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)

und zur Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI)

Fassung vom 22. März 2017

Inhaltsverzeichnis

1 Allgemeiner Teil

1.1 Ausgangslage

Das Parlament hat das Bundesgesetz über das elektronische Patientendossier (EPDG, SR 816.1, 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 und in welchem Umfang sie ihren Gesundheitsfachpersonen Zugriffsrechte erteilt.

Der Grundsatz der Freiwilligkeit gilt auch für die Gesundheitsfachpersonen und ihre Einrichtungen. Ausgenommen sind die Leistungserbringer nach den Artikeln 39 und 49*a* Absatz 4 des Bundesgesetzes vom 18. März 1994[1] über die Krankenversicherung: Spitäler müssen sich innerhalb von drei Jahren nach Inkrafttreten des EPDG – d.h. bis zum 14. April 2020 – einer zertifizierten Gemeinschaft oder Stammgemeinschaft anschliessen, Geburtshäuser und Pflegeheime innerhalb von fünf Jahren, d.h. bis zum 14. April 2022.

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, einzelnen Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen ein Zugriffsrecht zu vergeben.

Identifikationsmittel
Für eine sichere Datenbearbeitung braucht es eine eindeutige und sichere Identifikation und Authentisierung der Patientinnen und Patienten wie auch der Gesundheitsfachpersonen. Diese erfolgt mittels einem Identifikationsmittel eines zertifizierten Herausgebers.

Patientenidentifikationsnummer
Um alle medizinischen Daten und Dokumente, die zu einer Patientin oder einem Patienten im elektronischen Patientendossier erfasst sind, korrekt und vollständig zusammenführen zu können, wird die neue Patientenidentifikationsnummer als zusätzliches Identifikationsmerkmal 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
Um eine sichere und mit den rechtlichen Vorgaben konforme Datenbearbeitung zu gewährleisten, werden für alle Beteiligten (Gemeinschaften, Stammgemeinschaften, Herausgeber von Identifikationsmitteln) detaillierte Zertifizierungsanforderungen festgelegt. Die Einhaltung dieser technischen und organisatorischen Voraussetzungen wird mit einem Zertifizierungsverfahren sichergestellt.

Abfragedienste
Der Bund betreibt die für die Kommunikation zwischen Gemeinschaften und Stammgemeinschaften notwendigen zentralen Abfragedienste.

Finanzhilfen
Zudem unterstützt der Bund den Aufbau und die Zertifizierung von Gemeinschaften und Stammgemeinschaften während drei Jahren nach Inkrafttreten des EPDG durch Finanzhilfen in der Höhe von insgesamt 30 Millionen Franken. Diese sind an eine Mitfinanzierung durch Kantone oder Dritte in gleicher Höhe 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 Kommunikation und der

[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.

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

Das Ausführungsrecht zum elektronischen Patientendossier besteht aus der Verordnung über das elektronische Patientendossier (EPDV), der Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI) sowie der Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV). Die Details sind in der nachfolgenden Tabelle dargestellt

<table>
<tr>
<td rowspan="2">Stufe Bundesrat</td>
<td rowspan="2">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: Inkrafttreten</td>
<td>Verordnung über die Finanzhilfen für das elektronische Patientendossier (EPDFV)
– 1. Abschnitt: Allgemeine Bestimmungen
– 2. Abschnitt: Kriterien und Bemessung
– 3. Abschnitt: Verfahren
– 4. Abschnitt: Inkrafttreten</td>
</tr>
<tr>
<td>– Anhang: Anrechenbare Kosten</td>
</tr>
<tr>
<td>Stufe Departement</td>
<td>Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI)
– Anhang 1: Patientenidentifikationsnummer
– Anhang 2: Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften
– Anhang 3: Metadaten
– Anhang 4: Austauschformate
– Anhang 5: Integrationsprofile
– Anhang 6: Evaluation und Forschung
– Anhang 7: Mindestanforderungen an die Qualifikation des Personals der Zertifizierungsstellen
– Anhang 8: Technische und organisatorische Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln</td>
<td></td>
</tr>
</table>

[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 durch die ZAS (2. Kapitel), die Vorgaben für den Aufbau und den Betrieb von Gemeinschaften und Stammgemeinschaften (Zertifizierungsvoraussetzungen; 3. Kapitel), die Vorgaben an die Identifikationsmittel und deren Herausgeber (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 regelt in *Anhang 1* die Anforderungen an die Patientenidentifikationsnummer. Dazu gehören die Vorgaben für den Aufbau der Patientenidentifikationsnummer und für die Berechnung der Prüfziffer nach Artikel 5 Absatz 2 EPDV.

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. 10, Abs. 3, Bst. a EPDV) 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. 10, Abs. 3, Bst. b 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. 10 Abs. 3, Bst. c EPDV) 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.

Anhang 6 (vgl. Art. 22 Abs. 2 EPDV) wird die für die Evaluation zu liefernden Daten und die für die Datenlieferung relevanten Fristen festlegen; die entsprechenden Angaben werden in einer zukünftigen Revision ins Ausführungsrecht aufgenommen.

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

Anhang 8 (vgl. Art. 31 Abs. 2 EPDV) legt die technischen und organisatorischen Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln fest.

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 Bundesamt für Gesundheit (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. 10 Abs. 5, Art. 30 Abs. 3 und Art. 31 Abs. 3 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» den Zertifizierungsstellen ein Zertifizierungstestsystem zur Verfügung, welches als Testsystem im Rahmen der Zertifizierung die Einhaltung der Normen, Standards und Integrationsprofile überprüft, und kümmert sich um Betrieb und Weiterentwicklung desselben (Art. 28 Abs. 4 EPDV).

Das BAG baut die für das Funktionieren des elektronischen Patientendossiers elementaren Abfragedienste auf und betreibt diese (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 (Art. 20–23 EPDG). 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. 18 EPDG und Art. 22 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 Schweizerische Akkreditierungsstelle SAS anerkennt Stellen für die Auditierung und Zertifizierung von Managementsystemen, welche Zertifizierungen nach EPDG durchzuführen gedenken. Bei der Akkreditierung wird geprüft, ob die festgelegte Organisation und das festgelegte Kontrollverfahren 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 *ZAS* ist zuständig für die Vergabe und die Verwaltung der Patientenidentifikationsnummer nach Artikel 6 Absatz 1 EPDV. 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 das zuständige Amt für die Revision des Gesetzes- und Ausführungsrechts zum EPD 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; Art. 39 Abs. 1 Bst. f und Art. 49*a* 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 medizinischen Daten des elektronischen Patientendossiers drei unterschiedlichen Vertraulichkeitsstufen (Bst. a–c) zuordnen. Es steht im freien Ermessen der Patientin oder des Patienten, welche Daten sie oder er welcher Stufe zuordnet, so ist beispielsweise folgende Zuteilung denkbar:

a) «normal zugänglich»: z. B. behandlungsrelevante Dokumente und Daten wie z. B. Berichte, Befunde, durchgeführte Behandlungen etc. sowie auch Informationen über Allergien und Unverträglichkeiten oder besondere Erkrankungen, Kostengutsprachen, Patientenverfügung, Willensäusserung zur Organspende, Kontaktdaten von im Notfall zu benachrichtigenden Personen;
b) «eingeschränkt zugänglich»: Medizinische Daten, die aus Sicht der Patientin oder des Patienten sensibel sind und nur Gesundheitsfachpersonen mit der Zugriffsstufe «erweitert» zugänglich sein sollen;
c) «geheim»: 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 «normal zugänglich» zugewiesen (Abs. 2). Diese Standardeinstellung kann der Patient verändern (vgl. Erläuterungen zu Art. 4 Bst. a). Auch Gesundheitsfachpersonen können abweichend von der Standardeinstellung Daten, die sie neu einstellen, der Vertraulichkeitsstufe «eingeschränkt zugänglich» zuweisen. Von dieser Möglichkeit kann eine Gesundheitsfachperson aber nur dann Gebrauch machen, wenn die Patientin oder der Patient nicht von der Option nach Artikel 4 Buchstabe a Gebrauch gemacht hat. In diesem Fall geht die explizite Anweisung der Patientin oder des Patienten vor.

Die Vertraulichkeitsstufen kommen nur für die im elektronischen Patientendossier eingestellten und in den Dokumentenablagen gespeicherten bzw. in den Dokumentenregistern verzeichneten medizinischen Dokumente und Daten zur Anwendung. Die demografischen Daten des Patienten sind davon nicht betroffen. Diese Daten befinden sich insbesondere im Patientenindex der Gemeinschaft oder Stammgemeinschaft. Demografische Daten sind für alle Beteiligten des elektronischen Patientendossiers verfügbar. Das ist zwingend, damit elektronische Patientendossiers überhaupt gesucht und gefunden werden können. Auch Notfallzugriffe können nur getätigt werden, wenn die demografischen Daten für die Suche des elektronischen Patientendossiers nutzbar sind. Über die Suche werden nur demografische Daten sichtbar. Der Zugriff erfolgt in einem zweiten Schritt (entweder über ein erteiltes Zugriffsrecht oder einen berechtigten Notfallzugriff). Die Patientin oder der Patient muss im Rahmen der Ein-

willigung für die Eröffnung des elektronischen Patientendossier über diese Datenbearbeitungsmöglichkeiten informiert werden, damit ihre oder seine Einwilligung die entsprechenden Datenbearbeitungen abzudecken vermag. Durchgeführte Such- und Datenbearbeitungsvorgänge sind über die Protokolldaten (Logfiles) jederzeit nachvollziehbar.

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 *Absatz 1* kann die Patientin oder der Patient Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen unterschiedliche Zugriffsrechte zuweisen. Es besteht einerseits die Möglichkeit, das Zugriffsrecht auf die Vertraulichkeitsstufe «normal zugänglich» zu erteilen, womit nur Zugriff auf die normal zugänglichen Daten ermöglicht wird. Andererseits kann auch das Zugriffsrecht auf die beiden Vertraulichkeitsstufen «normal zugänglich» und «eingeschränkt zugänglich» erteilt werden, was einem erweiterten Zugriff entspricht. Auf die Vertraulichkeitsstufe «geheim» hat ausschliesslich der Patient oder die Patientin Zugriff.

In medizinischen Notfallsituationen können Gesundheitsfachpersonen ohne vorgängig erteiltes Zugriffsrecht auf das elektronische Patientendossier zugreifen (Abs. 2). Sie erhalten in diesem Fall standardmässig Zugriff auf die Vertraulichkeitsstufen «normal zugänglich». Von dieser Möglichkeit darf ausschliesslich in einer medizinischen Notfallsituation Gebrauch gemacht werden. Wann eine solche vorliegt, entscheidet sich allein nach medizinischen Kriterien. Als Sicherungsmassnahme gegen eine missbräuchliche Verwendung des Notfallzugriffs, beispielsweise aufgrund automatisierter Angriffe auf ein Endgerät, muss der Notfallzugriff von der Gesundheitsfachperson anhand einer nicht automatisiert reproduzierbaren und manuellen Interaktion bestätigt werden (Ziff. 2.2 Bst. a Anhang 2 EPDV-EDI). Denkbar sind hier zusätzliche Sicherungselemente, wie beispielsweise der Erhalt eines Einmalpasswortes oder die erneute Eingabe eines sonstigen Sicherheitsmerkmals. Gesundheitsfachpersonen, die auf der Ausschlussliste stehen, können keine Notfallzugriffe tätigen. Ebenfalls keine Notfallzugriffe sind möglich, wenn die Patientin oder der Patient von der Option, den Notfallzugriff auszuschliessen, Gebrauch gemacht hat (vgl. Erläuterungen zu Art. 4 Bst. e). 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). Die Gemeinschaft oder Stammgemeinschaft, in der der Notfallzugriff erfolgt, ist dafür verantwortlich, dass diese Informationspflicht innert nützlicher Frist erfüllt wird (Ziff. 2.2 Bst. b Anhang 2 EPDV-EDI). Diese 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. Soweit die informierende Stelle über einen ungesicherten Kanal kommuniziert, muss sie sicherstellen, dass die Information keine medizinischen Informationen enthält (Ziff. 2.2 Bst. c Anhang 2 EPDV-EDI).

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 Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen (Art. 41 EPDV) suchen und ihre Zusammensetzung zur Kenntnis nehmen kann. Nach *Absatz 3* sind bei Gruppen von Gesundheitsfachpersonen die Zugriffsrechte abhängig von der Zugehörigkeit zur Gruppe: Tritt eine Gesundheitsfachperson einer Gruppe 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, so wird ihr das mit der Gruppe verbundene Zugriffsrecht automatisch entzogen.

Art. 3 Dauer der Zugriffsrechte

Artikel 3 regelt, wie lange erteilte Zugriffsrechte gültig sind.

Nach *Absatz 1* gelten an Gesundheitsfachpersonen erteilte 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. 4 Bst. d).

Nach *Absatz 2* sind Zugriffsrechte, die an Gruppen von Gesundheitsfachpersonen vergeben werden, durch die Patientin oder den Patienten zu befristen. Diese Vorgabe erfolgt aus Gründen der Verhältnismässigkeit. Sie rechtfertigt sich einerseits dadurch, dass eine Behandlung in einer stationären Gesundheitseinrichtung in aller Regel nicht über einen allzu langen Zeitraum erfolgt. Da bei Gruppenzugriffsrechten andererseits immer mehr Gesundheitsfachpersonen berechtigt werden, als effektiv an der Behandlung beteiligt sind, soll dieser in der Natur des Gruppenzugriffsrecht liegende Nachteil dadurch aufgefangen werden, dass die Patientin bzw. der Patienten bewusst über die Dauer solcher Zugriffsrechte entscheidet. Die Stammgemeinschaft kann dem Patienten als Entscheidungshilfe beispielsweise ein Set mit unterschiedlichen Befristungsmöglichkeiten anbieten.

Art. 4 Optionen der Patientinnen und Patienten

Der Patientin oder dem Patienten stehen bezüglich der Anwendung der Vertraulichkeitsstufen und der Erteilung von Zugriffsrechten diverse Optionen offen, die in *Artikel 4* 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 für neu eingestellte Daten standardmässig geltende Vertraulichkeitsstufe zu bestimmen. Er oder sie kann die Einstellung so anpassen, dass neu eingestellten Daten die Vertraulichkeitsstufe «eingeschränkt zugänglich» zugewiesen wird. Mit dieser Option kann die Patientin oder der Patient Daten, die für sie oder ihn offensichtlich sensibel sind, von Beginn weg der Vertraulichkeitsstufe mit restriktiverer Zugriffsmöglichkeit zuordnen. Dies kann z. B. der Fall sein, wenn es um eine stigmatisierende Diagnose geht. Selbstverständlich kann er oder sie auch jederzeit wieder zur Standardeinstellung «normal zugänglich» zurückkehren.

Die Patientin oder der Patient hat nach *Buchstabe b* die Möglichkeit, einzelne Gesundheitsfachpersonen vom Zugriff auf ihr oder sein elektronisches Patientendossier auszuschliessen (vgl. Art. 9 Abs. 3 EPDG). Die entsprechenden Gesundheitsfachpersonen werden auf eine so genannte «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 kann nach *Buchstabe c* verlangen, dass er oder sie benachrichtig wird, wenn eine Gesundheitsfachperson in eine Gruppe eintritt, der sie oder er bereits ein Gruppenzugriffsrecht erteilt hat (vgl. Erläuterungen zu Art. 9 Abs. 2 Bst. f). Dadurch können die Patientinnen und Patienten, die Zusammensetzung der Gruppe bei Bedarf überprüfen und den neu eingetretenen Gesundheitsfachpersonen das in Folge des Eintritts in die Gruppe automatisch erhaltene Zugriffsrecht allenfalls entziehen.

Die Patientin oder der Patient hat nach *Buchstabe d* die Möglichkeit, die einer Gesundheitsfachperson erteilten Zugriffsrechte auf eine von ihr oder ihm frei wählbare zeitliche Dauer zu befristen. Damit kann sichergestellt werden, dass Gesundheitsfachpersonen, die voraussichtlich nur einmal oder nur für kurze Zeit in die Behandlung involviert werden, nicht unverhältnismässig lange auf das elektronische Patientendossier zugreifen können. Befristete Zugriffsrechte erlöschen nach Ablauf der festgesetzten Frist

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 e* die Möglichkeit, den Notfallzugriff auf die Vertraulichkeitsstufe «eingeschränkt zugänglich» auszuweiten oder ihn auszuschliessen.

Die Patientin oder der Patient hat nach *Buchstabe f* 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 Angehörige oder andere Vertrauenspersonen.

Die Patientin oder der Patient hat nach *Buchstabe g* die Möglichkeit, Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft zu ermächtigen, das ihnen erteilte Zugriffsrecht an weitere Gesundheitsfachpersonen oder auch an Gruppen von Gesundheitsfachpersonen weiterzugeben. Diese beiden Optionen stehen unabhängig voneinander zur Verfügung. Die ermächtigte Gesundheitsfachperson kann ein Zugriffsrecht jeweils höchstens in dem Mass weitergeben, wie sie es selber besitzt.

2. Kapitel: Patientenidentifikationsnummer

Art. 5 Format

Absatz 1 legt das Format und die Zusammensetzung der Patientenidentifikationsnummer nach Artikel 4 EPDG fest. Die Patientenidentifikationsnummer umfasst 18 Stellen inklusive einer Prüfziffer. Deren Aufbau richtet sich nach der «*Global Service Relation Number*» (GSRN) von GS1 (vgl. Abbildung). Die Basisnummer umfasst einen Ländercode sowie eine Teilnehmernummer, welche BAG referenziert. Die Identifikationsnummer ist nach der GS1 Nummerierungsstruktur 10-stellig. Die erste Stelle der Identifikationsnummer wird verwendet, um den Anwendungsfall «elektronisches Patientendossier» zu kennzeichnen. Der Nummernkreis kann somit erweitert werden für weitere Anwendungsfälle.

Stelle	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}
Bezeichnung	Ländercode		Teilnehmernummer					EPD	Identifikationsnummer									Prüfziffer
Wert	**7**	**6**	**1**	**3**	**3**	**7**	**6**	**1**	$\mathbf{I_1}$	$\mathbf{I_2}$	$\mathbf{I_3}$	$\mathbf{I_4}$	$\mathbf{I_5}$	$\mathbf{I_6}$	$\mathbf{I_7}$	$\mathbf{I_8}$	$\mathbf{I_9}$	**P**

Die Patientenidentifikationsnummer wird durch die ZAS verwaltet und bei der Eröffnung eines elektronischen Patientendossiers der Patientin oder dem Patienten eindeutig zugeordnet. Sie ist eine nichtsprechende Nummer und darf nach Absatz 1 weder Rückschlüsse auf die Patientin oder den Patientin noch auf deren Versichertennummer nach Artikel 50*c* AHVG (AHVN13) zulassen.

Die Vorgaben für der Aufbau der Patientenidentifikationsnummer sowie für die Berechnung der Prüfziffer sind in der EPDV-EDI im Anhang 1 festgelegt.

Art. 6 Antrag auf Vergabe

Für die Eröffnung eines elektronischen Patientendossiers ist die Stammgemeinschaft der Patientin oder des Patienten zuständig (Art. 15 ff.). Daher hält *Absatz 1* fest, dass die Stammgemeinschaft für die

Beantragung der Patientenidentifikationsnummer bei der ZAS nach *Artikel 17 Absatz 1 Buchstabe d* zuständig ist (vgl. Art. 4 Abs. 1 EPDG). Vorgängig muss die Patientin oder der Patient nach Massgabe von Ziffer 8.2.1 Buchstabe a Anhang 2 EPDV-EDI identifiziert werden.

Die *Absätze 2 und 3* betreffen die Sicherstellung der Qualität bei der Vergabe der Patientenidentifikationsnummer. Standardmässig sollten die Angaben nach *Absatz 2* ausreichen, um eine Patientin oder einen Patienten in der Identifikationsdatenbank der ZAS 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.

Wird die Patientin oder der Patient nicht in der Identifikationsdatenbank der ZAS geführt und besitzt die Patientin oder der Patient keine Versichertennummer nach Artikel 50*c* AHVG, so kann die Stammgemeinschaft bei der ZAS eine Versichertennummer beantragen. Sie dient ausschliesslich dem Zweck der Vergabe einer Patientenidentifikationsnummer.

Art. 7 Abfrage und Erfassung

Die Abfrage, wozu auch die Vergabe (Art. 6) und die Annullierung (Art. 8) der Patientenidentifikationsnummer gehören, kann über ein elektronisches Abrufverfahren erfolgen.

Art. 8 Annullierung

Widerruft eine Patientin oder ein Patient ihre oder seine Einwilligung, so wird das elektronische Patientendossier nach *Artikel 21* 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 7* nicht mehr zur Verfügung.

Nach *Absatz 2* informiert die ZAS die Gemeinschaften und Stammgemeinschaften über annulierte Patientenidentifikationsnummern in einem Broadcast-Verfahren über die Datenaustauschplattform SEDEX («*secure data exchange*») des Bundesamtes für Statistik (Ziff. 2.9.29 Anhang 2 der EPDV-EDI).

Absatz 3 legt fest, dass eine annullierte Patientenidentifikationsnummer nicht nochmals vergeben werden darf, um eine mögliche falsche Referenzierung zu verhindern. Eröffnet eine Patientin oder ein Patient nach Widerruf des ersten elektronischen Patientendossiers erneut ein elektronisches Patientendossier, so wird für dieses eine neue Patientenidentifikationsnummer vergeben.

3. Kapitel: Gemeinschaften und Stammgemeinschaften

1. Abschnitt: Gemeinschaften

Die Bestimmungen dieses Abschnitts (Art. 9 bis 13) beziehen sich, sofern nicht ausdrücklich anders definiert, immer auf Gemeinschaften und Stammgemeinschaften. Die Bestimmungen des zweiten Abschnitts (Art. 14 bis 21) und deren entsprechenden Erläuterungen gelten ausschliesslich für Stammgemeinschaften.

Art. 9 Objektidentifikator und Verwaltung

Nach *Absatz 1* müssen Gemeinschaften einen Objektidentifikator (Object Identifier, OID) für sich selbst sowie für ihre zugehörigen Gesundheitseinrichtungen bei dem nach Artikel 39 Buchstabe d vorgesehenen Dienst zur Abfrage der OID beantragen (vgl. Erläuterungen zu Art. 42).

Nach *Absatz 2* müssen Gemeinschaften geeignete Massnahmen (d.h. Richtlinien, Prozesse, Verfahren, Organisationsstrukturen und Verantwortlichkeiten) vorsehen (d. h. definieren, dokumentieren und kom-

munizieren) und einhalten oder vorgeben und deren Einhaltung einfordern, um Gesundheitseinrichtungen (z. B. Spitäler, Apotheken, Arztpraxen, Organisationen für die Pflege und Betreuung zu Hause, Pflegeheime), Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen gemäss den hier geltenden Anforderungen zu verwalten.

Die technischen und organisatorischen Zertifizierungsvoraussetzungen in Anhang 2 der EPDV-EDI konkretisieren in den Ziffern 1.2 bis 1.6 die Anforderungen an die Verwaltung von Gesundheitseinrichtungen, Gesundheitsfachpersonen und deren Hilfspersonen sowie Gruppen von Gesundheitsfachpersonen.

Verwaltung von Gesundheitseinrichtungen

Nach *Buchstabe a* müssen sie insbesondere den Eintritt von neu hinzukommenden und den Austritt von die Gemeinschaft verlassenden Gesundheitseinrichtungen, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen regeln.

Der Eintrittsprozess 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 (Ziff. 1.2.2 sowie 4.9 Anhang 2 der EPDV-EDI). 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 (Abs. 2 Bst. a–d). Die Aufnahme, die Mutation oder der Austritt einer Gesundheitsfachperson setzt zudem voraus, dass ihre Gesundheitseinrichtung bereits in die Gemeinschaft eingetreten ist.

Zudem müssen Gemeinschaften beim Austritt einer Gesundheitseinrichtung, die sich keiner anderen Gemeinschaft oder Stammgemeinschaft anschliesst, sicherstellen, dass diejenigen medizinischen Daten weiterhin zugänglich bleiben, die von der austretenden Gesundheitseinrichtung in ihren eigenen Dokumentenablagen für das elektronische Patientendossier erfasst wurden (Ziff. 1.2.3 Bst. b des Anhang 2 der EPDV-EDI).

Gemeinschaften müssen nach *Buchstabe d* sicherstellen, dass die Daten der ihnen angeschlossenen Gesundheitseinrichtungen im zentralen Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach *Artikel 41* aktuell sind oder von den Gesundheitseinrichtungen aktuell gehalten werden. 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 (Ziff. 1.2.4 Anhang 2 der EPDV-EDI).

Aus den Vorgaben zum Führen eines Inventars der Informatikmittel und Datensammlungen nach *Artikel 12 Absatz 1 Buchstabe b* und den Konkretisierungen in Ziffer 4.6 des Anhangs 2 der EPDV-EDI) ergibt sich zudem, dass Gemeinschaften dieses im Rahmen der Verwaltung von Gesundheitseinrichtungen (Eintritt, Mutation, Austritt), aktuell halten müssen.

Verwaltung von Gesundheitsfachpersonen

Gemeinschaften müssen nach *Buchstabe a* geeignete Prozesse definieren, dokumentieren, umsetzen und einhalten oder einfordern, um Gesundheitsfachpersonen, welche bei den ihr angeschlossenen Gesundheitseinrichtungen für einen Zugriff auf das elektronische Patientendossier vorgesehen sind, zu verwalten. Die Prozesse müssen dabei neben den in den *Buchstaben b, d, e und f* aufgeführten Anforderungen, die Einhaltung weiterer Vorgaben sicherstellen (Ziff. 1.3, 1.4, 1.6 und 4.7 Anhang 2 der EPDV-EDI). Dazu gehören insbesondere die Information der Gesundheitsfachpersonen über deren Aufgaben, Rechte und Pflichten bei der Bearbeitung von Daten des elektronischen Patientendossiers (Ziff.

4.7.1 Anhang 2 der EPDV-EDI) sowie 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 (Ziff. 1.2.2 Bst. b Anhang 2 der EPDV-EDI).

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. Beim Austritt, aber auch bei einem Wechsel des Tätigkeitsbereichs innerhalb der Gemeinschaft ist insbesondere zu prüfen, ob die Voraussetzungen für einen Zugriff auf das elektronische Patientendossier noch bestehen (vgl. Definition von Gesundheitsfachperson nach Art. 2 Bst. b EPDG). Andernfalls sind die entsprechenden Zugriffsmöglichkeiten («*Login*») auf das elektronische Patientendossier unverzüglich zu sperren (Ziff. 1.3.5 Bst. b Anhang 2 der EPDV-EDI). Die Aufnahme, die Mutation oder der Austritt einer Gesundheitsfachperson setzt zwingend voraus, dass ihre Gesundheitseinrichtung bereits in die Gemeinschaft eingetreten ist. Die Gemeinschaft kann die Aufgaben zur Verwaltung der Gesundheitsfachpersonen den ihr angeschlossenen Gesundheitseinrichtungen übertragen.

Die Identifikation einer Gesundheitsfachperson nach *Buchstabe b* muss, sofern sie nicht mit einem Identifikationsmittel eines nach *Artikel 31* zertifizierten Herausgebers durchgeführt werden kann, den Anforderungen nach *Artikel 24* entsprechen. Zusätzlich muss die Gemeinschaft sicherstellen, dass es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG handelt (Ziff. 1.3.3 Bst. c Anhang 2 der EPDV-EDI), d.h. dass es sich um eine nach eidgenössischem oder kantonalen Recht anerkannte Fachperson handelt, die an der Behandlung von Patientinnen und Patienten beteiligt ist. Dazu kann entweder ein Identifikationsmittel verwendet werden, dessen Herausgeber die berufliche Qualifikation im Rahmen der Herausgabe nach Artikel 25 Absatz 3 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 Nationalen Registers der Gesundheitberufe [NAREG]) abgestützt werden. Für Gesundheitsfachpersonen, die nach eidgenössischem oder kantonalem Recht anerkannt sind, die aber in keinem der aktuell bestehenden Berufsregister geführt werden, können bei Bedarf mit den kantonalen oder nationalen Berufsverbänden Vorgehensweisen zur Überprüfung der Diplome festgelegt werden.

Nach *Buchstabe c* müssen Gemeinschaften für Gruppen von Gesundheitsfachpersonen einen OID vergeben, welcher auf dem OID der Gemeinschaft nach *Absatz 1* basiert (vgl. Erläuterungen zu Art. 42). Die Vergabe und Zuweisung des OID an eine Gruppe erfolgt eigenverantwortlich durch die Gemeinschaft. Die Gemeinschaft erstellt zu diesem Zwecke unterhalb des Knotens der Gesundheitseinrichtung weitere OIDs und weist sie den Gruppen der entsprechenden Gesundheitseinrichtung für die Eintragung im Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen gemäss *Buchstabe d* zu.

Die Daten der Gesundheitsfachpersonen müssen nach *Buchstabe d* im Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen nach *Artikel 41* eingetragen, aktualisiert oder gegebenenfalls gelöscht werden. Sofern die Gesundheitsfachperson in einem eidgenössischen oder kantonalen Berufsregister (MedReg, NAREG, etc.) geführt wird, sind die entsprechenden Angaben für den Abfragedienst zu übernehmen (Ziff. 1.2.2 Bst. d Anhang 2 der EPDV-EDI). Die zu übernehmenden Angaben (Ziff. 1.9.5.1.2 Ergänzung 1 des Anhangs 5 der EPDV-EDI) umfassen Name, Vorname und GLN der Gesundheitsfachperson. Dabei ist insbesondere sicherzustellen, dass nur Gesundheitsfachpersonen im Abfragedienst geführt werden, die der Definition nach Artikel 2 Buchstabe b EPDG entsprechen, die für die jeweilige Gesundheitseinrichtung tätig sind und die einen Zugang zum elektronischen Patientendossier benötigen. Die Gemeinschaft muss für die zu ihr registrierten Daten sicherstellen, dass die Aktualität und Korrektheit der Daten regelmässig von ihr oder der für die Daten verantwortlichen Gesundheitseinrichtung überprüft wird (Ziff. 1.2.4 Anhang 2 der EPDV-EDI). Auch diese Aufgaben können den ihr angeschlossenen Gesundheitseinrichtungen übertragen werden. Die Gemeinschaft bleibt aber für die Korrektheit und Aktualität der eingetragenen Daten verantwortlich.

Nach *Buchstabe e* darf der Zugriff von Gesundheitsfachpersonen auf das elektronische Patientendossier nur mit einem gültigen Identifikationsmittel erfolgen, welches von einem nach *Artikel 31* zertifizierten Herausgeber herausgegeben wurde (Ziff. 1.4.3 Anhang 2 der EPDV-EDI). Dabei ist es unerheblich, ob der Zugriff über das Zugangsportal für Gesundheitsfachpersonen (Art. 11) oder über andere Systeme (z. B. über einen integrierten Zugang im Primärsystem) erfolgt. Das bedeutet, dass alle Zugänge, die von Gesundheitsfachpersonen oder Hilfspersonen für den Zugriff auf das elektronische Patientendossier genutzt werden, ein starkes Authentifizierungsverfahren nach dem aktuellen Stand der Technik mit mindestens zwei Authentifizierungsfaktoren unterstützen müssen. Obligatorisch ist ein solches Authentifizierungsverfahren dabei lediglich für die Bearbeitung von Daten des elektronischen Patientendossiers. Eine so erfolgte Authentifizierung anderer zertifizierter Gemeinschaften ist im Rahmen der gemeinschaftsübergreifenden Bearbeitung von Daten des elektronischen Patientendossiers als vertrauenswürdig anzuerkennen.

Gemeinschaften müssen sicherstellen, dass sowohl für die Gesundheitsfachpersonen wie auch für die Hilfspersonen der eindeutigen Identifikator nach Artikel 25 Absatz 1 zuverlässig mit der registrierten Identität der jeweiligen Person innerhalb der Gemeinschaft verbunden wird (Ziff. 1.4.2 Anhang 2 der EPDV-EDI; «Registrationsphase»).

Gesundheitsfachpersonen können Hilfspersonen für die Bearbeitung von Daten des elektronischen Patientendossiers einsetzen. Um die Persönlichkeitsrechte der Hilfspersonen zu schützen, werden diese nicht im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach *Artikel 41* geführt. Somit können sie von den Patientinnen und Patienten nicht als eigenständige Personen in der Berechtigungssteuerung verwaltet werden. Dennoch ist die Zugehörigkeit einer Hilfsperson zu der für sie verantwortlichen Gesundheitsfachperson gemeinschaftsintern zu verwalten, damit die Hilfspersonen mit den Berechtigungen der verantwortlichen Gesundheitsfachperson zugreifen können und deren Datenbearbeitungen protokolliert werden können. Für die Identifikation und den Zugriff von Hilfspersonen sind die Bestimmungen von *Artikel 9 Absatz 2 Buchstaben b und e* massgeblich (Ziff. 1.3 Anhang 2 der EPDV-EDI).

Verwaltung von Gruppen von Gesundheitsfachpersonen

Nach *Buchstabe d* müssen die Gemeinschaften die Verwaltung der Gruppen von Gesundheitsfachpersonen im Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen nach *Artikel 41* sicherstellen. Sie können diese Aufgabe den ihr angeschlossenen Gesundheitseinrichtungen übertragen, bleiben aber für die Korrektheit und Aktualität der eingetragenen Daten verantwortlich.

Patientinnen und Patienten können Zugriffsrechte auch an Gruppen von Gesundheitsfachpersonen zuweisen (Art. 2 Abs. 1). Die zu einem späteren Zeitpunkt in diese Gruppe eintretenden Gesundheitsfachpersonen erhalten das mit dieser Gruppe verbundene Zugriffsrecht (Art. 2 Abs. 3). Dies jedoch nur, sofern die Gesundheitsfachperson nicht generell durch den Patienten oder die Patientin vom Zugriff ausgeschlossen wurde (Art. 4 Bst. b).

Buchstabe f hält dazu fest, dass Patientinnen und Patienten auf Wunsch über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen zu informieren sind. Die Information kann automatisiert und elektronisch erfolgen.

Gemeinschaften sollten die Definition der Gruppenzusammensetzung und deren Grösse so gestalten, dass Patientinnen und Patienten die Zugriffsrechte angemessen verwalten können. Insbesondere sollten nicht unverhältnismässig viele Gesundheitsfachpersonen ohne konkreten Behandlungskontext durch das Zugriffsrecht für eine Gruppe von Gesundheitsfachpersonen mitberechtigt werden. Grundsätzlich müssen Gemeinschaften, resp. deren angeschlossene Gesundheitseinrichtungen für sich klären, wie sie die Zugriffsmöglichkeiten auf das elektronische Patientendossier intern organisieren wollen, welche Gesundheitsfachpersonen in der Folge einen Zugang benötigen und wie diese allenfalls in Gruppen von Gesundheitsfachpersonen geführt werden sollen. Die konkrete Ausgestaltung sollte verhältnis-

mässig und der Aufgabenerfüllung angemessen sein. Da sich Behandlungspfade beispielsweise in Spitälern oft über diverse organisatorische Einheiten erstrecken (z. B. Notfallaufnahme → Labor → Radiologie → Bettenstation Innere Medizin), kann es zweckmässig sein, die Gruppen so auszugestalten, dass sie Gesundheitsfachpersonen aller beteiligten Einheiten angemessen umfassen. Alternativ ist es auch denkbar, Gruppen zu definieren, die primär nur für die Übernahme von medizinischen Daten in das Primärsystem verantwortlich sind. Beispielsweise könnten für grössere Abteilungen oder Kliniken eines Spitals, Gruppen definiert werden, bei denen die Zusammensetzung weitgehend stabil und die Verfügbarkeit der enthaltenen Personen kontinuierlich gewährleistet ist. Die Mitglieder einer solchen Gruppe können dann im Rahmen der Aufnahme der Patientin oder des Patienten die behandlungsrelevanten medizinischen Daten in das Primärsystem des Spitals überführen und so den innerhalb der Gesundheitseinrichtung an der Behandlung der Patientin oder des Patienten beteiligten Gesundheitsfachpersonen zugänglich machen. Es ist daher weder notwendig, noch aus Gründen der Handhabbarkeit und auch nicht aus Patientensicht zweckmässig, tagesaktuelle Dienstpläne spitalinterner Abteilungen oder eines Pflegeheims im Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen zu führen. Bei den Organisationen der Pflege und Betreuung zu Hause können die Gruppen je nach gewähltem Betreuungsmodell (Rotationsprinzip versus Bezugspersonenkonzept) unterschiedlich gross ausfallen.

Art. 10 Datenhaltung und Datenübertragung

Umsetzung der Berechtigungssteuerung

Nach *Absatz 1 Buchstabe a* müssen Gemeinschaften die Berechtigungssteuerung so umsetzen, dass die Vorgaben nach Artikel 9 EPDG und die Bestimmungen zur Zuordnung zu Vertraulichkeitsstufen und für den Notfallzugriff nach den *Artikeln 1 und 2 Absatz 2 EPDV* korrekt umgesetzt und durchgesetzt werden (Ziff. 2.1–2.3 Anhang 2 der EPDV-EDI). Für Gemeinschaften gilt insbesondere, dass die von der Patientin oder dem Patienten über das Zugangsportal ihrer oder seiner Stammgemeinschaft vorgenommene Zuordnung von Daten des elektronischen Patientendossiers zu einer der drei Vertraulichkeitsstufen (Art. 1) übernommen werden muss (Ziff. 2.3.1 Anhang 2 der EPDV-EDI).

Darüber hinaus müssen Gemeinschaften sicherstellen, dass Zugriffe auf Daten ihrer Dokumentenablagen und Dokumentenregister nur gemäss einer zuvor eingeholten Zugriffsentscheidung der Stammgemeinschaft des jeweiligen Patienten oder der jeweiligen Patientin erfolgen können (Ziff. 2.3 Anhang 2 der EPDV-EDI). Zur weiteren Absicherung gegen sogenannte «*man-in-the-client*»-Angriffe fordert Ziffer 2.2 des Anhangs 2 der EPDV-EDI zudem für Notfallzugriffe, dass ein solcher auf eine Weise bestätigt werden muss, der den Missbrauch insbesondere durch eine auf dem Endgerät installierte Schadsoftware wirksam verhindert. Dies kann beispielsweise durch eine zusätzliche, nicht automatisiert reproduzierbare, manuelle Interaktion (z. B. durch die Eingabe eines Einmalpasswortes oder einer durch ein lokales Token generierten PIN) erzielt werden.

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 im Rahmen des Zertifizierungsverfahrens überprüft werden können (2.3.2 Anhang 2 der EPDV-EDI).

Datenablagen

Aus Datenschutz- und Datensicherheitsgründen dürfen die medizinischen Daten des elektronischen Patientendossiers nach *Buchstabe b* nur getrennt von anderen Datenbeständen der Gemeinschaft oder ihrer Gesundheitseinrichtungen gespeichert werden, so dass sie nicht unzulässig für andere Zwecke verwendet werden können. Unzulässig ist insbesondere das Überführen von medizinischen Daten aus den Dokumentenablagen heraus oder in diese hinein, sofern dies nicht durch Gesundheitsfachpersonen geschieht. Zulässig ist jedoch die direkte Übermittlung von medizinischen Daten an andere Gesundheitsfachpersonen und Gesundheitseinrichtungen mittels der Elemente der Informatikinfrastruktur des elektronischen Patientendossiers, sofern die Empfänger ebenfalls Mitglied einer zertifizierten Gemeinschaft sind.

Ziel der Regelung ist es, dass die medizinischen Daten des elektronischen Patientendossiers mindestens logisch von anderen Daten getrennt gehalten werden (Ziff. 2.4 Bst. b Anhang 2 der EPDV-EDI) und somit als Kopien der in den Primärsystemen der Gesundheitseinrichtungen erstellten medizinischen Daten in den entsprechenden Datenablagen gespeichert werden. Diese Trennung ist auch aufgrund der Tatsache, dass die Daten des elektronischen Patientendossiers einerseits anderen Aufbewahrungs- und Löschpflichten unterliegen als die Daten der Primärsysteme notwendig und andererseits nach der Aufhebung des elektronischen Patientendossiers (Abs. 1 Bst. e) vollumfänglich respektive auf Wunsch der Patientin oder des Patienten (Abs. 2 Bst. c) selektiv vernichtet werden.

Zudem würden Dokumentenablagen ohne wirksame Trennung der Datenbestände 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 einer unkontrollierten Diffusion von Daten in das elektronische Patientendossier und *vice versa* bestünde.

Die Isolation von anderen Datenbeständen muss sicherstellen, dass beispielsweise Personen, die über privilegierte Zugriffsrechte auf das Betriebssystems oder die Datenbank des Primärsystems verfügen, nicht gleichzeitig auf medizinische Daten des elektronischen Patientendossiers und andere Datenbestände zugreifen können. Unabhängig davon, ob die Trennung physisch (d. h. durch eigene Hardware, separate Rechenzentren), logisch (z. B. durch getrennte Datenbanken, virtuelle Maschinen, kryptographische Isolation, etc.) oder durch eine Kombination mehrerer Massnahmen geschieht, muss die Isolation eine sichere Abschottung der Bestände auf den technischen Ebenen erlauben. Eine unbeabsichtigte Durchlässigkeit (sog. Isolationsversagen) durch technisches Versagen, Schadsoftware oder durch unzulässiges menschliches Handeln ist mit geeigneten technischen Mitteln und allenfalls ergänzt durch organisatorische Massnahmen weitestgehend zu verhindern.

Eine genügende logische Isolation kann beispielsweise mittels Verschlüsselung auf Applikationsebene erreicht werden, sofern die Schlüssel für die Datenbestände vor unzulässigen Zugriffen geschützt verwaltet werden. Damit sind auch hybride Nutzungen von Dokumentenablagen auf der gleichen Hardware, dem gleichen Betriebssystem und mit den gleichen Datenbanken möglich. Für eine zulässige Überführung von Daten aus dem elektronischen Patientendossier in andere Bestände (oder vice versa) darf es neben den für die Gesundheitsfachpersonen vorgesehenen Verfahren (erfassen, herunterladen) lediglich eine weitere Rolle mit entsprechenden Systemprivilegien geben. Um dieses Restrisiko hinsichtlich unzulässiger Datenübertragung weiter zu vermindern sind die entsprechenden Zugänge oder Applikationsschlüssel geeignet abzusichern und beispielsweise durch weitergehende organisatorische Massnahmen («*segregation of duties*», «Vier-Augen-Prinzip») zu schützen.

Verschlüsselung

Buchstabe c legt fest, dass Gemeinschaften für die Speicherung und Übertragung der Daten geeignete Verschlüsselungsverfahren, d.h. kryptographische Verfahren nach aktuellem Stand der Technik verwenden müssen, um diese vor einem Verlust der Vertraulichkeit, Authentizität und Integrität zu schützen (Ziff. 4.12 Anhang 2 der EPDV-EDI; vgl. Erläuterungen zu Art. 12 Abs. 4).

Datenvernichtung

Buchstabe d hält fest, dass Daten, die durch die Gesundheitsfachpersonen im elektronischen Patientendossier erfasst werden, nach zwanzig Jahren vernichtet werden müssen. Ziel dieser Regelung ist es, medizinische Daten genügend lange zur Verfügung zu stellen. Die von der Patientin oder dem Patienten erfassten Daten unterliegen keiner Löschungsfrist. Auf Verlangen der Patientin oder des Patienten können gemäss *Absatz 2 Buchstabe b* Daten von dieser Vernichtung ausgenommen werden. So können Patientinnen und Patienten für Daten, die eine sehr lange zeitliche Behandlungsrelevanz aufweisen (z. B. bei chronischen oder angeborenen Krankheiten) sicherstellen, dass diese auch über diese Frist hinaus noch im elektronischen Patientendossier verfügbar bleiben.

In technisch begründeten Ausnahmefällen, namentlich bei Systemen zur Ablage von Dateien mit sehr grossem Datenvolumen, wie sie üblicherweise bei bildgebenden Verfahren beispielsweise in der Radiologie entstehen, müssen die medizinischen Daten resp. Dokumente nicht in Kopie bereitgestellt werden, sondern dürfen direkt aus den integrierten Ablagen der Primärsysteme abgerufen werden. In diesen Fällen beschränken sich die Vorgaben zum Löschen von Daten nach *Absatz 1 Buchstaben d und e* sowie nach *Absatz 2 Buchstabe c* auf den entsprechenden Eintrag im Dokumentenregister.

Eine Aufhebung des elektronischen Patientendossiers nach *Artikel 21 Absatz 1*, soll nach *Buchstabe e* 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 vernichten und die Patientenidentifikationsnummer aus allen Systemen zu entfernen (Ziff. 2.6 Bst. b Anhang 2 der EPDV-EDI). Die Verantwortung zur Information anderer Gemeinschaften über die Aufhebung eines elektronischen Patientendossiers liegt bei der Stammgemeinschaft des betroffenen Patienten oder der betroffenen Patientin (Art. 21 Abs. 3). Protokolldaten und Daten in den nicht abfragbaren Primärsystemen sowie in Datensicherungen sind davon nicht betroffen.

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 (Ziff. 2.7 Anhang 2 der EPDV-EDI).

<u>Wahlmöglichkeiten der Patientinnen und Patienten</u>
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 medizinische Daten nicht in seinem oder ihrem elektronischen Patientendossier zu erfassen. Diese Möglichkeit wird von den Patientinnen und Patienten in der Regel im konkreten Behandlungsfall und somit im Kontakt mit einer Gesundheitseinrichtung wahrgenommen werden. Dies sicherzustellen und eine entsprechende Umsetzung in den Gesundheitseinrichtungen einzufordern, liegt jedoch in der Verantwortung der Gemeinschaften.

Der Patient oder die Patientin kann nach *Absatz 2 Buchstabe b* jederzeit verlangen, Daten von der Vernichtung nach *Absatz 1 Buchstabe d* auszunehmen, so dass diese auf unbestimmte Zeit verfügbar bleiben.

Absatz 2 Buchstabe c räumt den Patientinnen und Patienten das Recht ein, zu veranlassen, dass bestimmte auf sie oder ihn bezogene Daten des elektronischen Patientendossiers vernichtet werden. Dies kann technisch über eine entsprechende Funktion im Zugangsportal der Stammgemeinschaft der Patientin oder des Patienten realisiert werden. Gemeinschaften haben eine solche Löschanweisung (Transaktion *Delete Document Set* [ITI-62] des «IHE-Integrationsprofils» *XDS Metadata Update*; Ziff. 2.9.13 und 2.9.14 Anhang 2 der EPDV-EDI) entsprechend umzusetzen. Dabei müssen die entsprechenden Einträge aus den Dokumentenregistern, sowie die medizinischen Daten aus den Dokumentenablagen des elektronischen Patientendossiers gelöscht werden. Für medizinische Daten, die direkt aus den Dokumentenablagen der Primärsysteme (z. B. integrierte Dokumentenablagen für Bilddateien der Radiologie) abgerufen werden, ist lediglich der Eintrag im Dokumentenregister zu löschen, damit geltende Dokumentations- und Aufbewahrungspflichten der Gesundheitsfachpersonen nicht tangiert werden.

<u>Technische Vorgaben für die Datenübertragung</u>
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 d* definierten Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers einhalten. Diese Vorgaben konkretisieren beispielsweise die zulässigen Medientypen (abschliessend in Ziff. 8 Anhang 3 der EPDV-EDI aufgeführt), die Suche nach Patientinnen

und Patienten im Patientenindex, die Kommunikation mit dem Dokumentenregister, den Dokumentenablagen und der Berechtigungssteuerung, die Kommunikation mit dem Herausgeber des Identifikationsmittels sowie die Kommunikation mit den Abfragediensten nach den Artikeln 40 und 41. 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 Zertifizierungstestsystem (Art. 28 Abs. 4) überprüft. 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 Primärsystemen zu erleichtern, steht den Herstellern ein Software-Adapter (der so genannte «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» nicht notwendig. Eine standardisierte Anbindung an die Schnittstellen in den Gemeinschaften kann für Anbieter, Anwender und Gemeinschaften als Investitionsschutz angesehen werden, da einmalige Aufwände vielfach verwendet werden können.

Metadaten

Metadaten beschreiben die im elektronischen Patientendossier bereitgestellten medizinischen Daten, resp. Dokumente in strukturierter Weise (z. B. das technische Dateiformat, den fachlichen Typ, den Autor, das Erstellungsdatum, die gesetzte Vertraulichkeitsstufe). Nach *Buchstabe a* 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 auf die medizinischen Daten bezogenen Metadaten sicherstellen. Für eine schweizweit einheitliche und technisch unterstützte Nutzung der Metadaten führt der Bund den Abfragedienst für die zugelassenen Metadaten nach *Artikel 39 Buchstabe c*. Nur die im Anhang 3 der EPDV-EDI aufgeführten Merkmale (Code und englische Bezeichnung) sind normativ. Die Übersetzungen in die Landessprachen und weitere Sprachen wie auch umgangssprachliche Begriffe werden durch eHealth Suisse in Form von Synonymlisten veröffentlicht werden.

Alle durch die Metadaten klassifizierbaren Typen von medizinischen Daten können als unstrukturierte Daten in Form von Dokumenten (z. B. Bilddateien oder PDF/A) bereitgestellt werden. Für die Bereitstellung strukturierter medizinischer Daten durch Gesundheitsfachpersonen gilt nach *Buchstabe c* jedoch, dass die in Anhang 4 der EPDV-EDI vorgegebenen Austauschformate für medizinische Inhalte zu verwenden sind.

Integrationsprofile

Nach *Buchstabe c* sind für die Informationsübertragung innerhalb der Gemeinschaften sowie zwischen Gemeinschaften die Transaktionen der in Anhang 5 der EPDV-EDI aufgeführten Integrationsprofile von *Integrating the Healthcare Enterprise* (IHE) mit den entsprechenden nationalen Anpassungen («*national extensions*») sowie für spezifische Anwendungsfälle die Transaktionen der nationalen Integrationsprofile des EDI zu verwenden. Integrationsprofile sind technische Leitfäden zur technisch interoperablen Umsetzung spezifischer Anwendungsfälle meist unter Verwendung allgemein anerkannter Normen und Standards.

Die unter Ziffer 1 des Anhangs 5 der EPDV-EDI aufgeführten «IHE-Integrationsprofile» 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 Identifikator zu verwenden ist und nicht 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 (Ziffer 2.9.21 Bst. b, 2.9.26, 2.9.28 Bst. b und 2.9.29 Anhang 2 der EPDV-EDI). 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 (Ziff. 2.9.30 Anhang 2 der EPDV-EDI).

Protokolldaten

Nach Artikel 10 Absatz 1 Buchstabe b 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 Daten des elektronischen Patientendossiers durch eine aussagekräftige und revisionsfeste Protokollierung aller datenschutzrelevanten Ereignisse.

Zu den zu protokollierenden Ereignissen zählen insbesondere die Bereitstellung und der Abruf von medizinischen Daten, die Änderung von Metadaten (z. B. der Vertraulichkeitsstufe), die Anpassungen an der Konfiguration der Berechtigungssteuerung sowie Authentisierungs- und Autorisierungsentscheide und die Daten, aufgrund dessen 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 (Ziff. 4.13.3 Anhang 2 der EPDV-EDI) differenziert werden. Die Anforderungen an die durch Patientinnen und Patienten einsehbaren Protokolldaten nach *Buchstabe d* werden in Ziffer 2.10 des Anhangs 2 der EPDV-EDI konkretisiert.

Die Protokolldaten müssen mit geeigneten technischen oder organisatorischen Mitteln gegen Veränderungen geschützt werden und sind während 10 Jahren aufzubewahren und dann zu vernichten (Ziff. 2.10.7 und 2.10.8 Anhang 2 der EPDV-EDI).

Konkretisierend zu *Artikel 12 Absatz 4* werden in Ziffer 4.13.3 des Anhangs 2 der EPDV-EDI weitere datenschutz- und datensicherheitsrelevante Protokollierungsanforderungen für Ereignisse im Rahmen des Systembetriebs aufgestellt, die jedoch nicht für die Einsichtnahme durch Patientinnen und Patienten vorgesehen sind. Andere Protokollierungen, die im Rahmen des technischen Betriebs erfolgen, aber nicht direkt datenschutz- oder datensicherheitsrelevant sind (z. B. Betriebsparameter oder Messgrössen wie etwa Abfragehäufigkeiten, Antwortzeiten oder Datendurchsatzmengen), sind nicht Gegenstand dieser Anforderungen, können aber für die Erkennung von Sicherheitsvorfällen nach *Artikel 12 Absatz 1 Buchstabe a* relevant sein.

Damit die Patientin oder der Patient die dezentral anfallenden Protokolldaten jederzeit einsehen kann, sind die Protokolldaten von den Gemeinschaften zum Abruf über das Zugangsportal für Patientinnen

und Patienten (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 (Ziff. 2.10.9 Anhang 2 der EPDV-EDI). 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).

Es ist vorgesehen, dass das EDI nach *Absatz 4* auf eine Übersetzung und eine amtliche Publikation der Anhänge der EPDV-EDI verzichtet, die nur mit Titel und Fundstelle veröffentlicht werden. Von einer Veröffentlichung in der AS kann nach *Artikel 5 Absatz 1* des Publikationsgesetzes vom 18. Juni 2004[7] (PublG) bei Texten abgesehen werden, welche nur einen kleinen Kreis von Personen betreffen oder von technischer Natur sind, sich nur an Fachleute wenden und sich für die Veröffentlichung in der AS nicht eignen. Diese werden stattdessen auf der Homepage des BAG zugänglich gemacht. Bei der EPDV-EDI soll auf die Publikation der Anhänge 2 (technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften), 3 (Metadaten), 4 (Austauschformate), 5 (nationale Anpassungen der Integrationsprofile und nationale Integrationsprofile) und 8 (Technische und organisatorische Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln) verzichtet werden. Insbesondere bei den Anhängen 5 und 8 handelt es sich um äusserst technische Anforderungen, die sich nur an einen sehr beschränkten Adressatenkreis, namentlich die für die technische Implementierung verantwortlichen Fachspezialisten richten. Zudem soll in Anwendung von *Artikel 14 Absatz 2 Buchstabe b* PublG bei den Anhängen 3, 4, 5 und 8 auf eine Übersetzung in die Amtssprachen verzichtet werden, da diese Anhänge durch die Betroffenen ausschliesslich in der für diesen Fachbereich üblichen und einheitlichen Sprache (englisch) benützt werden. Bei einer Übersetzung würde die Gefahr von Fehlinterpretationen und Informationsverlust bestehen (Art. 10 Abs. 4).

Artikel 12 Absatz 2 EPDG sieht zwar vor, dass der Bundesrat das BAG ermächtigen kann, die Anforderungen an die Zertifizierung dem Stand der Technik anzupassen, doch erscheint es sachgerechter, wenn das EDI konkret bestimmt, welche Vorgaben das BAG anpassen soll (Abs. 5).

Art. 11 Zugangsportal für Gesundheitsfachpersonen

Das Zugangsportal für Gesundheitsfachpersonen muss den in Ziffer 3 des Anhangs 2 der EPDV-EDI aufgeführten Anforderungen entsprechen. So muss z. B. die Darstellung der medizinischen Daten des elektronischen Patientendossiers alle relevanten Informationen korrekt und vollständig präsentieren (Ziff. 3.1 Anhang 2 der EPDV-EDI). Dies gilt insbesondere für die Darstellung strukturierter Daten wie beispielsweise medizinischer Austauschformate nach *Artikel 10 Absatz 3 Buchstabe b*. Das Zugangsportal muss darüber hinaus beispielsweise klar erkennen lassen, ob die medizinischen Daten durch eine Gesundheitsfachperson oder durch den Patienten oder die Patientin selbst bereitgestellt wurden, welche medizinischen Daten nicht mehr gültig sind oder welche weiteren Versionen gegebenenfalls auch vorhanden sind. Medizinische Daten, die von Gesundheitsfachpersonen bereitgestellt wurden, können aus Gründen der Nachvollziehbarkeit von diesen nicht gelöscht werden. Sie können jedoch von diesen mit der Statusinformation «annulliert» («*deprecated*») versehen werden. Auf diese Weise ist es beispielsweise möglich, medizinische Daten mit fehlerhaften oder veralteten Informationen durch korrigierte oder aktuellere Daten zu ersetzen. Den Patientinnen und Patienten, aber auch anderen Gesundheitsfachpersonen sollte auf dem Zugangsportal stets nur die aktuellste, nicht annullierte Version der medizinischen Daten, resp. eines Dokuments angezeigt werden. Bei Bedarf sollte der Versionsverlauf allerdings ebenfalls zur Verfügung stehen.

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

[7] SR **170.512**

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 (Ziff. 3.2 Anhang 2 der EPDV-EDI).

Aus Gründen der Interoperabilität und der Datensicherheit sind die für das elektronische Patientendossier zugelassenen Medientypen und Dateiformate in Ziffer 8 des Anhangs 3 der EPDV-EDI abschliessend aufgeführt (Ziff. 3.3 Anhang 2 der EPDV-EDI). Das Zugangsportal muss die Möglichkeit bieten, diese Medientypen bereitzustellen sowie abzurufen und darzustellen. Weitere Anforderungen betreffen einerseits die Möglichkeit medizinische Daten bzw. Dokumente einzeln, aber auch als Selektion gesammelt herunterzuladen (Ziff. 3.3 Bst. c Anhang 2 der EPDV-EDI). Andererseits muss sichergestellt werden, dass Austauschformate mit strukturierten medizinischen Daten nicht nur menschenlesbar darstell- und herunterladbar sind (Ziff. 3.3 Bst. d Anhang 2 der EPDV-EDI), sondern diese auch im strukturierten Originalformat heruntergeladen werden können (Ziff. 3.3 Bst. e Anhang 2 der EPDV-EDI), um sie gegebenenfalls auf strukturierte Weise weiterverarbeiten zu können.

Damit Gesundheitsfachpersonen ihrer Dokumentationspflicht nachkommen können, muss das Zugangsportal den Abruf von medizinischen Daten zum Abspeichern im Primärsystem der Gesundheitseinrichtung unterstützen («*Download*»). Aus Sicherheitsgründen sind für den Abruf und Download von medizinischen Daten Obergrenzen für die Anzahl an Einzeldateien (sog. «*rate limits*») zu definieren, welche beim Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen auslösen (Ziff. 3.3 Bst. f Anhang 2 der EPDV-EDI). Beispielsweise könnte ein Überschreiten der Obergrenze bedingen, dass zuvor ein sog. CAPTCHA («*Completely Automated Public Turing test to tell Computers and Humans Apart*») absolviert werden muss, um unzulässige, technisch automatisierte Massen-Abrufe zu begrenzen.

Art. 12 Datenschutz und Datensicherheit

Nach *Absatz 1* müssen Gemeinschaften ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem analog der Norm ISO/IEC 27001:2013 betreiben. Ein Datenschutz- und Datensicherheitsmanagementsystem analog der Norm ISO/IEC 27001:2013 verfolgt eine ganzheitliche, koordinierte Betrachtung der Datenschutz- und Datensicherheitsrisiken der Gemeinschaft, um ein umfassendes Paket von geeigneten Sicherheitsmassnahmen (Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen, etc.) im Rahmen eines einheitlichen Managementsystems planen, einführen, überprüfen und verbessern zu können. Es muss die Komplexität und Grösse der Gemeinschaft sowie insbesondere den Umfang der in der Gemeinschaft erfassten besonders schützenswerten Daten (v.a. medizinische Daten) des elektronischen Patientendossiers berücksichtigen (Ziff. 4.2.3 der Anhang 2 EPDV-EDI).

Die Sicherstellung der Einhaltung der Anforderungen dieses Artikels liegt auch dann in der Verantwortung der Gemeinschaften, wenn sie Leistungen durch Dritte (Betriebsorganisationen) erbringen lassen (Ziff. 4.1 Anhang 2 der EPDV-EDI).

<u>Datenschutz- und Datensicherheitsmanagementsystem</u>
Das durch eine Gemeinschaft zu führende Datenschutz- und Datensicherheitsmanagementsystem muss geeignete Massnahmen zur Erfüllung der hier aufgestellten Bestimmungen definieren und umsetzen. Dazu muss es die allgemeinen und spezifischen Verantwortlichkeiten für das Management von Datenschutz und Datensicherheit festlegen und den dafür verantwortlichen Personen zuordnen und alle dafür relevanten Aufzeichnungen vor Verlust, Zerstörung und Fälschung schützen.

Zusätzlich zu den vorgenannten und in den *Buchstaben a–c* aufgeführten Anforderungen muss das Datenschutz- und Datensicherheitsmanagementsystem unter anderem einen Risikokatalog und einen Risikobehandlungsplan umfassen (Ziff. 4.2.3 Anhang 2 der EPDV-EDI).

Nach *Buchstabe a* sind technische und organisatorische Verfahren zur Erkennung von und zum Umgang mit Sicherheitsvorfällen einzurichten (Ziff. 4.3 Anhang 2 der EPDV-EDI). Da eine *a priori* Sicherheit

nie vollständig erzielt werden kann, ist es umso wichtiger, allfällige Sicherheitsvorfälle zumindest *a posteriori* rasch zu erkennen, um mit definierten Massnahmen, Prozessen und klaren Verantwortlichkeiten darauf reagieren zu können. Dies kann durch den Aufbau eines so genannten «*Security Information and Event Management Systems*» (SIEM) gewährleistet werden, mit dem beispielsweise Anomalien im System und in den Bearbeitungsmustern erkannt werden können, damit diese entsprechend angemessen organisatorisch und technisch adressiert werden. Das SIEM wird gemeinschaftsspezifisch aufgebaut. Es sollte dabei insbesondere die spezifische Risikoexposition und -entwicklung der Gemeinschaft berücksichtigen und dieser jederzeit angemessen sein. 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 im Anhang 2 der EPDV-EDI betreffen beispielsweise die Erkennung und den Umgang mit Sicherheitsschwachstellen sowie den Schutz vor Schadcode (Ziff. 4.4 und 4.5 Anhang 2 der EPDV-EDI).

Für den Umgang mit erkannten Sicherheitsvorfällen enthält der Anhang 2 der EPDV-EDI in Ziffer 4.3.3 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 ist notwendig, um das potentielle Schadensausmass begrenzen zu können oder um andere vulnerable Systemteile nicht ebenfalls zu gefährden. Zur Erfüllung von *Absatz 3* müssen Gemeinschaften zudem formale Verfahren für die Eskalation (Meldung) von besonders kritischen Datenschutz- oder Datensicherheitsereignissen an das BAG definiert haben sowie deren Einhaltung einfordern und kontrollieren (Ziff. 4.3.3 Bst. a Anhang 2 der EPDV-EDI und Erläuterungen zu Abs. 3).

Zum Umgang mit Sicherheitsschwachstellen konkretisiert der Anhang 2 der EPDV-EDI in Ziffer 4.4 zudem die Verantwortung der Gemeinschaften, ein (präventives) Sicherheitsschwachstellenmanagement zu betreiben. Das heisst insbesondere, dass Informationen über vorhandene oder neu entdeckte Sicherheitsschwachstellen in den eingesetzten Informatikmitteln (z. B. Fehler in kritischen Software-Komponenten) rasch bearbeitet werden, damit – nach Bewertung – angemessene Gegenmassnahmen (z. B. «Patchen» der betroffenen Systeme) eingeleitet werden können (Ziff. 4.13.2 Bst. d Anhang 2 der EPDV-EDI).

Nach *Buchstabe b* ist insbesondere ein Verzeichnis aller in der Gemeinschaft für das elektronische Patientendossier verwendeten schützenswerten Informatikmittel und Datensammlungen («Inventar der Informatikinfrastruktur») vorzusehen (Ziff. 4.6 Anhang 2 der EPDV-EDI). Darin sind nach Ziffer 4.6.2. Buchstabe j des Anhangs 2 der EPDV-EDI auch alle angeschlossenen Primärsysteme zu führen, um eine Übersicht über alle Primärsysteme zu haben, welche Daten mit dem elektronischen Patientendossier austauschen. Bei diesem Inventar handelt es sich um einen Bestandteil des im Rahmen des Datenschutz- und Datensicherheitsmanagementsystem zu erstellenden «Inventars der für die Risikobeurteilung und Risikobehandlung relevanten Betriebsmittel». Die zu inventarisierenden Elemente werden in *Ziffer 4.2.3 Buchstabe c* Anhang 2 der EPDV-EDI weiter konkretisiert und umfassen neben den primären Schutzobjekten, d. h. den schützenswerten Daten des elektronischen Patientendossiers, auch die Prozesse zu deren Bearbeitung, da auch diese unmittelbar relevant für den Schutz der Daten sind (Ziff. 4.2.3. Bst. c Abs. i). Darüber hinaus sind auch die sogenannten sekundären Schutzobjekte im Rahmen des des Datenschutz- und Datensicherheitsmanagementsystems zu verwalten. Darunter sind vor allem die Systeme, Infrastrukturen und Anwendungen aber auch die Einrichtungen, organisatorischen Strukturen (Aufbauorganisationen, Verantwortlichkeiten, etc.), Personen und Prozesse zu verstehen, von denen der Schutz der primären Schutzobjekte abhängig ist (Ziff. 4.2.3. Bst. c Abs. ii). Beispielsweise ist es relevant zu wissen, welche Systeme schützenswerte Daten führen, von wem und wie diese überwacht werden und was mit den Informationen geschieht, resp. welche Reaktionsprozesse

und Verantwortlichkeiten existieren, wenn eine unzulässige Datenbearbeitung erkannt wurde.

Da Organisationen und ihre Betriebsmittel (Informatikmittel, Datensammlungen aber auch Prozesse, Organisationsstrukturen, etc.) und damit auch die Risikosituation steten Veränderungen unterworfen sind, müssen alle sicherheitsrelevanten Veränderungen an den vorgenannten Betriebsmitteln beurteilt und dokumentiert werden, damit das Datenschutz- und Datensicherheitsmanagementsystem mit aktuellen und korrekten Gegebenheiten arbeiten kann (Ziff. 4.2.4 Anhang 2 EPDV-EDI). Ebenso wie das «Inventar der für die Risikobeurteilung und Risikobehandlung relevanten Betriebsmittel» ist auch der Risikokatalog und der Risikobehandlungsplan aktuell zu halten (Ziff. 4.2.5 Anhang 2 EPDV-EDI). Da das Risikomanagement hinsichtlich Datenschutz und Datensicherheit ein strategisches Thema für eine Organisation darstellt, muss der Risikobehandlungsplan regelmässig überarbeitet und von der Geschäftsleitung genehmigt werden. Die für die Sicherstellung von Datenschutz und Datensicherheit relevanten Leitlinien sind zudem organisationsweit bekannt zu machen.

Nach *Buchstabe c* müssen Gemeinschaften über das Datenschutz- und Datensicherheitsmanagementsystem spezifische Datenschutz- und Datensicherheitsvorgaben für die angeschlossenen Gesundheitseinrichtungen, sowie indirekt auch für deren Gesundheitsfachpersonen und allfällige weitere Mitarbeitende wie z. B. Mitarbeitende der Spitalinformatik und Dritte festlegen (Ziff. 4.7 bis 4.10 Anhang 2 EPDV-EDI). 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 hinzuweisen (Ziff. 4.7.1 Bst. b Anhang 2 der EPDV-EDI, vgl. auch Ziff. 1.2.2. Bst. b und 1.3.3 Bst. a Anhang 2 der EPDV-EDI). 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 (Ziff. 4.7.1 und 4.7.2 Anhang 2 der EPDV-EDI). Gesundheitseinrichtungen wiederum müssen ihre Gesundheitsfachpersonen zur Einhaltung der geforderten Massnahmen verpflichten. Nach Ziffer 4.7.3 des Anhangs 2 der EPDV-EDI müssen Gemeinschaften mit geeigneten organisatorischen und allenfalls technischen Massnahmen sicherstellen, dass Endgeräte mit nicht mehr als sicher eingestuften Konfigurationen keine Daten des elektronischen Patientendossiers bearbeiten können. So gilt es beispielsweise zu verhindern, dass Endgeräte mit veralteten und daher unsicheren, weil vom Hersteller nicht mehr unterstützten Betriebssystemen auf Daten des elektronischen Patientendossiers zugreifen.

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 Gesundheitsfachpersonen und den Mitarbeitenden der Gemeinschaft (z. B. Personal der Kontaktstelle für Gesundheitsfachpersonen) auch allfällig beigezogene Dritte (z. B. Betriebsorganisationen oder Lieferanten) nach *Buchstabe c* die spezifischen Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft einhalten. Bezüglich des technischen oder administrativen Personals dieser Dritten legt der Anhang 2 der EPDV-EDI dazu insbesondere Anforderungen an die Verwaltung von Personen und deren Zugängen und Benutzerrechte fest (Ziff. 4.9 Anhang 2 der EPDV-EDI). Besondere Vorgaben gelten für Personen mit weitgehenden («privilegierten») Systemberechtigungen («Systemadministratoren») für Zugriffe auf besonders schützenswerte Datenbestände und Systeme (Ziff. 4.9.1 Anhang 2 der EPDV-EDI). Diese sogenannten «Schlüsselpersonen» können ein erhöhtes Sicherheitsrisiko darstellen, sofern sie bestehende Sicherheitsvorkehrungen umgehen können. Sie sind daher dem Datenschutz- und Datensicherheitsverantwortlichen bekannt zu machen und müssen von diesem verwaltet werden. Für diese Personen gelten besondere Anforderungen an deren Auswahl und sie müssen klar definierten Sicherheitsanforderungen der Gemeinschaften unterliegen.

Darüber hinaus gelten gemäss den Ziffern 4.9 und 4.10 Anhang 2 der EPDV-EDI weitergehende Regelungen zum Lieferantenmanagement, mit dem Ziel, dass ein durchgehend hohes Sicherheitsniveau für alle beteiligten Akteure (Gemeinschaften, Einrichtungen, Lieferanten und Unterlieferanten) unabhängig von der Organisationsstruktur aufrecht erhalten werden kann. 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 (Ziff. 4.9.4 Bst. a und e Anhang 2 der EPDV-EDI).

Datenschutz- und Datensicherheitsverantwortlicher

Nach *Absatz 2* 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 fachlichen Kompetenzen, Befugnisse und notwendigen Ressourcen verfügen. Sie ist für die Entwicklung, Umsetzung und Überwachung von Massnahmen zur Sicherstellung von Datenschutz und Datensicherheit, sowie für die Anwendung korrigierender Massnahmen im Rahmen der kontinuierlichen Weiterentwicklung des Datenschutzes und der Datensicherheit der Organisation verantwortlich (Ziff. 4.11 Anhang 2 der EPDV-EDI). Gemeinschaften können die operative Ausübung dieser Funktion auch an Dritte delegieren, bleiben aber für die Sicherstellung der Anforderungen verantwortlich.

Meldung von sicherheitsrelevanten Vorfällen

Die Meldepflicht für als sicherheitsrelevant eingestufte, also besonders schwerwiegende, Vorfälle an das BAG nach *Absatz 3* 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. Einerseits für Gemeinschaften selbst, aber auch für das BAG als regulierende Behörde in diesem Bereich des Datenschutzes und der Datensicherheit. So können durch regelmässige Auswertungen dieser Ereignisse allfällige Trends in der Bedrohungslandschaft aufgezeigt werden, die es den 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 in Anwendung der Schutzklausel nach *Artikel 37* weitergehende Massnahmen anordnen. Gemeinschaften , 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 bereitstellt sowie den Informationsaustausch zwischen den Betreibern von gefährdeten oder kritischen Infrastrukturen fördert.

Weitere Anforderungen

In Umsetzung von *Absatz 4* legt das EDI in den Ziffern 4.12 bis 4.18 Anhang 2 der EPDV-EDI weitere Anforderungen in Bezug auf Datenschutz und Datensicherheit fest. Diese umfassen unter anderem Vorgaben zu folgenden Bereichen:

- Verschlüsselung in der Kommunikation und Datenspeicherung sowie zur Verwaltung kryptographischer Schlüssel (Ziff. 4.12 Anhang 2 der EPDV-EDI);
- Betriebssicherheit, Systemwiederherstellung und Protokollierung des Systembetriebs (Ziff. 4.13 Anhang 2 der EPDV-EDI – die technisch-administrativen Protokolldaten im Rahmen des Systembetriebs nach Ziffer 4.13.3 Anhang 2 der EPDV-EDI dienen in erster Linie der anlassbezogenen Überprüfung der Einhaltung der Datensicherheits- und Datenschutzvorschriften. Daher dürfen sie nur denjenigen Personen oder Organen zugänglich sein, welche die Umsetzung der Vorgaben zu überwachen haben (Ziff. 4.13.3 Bst. g Anhang 2 der EPDV-EDI) und müssen gegen unzulässige oder unbemerkte Veränderungen geschützt werden (Ziff. 4.13.3 Bst. h Anhang 2 der EPDV-EDI);
- Anschaffung, sichere Entwicklung und Instandhaltung von Systemen (Ziff. 4.14 Anhang 2 der EPDV-EDI);
- Verwaltung von Netzwerken und Netzwerkdiensten, sowie Netzwerk-Sitzungen (Ziff. 4.15 bis 4.16 Anhang 2 der EPDV-EDI);

- Zwischenspeicher (Ziff. 4.17 der Anhang 2 der EPDV-EDI);
- Verfügbarkeit (Ziff. 4.18 Anhang 2 der EPDV-EDI).

Um auch rechtlich eine grösstmögliche Sicherheit der Daten des elektronischen Patientendossiers sicherzustellen, dürfen diese nach *Absatz 5* nur in Datenspeichern gespeichert werden, die sich in der Schweiz befinden und ausschliesslich Schweizer Recht unterstehen. Der Betrieb darf daher auch nur von juristischen Personen erbracht werden, die Schweizer Recht unterstehen (Ziff. 4.19 Anhang 2 der EPDV-EDI). Auf diese Weise unterliegen die Daten keiner vom Schweizer Recht abweichenden Gesetzgebung. Mögliche Kollisionen mit ausländischen Rechtsnormen können so zum Voraus verhindert werden.

Art. 13 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 (Ziff. 5.1.2 Anhang 2 der EPDV-EDI). 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 Fern-Zugriff auf die Endgeräte der Gesundheitsfachpersonen darf ausschliesslich mit Kenntnis und Einwilligung des Benutzers erfolgen und muss dokumentiert werden.

2. Abschnitt: Stammgemeinschaften

Die nachfolgenden Erläuterungen beziehen sich auf die ausschliesslich für Stammgemeinschaften geltenden Bestimmungen des zweiten Abschnitts der EPDV (Art. 14 bis 21).

Art. 14 Zusätzliche Anforderungen für Stammgemeinschaften

Stammgemeinschaften, also Gemeinschaften bei denen Patientinnen und Patienten ein elektronisches Patientendossier erstellen und die Zugriffsrechte verwalten können, müssen zusätzlich zu den Anforderungen des 1. Abschnitts (Art. 9 bis 13) auch die Anforderungen der Artikel 14 bis 21 erfüllen.

Art. 15 Information der Patientin oder des Patienten

Die Einwilligung der Patientin oder des Patienten muss durch eine angemessene und sachliche Information begleitet sein. Diese liegt in der Verantwortung der jeweiligen Stammgemeinschaft der Patientin oder des Patienten. 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 muss mindestens die in *Absatz 1* aufgeführten Punkte (Ziff. 6.1 Anhang 2 der EPDV-EDI) umfassen.

Nach *Buchstabe a* muss über den Zweck des elektronischen Patientendossiers informiert werden (Ziff. 6.1.1 Anhang 2 der EPDV-EDI). Dazu zählt die Information über die in Artikel 1 EPDG genannten Zwecke des elektronischen Patientendossiers (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 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 (Ziff. 6.1.2–6.1.5 Anhang 2 der EPDV-EDI). Dazu gehört insbesondere die Darlegung, welche Datenbearbeitungsmöglichkeiten der Patientin oder dem Patienten und seinen oder ihren Stellvertretern einerseits und den zugriffsberechtigten Gesundheitsfachpersonen und deren Hilfspersonen andererseits 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 sind. 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 (Ziff. 6.1.2 Bst. a Anhang 2 der EPDV-EDI). 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; Ziff. 6.1.3 Anhang 2 der EPDV-EDI). In dem Zusammenhang ist auf die Folgen des Widerrufs hinzuweisen. Dazu gehört beispielsweise auch die Information, dass die medizinischen Daten eines widerrufenen elektronischen Patientendossiers nach einer allfälligen erneuten Eröffnung eines elektronischen Patientendossiers in diesem nicht verfügbar sein werden (Ziff. 6.1.3 Bst. g Anhang 2 der EPDV-EDI), da bei einer erneuten Einwilligung eine neue Patientenidentifikationsnummer vergeben wird (vgl. Erläuterungen zu Art. 8). Ein nach einem Widerruf eröffnetes Patientendossier ist somit ein neues elektronisches Patientendossier, das «leer» ist und entsprechend wieder neu zu befüllen ist.

Nach *Buchstabe d* muss aus der Information unter anderem hervorgehen, wie und wem Zugriffsrechte auf bestimmte medizinische Daten vergeben werden können (vgl. Erläuterungen zu Art. 1–4). Dazu gehört insbesondere die Information über die Vertraulichkeitsstufen (Ziff. 6.1.4 Anhang 2 der EPDV-EDI) über die Zugriffsrechte (Ziff. 6.1.5 Anhang 2 der EPDV-EDI) und über die Möglichkeiten und Optionen zur Anpassung, zum Entzug und zur Befristung der Zugriffsrechte nach Artikel 4 sowie über die Möglichkeit, einzelne Gesundheitsfachpersonen vollständig vom Zugriff auszuschliessen (sog. Ausschlussliste; Art. 4 Bst. b).

Die Patientin bzw. der Patient ist nach *Absatz 2* zudem darüber zu informieren, welche Sicherheitsvorkehrungen empfohlen werden (Ziff. 6.1.6 Anhang 2 der EPDV-EDI). Dazu gehören z. B. Hinweise zum sicheren Umgang mit dem Identifikationsmittel und mit geheimen Authentifizierungsinformationen (z. B. Passwörtern), die Aufklärung über Risiken und Verhaltensempfehlungen zur Abwehr von patientengerichteten Bedrohungen und Betrugsversuchen wie «*Social Engineering*», «*Phishing*» u. ä., wie auch Hinweise zur Verwendung sicherer Endgeräte und Webbrowser sowie zum Einsatz von Schutzprogrammen gegen Schadprogramme oder Netzwerk-Bedrohungen.

Art. 16 Einwilligung

Das Gesetz sieht vor, dass die Einwilligung schriftlich erteilt werden muss. *Artikel 16* 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 unter welchen Bedingungen die elektronische Unterschrift der eigenhändigen gleichgestellt ist, nämlich dann, wenn eine elektronische Unterschrift verwendet wird, die den Anforderungen von Artikel 14 Absatz 2bis OR[8] genügt (qualifizierte elektronische Signatur im Sinne des Bundesgesetzes über die elektronische Signatur, ZertES[9]). Ist diese Voraussetzung erfüllt, gilt die Schriftform als eingehalten. Die Nachvollziehbarkeit der elektronischen Abgabe der Einwilligung wird über die Protokollierung sichergestellt.

[8] SR 202
[9] SR 943.03

Art. 17 Verwaltung

Verwaltung der Patientinnen und Patienten

Stammgemeinschaften müssen nach *Absatz 1* geeignete Prozesse für die Eröffnung, die Verwaltung und die Aufhebung des elektronischen Patientendossiers sowie für die Identifikation und Authentifizierung der Patientinnen und Patienten definieren, dokumentieren, umsetzen und einhalten (Ziff. 8.1 Anhang 2 EPDV-EDI).

Buchstabe a fordert von den Stammgemeinschaften Regelungen für die übergreifenden Prozesse zur Eröffnung, die Verwaltung und die 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 15*, sowie die Regelung zum Einholen der Einwilligung nach *Artikel 16*. Für den Prozess zur Aufhebung eines elektronischen Patientendossiers sind die Vorgaben nach *Artikel 21* massgeblich, die Anforderungen an Prozess zum Wechsel der Stammgemeinschaft werden in Ziffer 8.5 Anhang 2 der EPDV-EDI konkretisiert

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 (Ziff. 8.2 Anhang 2 der EPDV-EDI). Stammgemeinschaften müssen dazu die Patientin oder den Patienten nach *Buchstabe b* sicher identifizieren. Die Ziffer 8.2.1 Buchstabe a Anhang 2 der EPDV-EDI konkretisiert, dass – sofern dies nicht mit einem Identifikationsmittel eines nach *Artikel 31* zertifizierten Herausgebers durchgeführt werden kann – die Anforderungen nach *Artikel 24* erfüllt werden müssen, also eine Identitätsprüfung mittels der genannten Ausweise nach Ausweisgesetz resp. Ausländergesetz oder mittels einer qualifizierten elektronischen Signatur signierten Antrag erfolgen muss. Eine sichere und möglichst eindeutige Identifikation ist nicht zuletzt auch die Voraussetzung für die korrekte Vergabe der Patientenidentifikationsnummer nach *Buchstabe d*.

Buchstabe c legt fest, dass Stammgemeinschaften sicherstellen müssen, dass – analog wie bei den Gesundheitsfachpersonen (Art. 9 Bst. e) – der Zugriff auf das elektronische Patientendossier durch Patientinnen und Patienten sowie durch allfällige Stellvertreter nur mit gültigen Identifikationsmitteln von einem nach *Artikel 31* zertifizierten Herausgeber möglich ist (Ziff. 8.3 Anhang 2 der EPDV-EDI). Dies bedeutet, dass die Zugangsportale und Endgeräte, die von Patientinnen und Patienten für den Zugriff auf das elektronische Patientendossier genutzt werden, ein starkes Authentifizierungsverfahren nach dem aktuellen Stand der Technik mit mindestens zwei Authentifizierungsfaktoren unterstützen müssen.

Buchstabe d legt fest, dass Stammgemeinschaften im Rahmen der Eröffnung eines elektronischen Patientendossiers die Vorgaben der Artikel 6 und 7 für die Beantragung der Patientenidentifikationsnummer bei der ZAS einhalten müssen (Ziff. 8.2.1 Bst. d Anhang 2 der EPDV-EDI). Nach Ziffer 8.2.1 Bst. b Anhangs 2 der EPDV-EDI muss die Stammgemeinschaft zudem sicherstellen, dass vor der Erstellung eines elektronisches Patientendossier überprüft wird, dass die Patientin oder der Patient nicht schon bereits ein elektronisches Patientendossier besitzt 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 medizinischen Daten stets nur diesem einen elektronischen Patientendossier eindeutig zugeordnet sind.

Weitere Vorgaben im Anhang 2 der EPDV-EDI betreffen die Verpflichtung zur Übernahme der demographischen Daten der ZAS und der Patientenidentifikationsnummer in den Patientenindex (Ziff. 8.2.1 Bst. e Anhang 2 der EPDV-EDI) sowie die korrekte Zuordnung des eindeutigen Identifikator nach Artikel 25 Absatz 1 EPDV zum richtigen elektronischen Patientendossier (Ziff. 8.2.2 Anhang 2 der EPDV-EDI).

Buchstabe e stellt sicher, dass Patientinnen oder Patienten ihre Stammgemeinschaft wechseln können. Ziffer 8.5.2 Anhang 2 der EPDV-EDI fordert dementsprechend, dass die Stammgemeinschaften sicher-

stellen 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 das spezifizierte Format des nationalen Integrationsprofils CH:PPQ des EDI nach Ziffer 2 des Anhangs 5 der EPDV-EDI. Da die Konfiguration der Berechtigungssteuerung nur innerhalb der eigenen Stammgemeinschaft verwaltet werden kann, können Gesundheitsfachpersonen die Weitergabe von Zugriffsrechten nach *Artikel 4 Buchstabe g* 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. Ebenso müssen Stellvertreterinnen und Stellvertreter in der neuen Stammgemeinschaft erneut registriert werden.

Umsetzung der Berechtigungssteuerung

Nach *Absatz 2* müssen Stammgemeinschaften die technischen und organisatorischen Voraussetzungen erfüllen, um auch die Umsetzung der Bestimmungen nach Artikel 2 Absätze 1 und 3, Artikel 3 und Artikel 4 sicherzustellen (vgl. entsprechende Erläuterungen zu Ebendiesen sowie Ziff. 8.6 Anhang 2 der EPDV-EDI).

Die Umsetzung von Artikel 4 Buchstabe f (Benennung einer Stellvertretung) ist neben der technischen Umsetzung mit weiteren organisatorischen Aufgaben verbunden, die in Ziffer 8.4 Anhang 2 der EPDV-EDI konkretisiert werden. Stellvertreterinnen und Stellvertreter benötigen keine eigene Patientenidentifikationsnummer und auch kein eigenes elektronisches Patientendossier, dürfen aber nur mit einem eigenen Identifikationsmittel eines nach Artikel 31 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 (Ziff. 8.4.2 Bst. b Anhang 2 der EPDV-EDI). 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 31 zertifizierten Herausgebers durchgeführt werden kann, muss sie ebenfalls den Anforderungen nach Artikel 24 entsprechen (Ziff. 8.4.2 Buchstabe a Anhang 2 der EPDV-EDI). Darüber hinaus muss gewährleistet sein, dass der Zugang des Stellvertreters oder der Stellvertreterin nur für die Dauer der Stellvertretung besteht (Ziff. 8.4.2 Bst. d Anhang 2 der EPDV-EDI). 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. 18 Zugangsportal für Patientinnen und Patienten

Das Zugangsportal für Patientinnen und Patienten muss den in Ziffer 9.1 bis 9.5 des Anhangs 2 EPDV-EDI festgelegten Anforderungen entsprechen. Dazu zählen neben den Vorgaben, die auch für das Zugangsportal für Gesundheitsfachpersonen nach Artikel 11 gelten, insbesondere die Vorgabe nach Buchstabe a zur Umsetzung der verschiedenen Möglichkeiten der Vergabe von Vertraulichkeitsstufen und Zugriffsrechten nach Artikel 1 Absatz 1 und Artikel 2 Absatz 1 sowie der Optionen der Patientinnen und Patienten nach Artikel 4 Buchstaben a bis e sowie Buchstabe g. Dazu gehört auch die Darstellung der Zusammensetzung von Gruppen von Gesundheitsfachpersonen (Ziff. 9.1.1 Bst. c Anhang 2 der EPDV-EDI).

Die Darstellung der Daten des elektronischen Patientendossiers auf der Benutzeroberfläche des internen Zugangsportals für Patientinnen und Patienten muss korrekt und vollständig sein und muss beispielsweise klar erkennen lassen ob medizinische Daten durch eine Gesundheitsfachperson oder durch den Patienten oder die Patientin selbst bereitgestellt wurde (Ziff. 9.2 Anhang 2 der EPDV-EDI).

Weitere Vorgaben betreffen die patientengerechte Darstellung der durch Bearbeitung ihrer Daten protokollierten Protokolldaten aus allen Gemeinschaften und Stammgemeinschaften nach *Buchstabe b* (Ziffer 9.3 Anhang 2 der EPDV-EDI). Über das Zugangsportal für Patientinnen und Patienten müssen diese die Möglichkeit haben, jederzeit die bei jeder Bearbeitung des elektronischen Patientendossiers anfallenden Protokolldaten (Art. 10 Abs. 3 Buchstabe d) einzusehen (Ziff. 9.3 und Ziff. 2.10 Anhang 2 der EPDV-EDI). Da die Protokolldaten nach Ziffer 2.10 des Anhangs 2 der EPDV-EDI auch dezentral in anderen Gemeinschaften anfallen, müssen diese in einem Abrufverfahren aus den jeweiligen Gemeinschaften abgerufen werden 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 Anpassungen der Integrationsprofile nach Artikel 5 Buchstabe b der EPDV-EDI.

Nach *Buchstabe c* muss das Zugangsportal für Patientinnen und Patienten ihnen insbesondere die Möglichkeit bieten, medizinische Daten von einer Vernichtung nach Artikel 10 Absatz 2 Buchstabe b auszunehmen oder bestimmte medizinische Daten aus dem elektronischen Patientendossier nach Artikel 10 Absatz 2 Buchstabe c zu vernichten (Ziff. 9.4.1 Anhang 2 der EPDV-EDI). Hinsichtlich der von der Patientin oder dem Patienten selbst erfassten Daten, wird in Ziffer 9.4.3 des Anhangs 2 der EPDV-EDI konkretisiert, dass die Kernfunktionen des elektronischen Patientendossiers auf dem Zugangsportal klar von allfälligen Funktionalitäten abgegrenzt werden müssen, die nicht zum Regelungsgegenstand des EPDG und dessen Ausführungsbestimmungen gehören. 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 und somit aus dem Geltungsbereich des EPDG herausgeführt werden.

Zur Förderung der hindernisfreien Zugänglichkeit für Patientinnen und Patienten mit Behinderungen, altersbedingten oder sprachlichen Einschränkungen müssen die Zugangsportale nach *Buchstabe d* die gleichen Anforderungen erfüllen wie das Zugangsportal für Gesundheitsfachpersonen gemäss Artikel 11 (Ziff. 3.2 Anhang 2 der EPDV-EDI).

Art. 19 Von Patientinnen und Patienten erfasste Daten

Der Patient oder die Patientin hat die Möglichkeit, über das Zugangsportal seiner oder ihrer Stammgemeinschaft selber eigene medizinische Daten im elektronische Patientendossier zu erfassen (Art. 10 Abs. 2 Bst. b Ziff. 3 EPDG), ohne dass diese einer Löschungsfrist unterliegen (Ziff. 10.1.2 Anhang 2 der EPDV-EDI).

Die von der Patientin oder dem Patienten selbst erfassten Daten sollen unter anderem aus Datensicherheitsüberlegungen nicht in den Dokumentenablagen einer angeschlossenen Gesundheitseinrichtung gespeichert werden. Aus diesem Grund müssen Stammgemeinschaften nach Ziffer 10.1.1 des Anhangs 2 der EPDV-EDI 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 des Anhangs 2 der EPDV-EDI sieht zudem die Möglichkeit vor, dass Patientinnen und Patienten die medizinischen Daten 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. Damit bei einem Re-Import keine Duplikate entstehen, ist entweder die Export-Funktion mit einem Löschen der exportierten Daten zu verbinden oder beim Re-Import ein geeignetes Verfahren zum Erkennen von Duplikaten anzuwenden. 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 (Ziff. 10.2.3 Anhang 2 der EPDV-EDI).

Art. 20 Kontaktstelle für Patientinnen und Patienten

Stammgemeinschaften müssen zusätzlich zur Kontaktmöglichkeit für Gesundheitsfachpersonen nach Artikel 13 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 (Ziff. 5 Anhang 2 der EPDV-EDI). Im Fall von Konflikt- oder Beschwerde-Situationen gelten die bisherigen Anlaufstellen des Bundes und der Kantone (z. B. eidgenössischer oder kantonaler Datenschutzbeauftragter) als Beschwerde- oder Ombudsstellen.

Art. 21 Aufhebung des elektronischen Patientendossiers

Nach *Absatz 1* hebt die Stammgemeinschaft ein elektronisches Patientendossier auf, wenn die Patientin oder der Patient die Einwilligung zu dessen Führung widerruft. Dazu ist sicherzustellen, dass die widerrufende Patientin oder der widerrufende Patient zuvor sicher identifiziert wurde (Ziff. 12.2.2 Bst. a Anhang 2 der EPDV-EDI). Aus Gründen der Nachvollziehbarkeit hat die Stammgemeinschaft die Widerrufserklärung während zehn Jahren aufzubewahren.

Verstirbt eine Patientin oder ein Patient, so darf die Stammgemeinschaft ihr oder sein elektronisches Patientendossier frühestens zwei Jahre nach dem Todestag aufheben (*Abs. 2*). Diese Regelung dient der Umsetzung des Verhältnismässigkeitsprinzips. Elektronische Patientendossiers verstorbener Personen sollen nicht auf unbestimmte Zeit bestehen bleiben. Wenn die Stammgemeinschaft vom Tod einer Patientin oder eines Patienten Kenntnis erhält, so soll sie dieses nach einer Schutzfrist von zwei Jahren aufheben dürfen. Die Stammgemeinschaft ist aber nicht verpflichtet, aktiv Nachforschungen betreffend Lebendstatus, Todesdaten o.ä. anzustellen. Ebenso besteht keine Pflicht zur Meldung von Todesfällen von Seiten der ZAS oder der kantonalen Gemeinderegister an Stammgemeinschaften und Gemeinschaften. Den Kantonen steht es jedoch frei, eine entsprechende Meldepflicht im kantonalen Recht zu verankern, allenfalls – unter Schaffung der notwendigen gesetzlichen Grundlage – auch unter Verwendung der AHVN13.

Bei der Aufhebung des elektronischen Patientendossiers hat die Stammgemeinschaft nach *Absatz 3* die Zugriffsrechte unverzüglich zu entziehen sowie die ZAS und alle anderen Gemeinschaften und Stammgemeinschaften über die Aufhebung des Dossiers zu informieren. Wie und über welche Kanäle die Information erfolgt, bleibt der Stammgemeinschaft überlassen; sie muss aber sicherstellen, dass die Information die Empfänger erreicht und, dass dabei keine medizinischen Informationen weitergegeben werden. Sämtliche Daten sind gemäss Artikel 10 Absatz 1 Buchstabe e in der Stammgemeinschaft und allen anderen Gemeinschaften zu löschen (Ziff. 12.4 Bst. c und Ziff. 2.6 Bst. b Anhang 2 EPDV-EDI).

3. Abschnitt: Evaluation und Forschung

Art. 22

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 unter anderem auf der Basis eines Monitoringsystems, das die Verfügbarkeit der für die Evaluation notwendigen Daten sicherstellt. Für die Gewährleistung der Verfügbarkeit der Daten, wird in *Absatz 1* festgehalten, dass Gemeinschaften und Stammgemeinschaften dem BAG Daten für die Evaluation in pseudonymisierter Form zur Verfügung stellen. Ferner legt das EDI nach *Absatz 2* die Periodizität sowie die Fristen der zu liefernden Daten.

Weitere wichtige Quellen, die Daten für die Evaluation liefern, sind unter anderem Daten der Abfragedienste nach Artikel 39, insbesondere des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen (Abs. 3) sowie die Unterlagen welche im Rahmen einer Zertifizierung nach EPDG von den zu zertifizierenden Stellen oder von den Zertifizierungsstellen erstellt werden (Abs. 4).

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 31 zertifizierten Herausgeber herausgegeben wurde.

Die Zertifizierung der Herausgeber von Identifikationsmitteln sowie die festgelegten technischen Mindestanforderungen für das Sicherheitsniveau stellen die Vertrauenswürdigkeit des Identifikationsmittels in Bezug auf die Identität von Patientinnen und Patienten sowie Gesundheitsfachpersonen sicher 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 Herausgabe und Verwaltung eines Identifikationsmittels für den gesamten Lebenszyklus richtet sich nach dem in der Norm ISO/IEC 29115:2013 beschriebenen Ablauf, der sich in die Phasen Registrierung, Verwaltung und Einsatz der Identifikationsmittel im operativen Betrieb gliedert. Für die Vertrauenswürdigkeit der Authentifizierung ist das Management des Lebenszyklus des Identifikationsmittels bedeutsam. Dieser Lebenszyklus beinhaltet Teilprozesse wie die Erzeugung des Trägermediums einer elektronischen Identität, Personalisierung, Initialisierung und Bindung der elektronischen Identität an die Inhaberin oder den Inhaber sowie Ausgabe, Aktivierung, Widerruf und Erneuerung.

Die Teilprozesse können in unterschiedlicher Reihenfolge ablaufen, sofern die Sicherheit nachweislich gewährleistet ist. Beispielsweise kann der Schritt der Erfassung der Identitätsdaten mit anschliessender Bindung der elektronischen Identität nach Herausgabe des Identifikationsmittels erfolgen. Vorstellbar ist der folgende Ablauf: Eine Patientin oder ein Patient bzw. 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 mit Hilfe einer Video-Identifizierung sichergestellt werden. Bereits ausgestellte Trägermedien für die elektronische Identität – wie zum Beispiel die Versichertenkarte nach Artikel 42*a* des Bundesgesetz vom 18. März 1994[10] über die Krankenversicherung – müssen somit für die Erfüllung der Vorgaben nach den Artikeln 23 – 27 nicht erneut ausgestellt werden.

[10] SR **832.10**

Art. 23 Anforderungen

Die Anforderungen an die Registrierung und Verwaltung von Identifikationsmittel sowie die Schutzanforderungen für die Authentifizierung 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 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 (Art. 24 Abs. 1).

Nach *Buchstabe b* muss das Identifikationsmittel 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 fünf Jahren aufweisen.

Art. 24 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 mit Hilfe einer Video-Identifikation). 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 in Ziffer 4.2 des Anhangs 8 der EPDV-EDI («Sicherheitsziele für die Umgebung») festgelegt.

Art. 25 Daten

Nach *Absatz 1* weisst der Herausgeber der antragstellenden Person einen eindeutigen Identifikator (eID) zu. Dieser Identifikator muss verwendet werden um die Identität der Person in der Gemeinschaft

oder Stammgemeinschaft mit derjenigen des Herausgebers zu verbinden.

Der Herausgeber erfasst weiterhin die Identitätsattribute der Patientinnen und Patienten (Abs. 2) sowie der Gesundheitsfachpersonen (Abs. 3) für den Nachweis und die Überprüfung ihrer Identität. Der Identifikator nach *Absatz 1* sowie die Attribute nach *Absatz 2 Buchstabe a–d* und *Absatz 3* können an die internen Zugangsportale der Gemeinschaften und Stammgemeinschaften in der Authentifizierungsantwort zum Zweck der Prüfung und Zuordnung der Identität übermittelt werden.

Das Identifikationsmittel kann auch dazu verwendet werden, die berufliche Qualifikation der Gesundheitsfachpersonen zu bestätigen (Art. 9 Abs. 2 Bst. b und d). Der Herausgeber erfasst und bestätigt hierzu die GLN der Gesundheitsfachperson (Art. 25 Abs. 3 Bst. a). Gemäss *Absatz 3 Buchstabe b*, muss vorgängig der Nachweis erbracht werden, dass die antragstellende Person eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG ist. Hierzu führt der Herausgeber einen sorgfältigen Abgleich des Personendatensatzes mit einem eidgenössischen oder kantonalen Register (Medizinalberuferegister, Nationales Register der Gesundheitsberufe, etc.) durch, so dass sichergestellt werden kann, dass die Inhaberin oder der Inhaber des Identifikationsmittel über die entsprechende eidgenössische oder kantonal anerkannte Ausbildung und – im Fall der beruflichen Selbstständigkeit – über eine kantonale Bewilligung der Berufsausübung verfügt.

Die Bestätigung des Attributs «Gesundheitsfachperson» kann durch den Herausgeber des Identifikationsmittels nach *Absatz 3* an Dritte («*Registration Authority*» – Registrierungsstelle) delegiert werden. Die Überprüfung der Identitätsprüfung durch den Herausgeber, resp. durch die Registrierungsstelle ist in Ziffer 4.2 des Anhangs 8 der EPDV-EDI geregelt.

Absatz 5 verpflichtet die Herausgeber die antragstellende Person über die Sicherheitsvorkehrungen, die sie im Umgang mit dem Identifikationsmittel treffen müssen, zu informieren (Abs. 5). Dies schliesst den sicheren Umgang mit Passwörtern, Information über die Verarbeitung und Weitergabe von Identitätsattributen an Dritte ein.

Art. 26 Erneuerung

Nach Ablauf der Gültigkeit des Identifikationsmittels von höchstens 5 Jahren (Art. 23 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 (Art. 23).

Art. 27 Sperrung

Die Inhaberin oder der Inhaber des Identifikationsmittels muss jederzeit die Möglichkeit haben, das Identifikationsmittel für den Zugriff auf das elektronische Patientendossier vorübergehend oder unwiderruflich zu sperren. Da das Identifikationsmittel grundsätzlich für die Authentifizierung ausserhalb des elektronischen Patientendossiers verwendet werden kann, muss der Herausgeber technische Verfahren vorsehen, um eine gültige Authentifizierung am Zugangsportal für Patientinnen und Patienten sowie für Gesundheitsfachpersonen zu verhindern. Darüber hinaus muss der Herausgeber Vorkehrungen treffen, um eine unbefugte Sperrung zu verhindern.

5. Kapitel: Akkreditierung

Art. 28 Anforderungen

Zertifizierungsstellen, die Gemeinschaften, Stammgemeinschaften, Zugangsportale und Herausgeber von Identifikationsmitteln zertifizieren, müssen von der Schweizerischen Akkreditierungsstelle SAS anerkannt für die Auditierung und Zertifizierung von Managementsystemen anerkannt werden. Die Akkre-

ditierung richtet sich nach der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[11] (AkkBV). Nach Artikel 7 Absatz 1 dieser Verordnung muss eine Zertifizierungsstelle die international massgebenden Anforderungen erfüllen. Für Zertifizierungsstellen, die im Bereich des elektronischen Patientendossiers Prüfungen durchführen, ergeben sich die Anforderungen beispielsweise aus der Norm ISO/IEC 17021:2015, welche die Akkreditierung zur Zertifizierung von Managementsystemen festlegt (vgl. Anhang 2 AkkBV).

Gemeinschaften, Stammgemeinschaften sowie Herausgeber von Identifikationsmitteln haben unterschiedliche Aufgaben zu erfüllen, welche im Rahmen der Zertifizierung geprüft werden. Deshalb werden an die Akkreditierung der jeweiligen Zertifizierungsstellen unterschiedliche Anforderungen gestellt und je eine eigene Akkreditierung verlangt (*Abs. 2*).

Absatz 3 konkretisiert den Begriff des Kontrollverfahrens. Dieses umfasst die Kriterien, nach denen die Einhaltung der Zertifizierungsvoraussetzungen zu überprüfen ist (*Bst. a*) sowie Angaben zum Ablauf des Zertifizierungsverfahrens (einschliesslich der Überprüfung und der Rezertifizierung; *Bst. b*).

Absatz 4 schreibt vor, dass das vom BAG zur Verfügung gestellte Zertifizierungstestsystem zur Überprüfung der Einhaltung der Vorgaben in Bezug auf die Datenübertragung von Gemeinschaften und Stammgemeinschaften (Interoperabilität) zu verwenden ist. Mit der Hilfe dieses Zertifizierungstestsystems kann überprüft werden, ob eine zu zertifizierende Gemeinschaft oder Stammgemeinschaft in der Praxis korrekt mit anderen zertifizierten Gemeinschaften und Stammgemeinschaften kommunizieren kann.

Nach *Absatz 5* konkretisiert das EDI die Anforderungen an die Qualifikation des Personals, welches die Zertifizierungen durchführt (vgl. Anhang 6 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. 29 Verfahren

Mit dem Einbezug des BAG soll sichergestellt werden, dass einerseits die Schweizerische Akkreditierungsstelle SAS das Fachwissen der Bundesverwaltung nutzen kann und andererseits das BAG die Möglichkeit erhält, die Einzelheiten der Akkreditierung mit der Schweizerischen Akkreditierungsstelle SAS abzusprechen.

6. Kapitel: Zertifizierung

1. Abschnitt: Voraussetzungen

Art. 30 Gemeinschaften und Stammgemeinschaften

Eine nach Artikel 28 akkreditierte Zertifizierungsstelle stellt fest, ob eine Gemeinschaft oder Stammgemeinschaft die Zertifizierungsvoraussetzungen erfüllt. Dabei müssen Stammgemeinschaften zusätzlich zu den Zertifizierungsvoraussetzungen der Gemeinschaften (Art. 9–13) die Vorgaben nach den Artikeln 14–21 einhalten (Abs. 1).

Absatz 2 delegiert die Rechtssetzungskompetenz zur Festlegung der Einzelheiten für die Zertifizierungsvoraussetzungen an das EDI, was eine stufengerechte Regelung ermöglicht.

Die Kompetenz zur Anpassung der Zertifizierungsvoraussetzungen an den Stand der Technik kann nach *Absatz 3* vom EDI an das BAG übertragen werden (vgl. Erläuterungen zu Art. 10 Abs. 5). Dies ist

[11] SR **946.512**

insbesondere für die Zertifizierungsvoraussetzungen im Bereich der Datenhaltung und Datenübertragung (Art. 10) und dem Datenschutz und der Datensicherheit (Art. 12) von Bedeutung.

Art. 31 Herausgeber von Identifikationsmitteln

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

Buchstabe a verweist auf die Artikel 23–27, die von den Herausgebern von Identifikationsmitteln einzuhalten sind. Diese müssen damit insbesondere sicherstellen, dass die Identifikationsmittel der Vertrauensstufe 3 der Norm ISO/IEC 29115:2013 entsprechen (Art. 23), die Identität der antragstellenden Person überprüft wird (Art. 24) und die Identitätsattribute des Inhabers oder der Inhaberin des Identifikationsmittels korrekt zugeordnet werden (Art. 25).

Der Herausgeber muss mit geeigneten Verfahren sicherstellen, 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 beispielsweise nur befugte Mitarbeiter den Zugang zu Bereichen haben, in denen personenbezogene Daten, kryptografische oder andere sensible Informationen verarbeitet werden. Der Herausgeber des Identifikationsmittels muss für die Gewährleistung von Datenschutz und Datensicherheit bewährte Methoden einsetzen.

Die technischen und organisatorischen Zertifizierungsvoraussetzungen an die Identifikationsmittel und deren Herausgeber werden in Anhang 8 der EPDV-EDI in Form eines sogenannten Schutzprofils konkretisiert (Abs. 2). 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.

Der Evaluationsgegenstand (EVG) des Schutzprofils umfasst das Identifikationsmittel selbst, den Identitätsdienstleister (Identity Provider) für die Identifikation und Authentifizierung sowie die notwendigen technischen Schnittstellen und die sicheren Kommunikationskanäle für die Authentifizierung an den Zugangsportalen der Gemeinschaften bzw. Stammgemeinschaften. Im Zertifizierungsverfahren werden die Nachweise zu den Sicherheitsanforderungen mit einer definierten Prüftiefe, dem sogenannten Evaluation Assurance Level (EAL), durch die Zertifizierungsstelle erhoben und geprüft. Die Prüfung umfasst die Bereiche «Development», «Life-Cycle Support», «Security Target Evaluation» oder« Vulnerability Assessment». Die in Ziffer 5.4 des Anhangs 8 der EPDV-EDI festgelegte Prüftiefe EAL 2 besagt, dass der EVG funktional und strukturell geprüft wird.

Absatz 2 delegiert die Rechtssetzungskompetenz zur Festlegung der Einzelheiten für die Zertifizierungsvoraussetzungen an das EDI, was eine stufengerechte Regelung ermöglicht.

Die Kompetenz zur Anpassung der Zertifizierungsvoraussetzungen an den Stand der Technik wird nach *Absatz 3* via dem EDI an das BAG übertragen (vgl. Erläuterungen zu Art. 10 Abs. 5). Zu denken ist dabei insbesondere an die Anpassung von sehr technischen Vorgaben der Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln.

2. Abschnitt: Zertifizierungsverfahren

Art. 32 Ablauf

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

Die Prüfung nach *Absatz 1* ermöglicht der Zertifizierungsstelle anhand 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 Zertifizierungsvoraussetzungen von den Gemeinschaften oder Stammgemeinschaften oder den Herausgebern von Identifikationsmitteln 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 Anforderungen erfüllt, erteilt sie nach *Absatz 3* das Zertifikat.

Absatz 4 hält fest, dass vor dem Ablauf eines Zertifikats eine sogenannte Rezertifizierung durchzuführen ist. Die Anforderungen einer Rezertifizierung entsprechen jenen eines Zertifizierungsaudits nach Absatz 2. Mit diesem Vorgehen soll ein lückenloser Betrieb einer Gemeinschaft oder Stammgemeinschaft oder aber auch einer Herausgebers von Identifikationsmitteln sichergestellt werden, in dem verhindert wird, dass ein Zertifikat nicht einfach ausläuft und die betreffende Organisation in der Folge von der Teilnahme am elektronischen Patientendossier ausgeschlossen werden muss.

Art. 33 Meldung und Veröffentlichung der Zertifikate

Um den gemeinschaftsübergreifenden Datenaustausch sicherzustellen, müssen die zertifizierten Gemeinschaften und Stammgemeinschaften nach *Absatz 1* in den Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 eingetragen werden. Daher ist jede erfolgreiche Zertifizierung dem BAG zu melden, damit dieses den entsprechenden Eintrag vornehmen kann (Art. 40 Abs. 2). Zudem ist jede Sistierung und jeder Entzug einer Zertifizierung umgehend dem BAG zu melden, damit die betroffene Gemeinschaft oder Stammgemeinschaft im Dienst zur Abfrage der zertifizierten Gemeinschaften und Stammgemeinschaften gesperrt werden kann und somit von der Teilnahme am elektronischen Patientendossier ausgeschlossen wird.

Zusätzlich zum Eintrag der Daten in den Dienst zur Abfrage der zertifizierten Gemeinschaften und Stammgemeinschaften 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. 34 Überprüfung

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 37 Absatz 1 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. Die Zertifizierungsstelle hat zudem die Möglichkeit, Sanktionen zu ergreifen, wenn die entsprechenden Anforderungen nach Artikel 38 Absatz 1 erfüllt sind.

Die Zertifizierungsstelle hat das BAG über festgestellte wesentliche Abweichungen zu informieren, damit dieses mögliche Schwachstellen des Ausführungsrechts frühzeitig erkennen und gegebenenfalls notwendige Massnahmen in die Wege leiten kann.

Art. 35 Geltungsdauer

Ein einmal erteiltes Zertifikat ist während drei Jahren gültig. Vorbehalten bleiben Artikel 36 und 37 Absatz 1 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 32.

Art. 36 Meldung wesentlicher technischer oder organisatorischer Anpassungen

Wesentliche Anpassungen sind nach *Absatz 1* der Zertifizierungsstelle zu melden. 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.

Nach *Absatz 2* entscheidet die Zertifizierungsstelle, ob die gemeldeten Anpassungen im Rahmen der Überprüfung nach Artikel 34, einer Rezertifizierung oder einer ausserordentlichen Rezertifizierung nach *Artikel 37 Absatz 1 Buchstabe c* geprüft werden. Die Überprüfung und die Rezertifizierung finden im üblichen Rhythmus statt, eine ausserordentliche Rezertifizierung muss so rasch wie möglich erfolgen. 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 38 (Sanktionen) oder durch das BAG – wenn dieses durch die Zertifizierungsstelle nach Artikel 34 über wesentliche Abweichungen von den Zertifizierungsvoraussetzungen informiert wird – gestützt auf Artikel 37 (Schutzklausel) vorgenommen werden.

Art. 37 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 38 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. Es geht mit anderen Worten nicht darum, ein Identifikationsmittel eines einzelnen Patienten oder einer einzelnen Gesundheitsfachperson zu sperren, sondern eine Technologie, welche (vorübergehend) nicht den Sicherheitsstandards entspricht, 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 12 Absatz 3 vorliegt, der darauf hindeutet, dass die Zertifizierungsvoraussetzungen nicht mehr erfüllt sind. Sie kann auch angeordnet werden, wenn durch die Zertifizierungsstelle im Rahmen der Überprüfung nach Artikel 34 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.

Das BAG hat nach *Absatz 2* die Möglichkeit, sowohl von der Zertifizierungsstelle als auch von den zertifizierten Stellen diejenigen Unterlagen einzufordern, welche für die Zertifizierung oder Rezertifizierung massgebend sind. Nur aufgrund dieser Unterlagen ist es dem BAG unter Umständen überhaupt möglich, eine schwerwiegende Gefährdung des elektronischen Patientendossiers zu erkennen, um anschliessend entsprechende Massnahmen in die Wege zu leiten.

3. Abschnitt: Sanktionen

Art. 38

Werden bei der regelmässigen Überprüfung der Zertifizierung (Art. 34) 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 (Bst. a). 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 gemeinschaftsübergreifende 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 (Art. 40 Abs. 2) gesperrt. *Buchstabe b* betrifft Fälle, in denen ein Zertifikat irreführend oder täuschend verwendet wird. Dies ist beispielsweise der Fall, wenn Patientinnen oder Patienten betreffend die Bedeutung des Zertifikats getäuscht werden, indem etwa eine Stammgemeinschaft vorgibt, ebenfalls für die Herausgabe von Identifikationsmittel zertifiziert zu sein.

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. 39

Die Daten der Abfragedienste nach den *Buchstaben a–d* sind für eine gesetzeskonforme Kommunikation zwischen Gemeinschaften und Stammgemeinschaften notwendig.

Im Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach *Buchstabe a* werden insbesondere die technischen Angaben geführt, welche zur elektronischen Kommunikation mit den jeweiligen Zugangspunkten erforderliche sind. Für die Sicherstellung der Integrität der elektronischen Nachrichten der Zugangspunkte enthält er zudem auch die öffentlichen Schlüssel mit denen die Gemeinschaften und Stammgemeinschaften die Authentizität der von anderen Zugangspunkten übermittelten Nachrichten verifizieren können (Art. 40 Abs. 1 Bst. c).

Die Angaben zu den Gesundheitseinrichtungen und den Gesundheitsfachpersonen, welche die Daten des elektronischen Patientendossiers bearbeiten dürfen, werden im Abfragedienst nach *Buchstabe a und b* geführt. Dieser umfasst auch die Zugehörigkeiten von Gesundheitsfachpersonen zu Gruppen von Gesundheitsfachpersonen. Aufgrund dieser Information kann die Patientin oder der Patient die Zugriffsrechte für Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen nach *Artikel 2 Absatz 1* zuweisen.

Der Dienst zur Abfrage der Metadaten nach *Buchstabe c* enthält die nach Artikel 9 Absatz 5 Buchstabe a zu verwendenden Metadaten für die strukturierte Beschreibung der im elektronischen Patientendossier erfassten Daten. Die Werte und Wertebereiche der Metadaten sind im Anhang 3 der EPDV-EDI festgelegt.

Der Abfragedienst nach *Buchstabe d* enthält die notwendigen OID für Gemeinschaften und Stammgemeinschaften.

Das BAG trägt die Verantwortung für das Führen der Abfragedienste gemäss Artikel 14 Absatz 1 EPDG., Darunter fällt auch der Aufbau, der Betrieb und die Weiterentwicklung der Abfragedienste.

Das BAG definiert im Rahmen des Aufbaus der Abfragedienste Standardschnittstellen, über welche die zertifizierte Gemeinschaften und Stammgemeinschaften Daten beziehen oder liefern können.

2. Abschnitt: Inhalt

Art. 40 Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften

Damit das BAG die zertifizierten Gemeinschaften und Stammgemeinschaften gemäss Artikel 33 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 der Bezeichnung (Bst. a) und dem OID (Bst. b) auch Angaben von erforderlich, die es erlauben die Zugangspunkte und Nachrichten der zertifizierten Gemeinschaften und Stammgemeinschaften sicher zu authentisieren (Bst. c und d). 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.

Eine Bearbeitung der Daten gemäss *Absatz 2* ist nur dem BAG erlaubt. Gemeinschaften und Stammgemeinschaften haben nur lesenden Zugriff.

Art. 41 Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen

Gemeinschaften und Stammgemeinschaften müssen nach Artikel 9 Buchstabe d sicherstellen, dass die Daten im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen aktuell sind. Der Dienst zur Abfrage verfügt über eine Standardschnittstelle, über die die Daten im zentralen Verzeichnis der Gesundheitseinrichtungen und Gesundheitsfachpersonen aktualisiert und anderen Gemeinschaften und Stammgemeinschaften verfügbar gemacht werden können. Artikel 41 präzisiert die durch Gemeinschaften und Stammgemeinschaften zu liefernden Daten.

Zu den Daten über die Gesundheitseinrichtungen und Gruppen von Gesundheitsfachpersonen nach Absatz 1 *Buchstabe a* gehören insbesondere die Bezeichnung und die Adresse (Ziff. 1), der *OID* (Ziff. 2) sowie für die Gesundheitseinrichtungen zusätzlich die BUR-Nummer nach der Verordnung vom 30. Juni 1993[12] über das Betriebs und Unternehmensregister (Ziff. 3). Gemeinschaften und Stammgemeinschaften müssen die OID nach Ziffer 2 für die ihnen zugehörigen Gesundheitseinrichtungen beantragen. Sie können unterhalb der ihnen zugeteilten OID weitere OIDs für die Bezeichnung der Gruppen innerhalb einer Gesundheitseinrichtung selbst verwalten (Art. 8 Abs. 1).

Die Eintragung der BUR-Nummer nach *Ziffer 3* ist für die Zusammenführung der Gesundheitseinrichtung mit Daten der amtlichen Statistiken des BFS für die Datenerhebung im Rahmen der Evaluation des Gesetzes erforderlich (Art. 22 Abs. 3).

Zu den Daten über die Gesundheitsfachpersonen nach *Buchstabe b* gehören insbesondere die Personalien (Ziff. 1), die OID, welche die GLN enthält (Ziff. 2) sowie die Bezeichnung und die Adresse der Gesundheitseinrichtungen oder der Gruppen von Gesundheitsfachpersonen, der sie angehören (Ziff. 3). Die OID nach *Ziffer 2* setzt sich zusammen aus der OID für Global Location Numbers (2.51.1.7) allgemein und der konkreten GLN, welche der Gesundheitsfachperson zugewiesen wurde. Lautet die GLN für eine Gesundheitsfachperson 7601000000000 so ist die OID 2 2.51.1.7.7601000000000.

Die weiteren Daten nach *Absatz 2* für den Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen sind in Ziffer 1.10 der Ergänzung 1 zu Anhang 5 der EPDV-EDI festgelegt.

Art. 42 Dienst zur Abfrage der OID

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 OID 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 OID 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 OID dürfen Organisationen eigene OID für ihre Organisation erstellen und unterhalb ihres organisationseigenen Knotens weitere OID eigenverantwortlich erstellen und verwenden. Von OID-Inhabern wird verlangt, dass sie eigene Identifikatoren ebenfalls datenschutzkonform publizieren, wenn sie mit den OID eigene Objektdomänen referenzieren.

[12] **SR** 431.903

Besonders schützenswert sind referenzierte Objekte, deren OID-Referenz – in Verbindung mit personenidentifizierenden Daten im Objekt – Rückschlüsse auf den Gesundheitszustand der Person erlauben.

Die Verwaltung der OID wird seit dem 1. Januar 2011 von der Stiftung RefData als Stammregistrierungsstelle wahrgenommen. Gemeinschaften und Stammgemeinschaften können dort OID für die Verwendung nach Artikel 9 Absatz 1 (Gemeinschaft resp. Stammgemeinschaft) und Absatz 2 Buchstabe c (Gesundheitseinrichtung) beantragen und abrufen. Die OID für die Gruppen von Gesundheitsfachpersonen werden von den Gemeinschaften und Stammgemeinschaften selbst verwaltet. Der OID einer Gesundheitsfachperson ergibt sich aus der GLN (vgl. Erläuterungen zu Art. 41).

Art. 43 Gebühren

Ausgehend von der Schätzung, dass in der Schweiz in etwa 10 Gemeinschaften und Stammgemeinschaften entstehen werden, erscheint eine jährliche zu entrichtende Gebühr von 40 000 als angemessen. Dies ermöglicht eine Refinanzierung der Kosten für Aufbau und Betrieb der Abfragedienste über 10 Jahre (Abs. 1). Die Gebühr ist als Pauschalgebühr ausgestaltet, da die Abfragedienste von allen Gemeinschaften und Stammgemeinschaften gleichermassen verwendet werden. Zudem ist für die Berechnung der Kosten das von einer Gemeinschaft oder Stammgemeinschaft zu verarbeitende Datenvolumen für die Berechnung der Kosten vernachlässigbar, da der Aufbau der Abfragedienste der Hauptanteil an den Kosten ausmacht.

Absatz 2 legt fest, dass im Übrigen die allgemeine Gebührenverordnung vom 8. September 2004 (SR 172.041.1) anwendbar ist, welche insbesondere Vorgaben betreffend Rechnungsstellung, Fälligkeit und Verjährung enthält.

8. Kapitel: Inkrafttreten

Art. 44

Das EPDG und das Ausführungsrecht (EPDV, EPDV-EDI sowie EPDFV) treten am 15. April 2017 in Kraft.