Revisionsentwurf zum Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier

Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften

Änderungsnachweis seit Inkrafttreten 15. April 2017

Die Anpassungen der Anhänge zur EPDV-EDI werden durch das BAG laufend vorgenommen und die Zwischenstände durch eHealth Suisse der Öffentlichkeit zugänglich gemacht. Der Nachweis ermöglicht eine Vorschau auf eine mögliche künftige Version der normativen Vorgaben.
Bis zur Inkraftsetzung der revidierten Verordnung gilt formell die Ausgabe, welche am 15. April 2017 in Kraft getreten ist.

Version: 1.4
Datum: 29. Juni 2018

Anpassungen:

Version	Kapitel	Ticket	Vorgenommene Anpassung
1.3	1.1.1a	EPD-121	Transaktion *Delete Document Set* [ITI-62]; rausgenommen, da das gemeinschaftsübergreifende Löschen von Dokumenten über ein anderes Profil gelöst werden wird.
1.4	1.2.4a		Typo korrigiert: Personen nach Person.
1.2	1.4.3		Mandat XUA: Neue Bestimmung zur Verknüpfung der Identifikatoren als Ziff. 1.4.3 eingefügt.
1.2	1.6.3		Mandat XUA: Bestimmung bei Ziff. 1.6.3 mit Ziff. 1.4.3 ergänzt.
1.4	1.6.3	EPD-29	Für Hilfspersonen werden keine GLN vorgeschrieben. Aus diesem Grund den Verweis auf das Kapitel 1.4.3 entfernt.
1.2	1.7		Mandat XUA: Verwaltung weiterer Rollen (z.B. Administrator).
1.2	2.9.8 2.9.9	EPD-221	Mandat XUA: X-Service Provider muss nur ITI-40 beherrschen: Ziff. 2.9.8 angepasst, neue Ziff. 2.9.9 ergänzt.
1.3	2.9.6	EPD-65	Mandat ATC: Ziffer für den Abruf von Protokolldaten ergänzt gem. ATC-Profil.
~~1.4~~	~~Früher: 2.9.14~~	~~EPD-241~~	~~Bestimmung 2.9.14 bezüglich *On-Demand Document Source* (Akteur) und Register On-Demand Document Entry [ITI-61] entfernt, weil dank dem CH:ATC-Profil On-Demand documents nicht mehr benötigt werden.~~

ENTWURF

Version	Kapitel	Ticket	Vorgenommene Anpassung
1.1	2.9.14	EPD-121	Anforderung in Ziff. 2.9.13 Bst. b (ITI-62 Delete Document Set) entfällt zu Gunsten einer späteren, Gemeinschaftsübergreifenden Lösung für das Löschen von Dokumenten.
1.4	2.9.15	EPD-242	Neues Profil RMU: Neue Bestimmung aufgenommen: IHE-Akteure *Update Initiator* und *Update Responder* mit der Transaktion *Restricted Update Document Set [ITI-X1]* festgelegt.
1.4	Früher 2.9.16 d	EPD-241	Transaktion «Register On-Demand Document Entry [ITI-61];» entfernt, da On-Demand Documents nicht mehr erforderlich sind.
1.3	2.9.18	EPD-11	Profil XDM: Neben *Portable Media Creator* auch noch den *Portable Media Importer* aufgenommen.
1.4	2.9.26	EPD-247	Policy Repository muss CH:ADR-Transaktion nicht unterstützen. Aus diesem Grund das Policy Repository entfernt.
1.3	2.10.1	EPD-65	Bestimmung ergänzt wegen CH:ATC.
1.4	2.10.6	EPD-243	Bst. b. und c. entfernt, da diese mittels ATNA nicht geloggt werden können.
1.4	2.10.10	EPD-65	Bestimmung ergänzt wegen CH:ATC.
1.4	2.10.11	EPD-65	Bestimmung ergänzt wegen CH:ATC.
1.3	4.6.2d	EPD-65	Bestimmung mit Berücksichtigung von CH:ATC angepasst.
1.2	8.2.3		Mandat XUA: TOZ mit neuer Ziff. 8.2.3 ergänzt, damit das Mapping zwischen Identifikatoren gewährleistet werden kann.
1.4	9.4.1b	EPD-119	Typo: «*Daten*» durch «**medizinische** Daten» ergänzt.

ENTWURF

ENTWURF

ENTWURF

A. Anforderungen an Gemeinschaften

1 Objektidentifikator und Verwaltung (Art. 9 EPDV)

1.1 Objektidentifikator (Art. 9 Abs. 1)

Gemeinschaften müssen beim Dienst zur Abfrage der Objektindentifikatoren (OID) nach Artikel 42 EPDV für sich sowie für die ihnen angehörenden Gesundheitseinrichtungen einen OID beantragen.

1.2 Verwaltung von Gesundheitseinrichtungen (Art. 9 Abs. 2 Bst. a und d EPDV)

1.2.1 Die Gemeinschaften legen die Prozesse für den Eintritt, die Verwaltung und den Austritt von Gesundheitseinrichtungen fest.

1.2.2 Der Prozess für den Eintritt von Gesundheitseinrichtungen muss sicherstellen, dass:

a. für diese ein OID beim Dienst zur Abfrage der OID nach Artikel 42 EPDV beantragt wird;
b. Vereinbarungen mit den Gesundheitseinrichtungen betreffend deren Aufgaben und Pflichten, insbesondere im Bereich Datenschutz und Datensicherheit, abgeschlossen werden;
c. der Prozess «Eintritt von Gesundheitsfachpersonen» (vgl. Ziff. 1.3.2) für alle mit einer Gesundheitseinrichtung eintretenden Gesundheitsfachpersonen ausgelöst wird;
d. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden;
e. das «Inventar der Informatikinfrastruktur» nach Ziffer 4.6 aktualisiert wird.

1.2.3 Der Prozess für den Austritt von Gesundheitseinrichtungen muss sicherstellen, dass:

a. der Prozess «Austritt von Gesundheitsfachpersonen» (vgl. Ziff. 1.3.5) für alle Gesundheitsfachpersonen der austretenden Gesundheitseinrichtung ausgelöst wird;
b. sofern sich die austretende Gesundheitseinrichtung keiner anderen Gemeinschaft anschliesst, die Daten der austretenden Gesundheitseinrichtung über das elektronische Patientendossier zugänglich bleiben;
c. das «Inventar der Informatikinfrastruktur» nach Ziffer 4.6 aktualisiert wird.

1.2.4 Die Gemeinschaften müssen für die von ihr registrierten Daten im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV:

a. eine verantwortliche Person benennen;
b. sicherstellen, dass die Aktualität und Korrektheit der Daten regelmässig überprüft wird.

1.3 Verwaltung von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a bis f EPDV)

1.3.1 Die Gemeinschaften legen die Prozesse für den Eintritt, die Verwaltung und den Austritt von Gesundheitsfachpersonen fest.

1.3.2 Sie stellen sicher, dass die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden.

ENTWURF

1.3.3 Der Prozess für den Eintritt von Gesundheitsfachpersonen muss sicherstellen, dass:

a. die Gesundheitsfachperson zur Einhaltung der spezifischen Richtlinien der Gemeinschaft zum Umgang mit dem elektronischen Patientendossier verpflichtet wird;

b. die Identifikation der Gesundheitsfachperson anhand eines Identifikationsmittels eines zertifizierten Herausgebers erfolgt oder den Anforderungen nach Artikel 24 EPDV entspricht;

c. es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG handelt;

d. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden;

e. im Fall von Gesundheitsfachpersonen, die in einem eidgenössischen oder kantonalen Berufsregister geführt werden, die entsprechenden Angaben übernommen werden.

1.3.4 Der Prozess für die Verwaltung von Gesundheitsfachpersonen muss sicherstellen, dass:

a. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden;

b. die Voraussetzungen für den Zugriff auf das elektronische Patientendossier regelmässig überprüft werden.

1.3.5 Der Prozess für den Austritt von Gesundheitsfachpersonen muss sicherstellen, dass:

a. die Daten des Dienstes zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden;

b. der Zugriff auf das elektronische Patientendossier für die austretende Gesundheitsfachperson deaktiviert wird.

1.4 Identifizierung und Authentifizierung (Art. 9 Abs. 2 Bst. e EPDV)

1.4.1 Gesundheitsfachpersonen müssen sich für den Zugriff auf das elektronische Patientendossier mit gültigen Identifikationsmitteln authentifizieren, die von einem nach Artikel 31 EPDV zertifizierten Herausgeber herausgegeben wurden.

1.4.2 Gemeinschaften müssen sicherstellen, dass der eindeutige Identifikator nach Artikel 25 Absatz 1 EPDV mit der richtigen Gesundheitsfachperson sowie mit ihrer GLN verbunden wird.

1.4.3 Gemeinschaften müssen sicherstellen, dass die Daten und die Verknüpfung von Identifikator und GLN der Gesundheitsfachperson gemäss Artikel 26 und Artikel 27 EPDV aktualisiert werden.

1.4.4 Gemeinschaften müssen eine Authentifizierung nach Ziffer 1.4.1 einer anderen zertifizierten Gemeinschaft oder Stammgemeinschaft anerkennen.

1.5 Verwaltung von Gruppen von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a, c, d und f EPDV)

1.5.1 Gemeinschaften sind für die Verwaltung der Gruppen von Gesundheitsfachpersonen verantwortlich. Sie legen den Prozess zu deren Verwaltung fest.

1.5.2 Der Prozess muss sicherstellen, dass:

a. für Gruppen von Gesundheitsfachpersonen ein OID vergeben wird, der auf dem OID der Gesundheitseinrichtung basiert;

b. die Daten im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden;

ENTWURF

c. die Patientinnen und Patienten auf deren Verlangen über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen informiert werden.

1.6 Verwaltung von Hilfspersonen von Gesundheitsfachpersonen

1.6.1 Die Gemeinschaften legen den Prozess für die Verwaltung von Hilfspersonen fest.

1.6.2 Hilfspersonen müssen sich für den Zugriff auf das elektronische Patientendossier mit eigenen gültigen Identifikationsmitteln authentifizieren, die von einem nach Artikel 31 EPDV zertifizierten Herausgeber herausgegeben wurden.

1.6.3 Für die Verwaltung von Hilfspersonen gelten die Ziffern 1.3, 1.4.2 analog. Ausgenommen ist die Aktualisierung des Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV.

1.7 Verwaltung von weiteren Rollen

1.7.1 Die Gemeinschaften müssen einen Prozess festlegen für die Erstellung und die Verwaltung von administrativen Rollen, die für Aufbau und Betrieb des elektronischen Patientendossiers notwendig sind.

1.7.2 Personen, die in einer administrativen Rolle auf das elektronische Patientendossier zugreifen wollen, müssen sich für den Zugriff mit eigenen gültigen Identifikationsmitteln authentifizieren, die von einem nach Artikel 31 EPDV zertifizierten Herausgeber herausgegeben wurden.

1.7.3 Die Gemeinschaften stellen sicher, dass alle Prozesse, welche die Nutzung von administrativen Rollen benötigen, dokumentiert sind.

1.7.4 Die Gemeinschaften stellen sicher, dass Personen in einer administrativen Rolle:

a. sich ihrer besonderen Rechte bewusst und hinsichtlich des Datenschutzes angemessen ausgebildet sind;
b. die für ihre Aufgabe relevanten Prozesse kennen und verstehen;
c. nur die Zugriffsrechte nutzen können, welcher für die Erfüllung ihrer Aufgabe zwingend nötig sind;
d. nur im Auftrag einer autorisierten Person, den Zugriff auf die medizinischen Daten eines einzelnen Patientendossiers vornehmen;

1.7.5 Die Gemeinschaften stellen sicher, dass die Tätigkeiten von Personen in einer administrativen Rolle:

a. jederzeit protokolliert werden;
b. mit Hilfsmitteln durchgeführt werden, welche die Personen in Ihrer Tätigkeit unterstützen und Fehler vermeiden helfen;
c. nur unter Verwendung des persönlichen Identifikationsmittels zugegriffen werden können;
d. nur in begründeten Ausnahmefällen den Zugriff auf die Daten eines Patientendossiers erfordern;

ENTWURF

2 Datenhaltung und Datenübertragung (Art. 10 EPDV)

2.1 Umsetzung der Vertraulichkeitsstufen (Abs. 10 Abs. 1 Bst. a EPDV)

Gemeinschaften müssen sicherstellen, dass:

a. die Patientin oder der Patient die medizinischen Daten des elektronischen Patientendossiers den Vertraulichkeitsstufen nach den Vorgaben von Artikel 1 EPDV zuordnen kann;

b. neu eingestellten Daten die Vertraulichkeitsstufe gemäss Artikel 1 Absatz 2 EPDV oder entsprechend der Festlegung der Patientin oder des Patienten nach Artikel 4 Buchstabe a EPDV zugewiesen wird;

c. Gesundheitsfachpersonen neu eingestellten Daten die Vertraulichkeitsstufe «eingeschränkt zugänglich» zuweisen können.

2.2 Notfallzugriff (Art. 10 Abs. 1 Bst. a EPDV)

Gemeinschaften müssen bei Zugriffen in medizinischen Notfallsituationen sicherstellen, dass:

a. die zugreifende Gesundheitsfachperson den Zugriff auf eine Weise bestätigen muss, die den Missbrauch insbesondere durch eine auf dem Endgerät installierte Schadsoftware wirksam verhindert;

b. die Patientin oder der Patient innert angemessener Frist informiert wird;

c. die Information über einen Notfallzugriff, sofern sie ausserhalb des elektronischen Patientendossiers elektronisch (z. B. SMS, E-Mail) übermittelt wird, keine besonders schützenswerten Daten enthält.

2.3 Durchsetzen der Zugriffsentscheidung (Art. 10 Abs. 1 Bst. a EPDV)

2.3.1 Gemeinschaften müssen sicherstellen, dass Zugriffe auf Daten ihrer Dokumentenablagen und Dokumentenregister nur gemäss der zuvor eingeholten Zugriffsentscheidung der Stammgemeinschaft der Patientin oder des Patienten erfolgen können.

2.3.2 Die Berechtigungssteuerung muss die Möglichkeit bieten, die Korrektheit der Zugriffsentscheide im Rahmen des Zertifizierungsverfahrens mittels Zertifizierungstestsystem zu überprüfen.

2.4 Dokumentenablage (Art. 10 Abs. 1 Bst. b und Abs. 3 EPDV)

Gemeinschaften müssen sicherstellen, dass:

a. die angeschlossenen Gesundheitseinrichtungen über Regelungen verfügen, wonach nur behandlungsrelevante Daten aus der Krankengeschichte der Patientin oder des Patienten im elektronischen Patientendossier bereitgestellt werden;

b. die medizinischen Daten des elektronischen Patientendossiers in den Dokumentenablagen so getrennt von anderen Datenbeständen gespeichert werden, dass sie gegen unzulässige Verwendung geschützt sind;

c. in den Dokumentenablagen nur die gemäss Ziffer 2.8 des Anhangs 3 der EPDV-EDI zugelassenen Medientypen («*MIME MediaType*») gespeichert werden;

d. Dateien im Dateiformat «*Portable Document Format*» (PDF) nur in der Ausprägung PDF/A-1 oder PDF/A-2 gespeichert werden;

ENTWURF

e. Dateien des Medientyps «*Portable Document Format*» (PDF) keinen ausführbaren Code enthalten oder nachladen können oder anderweitig sichergestellt wird, dass sie keinen Schadcode enthalten;

f. als Kodierung von Zeichen in abrufbaren Daten Unicode UTF-8 verwendet wird.

2.5 Verschlüsselte Speicherung und Übertragung von Daten (Art. 10 Abs. 1 Bst. c EPDV)

Gemeinschaften müssen sicherstellen, dass Daten des elektronischen Patientendossiers mit geeigneten und dem aktuellen Stand der Technik entsprechenden kryptografischen Massnahmen:

a. bei jeglicher Übertragung gegen den Verlust der Vertraulichkeit, Authentizität und Integrität abgesichert werden;

b. verschlüsselt gespeichert werden und gegen unzulässige oder unbemerkte Veränderung geschützt werden.

2.6 Löschen von Daten (Art. 10 Abs. 1 Bst. d und e EPDV)

Gemeinschaften müssen Verfahren vorsehen, die sicherstellen, dass:

a. die bei ihnen von den Gesundheitsfachpersonen im elektronischen Patientendossier erfassten Daten nach 20 Jahren vernichtet werden. Vorbehalten bleibt Ziffer 2.7 Buchstabe b;

b. bei einer Aufhebung gemäss Artikel 21 EPDV sämtliche Daten des elektronischen Patientendossiers vernichtet werden. Dabei sind insbesondere die entsprechenden Daten in den Elementen der Informatikinfrastruktur, die in Ziffer 4.6.2 Buchstaben a–i des «Inventars der Informatikinfrastruktur» aufgeführt werden, zu vernichten und die Patientenidentifikationsnummer aus allen Systemen zu entfernen.

2.7 Optionen der Patientinnen und Patienten (Art. 10 Abs. 2 EPDV)

Gemeinschaften müssen technische und organisatorische Verfahren vorsehen, damit auf Verlangen der Patientin oder des Patienten bestimmte auf diese oder diesen bezogene medizinische Daten:

a. nicht im elektronischen Patientendossier erfasst werden;

b. von der Vernichtung nach Artikel 10 Absatz 1 Buchstabe d EPDV ausgenommen werden;

c. aus dem elektronischen Patientendossier vernichtet werden.

2.8 Metadaten (Art. 10 Abs. 3 Bst. a EPDV)

Gemeinschaften müssen sicherstellen, dass die Metadaten nach Anhang 3 der EPDV-EDI verwendet werden.

ENTWURF

2.9 Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers (Art. 10 Abs. 3 Bst. c EPDV)

Standardschnittstelle zur Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS)

2.9.1 Die Zugangspunkte der Gemeinschaften müssen die von der ZAS angebotenen technischen Schnittstellen zur Identifikationsdatenbank für die Ausgabe und Nutzung der Patientenidentifikationsnummer gemäss dem Bearbeitungsreglement der ZAS verwenden.

2.9.2 Neben der korrekten technischen Verwendung der Schnittstellen sind auch die organisatorischen Vorgaben des Bearbeitungsreglements der ZAS einzuhalten.

IHE-Integrationsprofile, nationale Anpassungen der IHE-Integrationsprofile und nationale Integrationsprofile

2.9.3 Die Gemeinschaften müssen für die Informationsübertragung die IHE-Integrationsprofile, deren nationale Anpassungen und nationalen Integrationsprofile nach Anhang 5 der EPDV-EDI verwenden.

Gemeinschaftsübergreifende Kommunikation

2.9.4 Die IHE-Akteure *Initiating Gateway* und *Responding Gateway* müssen folgende Transaktionen der Integrationsprofils IHE XCA und IHE XCPD in den Versionen nach Anhang 5 der EPDV-EDI unterstützen:

a. Cross Gateway Query [ITI-38];
b. Cross Gateway Retrieve [ITI-39];
c. Cross Gateway Patient Discovery [ITI-55].

2.9.5 Die IHE-Akteure *Initiating Imaging Gateway* und *Responding Imaging Gateway* müssen die Transaktion *Cross Gateway Retrieve Image Document Set* [RAD-75] des Integrationsprofils IHE XCA-I in der Version nach Anhang 5 der EPDV-EDI unterstützen.

Abruf von Protokolldaten

2.9.6 Für den Abruf von Protokolldaten für die Anzeige im Patientenportal ist die Transaktion *Retrieve Audit Event* [ITI-81] gepaart mit *Incorporate Authorization Token* [ITI-72] gemäss nationalem Integrationsprofil Audit Trail Consumption (CH:ATC) nach Anhang 5 der EPDV-EDI zu verwenden. Diese Vorgaben gelten sowohl für die gemeinschaftsinterne wie auch für die gemeinschaftsübergreifende Abfrage von Protokolldaten.

Kommunikation beglaubigter Identitäten

2.9.7 Die IHE-Akteure *X-Service Provider* und *X-Service User* des IHE-Integrationsprofils IHE XUA werden mit anderen IHE-Akteuren gruppiert nach den Vorgaben der nationalen Integrationsprofile und nach den Anpassungen der Integrationsprofile nach Anhang 5 der EPDV-EDI.

2.9.8 Der IHE-Akteur *X-Service User* muss folgende Transaktionen des Integrationsprofils IHE XUA in der Version nach Anhang 5 der EPDV-EDI unterstützen:

a. Authenticate User;
b. Get X-User Assertion;
c. Provide X-User Assertion [ITI-40].

ENTWURF

2.9.9 Der IHE-Akteur *X-Service Provider* muss die Transaktion *Provide X-User Assertion [ITI-40]* des Integrationsprofils IHE XUA in der Version nach Anhang 5 der EPDV-EDI unterstützen.

Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen

2.9.10 Die IHE-Akteure *Provider Information Consumer* und *Provider Information Source* müssen folgende Transaktionen des Integrationsprofils IHE HPD in der Version nach Anhang 5 der EPDV-EDI unterstützen:

a. Provider Information Query [ITI-58];
b. Provider Information Feed [ITI-59];
c. Provider Information Delta Download (CH:PIDD).

Medizinische Daten abrufen

2.9.11 Der IHE-Akteur *Document Consumer* muss folgende Transaktionen des Integrationsprofils IHE XDS.b in der Version nach Anhang 5 der EPDV-EDI unterstützen:

a. Registry Stored Query [ITI-18];
b. Retrieve Document Set [ITI-43].

2.9.12 Der IHE-Akteur *Image Document Consumer* muss folgende Transaktionen des Integrationsprofils IHE XDS.b in der Version nach Anhang 5 der EPDV-EDI unterstützen:

a. WADO Retrieve [RAD-55];
b. Retrieve Imaging Document Set [RAD-69].

Medizinische Daten bereitstellen

2.9.13 Der IHE-Akteur *Document Source* muss die Transaktion *Provide and Register Document Set-b* [ITI-41] des Integrationsprofils IHE XDS.b in der Version nach Anhang 5 der EPDV-EDI unterstützen.

Metadaten medizinischer Daten mutieren

2.9.14 Der IHE-Akteur *Document Administrator* muss folgende Transaktionen des Integrationsprofils IHE XDS Metadata Update in der Version nach Anhang 5 der EPDV-EDI unterstützen:

a. Update Document Set [ITI-57].

2.9.15 Die IHE-Akteure *Update Initiator* und *Update Responder* müssen folgende Transaktion des Integrationsprofils IHE Restricted Metadata Update (RMU) nach Anhang 5 der EPDV-EDI unterstützen:

a. Restricted Update Document Set [ITI-X1]

Dokumentenregister

2.9.16 Der IHE-Akteur *Document Registry* muss folgende Transaktionen der Integrationsprofile XDS.b und XDS Metadata Update in den Versionen nach Anhang 5 der EPDV-EDI unterstützen:

a. Register Document Set-b [ITI-42];
b. Registry Stored Query [ITI-18];
c. Update Document Set [ITI-57];
d. Patient Identity Feed HL7 V3 [ITI-44].

ENTWURF

Dokumentenablage

2.9.17 Der IHE-Akteur *Document Repository* muss folgende Transaktionen des Integrationsprofils IHE XDS.b in der Version nach Anhang 5 der EPDV-EDI unterstützen:

a. Provide and Register Document Set-b [ITI-41];
b. Retrieve Document Set [ITI-43].

2.9.18 Die IHE-Akteure *Portable Media Creator* und *Portable Media Importer* müssen die Transaktion *Distribute Document Set on Media* [ITI-32] des Integrationsprofils XDM in der Version nach Anhang 5 der EPDV-EDI unterstützen.

Daten für den Patientenindex bereitstellen

2.9.19 Der IHE-Akteur *Patient Identity Source* muss die Transaktion *Patient Identity Feed HL7 V3* [ITI-44] des Integrationsprofils PIX V3 in der Version nach Anhang 5 der EPDV-EDI unterstützen.

Patientenindex bereitstellen und abfragen

2.9.20 Die IHE-Akteure Patient *Demographics Supplier* und *Patient Demographics Consumer* müssen die Transaktion *Patient Demographics Query V3* [ITI-47] des Integrationsprofils PDQ V3 in der Version nach Anhang 5 der EPDV-EDI unterstützen.

Patientenindex verwalten

2.9.21 Der IHE-Akteur *Patient Identifier Cross-reference Manager* muss die folgenden Transaktionen des Integrationsprofils IHE PIX V3 in den Versionen nach Anhang 5 der EPDV-EDI unterstützen:

a. Patient Identity Feed HL7 V3 [ITI-44];
b. PIX V3 Query [ITI-45];
c. PIX V3 Update Notification [ITI-46].

Authentisierung von Systemen und Protokollierung von IHE-Transaktionen

2.9.22 Die IHE-Akteure *Secure Application* und *Secure Node* des Integrationsprofils IHE ATNA (resp. deren nationale Anpassungen) werden mit anderen IHE-Akteuren gruppiert nach den Vorgaben der IHE-Integrationsprofile, der nationalen Integrationsprofile und den Anpassungen der Integrationsprofile nach Anhang 5 der EPDV-EDI.

2.9.23 Alle IHE-Akteure in der Rolle *Secure Node* gemäss Ziffer 2.9.22 müssen die folgenden Transaktionen des Integrationsprofils IHE ATNA und seiner nationalen Anpassung gemäss Anhang 5 der EPDV-EDI unterstützen:

a. Maintain Time [ITI-1];
b. Authenticate Node [ITI-19];
c. Record Audit Event [ITI-20].

2.9.24 Die IHE-Akteure in der Rolle *Secure Application* müssen die folgenden Transaktionen des Integrationsprofils IHE ATNA und seiner nationalen Anpassung nach Anhang 5 der EPDV-EDI unterstützen:

a. Maintain Time [ITI-1];
b. Record Audit Event [ITI-20].

ENTWURF

Autorisierungsentscheid abfragen

2.9.25 Der IHE-Akteur *Authorization Decision Consumer* des nationalen Integrationsprofils CH:ADR wird mit anderen IHE-Akteuren nach den Vorgaben des nationalen Integrationsprofils CH:ADR nach Anhang 5 der EPDV-EDI gruppiert.

2.9.26 Die IHE-Akteure *Authorization Decision Provider* and *Authorization Decision Consumer* und müssen die Transaktion *Authorization Decision Request* [CH:ADR] des nationalen Integrationsprofils CH:ADR nach Anhang 5 der EPDV-EDI unterstützen.

Berechtigungskonfiguration verwalten

2.9.27 Die IHE-Akteure *Policy Repository* und *Policy Manager* müssen die Transaktion *Privacy Policy Query* [CH:PPQ] des nationalen Integrationsprofils CH:PPQ nach Anhang 5 der EPDV-EDI unterstützen.

Authentisierung mit gültigen Zertifikaten

2.9.28 Gemeinschaften müssen über ein gültiges elektronisches Zertifikat verfügen, das bei einer nach dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES; SR 943.03) anerkannten Anbieterin von Zertifikatsdiensten bezogen wurde, für:

a. die gegenseitige Authentisierung ihrer Zugangspunkte;
b. die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber den Abfragediensten nach Artikel 39 Buchstaben a bis c EPDV;
c. die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber der Identifikationsdatenbank der ZAS.

Datenaustausch mit den Abfragediensten nach Artikel 39

2.9.29 Gemeinschaften müssen für den Datenaustausch mit den Abfragediensten nach Artikel 39 Buchstaben a und c EPDV die folgenden Transaktionen des Integrationsprofils IHE SVS nach Anhang 5 der EPDV-EDI verwenden:

a. Retrieve Value Set [ITI-48];
b. Retrieve Multiple Value Sets [ITI-60].

2.9.30 Gemeinschaften müssen für den Datenaustausch mit den Abfragediensten nach Artikel 39 Buchstaben a bis c EPDV die folgenden Transaktionen des Integrationsprofils IHE ATNA nach Anhang 5 der EPDV-EDI verwenden:

a. Maintain Time [ITI-1];
b. Authenticate Node [ITI-19];
c. Record Audit Event [ITI-20].

2.9.31 Gemeinschaften müssen für den Datenaustausch mit der Identifikationsdatenbank der ZAS die Datenaustauschplattform SEDEX («*secure data exchange*») des Bundesamtes für Statistik verwenden.

Massgebende Zeit

2.9.32 Für Zeitstempel in der Kommunikation und Protokollierung ist die gesetzliche Zeit der Schweiz der METAS zu verwenden (vgl. Ziff. 2.9.23 und 2.9.24).

ENTWURF

2.10 Protokolldaten (Art. 10 Abs. 3 Bst. d EPDV)

2.10.1 Die Bestimmungen von Ziffer 2.10.2 bis 2.10.9 gelten insbesondere aber nicht ausschliesslich für den Einsatz der nationalen Anpassung zum IHE-Profil ATNA nach Anhang 5 der EPDV-EDI.

2.10.2 Jede Bearbeitung von Daten des elektronischen Patientendossiers ist zu protokollieren und mit einem aktuellen Zeitstempel zu versehen.

2.10.3 Die Bearbeitung folgender Daten ist sowohl für erfolgreiche als auch für abgewiesene Versuche zu protokollieren:

a. der medizinischen Daten in den Dokumentenablagen;
b. der Einträge im Dokumentenregister;
c. der Konfiguration der Berechtigungssteuerung;
d. der Daten des Patientenindex.

2.10.4 Zudem sind folgende Ereignisse zu protokollieren:

a. Authentifizierungen am System (Login/Logout);
b. gemeinschaftsübergreifende Transaktionen über die Zugangspunkte der Gemeinschaften;
c. die Suche nach einer Patientin oder einem Patienten;
d. die Suche nach medizinischen Daten eines elektronischen Patientendossiers;
e. ein Notfallzugriff auf ein elektronisches Patientendossier;
f. Zugriffe und Zugriffsversuche auf medizinische Daten eines elektronischen Patientendossiers.

2.10.5 Mindestens zu protokollieren ist in jedem Fall:

a. das Ereignis selbst («*Event Identification*») und der Kontext, in dem es eingetreten ist (Normalbetrieb, Notfallzugriff, Verwendung von privilegierten Sonderzugriffsrechten);
b. der Zeitpunkt des Ereignisses («*Event Timestamp*»);
c. die Person, die das Ereignis ausgelöst hat («*Active Participant Identification*»);
d. der Ort, an dem das Ereignis ausgelöst wurde («*Network Access Point Identification*»);
e. die Ursache des Ereignisses («*Audit Source Identification*»);
f. die betroffenen Datensätze («*Participant Object Identification*»);
g. das Resultat des Ereignisses («*Event Outcome Indicator*»).

2.10.6 Bei einer Suche muss mindestens protokolliert werden:

a. die Suchkriterien;

2.10.7 Die Protokolldaten sind auf das erforderliche Mass zu beschränken und dürfen keine medizinischen Daten enthalten.

2.10.8 Die Protokollierung muss folgende Anforderungen erfüllen:

a. Zusätzlich zu den Identifikatoren muss auch ein menschenlesbarer Text protokolliert werden, der die referenzierte Entität zum Zeitpunkt der Protokollierung namentlich bezeichnet.
b. Vorgeschriebene Protokollierungen dürfen nicht umgangen werden können.
c. Eine nachträgliche Veränderung von Protokolldaten muss erkennbar und nachvollziehbar sein.

ENTWURF

d. Bei der Protokollierung muss unterschieden werden zwischen Zugriffen, die aus der Nutzung des elektronischen Patientendossiers resultieren, und technisch-administrativen Zugriffen im Rahmen des Systembetriebs.

e. Für Systemadministratoren darf keine Möglichkeit bestehen, die Protokollierung ihrer eigenen Aktivitäten zu löschen oder zu deaktivieren.

2.10.9 Die Protokolldaten nach den Ziffern 2.10.1 bis 2.10.4 sind 10 Jahre aufzubewahren und dann zu vernichten.

2.10.10 Der Abruf und die Darstellung von Protokollinformationen für die Einsichtnahme durch die Patientin oder den Patienten richten sich nach dem nationalen Integrationsprofil CH:ATC gemäss Anhang 5 der EPDV-EDI.

2.10.11 Für die Erfüllung der Anforderungen des nationalen Integrationsprofils CH:ATC und den Bestimmungen zu Forschung und Evaluation müssen neben ATNA weitere Informationen geloggt werden.

2.11 Verknüpfung der Patientenidentifikationsnummer mit medizinischen Daten (Art. 10 Abs. 3 EPDV)

Gemeinschaften müssen sicherstellen, dass die Patientenidentifikationsnummer der ZAS nicht in den Dokumentenablagen oder Dokumentenregistern gespeichert wird.

3 Zugangsportal für Gesundheitsfachpersonen (Art. 11 EPDV)

3.1 Darstellung

Die Darstellung auf den Benutzeroberflächen des Zugangsportals muss korrekt und vollständig sein und klar erkennen lassen:

a. ob medizinische Daten durch eine Gesundheitsfachperson oder durch die Patientin oder den Patienten selbst bereitgestellt wurden;

b. welche medizinischen Daten von der zugreifenden Gesundheitsfachperson selbst bereitgestellt wurden;

c. welche medizinischen Daten annulliert wurden;

d. welche Versionen eines Dokumentes vorhanden sind.

3.2 Barrierefreiheit

Das Zugangsportal muss den Konformitätsbedingungen gemäss Web Content Accessibility Guidelines (WCAG) 2.0 entsprechen und mindestens die Konformitätsstufe AA erreichen.

3.3 Abruf und Medientypen von medizinischen Daten

Das Zugangsportal muss:

a. die Medientypen nach Ziffer 2.8 des Anhangs 3 der EPDV-EDI unterstützen;

b. den Import von medizinischen Daten sowie den Abruf von medizinischen Daten zum Abspeichern im Primärsystem der Gesundheitseinrichtung unterstützen;

ENTWURF

c. die Möglichkeit bieten, medizinische Daten einzeln oder gesammelt zu importieren oder herunterzuladen;

d. strukturierte Daten menschenlesbar, korrekt und vollständig darstellen;

e. das Herunterladen von strukturierten Daten sowohl im Originalformat wie auch als menschenlesbares Format unterstützen;

f. für den Abruf von medizinischen Daten zur Darstellung oder zum Abspeichern zulässige Obergrenzen für die erlaubte Anzahl von medizinischen Daten pro Zeiteinheit vorsehen, bei deren Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen ausgelöst werden.

4 Datenschutz und Datensicherheit (Art. 12 EPDV)

4.1 Anforderungen an Dritte

Die Sicherstellung der Anforderungen dieser Ziffer liegt auch dann in der Verantwortung der Gemeinschaften, wenn sie Leistungen durch Dritte (Betriebsorganisationen) erbringen lassen.

4.2 Datenschutz- und Datensicherheitsmanagementsystem (Art. 12 Abs. 1 EPDV)

4.2.1 Gemeinschaften müssen ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem betreiben, das:

a. geeignete Massnahmen, insbesondere Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen zur Erfüllung der Anforderungen definiert, die den hier aufgestellten Bestimmungen entsprechen;

b. die allgemeinen und spezifischen Verantwortlichkeiten für das Management von Datenschutz und Datensicherheit auf definierte Funktionen festlegt und den dafür verantwortlichen Personen zuordnet;

c. alle relevanten Aufzeichnungen im Einklang mit den gesetzlichen Anforderungen vor Verlust, Zerstörung und Fälschung schützt.

4.2.2 Das Datenschutz- und Datensicherheitsmanagementsystem muss innerhalb der Gemeinschaft allen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen bekannt gemacht werden.

4.2.3 Das Datenschutz- und Datensicherheitsmanagementsystem muss mindestens umfassen:

a. einen von der oder dem Datenschutz- und Datensicherheitsverantwortlichen (vgl. Ziff. 4.11) beurteilten Risikokatalog;

b. einen Risikobehandlungsplan;

c. ein aktuelles Inventar der für die Risikobeurteilung und Risikobehandlung relevanten Betriebsmittel der Gemeinschaft. Dazu gehören insbesondere:

i. die Daten des elektronischen Patientendossiers sowie die Prozesse zu deren Bearbeitung (primäre Schutzobjekte);

ii. die Systeme, Infrastrukturen, Anwendungen, Einrichtungen, organisatorischen Strukturen, Personen und Prozesse, von denen der Schutz der primären Schutzobjekte abhängt.

4.2.4 Sicherheitsrelevante Veränderungen an den Betriebsmitteln sind zu beurteilen und zu dokumentieren.

ENTWURF

4.2.5 Gemeinschaften müssen den Risikokatalog und den Risikobehandlungsplan aktuell halten und mindestens jährlich überprüfen.

4.3 Erkennen von und Umgang mit Sicherheitsvorfällen (Art. 12 Abs. 1 Bst. a EPDV)

4.3.1 Gemeinschaften müssen technische und organisatorische Verfahren zur Erkennung von und zum Umgang mit Sicherheitsvorfällen einrichten, betreiben und laufend verbessern, die:

a. mindestens die im «Inventar der Informatikinfrastruktur» nach Ziffer 4.6 als risikorelevant erfassten Elemente der Informatikinfrastruktur risikogerecht überwachen;

b. Anomalien im System erkennen;

c. Datenschutz- und Datensicherheitsereignisse so aufzeichnen, dass sie gegen unzulässige oder unbemerkte Veränderungen geschützt sind.

4.3.2 Die Verfahren zur Erkennung von Sicherheitsvorfällen sowie zur Analyse und Berichterstattung darüber müssen risikogerecht und gemeinschaftsspezifisch definiert sein und mindestens die folgenden Muster erkennen und adressieren:

a. Angriffe aus dem Internet auf Zugangsportale oder auf den Zugangspunkt der Gemeinschaft;

b. unübliche Muster schreibender oder lesender Zugriffe auf die Dokumentenablagen, das Dokumentenregister oder den Patientenindex, die auf eine missbräuchliche Nutzung oder automatisierte Attacke hinweisen;

c. ungewöhnliche und kritische Mutationen von Berechtigungsdaten in der Berechtigungssteuerung, dem Identitäts- und Zugangsmanagement-System (IAM) oder, sofern vorhanden, dem gemeinschaftsinternen Dienst zur Verwaltung von Gesundheitseinrichtungen und Gesundheitsfachpersonen.

4.3.3 Gemeinschaften müssen zu den unter Ziffer 4.3.1 beschriebenen Massnahmen:

a. Verfahren vorsehen für das unverzügliche Melden von Datenschutz- und Datensicherheitsereignissen an die vorgegebenen Stellen der Gemeinschaft und an das BAG (Art. 12 Abs. 3 EPDV);

b. Prozesse vorsehen zur raschen Reaktion auf Ereignisse und zur Behandlung von Ursachen, die den Datenschutz oder die Datensicherheit gefährden;

c. für sicherheitskritische Ereignisse einer definierten Stufe geeignete Notfallprozesse zur Eindämmung von Schadwirkungen vorsehen, insbesondere wie und unter welchen Bedingungen sicherheitskritische Systeme der Gemeinschaft von gefährdenden Zugriffen von aussen oder innen zu isolieren sind.

4.4 Umgang mit Sicherheitsschwachstellen (Art. 12 Abs. 1 Bst. a EPDV)

4.4.1 Gemeinschaften müssen über ein Sicherheitsschwachstellenmanagement verfügen, das Informationen über technische Sicherheitsschwachstellen der verwendeten Informatikmittel rechtzeitig einholt, die Anfälligkeit der Gemeinschaft für eine Ausnutzung solcher Sicherheitsschwachstellen bewertet und angemessene Massnahmen für den Umgang mit den damit einhergehenden Risiken ergreift.

4.4.2 Steht für die Beseitigung einer Sicherheitsschwachstelle noch keine Softwarekorrektur («*Patch*») zur Verfügung, so müssen alternative Sicherheitsmassnahmen in Betracht gezogen und nach Möglichkeit umgesetzt werden.

4.5 Schutz vor Schadsoftware (Art. 12 Abs. 1 Bst. a EPDV)

Gemeinschaften müssen:

ENTWURF

a. Massnahmen zum Schutz insbesondere der schützenswerten Elemente der Informatikinfrastruktur der Ziffern 4.6.2 Buchstaben a–i und k vor Schadsoftware treffen, die es insbesondere erlauben solche Software zu erkennen und zu entfernen;

b. die Aktualität der eingesetzten Software zur Erkennung und Entfernung von Schadsoftware regelmässig überprüfen.

4.6 Verwaltung schützenswerter Informatikmittel und Datensammlungen («Inventar der Informatikinfrastruktur») (Art. 12 Abs. 1 Bst. b EPDV)

4.6.1 Gemeinschaften müssen sicherstellen, dass alle schützenswerten Daten, Systeme und Einrichtungen des elektronischen Patientendossiers eindeutig identifiziert, klassifiziert und in einem «Inventar der Informatikinfrastruktur» erfasst und aktuell gehalten werden.

4.6.2 Im «Inventar der Informatikinfrastruktur» müssen mindestens folgende Elemente der Informatikinfrastruktur für das elektronische Patientendossier der Gemeinschaft erfasst und verwaltet werden:

a. die Zugangspunkte (IHE-Akteure *Initiating Gateway*, *Responding Gateway*);

b. die Dokumentenablagen (IHE-Akteur *Document Repository*);

c. das Dokumentenregister (IHE-Akteur *Document Register*);

d. die Systeme und Datenspeicher für die Protokolldaten (IHE-Akteure Audit *Record Repository* für ATNA sowie den Akteur *Patient Audit Record Repository* gemäss dem nationalen Integrationsprofil CH:ATC nach Anhang 5 der EPDV-EDI);

e. die Systeme zur Berechtigungssteuerung (IHE-Akteure *Policy Repository, Authorization Decision Provider*);

f. sofern vorhanden, die Systeme des gemeinschaftsinternen Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen (IHE-Akteure *Provider Information Directory*, *Provider Information Source*, *Provider Information Consumer*);

g. das Identitäts- und Zugangsmanagement-System (IAM);

h. der Patientenindex (IHE-Akteure *Patient Demographics Supplier*, *Patient Identifier Cross-reference Manager*, *Patient Identity Source*);

i. die Zugangsportale für Gesundheitsfachpersonen oder Patientinnen und Patienten;

j. die angeschlossenen Primärsysteme, sofern sie mindestens eine der folgenden IHE-Akteure oder analoge Funktionalitäten realisieren: *Document Source, Document Consumer, Policy Manager, Provider Information Source, Provider Information Consumer, Patient Demographics Consumer, Patient Identifier Cross-reference Consumer, Patient Identity Source, X-Service User, Document Audit Consumer*;

k. die Systeme, Anwendungen und Datenbestände des Systembetriebs, darunter solche für Protokolldaten, Backups und das Zugangsmanagement für Systemadministratoren.

4.6.3 Das «Inventar der Informatikinfrastruktur» umfasst für die Primärsysteme nach Ziffer 4.6.2 Buchstabe j zusätzlich mindestens das Clientzertifikat für die Transportschichtsicherheit (TLS-Clientzertifikat) des jeweiligen IHE-Akteurs oder des jeweiligen Elements der Informatikinfrastruktur.

4.6.4 Jedem Element im Inventar muss ein verantwortlicher Eigentümer oder eine verantwortliche Eigentümerin zugeordnet werden.

4.6.5 Der oder die Datenschutz- und Datensicherheitsverantwortliche muss das «Inventar der Informatikinfrastruktur» mindestens jährlich überprüfen.

ENTWURF

4.7 Datenschutz- und Datensicherheitsanforderungen an die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen sowie an deren Endgeräte (Art. 12 Abs. 1 Bst. c EPDV)

4.7.1 Gemeinschaften müssen die Gesundheitseinrichtungen:

a. auf die einzuhaltenden Sicherheitsmassnahmen (vgl. Ziff.1.3.3 Buchstabe a) hinweisen;

b. dazu verpflichten, ihre auf das elektronische Patientendossier zugreifenden Gesundheitsfachpersonen über die Rechte und Pflichten im Zusammenhang mit der Bearbeitung von Daten des elektronischen Patientendossiers zu informieren und zur Einhaltung der vorgeschriebenen Massnahmen zu verpflichten;

c. dazu verpflichten, eine sichere Konfiguration der Endgeräte sicherzustellen, die von den Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier genutzt werden.

4.7.2 Die Vorgaben zur Konfiguration der Endgeräte müssen mindestens umfassen:

a. den Einsatz einer regelmässig aktualisierten Software gegen Schadprogramme;

b. den Einsatz netzwerktechnischer Schutzsysteme;

c. eine regelmässige Aktualisierung des Betriebssystems und der sicherheitskritischen Software-Komponenten;

d. eine restriktive Handhabung von Systemadministratorrechten.

4.7.3 Gemeinschaften müssen sicherstellen, dass Endgeräte mit nicht als sicher eingestuften Konfigurationen keine Daten des elektronischen Patientendossiers bearbeiten.

4.8 Datenschutz- und Datensicherheitsanforderungen an das technische oder administrative Personal (Art. 12 Abs. 1 Bst. c EPDV)

4.8.1 Für den Zugang und die Bearbeitung der Daten des elektronischen Patientendossiers durch das technische und administrative Personal der Gemeinschaften, müssen diese Vorgaben erlassen und die zu deren Einhaltung notwendigen technischen und organisatorischen Vorkehrungen treffen.

4.8.2 Gemeinschaften müssen sicherstellen, dass:

a. Personen, die mit Daten oder Systemen des elektronischen Patientendossiers umgehen, für die vorgesehenen Aufgaben kompetent genug sind und ihre Verantwortlichkeiten wahrnehmen können sowie dem Datenschutz und der Datensicherheit sorgfältig nachkommen;

b. die Verwendung von geheimen Authentifizierungsdaten über einen formellen Verwaltungsprozess kontrolliert wird und Anforderungen an den sicheren Gebrauch (z. B. Vertraulichkeit, Passwortlänge, Gültigkeit) gefordert werden und bekannt sind;

c. Personen, die Zugang zu Daten des elektronischen Patientendossiers erlangen könnten, entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet werden;

d. auf die Anforderungen an Datenschutz und Datensicherheit ausgerichtete Prozesse für das Personalmanagement definiert, umgesetzt und eingehalten werden;

e. ein offizielles Verfahren vorsehen, um disziplinarische Massnahmen oder Sanktionen gegen Mitarbeitende einzuleiten, die gegen den Datenschutz und die Datensicherheit verstossen haben.

4.8.3 Gemeinschaften müssen:

a. eine von dem oder der Datenschutz- und Datensicherheitsverantwortlichen der Gemeinschaft visierte Liste aller Systemadministratoren führen, die auf Daten des elektronischen Patientendossiers zugreifen können;

ENTWURF

b. sicherstellen, dass diese Personen sorgfältig ausgewählt werden, einen einwandfreien Leumund haben und zur Einhaltung von klar definierten Sicherheitsanforderungen verpflichtet werden;

c. die Erfüllung dieser Sicherheitsanforderungen regelmässig überprüfen.

4.9 Datenschutz- und Datensicherheitsanforderungen an Dritte (Art. 12 Abs. 1 Bst. c EPDV)

4.9.1 Gemeinschaften müssen eine von dem oder der Datenschutz- und Datensicherheitsverantwortlichen visierte Liste mit allen Lieferanten und Dienstleistungserbringern («Dritte») führen, die unter Umständen auf Daten des elektronischen Patientendossiers zugreifen, sie verarbeiten, speichern, weitergeben oder Informatikinfrastrukturkomponenten dafür bereitstellen.

4.9.2 Mit Dritten müssen alle relevanten Datenschutz- und Datensicherheitsanforderungen formal festgelegt und in Liefervereinbarungen vereinbart werden.

4.9.3 Die Liefervereinbarungen müssen unmissverständlich die Verpflichtungen und Verantwortlichkeiten zur Erfüllung der relevanten Anforderungen an den Datenschutz und die Datensicherheit festhalten.

4.9.4 Sie müssen mindestens folgende Bestimmungen umfassen:

a. Verpflichtungen des Lieferanten, die relevanten Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft beim Einsatz oder der Bereitstellung von Informatikmitteln, Personal oder Dienstleistungen jederzeit einzuhalten;

b. Anforderungen und Verfahren für den Umgang mit Datenschutz- und Datensicherheitsvorfällen;

c. die Angabe von Kontaktpersonen für Fragen und bei Vorkommnissen im Bereich Datenschutz- und Datensicherheit;

d. das Recht zur regelmässigen Überprüfung der Lieferantenprozesse und Kontrollmassnahmen im Zusammenhang mit dem Vertrag;

e. die Verpflichtung zur Einhaltung der Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft innerhalb der gesamten Lieferkette weiter zu verpflichten für den Fall, dass die Lieferanten Unterlieferanten beauftragen;

f. die Vorschriften und Kontrollmassnahmen für Unterverträge;

g. die Verpflichtung, die Gemeinschaft über jede Änderung in den Vertragsbeziehungen zu involvierten Unterlieferanten zu informieren.

4.10 Überwachung und Überprüfung von Dienstleistungen (Art. 12 Abs. 1 Bst. c EPDV)

Die von Dritten und allfälligen Unterlieferanten gelieferten Dienstleistungen, Berichte und Aufzeichnungen müssen von den Gemeinschaften regelmässig überwacht und überprüft werden, sodass sichergestellt ist, dass:

a. die vertraglich festgelegten Bedingungen für den Datenschutz- und die Datensicherheit eingehalten werden;

b. Datenschutz- und Datensicherheitsvorfälle und -probleme angemessen bearbeitet werden;

c. Änderungen der Dienstleistungen einem gelenkten Änderungsmanagement unterliegen.

ENTWURF

4.11 Datenschutz- und Datensicherheitsverantwortlicher (Art. 12 Abs. 2 EPDV)

4.11.1 Für das Führen des Datenschutz- und Datensicherheitsmanagementsystems der Gemeinschaft ist eine Datenschutz- und Datensicherheitsverantwortliche oder ein Datenschutz- und Datensicherheitsverantwortlicher zu benennen und dessen Aufgabenprofil zu definieren.

4.11.2 Der oder die Datenschutz- und Datensicherheitsverantwortliche muss:

a. die Einhaltung der Datenschutz- und Datensicherheitsvorschriften überwachen;
b. seine oder ihre Funktion fachlich unabhängig ausüben können;
c. über die zur Erfüllung seiner oder ihrer Aufgaben erforderlichen fachlichen Kompetenzen und Ressourcen verfügen.

4.12 Verwaltung kryptografischer Schlüssel (Art. 12 Abs. 4 EPDV)

Gemeinschaften müssen sicherstellen, dass:

a. sichere Verfahren nach dem Stand der Technik für die Erzeugung, die Verteilung, die Aktivierung, die Aktualisierung, den Widerruf oder die Deaktivierung und die Löschung von kryptografischen Schlüsseln eingesetzt werden;
b. die verwendeten kryptografischen Schlüssel gegen Veränderung und Verlust geschützt werden;
c. geheime und private Schlüssel vor unbefugter Benutzung und Offenlegung geschützt werden;
d. Einrichtungen zur Erzeugung, Speicherung und Archivierung von Schlüsseln angemessen geschützt werden.

4.13 Betriebssicherheit (Art. 12 Abs. 4 EPDV)

4.13.1 Gemeinschaften müssen sicherstellen, dass:

a. Zugriffe mit Sonderrechten auf die produktive Betriebsumgebung (z. B. durch Betriebssystem-, Datenbank- und Applikations-Administratorinnen und Administratoren) eine starke 2-Faktor Authentisierung erfordern, überwacht und protokolliert werden und keinen widerrechtlichen Export, insbesondere von Patientendaten, ermöglichen;
b. externe Zugriffe von ausserhalb des lokalen Netzes (Remote-Zugriffe) durch Dritte und Unterlieferanten und insbesondere privilegierte externe Zugriffe mit Sonderrechten auf die produktive Betriebsumgebung zusätzlich entweder unterbunden oder angemessen geschützt sind, überwacht und protokolliert sowie nur befristet und bei Bedarf aktiviert werden;
c. Entwicklungs-, Test- und Inbetriebnahme-Aktivitäten neuer Systeme in ihren Umgebungen nachvollziehbar dokumentiert werden und nach einem kontrollierten Prozess ablaufen;
d. vollständige Backups gemacht werden und die enthaltenen Daten verschlüsselt sind;
e. Backups so gespeichert werden, dass sie gegen unzulässige oder unbemerkte Veränderungen geschützt sind;
f. die Verfahren zur Systemwiederherstellung ausreichend dokumentiert sind und regelmässig erprobt werden;
g. die technischen Logs nur für dazu autorisierte Personen zugänglich sind;
h. Logfiles mit einem Zeitstempel versehen werden und so gespeichert werden, dass sie gegen unzulässige oder unbemerkte Veränderungen geschützt sind;
i. Datenträger mit Patientendaten stets korrekt entsorgt oder vernichtet werden, sodass alle darauf befindlichen Daten unlesbar werden und nicht wiederhergestellt werden können;

ENTWURF

j. die Systemuhren mit der gesetzlichen Zeit der Schweiz abgeglichen sind.

4.13.2 Gemeinschaften müssen sicherstellen, dass die Produktivumgebung der gemeinschaftsinternen Informatikinfrastruktur des elektronischen Patientendossiers:

a. von anderen Umgebungen (z. B. Entwicklungs-, Abnahme- und Testumgebungen) isoliert ist;
b. ausschliesslich im Rahmen kontrolliert ablaufender Prozesse mit neuer Software versorgt wird;
c. regelmässig und aktiv durch sogenannte Penetrationstests auf Sicherheitsschwachstellen überprüft wird;
d. im Rahmen eines kontrollierten Patch-Management-Prozesses von erkannten Sicherheitsschwachstellen befreit wird.

4.13.3 Neben Ereignissen aufgrund der Bearbeitung von Daten des elektronischen Patientendossiers durch Gesundheitsfachpersonen sowie Patientinnen und Patienten nach Ziffer 2.10 sind mindestens folgende Ereignisse, die im Rahmen des Systembetriebs auftreten, aufzuzeichnen:

a. Login und Logout;
b. erfolgreiche und abgewiesene Versuche, auf das System zuzugreifen;
c. erfolgreiche und abgewiesene Versuche, auf Daten zuzugreifen;
d. Veränderungen an der Systemkonfiguration;
e. die Verwendung privilegierter Sonderzugriffsrechte;
f. Netzwerkadressen und -protokolle;
g. die Aktivierung und Deaktivierung von Schutz- oder Authentisierungs-Systemen;
h. die Modifikation von Systemberechtigungen und Zugängen;
i. das Anlegen, die Modifikation oder das Löschen von Benutzerkonten;
j. das Kopieren als schützenswert eingestufter Daten.

4.14 Anschaffung, Entwicklung und Instandhaltung von Systemen (Art. 12 Abs. 4 EPDV)

4.14.1 Gemeinschaften müssen den Datenschutz und die Datensicherheit über den gesamten Lebenszyklus der Systeme des elektronischen Patientendossiers sicherstellen. Dazu müssen sie Prozesse festlegen für die Dokumentation, die Spezifikation, das Testen, die Qualitätskontrolle und die kontrollierte Umsetzung bei:

a. der Einführung oder der Entwicklung neuer Systeme;
b. grösseren Änderungen oder Entwicklungen an bestehenden Systemen;
c. dem Wechsel der Betriebsplattformen.

4.14.2 Mindestens ist nachzuweisen, dass innerhalb jedes Entwicklungszyklus:

a. Sicherheitsanforderungen bereits in der Planung definiert werden und dafür eine strukturierte Analyse vorgenommen wird, bevor allfällige Entwicklungsaufträge vergeben oder Erweiterungen von bestehenden Informationssystemen vorgenommen werden;
b. Änderungen an Systemen einem formalen, dokumentierten Verfahren zur Änderungskontrolle unterliegen;
c. der Zugriff auf den eigenen Software-Quellcode beschränkt, kontrolliert und protokolliert wird;
d. Leitlinien für die sichere Entwicklung, auch bei ausgelagerten Systementwicklungstätigkeiten, vorhanden sind und im Entwicklungszyklus angewandt und umgesetzt werden;
e. sich in Testumgebungen keine produktiven Daten, insbesondere keine besonders schützenswerten Daten befinden;

ENTWURF

f. ausgelagerte Softwareentwicklung durch die Betriebsorganisation überwacht und beaufsichtigt werden.

4.15 Kommunikationssicherheit: Verwaltung von Netzwerken und Netzwerkdiensten (Art. 12 Abs. 4 EPDV)

4.15.1 Gemeinschaften müssen Richtlinien zur Netzwerksicherheit vorsehen und die Zuständigkeiten für die Verwaltung von Netzwerken innerhalb einer Gemeinschaft festlegen.

4.15.2 Gemeinschaften müssen sicherstellen, dass durch ein geeignetes Design des Netzwerks und seiner Komponenten sowie durch den geeigneten Aufbau und die Konfiguration der Netzwerkdienste, die Daten des elektronischen Patientendossiers in Anwendungen und Systemen geschützt sind.

4.15.3 Sie müssen dazu sichere Netzwerkstrukturen festlegen, durch Netzwerkpläne darstellen und umsetzen, die es erlauben, Gruppen von Informationsdiensten, Benutzern und Informationssystemen in Netzwerken voneinander getrennt zu halten; insbesondere müssen sie Firewalls, Router, Switches, etc. und technologische Umsetzungen für Netzwerkdienste so konfigurieren, dass:

a. die technischen Schnittstellen der gemeinschaftsinternen Informatikinfrastruktur einer Gemeinschaft («Services») nur von Systemen aufgerufen werden können, die zu einer zertifizierten Gemeinschaft gehören;

b. Systeme, die über das Internet auf einen Dienst zugreifen, sich diesem gegenüber mittels Transportschichtsicherheit (TLS) mit einem gültigen elektronischen Zertifikat authentisieren.

4.15.4 Die Netzwerkstrukturen müssen folgende Anforderungen erfüllen:

a. Für Zugangsportale sowie Zugangspunkte werden mindestens öffentliche Extended-Validation-TLS-Zertifikate eingesetzt, für andere Dienste entweder mindestens öffentliche *Extended-Validation*-TLS-Zertifikate oder TLS-Zertifikate, die nur innerhalb der Gemeinschaft gültig sind.

b. Alle Dienste, die aus dem Internet aufrufbar sind, müssen das aufrufende System mittels *TLS-Client-Authentication* authentisieren.

c. Antwortende Zugangspunkte (*Responding Gateways*) dürfen den Verbindungsaufbau nur zulassen, wenn das aufrufende System zu einer zertifizierten Gemeinschaft gehört, die im zentralen Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 EPDV geführt wird.

d. Alle gemeinschaftsinternen Dienste, die nicht aus dem Internet aufgerufen werden können, dürfen den Verbindungsaufbau nur zulassen, wenn das aufrufende System zur eigenen zertifizierten Gemeinschaft gehört und im Inventar der eigenen Gemeinschaft registriert und vom Datenschutz- und Datensicherheitsverantwortlichen akzeptiert wurde.

e. Die eingesetzten Verfahren müssen dokumentiert werden.

4.15.5 Gemeinschaften müssen:

a. alle Datenspeicher mit Patientendaten des elektronischen Patientendossiers der Gemeinschaft (darunter die Elemente aus dem «Inventar der Informatikinfrastruktur» nach Ziff. 4.8) netzwerktechnisch von allen anderen Systemen trennen, die ein tieferes Sicherheitsniveau aufweisen;

b. die hierzu eingesetzten Verfahren dokumentieren.

4.15.6 Gemeinschaften müssen insbesondere die zum Schutz der Zugangsportale implementierten Sicherheitsvorkehrungen dokumentieren. Die Dokumentation umfasst mindestens:

a. die Netzwerktopologie und die Art der Trennung des lokalen Netzwerks (LAN) vom Internet;

ENTWURF

b. die Versionen und Release-Stände der auf der Web-Application-Firewall (WAF) und dem Webserver eingesetzten Software sowie die Versionen verwendeter sicherheitsrelevanter Softwarekomponenten Dritter;

c. die vorgesehenen Massnahmen für die Erkennung und Behandlung von Angriffen und Sicherheitsschwachstellen.

4.16 Ablauf von Netzwerk-Sitzungen («*Session timeout*») (Art. 12 Abs. 4 EPDV)

4.16.1 Inaktive Netzwerk-Sitzungen müssen nach einer von dem oder der Datenschutz- und Datensicherheitsverantwortlichen der Gemeinschaft vorgegebenen Inaktivitätsperiode automatisch beendet werden.

4.16.2 Die Authentisierung auf den Zugangsportalen und Endgeräten muss vor dem nächsten Zugriff erneut durchgeführt werden, wenn bis zum Ablauf einer vorgegebenen Zeitspanne keine Interaktion des Benutzers oder der Benutzerin mit dem elektronischen Patientendossier stattfand.

4.17 Zwischenspeicher (Art. 12 Abs. 4 EPDV)

Elemente der gemeinschaftsinternen Informatikinfrastruktur, die der Übermittlung von medizinischen Daten des elektronischen Patientendossiers dienen, namentlich die Zugangspunkte, dürfen diese nicht dauerhaft, sondern nur für die Dauer der Transaktion speichern.

4.18 Verfügbarkeit (Art. 12 Abs. 4 EPDV)

Gemeinschaften müssen sicherstellen, dass:

a. die Daten des elektronischen Patientendossiers verfügbar sind;

b. die Verfügbarkeit der technischen Dienste und Systeme zur Bearbeitung und zum Schutz der Daten des elektronischen Patientendossiers vor Unterbrechungen geschützt sind;

c. nach einer Störung eine Wiederaufnahme des Systembetriebs sichergestellt werden kann;

d. die Daten des elektronischen Patientendossiers jederzeit geschützt sind;

e. die exponierten technischen Dienste der Informatikinfrastruktur eine vertraglich vereinbarte Verfügbarkeit über die Zeit von mindestens 98 % sowie unter aussergewöhnlicher Last aufweisen;

f. alle über das Internet erreichbaren Schnittstellen des elektronischen Patientendossiers gegen «*Denial-of-Service*»-(DoS)-Angriffe geschützt sind;

g. sie über erprobte Prozesse verfügen, die es erlauben, die Zeit für die Wiederherstellung von Informationswerten, die zum Beispiel in Folge von Naturkatastrophen, Unfällen, Anwendungs-, System- und Geräteausfällen oder mutwilligen Beschädigungen verloren gegangen sind, durch eine Kombination vorbeugender und wiederherstellender Massnahmen auf ein akzeptables Niveau zu minimieren.

4.19 Datenspeicher unter Schweizer Rechtshoheit (Art. 12 Abs. 5 EPDV)

Die Gemeinschaft muss sicherstellen, dass :

a. der Betrieb der gemeinschaftsinternen Datenspeicher des elektronischen Patientendossiers (insbesondere Dokumentenablagen, Dokumentenregister, Patientenindex) von juristischen Personen erbracht wird, die Schweizer Recht unterstehen;

b. sich diese Datenspeicher in der Schweiz befinden.

ENTWURF

5 Kontaktstelle für Gesundheitsfachpersonen (Art. 13 EPDV)

5.1.1 Die Gemeinschaften müssen für die Gesundheitsfachpersonen eine Kontaktstelle bezeichnen, die diese im Umgang mit dem elektronischen Patientendossier unterstützt.

5.1.2 Gemeinschaften müssen mindestens sicherstellen, dass:

a. die Mitarbeitenden der Kontaktstelle ihre Rechte und Pflichten sowie die Massnahmen bezüglich Datenschutz und Datensicherheit kennen;

b. die Mitarbeitenden mit Zugriff auf Daten des elektronischen Patientendossiers sorgfältig ausgewählt werden und entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet werden;

c. Zugriffe der Mitarbeitenden der Kontaktstelle auf die Endgeräte der Gesundheitsfachpersonen ausschliesslich mit Einwilligung der jeweiligen Gesundheitsfachperson erfolgen und dokumentiert werden.

ENTWURF

B. Zusätzliche Anforderungen für Stammgemeinschaften

6 Information der Patientin oder des Patienten (Art. 15 EPDV)

6.1 Information der Patientin oder des Patienten (Art. 15 EPDV)

6.1.1 Die Patientin oder der Patient muss informiert werden über:

a. den Zweck des elektronischen Patientendossiers;
b. die Grundzüge der Datenbearbeitung;
c. den Verbleib der medizinischen Daten in den Primärsystemen;
d. die Speicherung und allfällige Vernichtung von medizinischen Daten der Dokumentenablagen.

6.1.2 Die Patientin oder der Patient muss insbesondere darüber informiert werden, dass sie oder er:

a. der vermuteten Einwilligung nach Artikel 3 Absatz 2 EPDG zur Bereitstellung von medizinischen Daten im Behandlungsfall widersprechen kann;
b. medizinische Daten in den Dokumentenablagen des elektronischen Patientendossiers wieder vernichten kann;
c. welche Funktionen des Zugangsportals für Patientinnen und Patienten ihr oder ihm zur Verfügung stehen;
d. in die Protokolldaten Einsicht nehmen kann;
e. eine Stellvertreterin oder einen Stellvertreter benennen kann;
f. festlegen kann, dass sie oder er über den Eintritt von Gesundheitsfachpersonen in Gruppen, denen sie oder er ein Zugriffsrecht erteilt hat, informiert wird;
g. Gesundheitsfachpersonen ihrer oder seiner Stammgemeinschaft zur Weitergabe von Zugriffsrechten an weitere Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen ermächtigen kann.

6.1.3 Die Patientin oder der Patient muss über die Folgen der Einwilligung und des Widerrufs informiert werden, mindestens darüber:

a. dass, die Einwilligung freiwillig ist;
b. dass, nur ein Patientendossier pro Patientin oder Patient gleichzeitig geführt werden kann;
c. wie die Patientenidentifikationsnummer vergeben und verwendet wird;
d. dass, sie oder er die Stammgemeinschaft wechseln kann, und welche Konsequenzen mit einem solchen Wechsel in Bezug auf den Verbleib der Daten sowie für allfällige Stellvertretungen und Ermächtigungen von Gesundheitsfachpersonen verbunden sind;
e. dass sie oder er die Einwilligung formlos widerrufen kann und den Widerruf nicht begründen muss;
f. dass im Falle eines Widerrufs das elektronische Patientendossier aufgehoben und die darin enthaltenen Daten gelöscht werden;
g. dass, auch nach einem Widerruf erneut ein elektronisches Patientendossier eröffnet werden kann und diesem eine neue Patientenidentifikationsnummer zugeordnet wird.

ENTWURF

6.1.4 Die Patientin oder Patient muss informiert werden über die Vertraulichkeitsstufen für medizinische Daten, mindestens:

a. über die Möglichkeit, medizinische Daten des elektronischen Patientendossiers jederzeit einer von drei Vertraulichkeitsstufen zuzuordnen;
b. darüber, dass neu eingestellte medizinische Daten automatisch der Vertraulichkeitsstufe «normal zugänglich» zugeordnet werden;
c. darüber, dass Gesundheitsfachpersonen neu eingestellten medizinischen Daten die Vertraulichkeitsstufe «eingeschränkt zugänglich» zuordnen können;
d. über die Möglichkeit, selber zu bestimmen, welcher Vertraulichkeitsstufe neu eingestellte medizinische Daten zugeordnet werden und dass in der Folge diese von ihr oder ihm gewählte Zuordnung gilt (Übersteuerung der Buchstaben b und c).

6.1.5 Die Patientin oder Patient muss informiert werden wie Zugriffsrechte erteilt werden können, mindestens über die Möglichkeit:

a. einzelne Gesundheitsfachpersonen vollständig vom Zugriff auszuschliessen (Ausschlussliste);
b. medizinische Daten durch Zuordnung zu der Vertraulichkeitsstufe «geheim» von jeglichem Zugriff durch Gesundheitsfachpersonen auszuschliessen;
c. Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen entweder das Zugriffsrecht auf die Vertraulichkeitsstufe «normal zugänglich» oder das Zugriffsrecht auf die Vertraulichkeitsstufen «normal zugänglich» und «eingeschränkt zugänglich» zu erteilen;
d. diese Zugriffsrechte anzupassen, zu befristen oder zu entziehen;
e. dass auch registrierte Hilfspersonen von Gesundheitsfachpersonen mit dem Zugriffsrecht der jeweils verantwortlichen Gesundheitsfachperson zugreifen;
f. dass Gesundheitsfachpersonen in medizinischen Notfallsituationen auf die «normal zugänglichen» Daten zugreifen;
g. den Zugriff in medizinischen Notfallsituationen auch auf die Vertraulichkeitsstufe «eingeschränkt zugänglich» zu erweitern oder ganz auszuschliessen;
h. dass sie oder er nach einem Notfallzugriff eine entsprechende Information erhält.

6.1.6 Die Patientin oder der Patient muss über die empfohlenen Datenschutz- und Datensicherheitsmassnahmen informiert werden, mindestens über:

a. die Restrisiken und mögliche vorbeugende Massnahmen;
b. die sichere Authentisierung und den Umgang mit Identifikationsmitteln und geheimen Zugangsdaten;
c. die Massnahmen für eine sichere Nutzung von Endgeräten;
d. die Verhaltensempfehlungen zur Abwehr von Betrugsversuchen.

7 Einwilligung (Art. 16 EPDV)

7.1 Erstellung eines elektronischen Patientendossiers

7.1.1 Für die Erstellung eines elektronischen Patientendossiers ist die eigenhändige Unterschrift der Patientin oder des Patienten notwendig.

ENTWURF

8 Verwaltung (Art. 17 EPDV)

8.1 Eröffnung, Verwaltung und Aufhebung des elektronischen Patientendossiers (Art. 17 Abs. 1 Bst. a EPDV)

Die Stammgemeinschaften legen die Prozesse für die Eröffnung, die Verwaltung und die Aufhebung des elektronischen Patientendossiers fest.

8.2 Identifikation der Patientinnen und Patienten (Art. 17 Abs. 1 Bst. b und d EPDV)

8.2.1 Die Prozesse zur Identifikation der Patientinnen und Patienten müssen festgelegt werden. Diese müssen sicherstellen, dass:

a. die Patientin oder der Patient anhand des Identifikationsmittels eines zertifizierten Herausgebers oder gemäss den Anforderungen nach Artikel 24 Absatz 1 EPDV identifiziert wird;

b. die Patientin oder der Patient nicht schon bereits ein elektronisches Patientendossier besitzt;

c. die Patientin oder der Patient in den Patientenindex der Stammgemeinschaft aufgenommen wird;

d. eine Patientenidentifikationsnummer nach den Vorgaben der Artikel 6 und 7 EPDV angefordert und dem zu erstellenden elektronischen Patientendossiers korrekt zugeordnet wird;

e. die demografischen Daten der Patientin oder des Patienten aus der Identifikationsdatenbank der ZAS in den Patientenindex der Stammgemeinschaft übernommen werden.

8.2.2 Gemeinschaften müssen sicherstellen, dass der eindeutige Identifikator nach Artikel 25 Absatz 1 EPDV mit der richtigen Patientin oder dem richtigen Patienten und seiner oder ihrer Patientenidentifikationsnummer verbunden wird.

8.2.3 Gemeinschaften müssen sicherstellen, dass die Daten und die Verknüpfung von Identifikator und Patientenidentifikationsnummer gemäss Artikel 26 und Artikel 27 EPDV aktualisiert werden.

8.3 Identifikation und Authentifizierung beim Zugriff (Art. 17 Abs. 1 Bst. c EPDV)

8.3.1 Patientinnen und Patienten müssen sich für den Zugriff auf das elektronische Patientendossier mit gültigen Identifikationsmitteln authentifizieren, die von einem nach Artikel 31 EPDV zertifizierten Herausgeber herausgegeben wurden.

8.4 Stellvertretung (Art. 17 Abs. 1 Bst. c EPDV)

8.4.1 Die Stellvertreterin oder der Stellvertreter nach Ziffer 8.6.3 Buchstabe f muss mittels eigenem Identifikationsmittel eines nach Artikel 31 EPDV zertifizierten Herausgebers auf das elektronische Patientendossier der vertretenen Person zugreifen.

8.4.2 Die Stammgemeinschaft muss sicherstellen, dass:

a. der Stellvertreter oder die Stellvertreterin mit einem eigenen Identifikationsmittel eines zertifizierten Herausgebers nach Artikel 31 EPDV oder gemäss Artikel 24 Absatz 1 EPDV identifiziert wird;

ENTWURF

b. die Stellvertretung über die Grundzüge der Datenbearbeitung sowie die Möglichkeiten, die Rechte und die Pflichten im Zusammenhang mit der Nutzung des elektronischen Patientendossiers informiert wird;
c. der eindeutige Identifikator nach Artikel 25 Absatz 1 EPDV der Stellvertretung korrekt zugeordnet wird;
d. der Zugang der Stellvertretung zum elektronischen Patientendossier nur für die Dauer der Stellvertretung besteht.

8.5 Wechsel der Stammgemeinschaft (Art. 17 Abs. 1 Bst. e EPDV)

8.5.1 Der Prozess für den Wechsel der Stammgemeinschaft durch eine Patientin oder einen Patienten muss festgelegt werden.

8.5.2 Der Prozess zum Wechsel der Stammgemeinschaft muss sicherstellen, dass:
a. die individuelle Konfiguration der Berechtigungssteuerung in die neue Stammgemeinschaft überführt werden kann. Dabei sind die Vorgaben des technischen Austauschformats im nationalen Integrationsprofil CH:PPQ nach Anhang 5 der EPDV-EDI einzuhalten;
b. die Ermächtigung von Gesundheitsfachpersonen nach Artikel 4 Buchstabe g EPDV aufgehoben wird;
c. die Zugriffsmöglichkeit der Stellvertretung der Patientin oder des Patienten aufgehoben wird.

8.6 Berechtigungssteuerung (Art. 17 Abs. 2 EPDV)

8.6.1 Patientinnen und Patienten müssen die Möglichkeit haben, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen Zugriffsrechte zu erteilen, diese Zugriffsrechte anzupassen und zu entziehen. Dabei sind die Vorgaben der Artikel 2 und 3 EPDV einzuhalten.

8.6.2 Stammgemeinschaften müssen sicherstellen, dass eine Bearbeitung der Konfiguration der Berechtigungssteuerung nur gemäss dem Willen der Patientin oder des Patienten erfolgt.

8.6.3 Stammgemeinschaften müssen sicherstellen, dass Patientinnen und Patienten die Optionen nach Artikel 4 EPDV nutzen können. Dazu müssen sie der Patientin oder dem Patienten ermöglichen:
a. festzulegen, welcher Vertraulichkeitsstufe neu eingestellten medizinische Daten zugeordnet werden;
b. einzelne Gesundheitsfachpersonen vom Zugriff auf das elektronische Patientendossier auszuschliessen;
c. über Eintritte von Gesundheitsfachpersonen in berechtigte Gruppen informiert zu werden;
d. die Gesundheitsfachpersonen erteilten Zugriffsrechte nach eigenem Ermessen zu befristen;
e. den Notfallzugriff zu erweitern oder auszuschliessen;
f. eine Stellvertretung zu benennen;
g. Gesundheitsfachpersonen zur Weitergabe ihrer Zugriffsrechte an weitere Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen zu ermächtigen.

ENTWURF

9 Zugangsportal für Patientinnen und Patienten (Art. 18 EPDV)

9.1 Umsetzung der Berechtigungssteuerung (Art. 18 Bst. a EPDV)

Das Zugangsportal muss:

a. Patientinnen und Patienten die Möglichkeit bieten, die Berechtigungssteuerung unter Einhaltung der Vorgaben von Artikel 1 bis 4 EPDV vorzunehmen;

b. darstellen, welche Gesundheitsfachpersonen über welche Zugriffsrechte verfügen;

c. die Zusammensetzung der Gruppen von Gesundheitsfachpersonen darstellen.

9.2 Darstellung (Art. 18 Bst. a EPDV)

Die Darstellung auf der Benutzeroberfläche des Zugangsportals muss korrekt und vollständig sein und klar erkennen lassen:

a. ob medizinische Daten durch eine Gesundheitsfachperson oder durch die Patientin oder den Patienten bereitgestellt wurden;

b. welche medizinischen Daten annulliert wurden;

c. welche Versionen medizinischer Daten vorhanden sind;

d. welche medizinischen Daten welcher Vertraulichkeitsstufe zugeordnet sind.

9.3 Darstellung der Protokolldaten (Art. 18 Bst. b EPDV)

Patientinnen und Patienten müssen die Möglichkeit haben, die Protokolldaten zu ihrem elektronischen Patientendossier aus allen Gemeinschaften und Stammgemeinschaften in einer für sie lesbaren Form einzusehen.

9.4 Erfassung und Abruf von Daten (Art. 18 Bst. c EPDV)

9.4.1 Das Zugangsportal muss der Patientin oder dem Patienten die Möglichkeit bieten:

a. die von Gesundheitsfachpersonen erfassten medizinischen Daten von der Vernichtung nach Artikel 10 Absatz 1 Buchstabe d auszunehmen;

b. bestimmte auf sie oder ihn bezogene medizinische Daten aus dem elektronischen Patientendossier zu vernichten.

9.4.2 Das Zugangsportal muss betreffend der Medientypen die gleichen Anforderungen erfüllen wie das interne Zugangsportal für Gesundheitsfachpersonen gemäss Ziffer 3.3.

9.4.3 Das Zugangsportal muss hinsichtlich der Daten, die von der Patientin oder dem Patienten selber erfasst werden, mindestens folgende Voraussetzungen erfüllen:

a. Die von ihr oder ihm in Bereichen ausserhalb des elektronischen Patientendossiers bereitgestellten Daten dürfen nur dann im elektronischen Patientendossier erfasst werden, wenn sie oder er dazu die Einwilligung erteilt hat;

b. Die von der Patientin oder vom Patienten selbst bereitgestellten Daten müssen immer direkt, d.h. ohne Verwendung intermediärer Speicher, im elektronischen Patientendossier erfasst werden können.

ENTWURF

9.5 Barrierefreiheit (Art. 18 Bst. d EPDV)

Das Zugangsportal muss die gleichen Anforderungen erfüllen wie das Zugangsportal für Gesundheitsfachpersonen gemäss Ziffer 3.2.

10 Von Patientinnen oder Patienten erfasste Daten (Art. 19 EPDV)

10.1 Dokumentenablagen für medizinische Daten von Patientinnen und Patienten

10.1.1 Stammgemeinschaften müssen gemeinschaftsinterne Dokumentenablagen für die durch Patientinnen oder Patienten selbst erfassten medizinischen Daten bereitstellen.

10.1.2 Die medizinischen Daten dürfen keiner Löschungsfrist unterliegen.

10.1.3 Der Speicherplatz muss angemessen bemessen sein.

10.2 Offline-Archivierung von medizinischen Daten und Metadaten

10.2.1 Patientinnen und Patienten müssen die Möglichkeit haben, Daten aus ihrem elektronischen Patientendossier in einem interoperablen gängigen elektronischen Format herunterzuladen oder auf andere Weise zu beziehen (vgl. Ziff. 2.9.18).

10.2.2 Werden archivierte Daten erneut im elektronischen Patientendossier verfügbar gemacht, so müssen sie als von Patienten erfasste Daten, gekennzeichnet werden. Es sei denn, die Stammgemeinschaft kann mit geeigneten Verfahren sicherstellen, dass die archivierten Daten seit der Zurverfügungstellung unverändert geblieben sind.

11 Kontaktstelle für Patientinnen und Patienten (Art. 20 EPDV)

11.1.1 Stammgemeinschaften müssen für die Patientinnen und Patienten eine Kontaktstelle bezeichnen, die sie im Umgang mit dem elektronischen Patientendossier unterstützt.

11.1.2 Stammgemeinschaften müssen mindestens sicherstellen, dass:

a. die Mitarbeitenden ihre Rechte und Pflichten sowie die Risiken und Massnahmen bezüglich Datenschutz und Datensicherheit kennen;

b. die Mitarbeitenden mit Zugriff auf Daten des elektronischen Patientendossiers sorgfältig ausgewählt werden und entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet sind;

c. die Mitarbeitenden der Kontaktstelle ausschliesslich mit Einwilligung auf die Endgeräte der Patientinnen und Patienten der jeweiligen Patientin oder des Patienten zugreifen können und die Zugriffe dokumentiert werden.

ENTWURF

12 Aufhebung des elektronischen Patientendossiers (Art. 21 EPDV)

12.1 Prozess zur Aufhebung des elektronischen Patientendossiers (Art. 21 EPDV)

Stammgemeinschaften müssen Prozesse zur Aufhebung des elektronischen Patientendossiers vorsehen.

12.2 Widerruf der Einwilligung zur Führung eines elektronischen Patientendossiers (Art. 21 Abs. 1 EPDV)

12.2.1 Stammgemeinschaften müssen sicherstellen, dass das elektronische Patientendossier unverzüglich aufgehoben wird, wenn die Patientin oder der Patient die Einwilligung widerruft.

12.2.2 Der Prozess zur Aufhebung des elektronischen Patientendossiers aufgrund eines Widerrufs muss sicherstellen, dass:

a. die widerrufende Person anhand des Identifikationsmittels eines zertifizierten Herausgebers identifiziert wird und die widerrufende Person über die Folgen des Widerrufs informiert wird;
b. der Widerruf rechtsgültig dokumentiert wird;
c. die Widerrufserklärung während zehn Jahren aufbewahrt wird.

12.3 Aufhebung nach dem Tod der Patientin oder des Patienten (Art. 21 Abs. 2 EPDV)

Stammgemeinschaften müssen sicherstellen, dass die Aufhebung des elektronischen Patientendossiers frühestens zwei Jahre nach dem Tod der Patientin oder des Patienten erfolgt.

12.4 Aufhebung des elektronischen Patientendossiers (Art. 21 Abs. 3 EPDV)

Der Prozess zur Aufhebung des elektronischen Patientendossiers muss sicherstellen, dass:

a. das aufzuhebende elektronische Patientendossier korrekt identifiziert wird;
b. sämtliche Zugriffsrechte auf das entsprechende Patientendossier unverzüglich entzogen werden;
c. sämtliche Daten des entsprechenden Patientendossiers gemäss Ziffer 2.1 Buchstabe b vernichtet werden und die Patientenidentifikationsnummer aus allen Systemen entfernt wird;
d. alle Gemeinschaften und Stammgemeinschaften innert angemessener Frist über die Aufhebung des elektronischen Patientendossiers informiert werden;
e. die ZAS innert angemessener Frist über die Aufhebung des elektronischen Patientendossiers informiert wird.

ENTWURF