnahmen (z. B. Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen) im Rahmen eines einheitlichen Managementsystems planen, einführen, überprüfen und verbessern («*plan, do, check, act*»; vgl. Kapitel 4 – 10 der ISO/IEC 27001:2013) zu können.

Das durch eine Gemeinschaft zu führende Datenschutz- und Datensicherheitsmanagementsystem muss zusätzlich zu den in den *Buchstaben a–f* aufgeführten Anforderungen unter anderem einen Risikokatalog und einen Risikobehandlungsplan sowie ein Inventar relevanter Betriebsmittel (Hardware, Software, Datenbestände, Aufbauorganisation, Prozesse, etc.) umfassen (vgl. Ziff. 4.2.2 der TOZ). Zudem sind alle sicherheitsrelevanten Veränderungen an den Betriebsmitteln zu beurteilen und zu dokumentieren.

Nach *Buchstabe a* muss eine Gemeinschaft eine fachlich und organisatorisch unabhängige Person benennen, die für den Datenschutz und die Datensicherheit zuständig ist. Sie muss über die für die Aufgabenerfüllung erforderlichen Kompetenzen und Ressourcen verfügen und ist für die Entwicklung, Umsetzung und Überwachung von Massnahmen zur Sicherstellung von Datenschutz und Informationssicherheit, sowie für die Anwendung korrigierender Massnahmen verantwortlich (vgl. Ziff. 4.3 der TOZ).

Nach *Buchstabe b* ist ein System zur Erkennung von und zum Umgang mit Sicherheitsvorfällen einzurichten (vgl. Ziff. 4.4 der TOZ). Da eine *a priori* Sicherheit nie vollständig erzielt werden kann, ist es umso wichtiger, allfällige Sicherheitsvorfälle zumindest *a posteriori* rasch zu erkennen und mit definierten Massnahmen, Prozessen und klaren Verantwortlichkeiten darauf reagieren zu können. Gemeinschaften müssen dazu ein so genanntes *Security Information and Event Management System* (SIEM) einrichten, dass Anomalien im System und in den Bearbeitungsmustern erkennen kann und sicherstellt, dass diese angemessen organisatorisch und technisch adressiert werden. Das SIEM wird gemeinschaftsspezifisch aufgebaut, es erkennt und adressiert mindestens Angriffe aus dem Internet, unübliche Häufung von schreibenden oder lesenden Zugriffen auf die Dokumentenablagen, das Dokumentenregister oder den Patientenindex, welche auf eine missbräuchliche Nutzung oder automatisierte Attacke hinweisen. Weiter müssen ungewöhnliche und kritische Mutationen von Zugriffsrechten in der Berechtigungssteuerung oder dem Identitäts- und Zugangsmanagementsystem (IAM) erkannt und behandelt werden. Weitere Vorgaben in den TOZ betreffen beispielsweise den Schutz vor Schadcode und die Erkennung und den Umgang mit Sicherheitsschwachstellen(vgl. Ziff. 4.6 und 4.7 der TOZ).

Für den Umgang mit erkannten Sicherheitsvorfällen konkretisiert die TOZ in Ziffer 4.5 zudem Vorgaben an die Verfahren zur Meldung und Behandlung von Datenschutz- und Datensicherheitsereignissen. So müssen beispielsweise Anlaufstellen für die Meldung von Datenschutz- und Datensicherheitsereignissen sowohl innerhalb der Gemeinschaft selbst, als auch bei den Betriebsorganisationen bezeichnet werden und Notfallprozesse definiert werden, die geeignet sind, unter definierten Bedingungen, Systeme vom Gesamtsystem isolieren zu können («Containment»-Strategie). Dies um das potentielle Schadensausmass begrenzen zu können oder um andere vulnerable Systemteile nicht ebenfalls zu gefährden. Zur Erfüllung von Artikel 11 Absatz 2 müssen Gemeinschaften zudem formale Verfahren für die Eskalation von besonders kritischen Datenschutz- oder Datensicherheitsereignissen durch Meldung an das BAG und die Zertifizierungsstelle definiert haben sowie deren Einhaltung einfordern und kontrollieren (vgl. Ziff. 4.13 der TOZ).

Nach *Buchstabe c* ist ein Verzeichnis aller in der Gemeinschaft für das elektronische Patientendossier verwendeten Elemente der Informatikinfrastruktur vorzusehen (vgl. Ziff. 4.8.3 der TOZ). Das Verzeichnis aller angeschlossenen Primärsysteme nach *Buchstabe d* dient dazu, eine Übersicht über alle Primärsysteme zu haben, welche Daten mit dem elektronischen Patientendossier austauschen (vgl. Ziff. 4.8.3.8 der TOZ).

Nach *Buchstabe e* müssen Gemeinschaften über das Datenschutz- und Datensicherheitsmanagmentsystem spezifische Datenschutz- und Datensicherheitsvorgaben für die angeschlossenen Gesundheitseinrichtungen, sowie indirekt auch für deren Gesundheitsfachpersonen und allfällige weitere Mitarbeitende wie z.B. Mitarbeitende der Spitalinformatik festlegen (vgl. Ziff. 4.9 der TOZ). Dazu gehört beispielsweise die Vorgabe, dass Gemeinschaften die ihnen angeschlossenen Gesundheitseinrichtungen dazu verpflichten müssen, ihre auf das elektronische Patientendossier zugreifenden Gesundheitsfachpersonen über die Aufgaben, Rechte und Pflichten im Zusammenhang mit der Bearbeitung von Daten des elektronischen Patientendossiers sowie Risiken und Massnahmen bezüglich Datenschutz und Datensicherheit zu hinzuweisen. Gesundheitseinrichtungen müssen von den Gemeinschaften ebenfalls dazu verpflichtet werden, eine sichere Konfiguration (beispielsweise durch Programme zum Schutz vor Schad-Software und netzwerktechnische Schutzmassnahmen) derjenigen Endgeräte sicherzustellen, die von den Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier genutzt werden (vgl. Ziff. 4.9.3 der TOZ). Gesundheitseinrichtungen wiederum müssen ihre Gesundheitsfachpersonen zur Einhaltung der geforderten Massnahmen verpflichten.

Die Gemeinschaft kann den Datenschutz und die Datensicherheit nicht ohne die Mitwirkung der angeschlossenen Gesundheitseinrichtungen und allfälligen Lieferanten und Dienstleistungserbringern gewährleisten. Daher müssen neben den Mitarbeitenden der Gemeinschaft (z. B. Personal der Kontaktstelle für Gesundheitsfachpersonen) auch allfällig beigezogene Dritte (z. B. Betreiber der gemeinschaftsinternen Informatikinfrastruktur) nach *Buchstabe f* die spezifischen Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft einhalten. Bezüglich Personal legen die TOZ dazu insbesondere Anforderungen an die Verwaltung von Personen und deren Zugänge und Benutzerrechte fest (vgl. Ziff. 4.10 der TOZ). Darüber hinaus gelten gemäss den TOZ für Gemeinschaften weitergehende Regelungen zum Lieferantenmanagement, mit dem Ziel, dass ein durchgehend hohes Sicherheitsniveau für alle beteiligten Akteure (Gemeinschaften, Einrichtungen, Lieferanten und Unterlieferanten) unabhängig von der Organisations-Struktur aufrecht erhalten werden kann (vgl. Ziff. 4.11 und 4.12 der TOZ). Beispielsweise besteht die Verpflichtung für Gemeinschaften, die Einhaltung der Datenschutz- und Datensicherheitsanforderungen innerhalb der gesamten Lieferkette weiter zu verpflichten, für den Fall, dass die Lieferanten selbst wieder Unterlieferanten beauftragen (vgl. Ziff. 4.11.5.5 der TOZ).

Die Meldepflicht für sicherheitsrelevant eingestufte Vorfälle an die Zertifizierungsstelle und das BAG nach *Absatz 2* soll die notwendigen Informationen über gefundene oder ausgenützte Schwachstellen in der Organisation oder der Informatikinfrastruktur einer Gemeinschaft liefern, um nach Analyse und Beurteilung allenfalls Massnahmen zur Verhinderung weiterer Vorfälle einzuleiten. Im Vordergrund steht dabei vor allem der Erkenntnis- und Erfahrungsgewinn für Gemeinschaften und Stammgemeinschaften, aber auch für die Zertifizierungsstellen und nicht zuletzt auch das BAG als regulierende Behörde im Bereich des Datenschutzes und der Datensicherheit. So können durch regelmässige Auswertungen dieser Ereignisse allfällige Trends in der Bedrohungslandschaft aufgezeigt werden, die es Gemeinschaften erlauben rechtzeitig entsprechenden Gegenmassnahmen vorzusehen. Liegt eine schwerwiegende Gefährdung des Schutzes oder der Sicherheit der Daten des elektronischen Patientendossiers vor, so kann das BAG nach *Artikel 36* entsprechende Massnahmen anordnen. Gemeinschaften und Stammgemeinschaften, sowie deren Betriebsorganisationen können darüber hinaus auch von den freiwilligen Beratungs- und Informationsleistungen der Melde- und Analysestelle Informationssicherung des Bundes «MELANI» profitieren, welche ihren Kundenkreisen wertvolle Informationen über aktuelle Gefahren und geeignete Massnahmen bereitstellen kann sowie den Informationsaustausch auch zwischen den Betreibern von gefährdeten oder kritischen Infrastrukturen fördert.

Nach *Absatz 3* legt das EDI in den Ziffern 4.13 bis 4.23 der TOZ, ergänzend zu den Vorgaben von

Absatz 1 Buchstaben a–f, weitere Anforderungen in Bezug auf Datenschutz und Datensicherheit fest. Diese umfassen unter anderem Vorgaben zu folgenden Bereichen:

- Betriebssicherheit, Systemwiederherstellung und Protokollierung des Systembetriebs (vgl. Ziff. 4.14 der TOZ);
- Anschaffung, sichere Entwicklung und Instandhaltung von Systemen (vgl. Ziff. 4.15 der TOZ);
- Verschlüsselung in der Kommunikation und Datenspeicherung (vgl. Ziff. 4.16 bis 4.18 der TOZ);
- Verwaltung von Netzwerken und Netzwerkdiensten Systembetriebs (vgl. Ziff. 4.19 bis 4.22 der TOZ);
- Verfügbarkeit (vgl. Ziff. 4.23 der TOZ).

Im nachfolgenden sei ein Aspekt besonders erläutert: Bei der Umsetzung der Anforderungen im Bereich der Datenverschlüsselung sollte die Auswahl der geeigneten Massnahmen risikobasiert erfolgen und insbesondere die Menge der zu schützenden Daten berücksichtigen. Neben der Auswahl sicherer kryptographischer Algorithmen und Verfahren, ist insbesondere eine risikogerechte Verwendung einer oder mehrerer Ebenen von Verschlüsselung (z. B. Disk-, Datenbank- oder applikatorische Verschlüsselung) vorzusehen. Auf eine Verpflichtung zur konsequent durchgehenden Verschlüsselung der übertragenen Inhalte (nicht nur des Übertragungskanals) von Endgerät zu Endgerät (end-to-end-encryption; E2EE) wurde in diesen Ausführungsbestimmungen vorderhand verzichtet. Ein Grund dafür liegt in den noch nicht abschliessend beantwortbaren Fragen zur technischen und organisatorischen Umsetzung in der dezentral ausgerichteten Architektur des EPD. Die besondere Komplexität ergibt sich aus dem Umstand, dass es sich beim EPD nicht um eine klassische «Punkt-zu-Punkt-» oder «Einer-zu-Vielen-»Kommunikation handelt – für die bereits etablierte Verfahren existieren – sondern es sich hier um einen geteilten Zugriff auf dezentral und asynchron bereitgestellte Daten mit mehreren dynamisch berechtigten Teilnehmern handelt.

Mit Blick auf steigende Datenmengen in den elektronischen Patientendossiers der Schweiz und aufgrund technischer Weiterentwicklungen, die sowohl neue Schutz- aber auch neue Angriffs-Möglichkeiten mit sich bringen werden, müssen über die Zeit auch die Datenschutz- und Datensicherheits-Risiken stets neu bewertet werden. Im Rahmen von Revisionen werden daher auch neue Massnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu eruieren sein. Die Verwendung einer möglichst "weitreichenden" starken Verschlüsselung – im Idealfall end-to-end – als ein besonders geeignetes Mittel zur Vermeidung einer Vielzahl von Bedrohungen liegt somit nahe. Es empfiehlt sich daher den Einsatz entsprechender Technologien insbesondere bei der Konzeption von neu aufzubauenden Umgebungen zu antizipieren. Zumal sich dadurch andere Risiken deutlich vermindern oder sogar vollständig eliminieren lassen. Durch den Wegfall von – mitunter kostspieligen (z. B. organisatorischen) – Massnahmen und den dadurch erzielbaren Einsparungen, liessen sich allfällige Mehrkosten in Teilen wieder kompensieren.

Um eine grösstmögliche Sicherheit der Daten des elektronischen Patientendossiers sicherzustellen, dürfen diese nach *Absatz 4* nur auf Datenspeichern gespeichert werden, die von juristische Personen unter Schweizer Recht betrieben werden, und welche den Betrieb ausschliesslich unter Schweizer Recht und gesamtheitlich innerhalb der Schweizer Landesgrenzen erbringen (vgl. Ziff. 4.24 der TOZ). Auf diese Weise unterliegen die Daten keiner vom Schweizer Recht abweichenden Gesetzgebung, wodurch mögliche Komplikationen mit ausländischen Vorschriften zum Voraus verhindert werden können.

Art. 12 Kontaktstelle für Gesundheitsfachpersonen

Gemeinschaften müssen sicherstellen, dass für alle Gesundheitsfachpersonen eine Kontaktmöglichkeit zur technischen und funktionalen Unterstützung im Umgang mit dem elektronischen Patientendossier («*Service-Desk*») zur Verfügung steht. Für die Mitarbeitenden des Service-Desk gelten spezifische Anforderungen und Vorgaben (vgl. Ziff. 5.1.2 der TOZ). So müssen diese über ihre Aufgaben, Rechte und Pflichten sowie Risiken und Massnahmen bezüglich Datenschutz und Informationssicherheit informiert sein und einer der ärztlichen Schweigepflicht analogen Verpflichtung unterstehen. Ein Remote-Zugriff

auf die Endgeräte der Gesundheitsfachpersonen darf ausschliesslich mit Kenntnis und Einwilligung des Benutzers erfolgen und muss dokumentiert werden.

2. Abschnitt: Stammgemeinschaften

Art. 13 Zusätzliche Anforderungen für Stammgemeinschaften

Stammgemeinschaften, also Gemeinschaften bei denen Patientinnen und Patienten ein elektronisches Patientendossier erstellen und ihre Zugriffsrechte verwalten können, müssen zusätzlich zu den Anforderungen des 1. Abschnitts (Art. 8 bis 12) auch die Anforderungen der *Artikel 14 bis 20* erfüllen.

Art. 14 Information der Patientin oder des Patienten

Die Einwilligung der Patientin oder des Patienten muss durch eine angemessene und sachliche Information begleitet sein. Diese wird durch die Stammgemeinschaft der Patientin oder des Patienten vorgenommen. Die Patientin oder der Patient muss umfassend und verständlich über den Zweck des elektronischen Patientendossiers, den Vorgang der Erstellung und das Funktionieren des elektronischen Patientendossiers aufgeklärt sein. Sie oder er muss abschätzen können, welche Auswirkungen die Erteilung der Einwilligung und die verschiedenen Einstellungen in der Berechtigungssteuerung, sowie ein Widerruf haben. Fehlt die Information oder ist sie ungenügend, ist die Tragweite und Gültigkeit der erteilten Einwilligung entsprechend eingeschränkt.

Die Information umfasst mindestens die nachstehend aufgeführten Punkte (vgl. auch Ziff. 6.1 der TOZ):

Nach *Buchstabe a* muss über der Zweck des elektronischen Patientendossiers informiert werden (vgl. Ziff. 6.1.1 der TOZ). Hier ist insbesondere an Ausführungen zu den in Artikel 1 EPDG genannten Aspekte (Behandlungsqualität, Patientensicherheit, Effizienz und Gesundheitskompetenz) zu denken. Für eine sachgerechte Beurteilung der Chancen und Risiken des elektronischen Patientendossiers kann es sinnvoll sein, auch darüber zu informieren für welche Zwecke das elektronische Patientendossier aufgrund technischer (z. B. keine Punkt-zu-Punkt-Kommunikation) oder rechtlicher Beschränkungen (kein Zugriff für Versicherer, Arbeitgeber oder Gesundheitsbehörden) nicht vorgesehen ist.

Nach *Buchstabe b* müssen die Grundzüge der Datenbearbeitung im Rahmen des elektronischen Patientendossier erklärt werden (vgl. Ziff. 6.1.2 der TOZ). Dazu gehört insbesondere die Darlegung, welche Datenbearbeitungsmöglichkeiten einerseits der Patientin oder dem Patienten und andererseits den zugriffsberechtigten Gesundheitsfachpersonen offen stehen. Auch die Information über die Möglichkeit des Notfallzugriffs und die Konsequenzen eines allfälligen Ausschlusses des Notfallzugriffs gehören zu den grundlegenden Informationen.

Die Information hat nach *Buchstabe c* auch den Hinweis zu umfassen, dass die Erstellung und die Verwendung des elektronischen Patientendossiers freiwillig ist. Hat die Patientin oder der Patient seine Einwilligung zur Erstellung eines Patientendossiers erteilt, so darf jedoch nach Artikel 3 Absatz 2 EPDG davon ausgegangen werden, dass sie bzw. er das Erfassen von Daten im elektronischen Patientendossier grundsätzlich wünscht. Das bedeutet dass sie bzw. er, soweit gewisse Informationen oder Behandlungen nicht im elektronischen Patientendossier gespeichert werden sollen, dies der behandelnden Gesundheitsfachperson explizit mitteilen muss (vgl. Ziff. 6.1.2.2 der TOZ). Die Information umfasst zudem den Hinweis, dass die Einwilligung zur Führung des elektronischen Patientendossiers jederzeit formlos und ohne Angabe von Gründen widerrufen werden kann (Art. 3 Abs. 3 EPDG; vgl. Ziff. 6.1.3.5 der TOZ). In dem Zusammenhang ist zudem darauf hinzuweisen, dass Dokumente eines widerrufenen elektronischen Patientendossiers nach einer erneuten Einwilligung in die Erstellung eines elektronischen Patientendossiers nicht mehr über dieses verfügbar sein werden, da eine erneute Einwilligung die Vergabe einer neuen Patientenidentifikationsnummer bedingt (vgl. Ziff. 6.1.3.6 der TOZ).

Nach *Buchstabe d* muss aus der Information hervorgehen, wie und wem Zugriffsrechte vergeben werden können (vgl. Ziff. 6.1.4 der TOZ). Dazu gehört die Information über die nach Eröffnung geltenden Einstellungen bezüglich Vertraulichkeitsstufen (*Art. 1 Abs. 2*) und Zugriffsrechten (*Art. 2 Abs. 2*) und über die Möglichkeit, diese anzupassen (vgl. dazu die Erläuterungen zu Art. 3), die Information, dass und wie Zugriffsrechte angepasst oder entzogen werden können und die Information, dass die Möglichkeit besteht, einzelne Gesundheitsfachpersonen vollständig vom Zugriff auszuschliessen (sog. Ausschlussliste; Art. 9 Abs. 3 EPDG).

Die Patientin bzw. der Patient ist nach *Absatz 2* zudem darüber zu informieren, welche Sicherheitsvorkehrungen empfohlen werden (vgl. Ziff. 6.1.5 der TOZ). Dazu gehören z.B. Hinweise zum sicheren Umgang mit der elektronischen Identität, mit dem Identifikationsmittel und mit Passwörtern, die Aufklärung über Risiken und Verhaltensempfehlungen zur Abwehr von patientengerichteten Bedrohungen wie «Social Engineering», «Phishing» u.ä., Hinweise zur Verwendung sicherer Endgeräte und Webbrowser sowie zum Einsatz von Schutzprogrammen gegen Schadprogramme oder Netzwerk-Bedrohungen.

Art. 15 Einwilligung

Das Gesetz sieht vor, dass die Einwilligung schriftlich erteilt werden muss. *Absatz 1* präzisiert, dass die Einwilligung eigenhändig zu unterschreiben ist. Die gesetzliche Formvorschrift muss auch eingehalten werden, wenn die Einwilligung auf elektronischem Weg erteilt wird. Das Obligationenrecht regelt hier unter welchen Bedingungen die elektronische Unterschrift der eigenhändigen gleichgestellt ist, nämlich dann, wenn eine elektronische Unterschrift verwendet wird, die den Anforderungen von Art. 14 Abs. 2bis OR[7] genügt (qualifizierte elektronische Signatur im Sinne des Bundesgesetzes über die elektronische Signatur, ZertES[8]). Ist diese Voraussetzung erfüllt, gilt die Schriftform als eingehalten. Die Nachvollziehbarkeit der elektronischen Abgabe der Einwilligung wird über die Protokollierung sichergestellt.

Art. 16 Verwaltung

Stammgemeinschaften müssen nach *Absatz 1* geeignete Prozesse für die Verwaltung der Patientinnen und Patienten definieren, dokumentieren, umsetzen und einhalten (vgl. Ziff. 8 der TOZ).

Buchstabe a fordert von den Stammgemeinschaften Regelungen für die übergreifenden Prozesse zur Erstellung und Aufhebung des elektronischen Patientendossiers und dem damit verbundenen Eintritt eines Patienten oder eine Patientin in die – respektive dessen oder deren Austritt aus der – Stammgemeinschaft. Massgeblich für den Eintrittsprozess sind die *Buchstaben b bis d*, die Vorgaben zur Information der Patientinnen und Patienten nach *Artikel 14*, sowie die Regelung zum Einholen der Einwilligung nach *Artikel 15*. Für den Austrittsprozesses sind die Vorgaben nach Artikel 20 massgeblich – sofern es sich um eine Aufhebung des elektronischen Patientendossiers handelt – beziehungswiese die, in der Ziffer 8.4 der TOZ weiter konkretisierten, Anforderungen an den Wechsel der Stammgemeinschaft (*Bst. e*).

Möchte ein Patient oder eine Patientin ein elektronisches Patientendossier erstellen, widerrufen oder die Stammgemeinschaft wechseln, so muss sichergestellt werden, dass es sich dabei um die korrekte Person handelt (vgl. Ziff. 8.2 der TOZ). Stammgemeinschaften müssen dazu die Patientin oder den Patienten nach *Buchstabe b* sicher identifizieren. Die Ziffer 8.2.2 der TOZ konkretisiert, dass, sofern dies nicht mit einem Identifikationsmittel eines nach *Artikel 30* zertifizierten Herausgebers durchgeführt werden kann, die Anforderungen nach *Artikel 23* erfüllt werden müssen. Eine sichere und möglichst eindeutige Identifikation ist nicht zuletzt auch die Voraussetzung für die korrekte Zuweisung der Patientenidentifikationsnummer nach *Buchstabe d*.

Buchstabe c legt fest, dass Stammgemeinschaften sicherstellen müssen, dass – analog wie bei den

[7] SR 202
[8] SR 943.03

Gesundheitsfachpersonen (Art. 8 Bst. d) – der Zugriff auf das elektronische Patientendossier durch Patientinnen und Patienten sowie durch allfällige Stellvertreter nur mittels gültiger Identifikationsmittel von einem nach Artikel 30 zertifizierten Herausgeber möglich ist (vgl. Ziff. 8.3 der TOZ). Dies bedeutet konkret, dass auch hier die Bearbeitung von Daten des elektronischen Patientendossiers nur über Zugangsportale und Endgeräte erfolgen darf, die ein Authentisierungsverfahren nach aktuellem Stand der Technik und mit mindestens zwei starken Faktoren unterschiedlicher Kategorien (z. B. «Wissen» und «Haben») unterstützen und voraussetzen.

Buchstabe d legt fest, dass Stammgemeinschaften im Rahmen der Eröffnung eines elektronischen Patientendossiers die Vorgaben der *Artikel 5 und 6* für die Beantragung der Patientenidentifikationsnummer bei der ZAS einhalten müssen. Die konkretisierenden Anforderungen in der Ziffer 8.2.2.2 der TOZ fordern, dass die Stammgemeinschaft zudem sicherstellen muss, dass ein elektronisches Patientendossier nur dann neu erstellt wird, wenn zuvor sichergestellt werden konnte, dass zu der betreffenden Person nicht bereits ein elektronisches Patientendossier besteht, und somit auch keine aktive Patientenidentifikationsnummer für diese Person bei der ZAS existiert. Damit soll gewährleistet werden, dass zu jedem Zeitpunkt maximal ein Patientendossier für eine Patientin oder einen Patienten existiert und seine oder ihre Daten und Dokumente stets nur diesem einen elektronischen Patientendossier eindeutig zugeordnet sind.
Weitere Vorgaben in der TOZ betreffen die Verpflichtung zur Übernahme der demographischen Daten der ZAS und der Patientenidentifikationsnummer in den Patientenindex (vgl. Ziff. 8.2.2.6 der TOZ) sowie die zuverlässige Zuordnung des eindeutigen Identifikator des Identifikationsmittels zum richtigen elektronischen Patientendossier (vgl. Ziff. 8.2.2.4 der TOZ). Die Zuordnung einer elektronischen Identität zu einem elektronischen Patientendossier kann auch indirekt erfolgen, indem beispielsweise das Zugangsportal die elektronische Identität des Patienten oder der Patientin mit einer eigenen lokalen «Portal-ID» der Person verknüpft, und der Patientenindex die Zuordnung dieser «Portal-ID» auf die Patientenidentifikationsnummer führt.

Buchstabe e stellt sicher, dass Patientinnen oder Patienten ihre Stammgemeinschaft wechseln können. Die Ziffer 8.4.2.1 der TOZ fordert dazu, dass die Stammgemeinschaften sicherstellen müssen, dass sie die individuelle Konfiguration der Berechtigungssteuerung («Policy configuration») in eine neue Stammgemeinschaft überführen können, und, dass sie selber in der Lage sein müssen, eine Konfiguration der Berechtigungssteuerung einer anderen Stammgemeinschaft zu übernehmen. Unabhängig von der internen technischen Umsetzung und Repräsentation der Konfiguration der Berechtigungssteuerung, müssen Stammgemeinschaften diese in einem interoperablen Format (basierend auf XACML) exportieren können, respektive einen solchen Export in ihre eigene Berechtigungssteuerung übernehmen können. Massgeblich für den Austausch der Konfiguration ist daher das spezifizierte Format des nationalen Integrationsprofils CH:PPQ des EDI nach Anhang 5 Ziffer 2 der EPDV-EDI. Da die Konfiguration der Berechtigungssteuerung nur innerhalb der eigenen Stammgemeinschaft verwaltet werden kann, können Gesundheitsfachpersonen die Weitergabe von Zugriffsrechten nach *Artikel 3 Buchstabe h* nur dann ausüben, wenn sie in der Stammgemeinschaft des sie ermächtigenden Patienten oder Patientin erfasst sind. Bei einem Wechsel der Stammgemeinschaft müssen daher gegebenenfalls Gesundheitsfachpersonen aus der neuen Stammgemeinschaft ermächtigt werden (vgl. Ziff. 8.4.2.2 der TOZ). Ebenso müssen Stellvertreterinnen und Stellvertreter in der neuen Stammgemeinschaft erneut registriert werden.

Nach *Absatz 2* müssen Stammgemeinschaften die technischen und organisatorischen Voraussetzungen erfüllen, um die Umsetzung der Bestimmungen nach *Artikel 2 Absätze 1–4* und *Artikel 3* sicherzustellen (vgl. Erläuterungen zu Ebendiesen sowie die Ziff. 8.5 bis 8.7 der TOZ).

Die Umsetzung von *Artikel 3 Buchstabe g* (Benennung einer Stellvertretung) ist neben der technischen Umsetzung mit weiteren organisatorischen Aufgaben verbunden, die in Ziffer 8.8 der TOZ konkretisiert werden und daher an dieser Stelle erläutert werden. Stammgemeinschaften müssen nach *Artikel 3 Buchstabe g* sicherstellen, dass Patientinnen oder Patienten eine Stellvertretung benennen können. Diese benötigen keine eigene Patientenidentifikationsnummer und auch kein eigenes elektronisches

Patientendossier, dürfen aber nur mit einem eigenen Identifikationsmittel eines nach Artikel 30 zertifizierten Herausgebers auf das elektronische Patientendossier des oder der vertretenen Person zugreifen. Auch die Stellvertreterinnen und Stellvertreter müssen über die grundsätzliche Funktionsweise des elektronischen Patientendossiers, sowie die Möglichkeiten, Rechte und Pflichten im Zusammenhang mit der Nutzung des elektronischen Patientendossiers informiert werden (vgl. Ziff. 8.8.3.3 der TOZ). Zur Wahrung der Persönlichkeitsrechte der vertretenen Person ist sicherzustellen, dass der Stellvertreter oder die Stellvertreterin korrekt identifiziert wird und dass dessen oder deren Recht zur Stellvertretung gemäss den zivilrechtlichen Vorschriften gegeben ist. Analog den Bestimmungen zur Identifikation von Patientinnen und Patienten müssen auch Stellvertretungen sicher identifiziert werden. Sofern die Identifikation nicht mit einem Identifikationsmittel eines nach *Artikel 30* zertifizierten Herausgebers durchgeführt werden kann, muss sie ebenfalls den Anforderungen nach *Artikel 23* entsprechen (vgl. Ziff. 8.8.3.1 der TOZ). Darüber hinaus muss gewährleistet sein, dass der Zugang des Stellvertreters oder der Stellvertreterin nur für die Dauer der Stellvertretung besteht (Ziff. 8.8.3.5 der TOZ). Mögliche Anwendungsfälle sind beispielsweise die Vertretung eines Kindes oder betagten Menschen durch seine Angehörigen oder anderen Vertrauenspersonen, falls die Patientin oder der Patient nicht im Besitz der technischen oder geistigen Voraussetzungen zur eigenständigen Verwaltung seines oder ihres elektronischen Patientendossiers sein sollte.

Art. 17 Zugangsportal für Patientinnen und Patienten

Das Zugangsportal für Patientinnen und Patienten muss den im Anhang 2 der EPDV-EDI festgelegten Anforderungen entsprechen (vgl. Ziff. 9 der TOZ). Dazu zählen neben den Vorgaben, die im Wesentlichen auch für das Zugangsportal für Gesundheitsfachpersonen nach *Artikel 10* gelten (vgl. Erläuterungen zu Art. 10), insbesondere Vorgaben zur patientengerechten Darstellung der im elektronischen Patientendossier enthaltenen Informationen sowie Vorgaben zur Umsetzung der verschiedenen Möglichkeiten der Vergabe von Vertraulichkeitsstufen und Zugriffsrechten (*Art. 1 und 2*) sowie der Optionen der Patientinnen und Patienten (*Art. 3*). Ausgenommen sind die Bestimmungen nach *Artikel 1 Absätze 2 und 3, Artikel 2 Absätze 4 und 5* sowie *Artikel 3 Buchstabe g*, da diese keine direkten Funktionen des Zugangsportals für Patientinnen und Patienten darstellen.

Die Kernfunktionen des elektronischen Patientendossiers müssen auf dem internen Zugangsportal klar von allfälligen Funktionalitäten abgegrenzt werden, die nicht zum Regelungsgegenstand des EPDG und dessen Ausführungsbestimmungen gehören (vgl. Ziff. 9.1 der TOZ). Insbesondere muss sichergestellt werden, dass Daten des elektronischen Patientendossiers nicht automatisch und ohne explizite Einwilligung des Patienten oder der Patientin in funktionelle Bereiche oder Datenspeicher «ausserhalb» des elektronischen Patientendossiers überführt werden.

Auch die Darstellung von Daten des elektronischen Patientendossiers auf der Benutzeroberfläche des internen Zugangsportals für Patientinnen und Patienten muss korrekt und vollständig sein und beispielsweise klar erkennen lassen ob ein Dokument durch eine Gesundheitsfachperson oder durch den Patienten oder die Patientin selbst bereitgestellt wurde (vgl. Ziff. 9.2 der TOZ). Die Darstellung der vom EDI vorgeschriebenen Metadaten gemäss Anhang 3 der EPDV-EDI muss die als «preferred terms» bezeichneten Begriffsübersetzungen (DE/FR/IT) oder den englischen Begriff zur Darstellung verwenden (vgl. Ziff. 9.2.1.7 der TOZ).

Zur Förderung der hindernisfreien Zugänglichkeit für Patientinnen und Patienten mit Behinderungen, altersbedingten oder sprachlichen Einschränkungen müssen die Zugangsportale so ausgestaltet sein, dass sie für diese Personengruppen barrierefrei nutzbar sind, z. B. indem sie mit Vorleseprogrammen gelesen und auch ohne Maus angesteuert werden können (vgl. Ziff. 9.3 der TOZ). Massgeblich ist hierbei die Konformitätsstufe AA der Konformitätsbedingungen gemäss «Web Content Accessibility Guidelines 2.0». Da viele Anforderungen auch der allgemeinen Benutzbarkeit zuträglich sind, stellt die Einhaltung dieser Richtlinien einen Mehrwert auch für alle anderen Nutzer dar.

Über das Zugangsportal für Patientinnen und Patienten müssen diese die Möglichkeit haben, jederzeit

die bei jeder Bearbeitung des elektronischen Patientendossiers anfallenden Protokolldaten (*Art. 10 Absatz 1 Buchstabe b EPDG*) einzusehen (vgl. Ziff. 9.6 der TOZ). Da die Protokolldaten auch dezentral in anderen Gemeinschaften anfallen, müssen diese in einem Abrufverfahren aus den jeweiligen Gemeinschaften abgerufen (vgl. Erläuterungen zu *Art. 9 Abs. 3 Bst. e*) und über das Zugangsportal für Patientinnen und Patienten in konsolidierter und lesbarer Form zur Einsicht bereitgestellt werden. Die Darstellung der Protokolldaten für die Einsichtnahme richtet sich nach den nationalen Spezifikationen nach Artikel 5 Buchstabe c der EPDV-EDI.

Art. 18 Verfügbarkeit der von Patientinnen und Patienten erfassten Daten

Der Patient oder die Patientin hat die Möglichkeit, über das Zugangsportal seiner oder ihrer Stammgemeinschaft selber eigene Dokumente im elektronische Patientendossier einzustellen (*Art. 10 Abst. 2 Bst. b Ziff. 3 EPDG*), ohne dass diese einer Löschungsfrist unterliegen (vgl. Ziff. 10.1.2 der TOZ).

Die von der Patientin oder dem Patienten selbst erfassten Daten sollen, auch aus Datensicherheitsüberlegungen, nicht in den Dokumentenablagen einer angeschlossenen Gesundheitseinrichtung gespeichert werden. Aus diesem Grund müssen Stammgemeinschaften dedizierte gemeinschaftsinterne Dokumentenablagen für die von Patienten und Patientinnen selbst erfassten Daten bereitstellen. Der verfügbare Speicherplatz für selbst bereitgestellte eigene Daten ist ausreichend zu bemessen.

Ziffer 10.2 der TOZ sieht zudem die Möglichkeit vor, dass Patientinnen und Patienten die Dokumente ihres elektronischen Patientendossiers inklusive der sie beschreibenden Metadaten aus dem System exportieren können. Die exportierten Daten können dann beispielsweise physisch, d.h. «*offline*» aufbewahrt werden und müssen bei Bedarf ohne unverhältnismässigen Aufwand wieder im elektronischen Patientendossier verfügbar gemacht werden können. Dies entspricht dem gängigen Konzept der Archivierung von nicht mehr unmittelbar für die aktuelle Behandlungssituation relevanten Dokumenten und ist in dem Sinne auch eine Massnahme zur Erhöhung von Datenschutz und Datensicherheit. Um einen Integritätsverlust (z. B. durch Manipulation der «offline»-Daten) zu verhindern, muss mit geeigneten Verfahren (z. B. mittels kryptologischer Hashfunktionen, wie z. B. SHA-3) beim Export die Voraussetzung dafür geschaffen werden, dass eine Integritätsprüfung vor einer erneuten Verfügbarmachung möglich ist. Mittels des beim Export angewandten Verfahrens ist dann vor einer erneuten Verfügbarmachung zu prüfen, ob die Integrität der Daten erhalten geblieben ist (vgl. Ziff. 10.2.2 der TOZ).

Art. 19 Kontaktstelle für Patientinnen und Patienten

Stammgemeinschaften müssen zusätzlich zur Kontaktmöglichkeit für Gesundheitsfachpersonen nach *Artikel 12* auch für alle ihre Patientinnen und Patienten eine Kontaktmöglichkeit zur technischen und funktionalen Unterstützung («*Service-Desk*») im Umgang mit dem elektronischen Patientendossier zur Verfügung stellen. Mit dieser Kontaktmöglichkeit soll insbesondere sichergestellt werden, dass Patientinnen und Patienten Hilfe und Unterstützung in der Benutzung des elektronischen Patientendossiers erhalten. Es gelten die gleichen Vorgaben an das Personal und zur Protokollierung wie bei der Kontaktstelle für Gesundheitsfachpersonen (vgl. Ziff. 11 der TOZ). Im Fall von Konflikt- oder Beschwerde-Situationen gelten die bisherigen Anlaufstellen des Bundes und der Kantone (z. B. eidgenössische oder kantonale Datenschutzbeauftragte) als Beschwerde- oder Ombudsstellen.

Art. 20 Aufhebung des elektronischen Patientendossiers

Ein elektronisches Patientendossier wird nach *Absatz 1 Buchstabe a* aufgehoben wenn die Patientin oder der Patient die Einwilligung zu dessen Führung widerruft, während 10 Jahren niemand darauf zugreift oder die Patientin oder der Patient verstorben ist. In der Folge sind sämtliche Daten nach *Artikel 9 Absatz 1 Buchstabe b* zu löschen (vgl. Ziff. 12.1 der TOZ).

Absatz 2 und die konkretisierenden Bestimmungen in den Ziffern 12.3 und 12.4 der TOZ regeln, welche

Massnahmen die Stammgemeinschaft im Falle einer Aufhebung des elektronischen Patientendossiers umsetzen muss. Nach der sicheren Identifikation des widerrufenden Patienten oder der widerrufenden Patientin (vgl. Ziff. 12.3.1.1), hat die Stammgemeinschaft sicherzustellen, dass unverzüglich sämtliche Zugriffsrechte auf das aufzuhebende Patientendossier entzogen werden (*Abs. 2*). Gemeinschaften und Stammgemeinschaften müssen in der Folge sämtliche Daten und Dokumente des aufzuhebenden Patientendossiers gemäss Artikel 9 Absatz 1 Buchstabe b löschen (vgl. Erläuterungen ebenda). Dazu sind alle Gemeinschaften (*Abs. 2 Bst. a, Ziff. 1*) sowie auch die ZAS zuverlässig innert angemessener Frist über den erfolgten Widerruf zu informieren, damit diese ihrerseits die mit diesem elektronischen Patientendossier assoziierten Daten und Dokumente löschen. Aus Gründen der Nachvollziehbarkeit ist eine Widerrufserklärung während zehn Jahren in der Stammgemeinschaft aufzubewahren (*Abs. 2 Bst. a Ziff. 2*).

Um dem Prinzip der Datensparsamkeit Rechnung zu tragen, wird ein elektronisches Patientendossier auch aufgehoben, wenn auf dieses während 10 Jahren kein Zugriff erfolgt ist (*Abs. 1 Bst. b*). Um der Patientin oder dem Patienten Gelegenheit zu geben, die Aufhebung zu verhindern, muss er oder sie darüber gemäss *Absatz 2 Buchstabe b* 3 Monate vorher informiert werden.

Erlangt eine Stammgemeinschaft Kenntnis über den Tod der Patientin oder des Patienten (*Abs. 1 Bst. c*), so muss sie, analog zum Widerruf, die Aufhebung des elektronischen Patientendossiers und die Information der ZAS sowie der anderen Gemeinschaften veranlassen. Sämtliche Daten sind ebenfalls gemäss Art. 9 Absatz 1 Buchstabe b in der Stammgemeinschaft und allen anderen Gemeinschaften zu löschen. Bei der Festlegung des Prozesses sind die Vorgaben des Zivilrechts, beispielsweise hinsichtlich der Rechte der Angehörigen an den Daten des elektronischen Patientendossiers, zu beachten.

3. Abschnitt: Datenlieferung für die Evaluation

Art. 21 Datenlieferung für die Evaluation

Ziel und Zweck der Evaluation ist die Überwachung der Zweckmässigkeit, Wirksamkeit, und Wirtschaftlichkeit der Massnahmen des EPDG (Art. 18 EPDG). Die Evaluation des EPDG erfolgt auf der Basis eines Monitoring-Systems, das die Verfügbarkeit der für die Evaluation notwendigen Daten sicherstellt. Die entsprechenden Kennzahlen sind im Anhang 6 der EPDV-EDI aufgeführt. Dazu zählen insbesondere Daten zur Anzahl der Gesundheitsfachpersonen sowie Patientinnen und Patienten, welche sich bei einer Gemeinschaft oder Stammgemeinschaft angemeldet haben, aber auch Daten zur Erteilung von Zugriffsrechten, zur Anzahl der bereitgestellten Dokumenten und Dokumenttypen sowie Daten zur Verwendung des EPD durch Gesundheitsfachpersonen sowie Patientinnen und Patienten. Es handelt sich hierbei um Daten, die im laufenden Betrieb einer Gemeinschaft oder Stammgemeinschaft anfallen, so dass keine zusätzlichen Datenerhebungen durch die Gemeinschaften oder Stammgemeinschaften notwendig werden. Sofern die Indikatoren Rückschlüsse auf einzelne Gesundheitsfachpersonen oder Patientinnen und Patienten erlauben, sind die Daten in anonymisierter Form an das BAG zu übermitteln.

4. Kapitel: Identifikationsmittel

Für den Zugriff auf das elektronische Patientendossier benötigen Patientinnen und Patienten sowie Gesundheitsfachpersonen nach Artikel 7 EPDG ein Identifikationsmittel, welches von einem nach *Artikel 30* zertifizierten Herausgeber herausgegeben wurde.
Die Zertifizierung der Herausgeber von Identifikationsmitteln sowie die festgelegten technischen Mindestanforderungen für das Sicherheitsniveau bestimmen massgebend die Vertrauenswürdigkeit des Identifikationsmittels in Bezug auf die Identität von Patientinnen und Patienten sowie Gesundheitsfachpersonen und schaffen damit Gewissheit, dass es sich bei der Person, die eine bestimmte Identität beansprucht, tatsächlich um diejenige Person handelt, der diese Identität zugewiesen wurde.

Die Verwaltung eines Identifikationsmittels für den gesamten Lebenszyklus richtet sich nach dem in der Norm ISO/IEC 29115:2013 beschriebenen Ablauf in welchem die Beantragung, die Herausgabe und

der Widerruf der Identifikationsmittel sowie die Sicherheitskontrollziele des Authentifizierungsprozesses enthalten sind. Identifikationsmittel enthalten geheime und öffentliche Berechtigungsnachweise (*Credentials)*, z. B. geheime Passwortdatei, geheime Schlüssel, öffentliches Zertifikat oder andere Identifikationsdaten, welche beispielsweise in einem Hardwaregerät (z.B. Mobile Device, Tablett, PC usw.) oder in einem Trägermedium (z.B. Smartcard) als Datenobjekte sicher abgespeichert sind. Mit einem solchen Identifikationsmittel, welche der Inhaber unter seiner Kontrolle hat, authentisiert sich der Inhaber gegenüber einem vertrauenden Beteiligten (Zugangsportale von Gemeinschaften oder Stammgemeinschaften aber auch angeschlossene Primärsysteme, die von Gesundheitsfachpersonen für den Zugriff auf das EPD genutzt werden sowie Zugangsportale von Herausgeber von Identifikationsmitteln). Die Herausgabe von Identifikationsmitteln umfasst u.a. die Teilprozesse wie «Initialisierung», «Beantragung», «Registrierung» und «Erfassung und Verifikation der Identität». Ebenso besteht die Verwaltung der Identifikationsmittel aus Teilprozessen wie die Erzeugung, Personalisierung, Initialisierung und Bindung des Berechtigungsnachweises an die Person sowie Ausgabe, Aktivierung, Widerruf und Erneuerung.
Diese Teilprozesse können zusammengeführt werden oder in unterschiedlicher Reihenfolge ablaufen. Beispielsweise kann der Schritt der Erfassung der Identitätsdaten mit anschliessender Personalisierung nach Herausgabe des Identifikationsmittels erfolgen oder das herausgegeben Identifikationsmittel ist bereits personalisiert. Vorstellbar ist der folgende Ablauf: Eine Patientin bzw. ein Patient oder eine Gesundheitsfachperson bezieht von einem zertifizierten Herausgeber ein Identifikationsmittel, welches über einen eindeutigen elektronischen Identifikator und einen sicheren Authentifizierungsmechanismus für den Zugriff darauf verfügt. Im nächsten Schritt aktiviert die Person das Identifikationsmittel indem sie nachweist, dass sie über die notwendigen Authentifizierungsfaktoren (z. B. geheimes Passwort) verfügt. Abschliessend werden auf zuverlässige Art und Weise weitere personenidentifizierende Merkmale mit dem Identifikationsmittel verbunden. Diese Verbindung kann nach persönlicher Vorsprache oder prozedural sichergestellt werden. Bereits ausgestellte Trägermedien für die elektronische Identität wie zum Beispiel die Versichertenkarte nach Artikel 42a des Bundesgesetz über die Krankenversicherung (SR 832.10) können damit nachträglich die Anforderungen an Identifikationsmittel nach EPDV erfüllen.

Art. 22 Anforderungen an das Identifikationsmittel

Die Anforderungen an die Identifikationsprozesse, die Herausgabe und die Verwaltung von Identifikationsmittel, die technischen Verfahrensanforderungen und Anforderungen an die Identifikationsmittel für den Authentifizierungsprozess sowie die Schutzanforderungen an die entsprechenden Dienste, sind in der Norm ISO/IEC 29115:2013 bezogen auf die verschiedenen Vertrauensstufen vorgegeben. Je höher die Stufe, desto höher ist das Vertrauen in die behauptete Identität derjenigen Person, welche sich mit dem ihr ausgestellten Identifikationsmittel gegenüber einem vertrauenden Beteiligten (z. B. internes Zugangsportal einer Gemeinschaft oder Stammgemeinschaft) authentifiziert.

Die Vertrauensstufe 3 («hohes Vertrauen») gilt nach *Buchstabe a* gleichermassen für die Identifikationsmittel der Patientinnen und Patienten wie für die der Gesundheitsfachpersonen. Erfüllt ein elektronisches Identifikationsmittel die Anforderungen einer höheren Stufe, so wird davon ausgegangen, dass es die entsprechenden Anforderungen einer niedrigeren Vertrauensstufe ebenfalls erfüllt.

Die Vertrauensstufe 3 bedingt keine persönliche Vorsprache bei der Registrierung des Identifikationsmittels. Allerdings muss sichergestellt werden, dass das für die Registrierung erforderliche Ausweisdokument gültig ist und sich auf die reale Person bzw. den Antragsteller bezieht. Bei der Registrierung des Identifikationsmittels müssen demnach Vorkehrungen getroffen werden, um das Risiko zu mindern, dass die Identität des Antragstellers nicht mit der beanspruchten Identität übereinstimmt, z.B. im Hinblick auf verlorene, gestohlene, ausgesetzte, widerrufene oder abgelaufene Dokumente (vgl. *Art. 23 Abs. 1*).

Nach *Buchstabe b* muss das Identifikationsmitteln technisch und organisatorisch so ausgestaltet sein, dass es mit einem hohen Vertrauen nur von der berechtigten Person zur Anwendung gebracht werden kann. Es darf z. B. nicht möglich sein, das geschützte Schlüsselmaterial des Identifikationsmittels auf

ein anderes System oder Medium zu übertragen, z.B. durch Abfangen von im Klartext übermittelten Passwörtern.

Das in *Buchstabe c* vorgeschriebene Authentifizierungsverfahren muss die Anwendung einer Kombination von mindestens zwei Authentifizierungstechniken umfassen und dem aktuellen Stand der Technik entsprechen. Verbreitet sind Verfahren, welche die Faktoren «Wissen» (z. B. geheimes Passwort) und «Besitz» (z. B. Besitz einer Smart Card oder einer SIM Card als sicherer Träger des Schlüsselmaterials) kombinieren.

Nach *Buchstabe d* darf das Identifikationsmittel eine Gültigkeitsdauer von höchstens zehn Jahren aufweisen.

Art. 23 Identitätsprüfung

Der Herausgeber des Identifikationsmittels prüft die Identität der Antragstellerin oder des Antragstellers anhand eines gültigen Ausweisdokumentes nach dem Ausweisgesetz (SR 143.1) bzw. dem Ausländergesetz (SR 142.20). Für die Beantragung des Identifikationsmittels auf dem Korrespondenzweg muss die antragstellende Person eine echtheitsbestätigte Ausweiskopie dem Herausgeber nachweisen (zum Beispiel «Gelbe Identifikation» der Post oder sicheres Video-Ident-Verfahren). Eine Bestätigung der Identität bzw. der Identitätsattribute mit einer qualifizierten elektronischen Signatur nach dem Bundesgesetz über die elektronische Signatur (SR 943.03) ist gleichwertig.

Die Identitätsprüfung kann vom Herausgeber des Identifikationsmittels an Dritte delegiert werden, um in der Schweiz über ein weites Netz an Registrierungsstellen zu verfügen (*Abs. 2*). Die Anforderungen an die Registrierungsstelle (Registration Authority) sind im Schutzprofil nach Artikel 30 Absatz 2 im *Kapitel 4.2 Sicherheitsziele für die Umgebung* festgelegt.

Das Identifikationsmittel kann auch dazu verwendet werden, das Attribut «Gesundheitsfachperson» zu bestätigen (vgl. *Art. 8 Bst. b und d*). Der Herausgeber erfasst und bestätigt hierzu die GLN der Gesundheitsfachperson (vgl. *Art. 24 Abs. 2*). Gemäss *Absatz 3*, muss vorgängig der Nachweis erbracht werden, dass die antragstellende Person eine Gesundheitsfachperson nach *Artikel 2 Buchstabe b EPDG* ist. Dies kann zum Beispiel durch den Abgleich des Personendatensatzes mit den im Medizinalberuferegister erfassten Daten für Inhaberinnen und Inhaber von eidgenössischen oder anerkannten ausländischen Diplomen und Weiterbildungstiteln gemäss Bundesgesetz vom 23. Juni 2006 über die universitären Medizinalberufe (SR 811.11) erfolgen. Die Bestätigung des Attributs «Gesundheitsfachperson» kann durch den Herausgeber des Identifikationsmittels nach *Absatz 3* an Dritte delegiert werden. Vorstellbar ist, dass dieser Nachweis durch den jeweiligen Berufsverband oder der Gesundheitseinrichtung der Gemeinschaft bzw. Stammgemeinschaft erbracht wird.

Art. 24 Daten des Identifikationsmittels

Der Herausgeber erfasst die Identitätsattribute der Patientinnen und Patienten (*Abs. 1*) sowie der Gesundheitsfachpersonen (*Abs. 1 und 2*) für den Nachweis und die Überprüfung ihrer Identität. Diese Attribute können mit dem Identifikationsmittel an die internen Zugangsportale der Gemeinschaften und Stammgemeinschaften übertragen werden (*Abs. 3*).

Nach Absatz 4 muss der Herausgeber die antragstellende Person über die Sicherheitsvorkehrungen, die sie im Umgang mit dem Identifikationsmittel treffen müssen, informieren. Dies schliesst ein den sicheren Umgang mit Passwörtern, Information über die Verarbeitung und Weitergabe von Identitätsattributen an Dritte oder die Bekanntmachung der geltenden Geschäftsbedingungen im Rahmen einer Datenschutzerklärung.

Art. 25 Erneuerung der Gültigkeitsdauer des Identifikationsmittels

Nach Ablauf der Gültigkeit des Identifikationsmittels von höchstens 10 Jahren (vgl. *Art. 22 Bst. d*) muss dieses neu beantragt werden. *Absatz 2* statuiert, dass abweichend von der Norm ISO/IEC 29115:2013 für die Erneuerung des Identifikationsmittels eine Identitätsprüfung gemäss dem Vertrauensniveau der Stufe 3 durchgeführt werden muss (vgl. *Art. 23*).

Art. 26 Sperrung des Identifikationsmittels

Das Identifikationsmittel kann durch die beantragte Person jederzeit für den Zugriff auf das elektronische Patientendossier gesperrt werden. Der Herausgeber des Identifikationsmittels muss sich vergewissern, dass die Person, welche Sperrung beantragt, dazu berechtigt ist und er muss Vorkehrungen treffen, um eine unbefugte Sperrung zu verhindern. Einmal gesperrte Identifikationsmittel können nicht erneuert oder verlängert werden. Eine vorläufige Aussetzung des Identifikationsmittels ist nicht vorgesehen. Herausgeber von Identifikationsmittel müssen Vorkehrungen treffen, um die Authentifizierung nach einer Sperrung unverzüglich zu verhindern (z. B. durch Zertifikatssperrlisten oder andere Verfahren zur Validierung der gültigen Authentifizierungsantwort).

5. Kapitel: Akkreditierung

Art. 27 Anforderungen

Nach *Absatz 1* ergeben sich die Voraussetzungen, welche die Zertifizierungsstellen zu erfüllen haben, grundsätzlich aus der Norm ISO/IEC 17021:2015 für die Akkreditierung zur Zertifizierung von Managementsystemen, deren Anwendbarkeit in Artikel 7 Absatz 1 und Anhang 2 der Akkreditierungs- und Bezeichnungsverordnung (AkkBV; SR 946.512) geregelt ist. Dort wird namentlich das Unabhängigkeitserfordernis festgelegt und das Zertifizierungs- bzw. Produkteprüfungsverfahren geregelt. Eine zusätzliche Regelung in dieser Verordnung erübrigt sich. Die Zertifizierung darf nach Artikel 13 Absatz 1 Buchstabe a EPDG ausschliesslich durch akkreditierte Stellen durchgeführt werden.

Da sich die Zertifizierung von Gemeinschaften und Stammgemeinschaften auf ausgesuchte Elemente aus dem Rahmenwerk ISO/IEC 27001:2013 stützt, ist ISO/IEC 27006:2015:2013 eine zusätzliche Grundlage zur Akkreditierung.

Die Zertifizierung von Herausgebern von Identifikationsmitteln ist nach Artikel 22 Buchstabe a EPDV an die Vorgaben von ISO/IEC 29115:2013 gebunden, im Rahmen der Akkreditierung von Zertifizierungsorganisationen, welche Zertifizierungen für Herausgeber von Identifikationsmitteln anbieten, ist dieser Standard daher zusätzlich massgebend.

Gemeinschaften, Stammgemeinschaften sowie Herausgeber von Identifikationsmitteln haben spezifische Aufgaben, daher werden jeweils spezifische Inhalte im Rahmen der Zertifizierung geprüft. Deshalb werden an die Akkreditierung der jeweiligen Zertifizierungsstellen unterschiedliche Anforderungen gestellt (*Abs. 2*).
Absatz 3 konkretisiert den Begriff des Kontrollverfahrens. Dieses Kontrollverfahren umfasst einerseits die Begutachtungs- und Prüfkriterien, die inhaltlich vorgeben, wie die Einhaltung der Zertifizierungsvoraussetzungen zu überprüfen ist (Bst. a) sowie Angaben zum Ablauf des Zertifizierungsverfahrens (einschliesslich der Überwachung und der Re-Zertifizierung; Bst. b). Buchstabe c gibt zudem vor, dass das vom BAG zur Verfügung gestellte Zertifizierungssystem zur Überprüfung der Einhaltung der Vorgaben in Bezug auf die Datenübertragung von Gemeinschaften und Stammgemeinschaften (Interoperabilität) zu verwenden ist. Mit der Hilfe dieses Zertifizierungssystems kann überprüft werden, ob eine zu zertifizierende Gemeinschaft oder Stammgemeinschaft in der Praxis korrekt mit anderen zertifizierten Gemeinschaften und Stammgemeinschaften kommunizieren kann.

Nach *Absatz 4* konkretisiert das EDI die Anforderungen an die Qualifikation des Personals, welches die

Zertifizierungen durchführt (vgl. Anhang 7 der EPDV-EDI). Es ist dabei zu berücksichtigen, dass es im Bereich der Medizininformatik und des Datenschutzes keine standardisierten Ausbildungen gibt und dass Expertinnen und Experten vergleichsweise rar sind. Entsprechende Praxiserfahrung ist daher zu berücksichtigen.

Art. 28 Akkreditierungsverfahren

Diese Bestimmung stellt eine Konkretisierung von Artikel 11 Absätze 1 und 2 AkkBV dar, indem der Einbezug des BAG vorgesehen wird.

6. Kapitel: Zertifizierung

1. Abschnitt: Zertifizierungsvoraussetzungen

Art. 29 Gemeinschaften und Stammgemeinschaften

Eine nach Artikel 27 akkreditierte Zertifizierungsstelle stellt fest, ob eine Gemeinschaft oder Stammgemeinschaft die Zertifizierungsvoraussetzungen erfüllt. Dabei müssen Stammgemeinschaften zusätzlich zu den Zertifizierungsvoraussetzungen der Gemeinschaften (Art. 8–12) die Vorgaben nach den Artikeln 13–20 einhalten.

Absatz 2 delegiert die Rechtssetzungskompetenz zur Festlegung der Einzelheiten für die Zertifizierungsvoraussetzungen an das EDI.

Die Kompetenz zur Anpassung der Zertifizierungsvoraussetzungen an den Stand der Technik wird in *Absatz 3* basierend auf Artikel 12 Absatz 2 EPDG dem BAG übertragen. Dies ist insbesondere für die Zertifizierungsvoraussetzungen im Bereich der Daten und Datenübertragung (Art. 9) und dem Datenschutz und der Datensicherheit (Art. 11) von Bedeutung.

Art. 30 Herausgeber von Identifikationsmitteln

Absatz 1 führt die Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln abschliessend auf.

Der Herausgeber stellt mit geeigneten Verfahren sicher, dass alle Mitarbeiter und Unterauftragnehmer über eine ausreichende Ausbildung, Qualifikation und Erfahrung bezüglich der ihnen übertragenen Aufgaben verfügen (*Bst. b*).

Nach *Buchstabe c* müssen die verwendeten Informatiksysteme und -produkte vertrauenswürdig sein. Der Begriff der Vertrauenswürdigkeit bringt zum Ausdruck, wie sorgfältig diese Produkte entwickelt wurden und wie sehr sich ein Anwender dieser Produkte auf die angebotene Sicherheitsfunktionalität verlassen kann.

Bei der Ausstellung des Identifikationsmittels müssen die Herausgeber nach *Buchstabe d* sicherstellen, dass neben technischen Kontrollen auch organisatorische Massnahmen ergriffen werden, welche den Datenschutz und die Datensicherheit sicherstellen. Hierzu gehört unter anderem die ständige Überwachung der für die Ausstellung des Identifikationsmittels erforderlichen Einrichtungen sowie der Schutz vor unbefugtem Zugriff, so dass nur befugte Mitarbeiter den Zugang zu Bereichen haben, in denen personenbezogene Daten, kryptografische oder andere sensible Informationen verarbeitet werden. Der Herausgeber des Identifikationsmittels bringt betreffend Datenschutz und Datensicherheit bewährte Methoden zur Anwendung und solche, welche in den Grundsätzen der Normenreihe ISO/IEC 27000 und 20000 verankert sind.

Die Identifikations- und Authentifizierungsdienste der Herausgeber von Identifikationsmitteln sowie die

internen Zugangsportale von Gemeinschaften bzw. Stammgemeinschaften unterliegen definierten Sicherheitsanforderungen. Bezüglich des Authentifizierungsverfahrens wird in der Norm ISO/IEC 29115:2013 eine nicht abschliessende Liste von Bedrohungen aufgeführt. Für alle der genannten Bedrohungen legt die Norm Sicherheitsanforderungen fest, ohne eine Aussage darüber zu treffen, welche Anforderungen wie, wann und in welcher Kombination zu erfüllen sind.

Für die Konkretisierung der Umsetzung dieser Sicherheitsanforderungen in Bezug auf die Dienste, Anwendungen, Identifikationsmittel und Einrichtungen der Herausgeber erlässt das EDI nach *Absatz 2* ein Schutzprofil (funktionale Sicherheitsanforderungen) gemäss der Normen ISO/IEC 15408-1:2009, 15408-2:2008 und 15408-3:2008 (vgl. Anhang 8 der EPDV-EDI). Dieses hat der Evaluierungsstufe 2 zu entsprechen (vgl. unten).

Das Schutzprofil dient der Formulierung von Sicherheitsbedürfnissen an eine Produktklasse (u. a. im Software- oder im Hardwarebereich) und im speziellen nach dieser Verordnung an die Klasse aller der für das elektronische Patientendossier zulässigen Identifikationsmitteln. Im Gegensatz zu den produkt- und herstellerspezifischen Sicherheitsanforderungen dient es als Lastenheft die für Sicherheitsprodukte in dem jeweiligen Einsatzumfeld zu geltenden Anforderungen und definiert die Prüftiefe zur Sicherstellung von deren Umsetzung.

Der Evaluationsgegenstand (EVG) des Schutzprofils umfasst das Identifikationsmittel selbst (Berechtigungsnachweise und Identifizierungsmerkmale, welche auf Geräten unterschiedlicher Ausprägung enthalten sind) den Identitätsdienstleister (Identity Provider) für die Identifikation und Authentifizierung sowie die notwendigen technischen Schnittstellen und die sicheren Kommunikationskanäle für die Authentifizierung am internen Zugangsportal der Gemeinschaften bzw. Stammgemeinschaften. Zu den durch die Sicherheitsfunktionen des EVG unterstützten Teilen können auch aufzubauende Kanäle zu externen Komponenten ausserhalb des EVG gehören, sowie Kanäle zwischen den Komponenten des EVG. Wichtig für die Sicherheitsbetrachtung des EVG ist auch die geplante Einsatzumgebung, an welche verschiedene Annahmen zu stellen sind für einen sicheren Betrieb. Dies impliziert Anforderungen an den sicheren Betrieb des Identitätsdienstleister gemäss der Norm ISO/IEC 27001:2013.

Die Prüftiefe zur Sicherstellung der Umsetzung der Sicherheitsanforderungen werden in der Norm ISO/IEC 15408-3:2008 durch sogenannte Assurance Packages, namentlich EAL-Stufen, festgelegt. Diese Evaluierungsstufen umfassen unter anderem die Bereiche Development, Life-Cycle Support, Security Target Evaluation oder Vulnerability Assessment. Für eine Prüfung des EVG sind die Anweisungen für die verschiedenen Assurance Klassen durchzuführen unter Sicherstellung der für die Umgebung des EVG definierten Anforderungen. Dazu werden im Zertifizierungsverfahren die entsprechenden Nachweise erhoben und geprüft.

3. Abschnitt: Zertifizierungsverfahren

Art. 31 Ablauf

Der in Artikel 31 geregelte Ablauf des Zertifizierungsverfahrens orientiert sich an den Begriffen der Norm ISO/IEC 17021:2015 und hält in chronologischer Reihenfolge die Etappen des Zertifizierungsverfahrens fest.

Das Voraudit nach *Absatz 1* ermöglicht der Zertifizierungsstelle anhand einer Prüfung der eingereichten Dokumente einzuschätzen, ob die Gemeinschaft, die Stammgemeinschaft oder der Herausgeber von Identifikationsmitteln ausreichend für das Zertifizierungsaudit vorbereitet ist. Dies hilft, unnötige Kosten zu vermeiden und die Chance auf Absolvierung eines erfolgreichen Zertifizierungsaudits zu erhöhen.

Im Rahmen des Zertifizierungsaudits nach *Absatz 2* wird durch die Zertifizierungsstelle auch vor Ort geprüft, ob die Vorgaben nach dieser Verordnung eingehalten werden.
Kommt die Zertifizierungsstelle nach der Dokumentenprüfung und dem Zertifizierungsaudit zum

Schluss, dass die Gemeinschaft, die Stammgemeinschaft oder der Herausgeber von Identifikationsmitteln die entsprechenden Vorgaben erfüllt, erteilt sie nach *Absatz 3* das Zertifikat.

Art. 32 Meldung an das BAG

Um den gemeinschaftsübergreifenden Datenaustausch sicherzustellen, müssen die zertifizierten Gemeinschaften und Stammgemeinschaften nach *Absatz 1* in den Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften nach Artikel 39 eingetragen werden, daher ist jede erfolgreiche Zertifizierung dem BAG zu melden.

Zudem ist jede Sistierung und jeder Entzug einer Zertifizierung umgehend zu melden, damit die betroffene Gemeinschaft oder Stammgemeinschaft im Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften gesperrt werden kann.

Zusätzlich zum Eintrag der Daten in den Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften (*Abs. 1*) veröffentlicht das BAG ein Verzeichnis aller erteilten Zertifikate (*Abs. 2*). Dieses Verzeichnis bietet den Patientinnen und Patienten die Möglichkeit, sich einen Überblick darüber zu verschaffen, wo ein elektronisches Patientendossier nach EPDG angeboten wird und welche Herausgeber von Identifikationsmitteln zertifiziert sind.

Art. 33 Überwachung

Die Zertifizierungsstelle überprüft nach *Absatz 1* jährlich, ob weiterhin davon ausgegangen werden kann, dass die Zertifizierungsvoraussetzungen integral erfüllt werden. Sollte festgestellt werden, dass dies nicht der Fall ist, informiert sie das BAG, das nach Artikel 36 Buchstabe c eine ausserordentliche Rezertifizierung anordnen kann. Im Falle, dass die Nichteinhaltung der Zertifizierungsvoraussetzungen auf einen isolierten Teilbereich beschränkt, ist es möglich, dass sich die Prüfung auf diesen beschränkt.

Art. 34 Geltungsdauer

Ein einmal erteiltes Zertifikat ist während drei Jahren gültig. Vorbehalten bleiben Artikel 33 Absatz 2, Artikel 35 und Artikel 36 Buchstabe c. Um als Gemeinschaft oder Stammgemeinschaft ohne Unterbrechung im Rahmen des elektronischen Patientendossiers Daten austauschen zu können, bzw. für Gemeinschaften und Stammgemeinschaften als Herausgeber von Identifikationsmitteln tätig zu sein, muss vor Ablauf der Gültigkeit des Zertifikats die Rezertifizierung abgeschlossen werden. Diese richtet sich nach Artikel 31.

Art. 35 Meldung wesentlicher technischer oder organisatorischer Anpassungen

Werden durch eine Gemeinschaft oder eine Stammgemeinschaft oder einen Herausgeber von Identifikationsmitteln Anpassungen nach *Absatz 1* gemeldet, entscheidet nach Absatz 2 die Zertifizierungsstelle, ob diese Anpassungen im Rahmen der Überwachung nach Artikel 33, einer Rezertifizierung oder einer ausserordentlichen Rezertifizierung nach *Artikel 36 Buchstabe c* geprüft werden. Die Überwachung und die Rezertifizierung finden im üblichen Rhythmus statt, eine ausserordentliche Rezertifizierung muss so rasch wie möglich stattfinden. Sollte es die Situation erfordern kann die Gemeinschaft oder die Stammgemeinschaft so lange vom elektronischen Patientendossier ausgeschlossen werden, bis die ausserordentliche Rezertifizierung erfolgreich abgeschlossen ist. Ein solcher Ausschluss kann entweder durch die Zertifizierungsstelle gestützt auf Artikel 37 (Sanktionen) oder durch das BAG - wenn dieses durch die Zertifizierungsstelle nach Art. 33 über wesentliche Abweichungen von den Zertifizierungsvoraussetzungen informiert wird – gestützt auf Art. 36 (Schutzklausel) vorgenommen werden.

Unter wesentlichen technischen oder organisatorischen Anpassungen sind insbesondere neue oder geänderte (zertifizierungsrelevante) Prozessabläufe oder Anpassungen an der Informatikinfrastruktur

für den gemeinschaftsübergreifenden Datenaustausch bei Gemeinschaften oder Stammgemeinschaften oder ein verändertes Verfahren zur Authentifizierung bei Herausgebern von Identifikationsmitteln zu verstehen.

Art. 36 Schutzklausel

Die Anwendung der Schutzklausel erfolgt unabhängig von einem allfälligen Fehlverhalten einer Gemeinschaft, Stammgemeinschaft oder eines Herausgebers von Identifikationsmitteln. Zu denken ist beispielsweise an Fälle, in denen aufgrund akuter Gefährdungen im IKT-Bereich (z.B. durch Viren, Trojaner etc.) eine sofortige Unterbrechung der gemeinschaftsübergreifenden Kommunikation angezeigt ist oder die Verwendung bestimmter Arten von Identifikationsmittel zu einer Gefährdung des elektronischen Patientendossiers führen kann. In Fällen, in denen eine Gemeinschaft, Stammgemeinschaft oder der Herausgeber eines Identifikationsmittels gegen die Zertifizierungsvoraussetzungen verstösst, kommt Artikel 37 zur Anwendung.

Buchstabe a ermöglicht es dem BAG, zertifizierte Gemeinschaften oder Stammgemeinschaften, die ein Risiko in Bezug auf Datenschutz oder Datensicherheit darstellen, durch Sperrung des Eintrags im Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften von der Bearbeitung von Daten des elektronischen Patientendossiers vorübergehend auszuschliessen.
Nach nachgewiesener Behebung des oder der Risikofaktoren durch die betroffene Gemeinschaft oder Stammgemeinschaft kann der Eintrag im Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften wieder aktiviert werden.

Buchstabe b ermöglicht es dem BAG, die Verwendung von Identifikationsmitteln, welche kollektiv ein Sicherheitsproblem aufweisen, zu verbieten.

Eine ausserordentliche Rezertifizierung nach *Buchstabe c* kann durch das BAG dann angeordnet werden, wenn eine Meldung durch Gemeinschaften oder Stammgemeinschaften über einen im Datenschutz- und Datensicherheitsmanagementsystem als sicherheitsrelevant eingestuften Vorfall nach Artikel 11 Absatz 2 vorliegt, der darauf hindeutet, dass die Zertifizierungsvoraussetzungen nicht mehr erfüllt sind.
Sie kann auch angeordnet werden, wenn durch die Zertifizierungsstelle im Rahmen der Überwachung festgestellt wird, dass eine Gemeinschaft, Stammgemeinschaft oder ein Herausgeber von Identifikationsmitteln die Zertifizierungsvoraussetzungen nicht mehr erfüllt oder ein begründeter Verdacht besteht, dass die Zertifizierungsvoraussetzungen nicht mehr erfüllt werden.
Solange Gemeinschaften oder Stammgemeinschaften die ausserordentliche Rezertifizierung nicht erfolgreich bestanden haben, ist es je nach Umfang der zu prüfenden Elemente möglich, dass sie bis zum erfolgreichen Abschluss dieser ausserordentlichen Rezertifizierung nicht mehr am Datenaustausch im Rahmen des elektronischen Patientendossiers teilnehmen können.
Für Herausgeber von Identifikationsmitteln kann es bedeuten, dass sie keine Verfahren zur Identifikation und Authentisierung von Gesundheitsfachpersonen oder Patientinnen und Patienten durchführen können, solange die ausserordentliche Rezertifizierung nicht erfolgreich absolviert wurde.

4. Abschnitt: Sanktionen

Art. 37

Werden bei der regelmässigen Überwachung der Zertifizierung (Art. 33) schwerwiegende Mängel festgestellt, kann die Zertifizierungsstelle die Zertifizierung nach *Absatz 1* sistieren oder entziehen. Ein schwerer Mangel liegt insbesondere vor, wenn wesentliche Voraussetzungen der Zertifizierung nicht mehr erfüllt sind. Dies wäre bei Gemeinschaften oder Stammgemeinschaften z.B. dann der Fall, wenn wiederholt festgestellt wird, dass die Einbindung der Identifikationsmittel nicht einwandfrei funktioniert, das Zugangsmanagementsystem oder die Berechtigungssteuerung fehlerhaft arbeitet, die gemein-

schaftsübergreifende Kommunikation nicht sichergestellt ist oder das Zugangsportal einem Berechtigten keinen Zugriff oder einem Unberechtigten Zugriff auf das elektronische Patientendossier ermöglicht. In der Folge wird der Eintrag im Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften gesperrt (vgl. Art. 39 Abs. 2).

Diese Sanktionsmöglichkeit ist schon im Rahmen der Norm ISO/IEC 17021:2015 vorgesehen. Da diese eine für die Akkreditierung massgebliche Grundlage darstellt, handelt es sich hier um eine deklaratorische Bestimmung, die indessen der Klarheit halber in der Verordnung verankert werden soll. Die Einzelheiten der Regelung von Sistierung und Entzug sind denn auch nicht in der Verordnung festzulegen. Zu beachten ist namentlich, dass mit der vorliegenden Bestimmung *nicht* die Kompetenz zum Erlass einer Verfügung an die Zertifizierungsstellen delegiert wird. *Absatz 2* hält ausdrücklich fest, dass sich bei Streitigkeiten sowohl das Verfahren als auch die materielle Beurteilung nach den einschlägigen vertragsrechtlichen Bestimmungen richten.

Das BAG hat nach *Absatz 3* die Möglichkeit eine Überprüfung durch die Zertifizierungsstelle anzuordnen. Damit verfügt das BAG über die Rechtsgrundlage, um bei einem begründeten Verdacht– im Interesse der Sicherheit des Systems des elektronischen Patientendossiers – gegen bereits zertifizierte Gemeinschaften, Stammgemeinschaften oder Herausgeber von Identifikationsmitteln vorzugehen.

7. Kapitel: Abfragedienste

1. Abschnitt: Allgemeines

Nach Artikel 14 EPDG führt das BAG die Abfragedienste, welche die für die Kommunikation zwischen Gemeinschaften, Stammgemeinschaften und Zugangsportalen notwendigen Referenzdaten schweizweit einheitlich zur Verfügung stellen. Gegenstand der Bestimmungen dieses Kapitels der EPDV sind die Anforderungen hinsichtlich Inhalt und Nutzung der Abfragedienste sowie die Voraussetzungen für deren Betrieb.

Art. 38

Die Daten der Abfragedienste nach den *Buchstaben a–d* sind für eine gesetzeskonforme Kommunikation zwischen Gemeinschaften und Stammgemeinschaften notwendig. Der Abfragedienst nach *Buchstabe c* stellt darüber hinaus die semantische Interoperabilität strukturierter medizinischer Austauschformate sicher. Diese werden den Gemeinschaften und Stammgemeinschaften über Abfragedienste schweizweit einheitlich zur Verfügung gestellt. In den Abfragediensten werden keine medizinischen Daten geführt.

Die Einträge im Dienst zur Abfrage der zertifizierten Gemeinschaften und Stammgemeinschaften nach *Buchstabe a Ziffer 1* führen insbesondere die technischen Angaben zur elektronischen Kommunikation mit den jeweiligen Zugangspunkten. Für die Sicherstellung der Integrität der elektronischen Nachrichten der Zugangspunkte enthält er zudem auch Daten mit denen die Gemeinschaften und Stammgemeinschaften die Authentizität der von anderen Zugangspunkten übermittelten Nachrichten verifizieren können (vgl. Art. 39 Abs. 1 Bst. d).

Die Angaben zu den Gesundheitseinrichtungen und den Gesundheitsfachpersonen, die Daten des elektronischen Patientendossiers bearbeiten dürfen, werden beide im gleichen Abfragedienst geführt und verfügbar gemacht (Abs. 1 *Bst. a Ziff. 2*). Hier werden auch die Zugehörigkeiten von Gesundheitsfachpersonen zu Gruppen von Gesundheitsfachpersonen abgebildet. Aufgrund dieser Informationen kann die Patientin oder der Patient die Zugriffsrechte für Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen nach Artikel 2 Absatz 1 zuweisen.

Metadaten beschreiben die im elektronischen Patientendossier bereitgestellten Dokumente in strukturierter Weise (z. B. Dateityp, Dokumententyp, Autor, Erstellungsdatum, Vertraulichkeitsstufe). Der

Dienst zur Abfrage der zugelassenen Metadaten nach *Absatz 1 Buchstabe b* enthält die gemäss Artikel 9 Absatz 3 Buchstabe c zu verwendenden Metadaten für die Beschreibung der im elektronischen Patientendossier bereitgestellten Dokumente. Er enthält die im Anhang 3 der EPDV-EDI definierten und somit obligatorisch für Dokumente zu verwendenden Metadaten-Attribute sowie deren zulässige Werte oder Wertebereiche. Dabei kommen vielfach Wertelisten aus standardisierten semantischen Codierungen zum Einsatz (z. B. aus der Terminologie «Snomed CT»), die eine semantische Interoperabilität der Dokument-bezogenen Metadaten sicherstellen können.

Über den Abfragedienst für Austauschformate nach Absatz 1 Buchstabe c können Austauschformate und deren voneinander unabhängige Daten-Sets oder Bausteine abgefragt werden, die für die Definition von neuen strukturierten medizinischen Austauschformaten für den Datenaustausch im elektronischen Patientendossier zu verwenden sind. Neue medizinische Austauschformate dürfen erst dann im elektronischen Patientendossier verwendet werden, wenn sie vom EDI als zulässiges Austauschformat im Anhang 3 der EPDV-EDI geführt werden.

Objektidentifikatoren (Object Identifier, OID) sind hierarchisch aufgebaute Zahlenketten zur weltweit eindeutigen Kennzeichnung von Objekten aller Art, wie zum Beispiel Institutionen, Systeme, Dokumente, Nachrichten, Zertifikate, Klassifikationen usw. Für die einheitliche Handhabung der Registrierung, Vergabe und Anwendung der Objektidentifikatoren im Gesundheitswesen ist der OID-Knoten «eHealth-CH; 2.16.756.5.30» vorgesehen, dessen Verwaltung per 1. Januar 2011 von der Stiftung RefData als Stammregistrierungsstelle wahrgenommen wird. Durch Registrierung gesundheitsspezifischer Objektidentifikatoren unter dem «eHealth-CH»-Knoten können weitere Unterbäume für das Gesundheitswesen unter dem nationalen OID-Länderknoten vermieden werden. Gemäss dem von eHealth Suisse erarbeiteten Konzept zur Verwendung von OIDs sollen Organisationen eigene OIDs für ihre Organisation erstellen dürfen und unterhalb ihres organisationseigenen Knotens weitere OIDs eigenverantwortlich erstellen und verwenden dürfen. Von OID-Inhabern wird verlangt, dass sie eigene Identifikatoren ebenfalls datenschutzkonform publizieren, wenn sie mit den OIDs eigene Objektdomänen referenzieren. Besonders schützenswert sind referenzierte Objekte deren OID-Referenz - in Verbindung mit personenidentifizierenden Daten im Objekt - Rückschlüsse auf den Gesundheitszustand der Person erlauben.

Absatz 2 präzisiert die Verantwortung des BAG für das Führen der Abfragedienste gemäss Artikel 14 Absatz 1 EPDG dahingehend, dass darunter der Aufbau, der Betrieb und die Weiterentwicklung der Abfragedienste fallen.

Das BAG definiert im Rahmen des Aufbaus Standardschnittstellen, über welche die zertifizierte Gemeinschaften und Stammgemeinschaften Daten beziehen (Abfragedienste nach Art. 38 Abs. 1 Bst. a–d) oder liefern können (Art. 38 Abs. 1 Bst. a Ziff. 2). Die Kosten für die Anbindung an die Standardschnittstelle oder Anpassungen für die Verwendung dieser Standardschnittstelle sowie alle andern anfallenden Kosten müssen von den Gemeinschaften und Stammgemeinschaften getragen werden.

2. Abschnitt: Inhalt

Art. 39 Abfragedienst der zertifizierten Gemeinschaften und Stammgemeinschaften

Damit das BAG die zertifizierten Gemeinschaften und Stammgemeinschaften gemäss Artikel 32 Absatz 1 verwalten kann, müssen die Zertifizierungsstellen dem BAG die in Absatz 1 aufgeführten Informationen über die zertifizierten Gemeinschaften und Stammgemeinschaften bekannt geben. Dabei sind neben dem Namen und Kontaktinformationen (*Bst. a*) und eindeutigen Identifikatoren (Global Location Number GLN; Objektidentifikator OID;) auch Angaben von Nöten, die es erlauben die Zugangspunkte und Nachrichten der zertifizierten Gemeinschaften und Stammgemeinschaften sicher zu authentisieren (*Bst. d und e*). Mit Hilfe dieser Angaben kann geprüft werden, ob der Absender einer Nachricht ein legitimer Teilnehmer im Vertrauensraum des elektronischen Patientendossiers ist und der Kommunikation vertraut werden kann. Diese Überprüfung muss so regelmässig durchgeführt werden, dass die

Kommunikation beispielsweise mit einem nicht mehr vertrauenswürdigen Teilnehmer rasch unterbunden wird. Dazu müssen, gemäss den Bestimmungen des EDI nach Artikel 9 Absatz 4 die Gemeinschaften und Stammgemeinschaften entsprechend vertrauenswürdige digitale Zertifikate erwerben und die entsprechenden Angaben den Zertifizierungsstellen vorlegen. Diese geben die Angaben nach erfolgter Zertifizierung an das BAG weiter.

Die Korrektheit der Authentisierungsangaben (Abs. 1 Bst. d und e) ist in besonderer Weise für die Integrität der ausgetauschten Daten relevant. Eine Bearbeitung dieser Daten ist daher gemäss *Absatz 2* nur dem BAG erlaubt. Gemeinschaften und Stammgemeinschaften haben nur lesenden Zugriff.

Art. 40 Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen

Dieser Abfragedienst kombiniert den Dienst zur Abfrage der Gesundheitseinrichtungen (Health Organisation Index; «HOI») und den Dienst zur Abfrage der Gesundheitsfachpersonen (Health Professional Index; «HPI») in einem gemeinsamen System (Health Provider Directory; «HPD»). Somit kann einerseits abgefragt werden, welche Gesundheitseinrichtungen (z. B. Spitäler, Apotheken, Arztpraxen, Spitexorganisationen, Pflegeheime) Mitglied einer zertifizierten Gemeinschaft oder Stammgemeinschaft sind, und andererseits, welche Gesundheitsfachpersonen bei den zertifizierten Gemeinschaften und Stammgemeinschaften für einen Zugriff auf das elektronische Patientendossier erfasst sind und zu welchen Einrichtungen diese gehören. Die Verknüpfung der Daten kann gemäss Artikel 2 Absatz 1 dazu genutzt werden, nicht nur einzelnen Gesundheitsfachpersonen eine bestimmte Zugriffsberechtigung zu erteilen, sondern auch ganzen Gruppen von Gesundheitsfachpersonen, wie etwa einer Abteilung eines Spitals.

Gemäss den im Bearbeitungsreglement zu definierenden Bearbeitungsrechten erhalten die berechtigten Stellen die Möglichkeit, über die vom BAG zur Verfügung gestellte Standardschnittstelle Daten systematisch in Form von definierten Formaten im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen einzutragen und abzurufen. Nach Artikel 9 Absatz 3 in Verbindung mit Artikel 8 Buchstabe c müssen die zertifizierten Gemeinschaften und Stammgemeinschaften sicherstellen, dass die im Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen eingetragenen Daten aktuell sind.

Die zertifizierten Gemeinschaften und Stammgemeinschaften müssen nach *Buchstabe a* sicherstellen, dass die in ihrem Verantwortungsbereich liegenden Einrichtungen und Gruppen von Gesundheitsfachpersonen mit den in den Ziffern 1–3 genannten Daten eingetragen werden. Sie sind dabei frei auch einrichtungsübergreifende Gruppen (z.B. Tumorboard) oder kleinere Untereinheiten der Organisation als Gruppen von Gesundheitsfachpersonen im Abfragedienst abzubilden.

Die zertifizierten Gemeinschaften und Stammgemeinschaften müssen nach *Buchstabe b* sicherstellen, dass die Gesundheitsfachpersonen der in ihrem Verantwortungsbereich liegenden Einrichtungen mit den in den Ziffern 1–3 genannten Daten eingetragen werden.

3. Abschnitt: Übertragung an Dritte

Art. 41 Leistungsvertrag

Nach Artikel 19 EPDG kann der Bund die Erfüllung der Aufgaben aus Artikel 14 EPDG Absätze 1 und 2 an Dritte übertragen. *Absatz 1* konkretisiert, dass die Aufgabenübertragung mittels Leistungsvertrag erfolgt.

Absatz 2 nennt die im Leistungsvertrag mindestens zu regelnden Aspekte. Besonders hervorzuheben sind die Vorgaben zum Einhalten des Datenschutzes und der Datensicherheit (*Bst. b*). Dabei können einerseits die in den Abfragediensten befindlichen Daten selbst schützenswert sein (z.B. personenbe-

zogene Daten zu Gesundheitsfachpersonen im *Abfragedienst für Gesundheitsfachpersonen und Gesundheitseinrichtungen*), andererseits kann über die Verletzung der Integrität gewisser Daten in den Abfragediensten sekundärer Schaden entstehen, indem z. B. ein unzulässiger Zugang zu medizinischen Daten ermöglicht wird oder eine semantische Codierung fehlerhaft ist. Auch die Verfügbarkeit und Performanz der Abfragedienste sind als Teilbereich der Datensicherheit in den Vorgaben der Leistungsverträge zu regeln.

Buchstabe e verpflichtet die beauftragten Dritten zu einer periodischen Berichterstattung hinsichtlich der im Leistungsvertrag definierten Kriterien.

Absatz 3 verpflichtet die beauftragten Dritte, das BAG umgehend über wesentliche Änderungen hinsichtlich der im Leistungsvertrag definierten Vorgaben zu informieren.

Art. 42 Gebühren

Ausgehend von der Schätzung, dass in der Schweiz 20 Gemeinschaften und Stammgemeinschaften entstehen werden, wird die jährliche zu entrichtende Gebühr auf 20 000 Franken festgelegt. Dies ermöglicht unter eine Refinanzierung der Kosten für Aufbau und Betrieb der Abfragedienste über 10 Jahre (*Absatz 1*).
Absatz 2 legt fest, dass im Übrigen die allgemeine Gebührenverordnung vom 8. September 2004 (SR 172.041.01) anwendbar ist, welche insbesondere Vorgaben betreffend Rechnungsstellung, Fälligkeit und Verjährung enthält.

Art. 43 Aufsicht

Die Aufsicht über die beauftragten Dritten obliegt dem BAG (*Abs. 1*).

Die Aufsichtstätigkeit des BAG wird in *Absatz 2* konkretisiert. So prüft das BAG jährlich die Einhaltung der Leistungsverträge (*Bst. a*). Neben der periodischen Einforderung von Berichten (*Bst. b*) kann das BAG zum Zwecke der Aufsicht in begründeten Fällen auch Kontrollen vor Ort durchführen (*Bst. c*). Dabei ist insbesondere an die Überprüfung der Vorgaben zum Datenschutz und der Datensicherheit zu denken, da eine Verletzung der Auflagen von besonderer Tragweite für die Patientensicherheit und die Wahrung der Persönlichkeitsrechte sein können.

8. Kapitel: Inkrafttreten

Art. 48

Das Inkrafttreten ist geplant für Anfang 2017.