Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

**Bundesamt für Gesundheit BAG**
Direktionsbereich Gesundheitspolitik

SR 816.11.n / Anhang 2 der Verordnung des EDI vom ... über das elektronische Patientendossier

# Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften

Ausgabe: 1.0 22.03.2016
Inkrafttreten: ...

# Anforderungen an Gemeinschaften

## 1 Verwaltung (Art. 8 EPDV)

### 1.1 Verwaltung von Gesundheitseinrichtungen (Bst. a und c)

1.1.1 Die Prozesse für den Eintritt und den Austritt von Gesundheitseinrichtungen müssen definiert, dokumentiert, umgesetzt und eingehalten werden.

1.1.2 Der Prozess für den Eintritt von Gesundheitseinrichtungen muss sicherstellen, dass:
1.1.2.1 Vereinbarungen zur Einforderung und Überprüfung von Aufgaben und Pflichten der Gesundheitseinrichtung, mindestens im Bereich Datenschutz und Datensicherheit abgeschlossen werden;
1.1.2.2 die Daten des Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV aktualisiert werden;
1.1.2.3 der Prozess «Eintritt von Gesundheitsfachpersonen» (vgl. Ziffer 1.2.2) für alle mit einer Gesundheitseinrichtung eintretenden Gesundheitsfachpersonen ausgelöst wird.

1.1.3 Der Prozess für den Austritt von Gesundheitseinrichtungen muss sicherstellen, dass:
1.1.3.1 der Prozess «Austritt von Gesundheitsfachpersonen» (vgl. Ziffer 1.2.4) für alle mit einer Gesundheitseinrichtung austretenden Gesundheitsfachpersonen ausgelöst wird;
1.1.3.2 sofern sich die austretende Gesundheitseinrichtung keiner anderen Gemeinschaft anschliesst:
1.1.3.2.1 die Dokumente in den Dokumentenablagen der austretenden Gesundheitseinrichtung gelöscht werden;
1.1.3.2.2 die Einträge im Dokumentenregister, die auf Dokumente in den Ablagen der austretenden Einrichtung verweisen, gelöscht werden;
1.1.3.2.3 die betroffenen Patientinnen und Patienten rechtzeitig informiert werden.

1.1.4 Die Gemeinschaft muss für die von ihr registrierten Daten im zentralen Abfragedienst der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV:
1.1.4.1 eine verantwortliche Person benennen;
1.1.4.2 sicherstellen, dass die Aktualität und Korrektheit der Daten:
1.1.4.2.1 der Gesundheitseinrichtungen mindestens halbjährlich überprüft und bestätigt wird;
1.1.4.2.2 der Gruppen von Gesundheitsfachpersonen mindestens vierteljährlich überprüft und bestätigt wird.

### 1.2 Verwaltung von Gesundheitsfachpersonen (Bst. a bis d)

1.2.1 Die Prozesse für den Eintritt, die Verwaltung und den Austritt von Gesundheitsfachpersonen müssen definiert, dokumentiert, umgesetzt und eingehalten werden.

1.2.2 Der Prozess für den Eintritt von Gesundheitsfachpersonen muss sicherstellen, dass:
1.2.2.1 die Einwilligung der Gesundheitsfachperson zu den spezifischen Richtlinien der Gemeinschaft oder der Gesundheitseinrichtung dokumentiert wird;
1.2.2.2 die Identifikation der Gesundheitsfachperson

1.2.2.2.1 anhand des Identifikationsmittels eines nach Artikel 30 EPDV zertifizierten Herausgebers erfolgt, oder
1.2.2.2.2 den Anforderungen nach Artikel 23 EPDV entspricht;
1.2.2.3 es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG handelt;
1.2.2.4 das von einem nach Artikel 30 EPDV zertifizierten Herausgeber herausgegebene Identifikationsmittel der Gesundheitsfachperson registriert wird;
1.2.2.5 die Daten des Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV aktualisiert werden. Ist die Gesundheitsfachperson in einem eidgenössischen oder kantonalen Berufsregister ((z. B. des Registers über die universitären Medizinalberufe «MedReg», des Registers der Psychologieberufe «PsyReg» oder des Gesundheitsberuferegisters «NAREG») geführt, so sind die entsprechenden Angaben von dort zu übernehmen.

1.2.3 Der Prozess für die Verwaltung von Gesundheitsfachpersonen muss sicherstellen, dass:
1.2.3.1 die Daten des Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV aktualisiert werden;
1.2.3.2 der Zugang zum elektronischen Patientendossier überprüft wird;
1.2.3.3 die Zugriffsrechte angepasst werden.

1.2.4 Der Prozess für den Austritt von Gesundheitsfachpersonen muss sicherstellen,:
1.2.4.1 dass die Daten des Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV aktualisiert werden;
1.2.4.2 der Zugang zum elektronischen Patientendossier deaktiviert wird;
*1.2.4.3* die Zugriffsrechte gelöscht werden.

### 1.3 Verwaltung von Hilfspersonen von Gesundheitsfachpersonen

1.3.1 Gemeinschaften müssen Prozesse vorsehen, dass Hilfspersonen von Gesundheitsfachpersonen in einem gemeinschaftsinternen Dienst zur Verwaltung von Gesundheitseinrichtungen und Gesundheitsfachpersonen erfasst, verwaltet und gelöscht werden können.

1.3.2 Für die Verwaltung von Hilfspersonen gelten, mit Ausnahme der unten aufgeführten Anforderungen, dieselben Anforderungen wie für Eintritt, die Verwaltung oder den Austritt von Gesundheitsfachpersonen. Ausgenommen sind:
1.3.2.1 die Sicherstellung, dass es sich um eine Gesundheitsfachperson nach Artikel 2 Buchstabe b EPDG handelt;
1.3.2.2 die Aktualisierung des Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV.

### 1.4 Identifikation und Authentisierung (Art. 8 Bst. d)

1.4.1 Für den Zugriff von Gesundheitsfachpersonen auf das elektronische Patientendossier dürfen nur gültige Identifikationsmittel verwendet werden, die von einem nach Artikel 30 EPDV zertifizierten Herausgeber herausgegeben wurden.

1.4.2 Gemeinschaften müssen sicherstellen, dass die eindeutigen Identifikatoren der Identifikationsmittel von Gesundheitsfachpersonen und Hilfspersonen zuverlässig mit der registrierten Identität der jeweiligen Person in der Gemeinschaft verbunden wird.

1.4.3 Gemeinschaften müssen sicherstellen, dass alle technischen Systeme, wie beispielsweise angeschlossene Primärsysteme oder Zugangsportale, die von Gesundheitsfachpersonen oder Hilfspersonen für den Zugriff auf das elektronische Patientendossier genutzt werden:

1.4.3.1 ein starkes Authentifizierungsverfahren nach aktuellem Stand der Technik mit mindestens zwei Authentifizierungsfaktoren als Voraussetzung für die Bearbeitung von Daten des elektronischen Patientendossiers unterstützen.

1.4.3.2 einen vertrauenswürdigen Endpunkt für die sichere Kommunikation mit dem Identitätsdienstleister (Herausgeber des Identifikationsmittels) gemäss Kapitel 3.2 (*P.TrustedCommunityEndpoint*) des Schutzprofils nach Art. 8 EPDV-EDI zur Verfügung stellen.

1.4.4 Gemeinschaften müssen eine so erfolgte Authentifizierung anderer zertifizierter Gemeinschaften und Stammgemeinschaften anerkennen.

### 1.5 Verwaltung von Gruppen von Gesundheitsfachpersonen (Art. 8 EPDV Bst. a, c, e und f)

1.5.1 Gemeinschaften sind für die Verwaltung der Gruppen von Gesundheitsfachpersonen verantwortlich. Die Richtlinien und Prozesse zur Verwaltung der Gruppen von Gesundheitsfachpersonen müssen definiert, dokumentiert, umgesetzt und eingehalten werden.

1.5.2 Die Prozesse und Richtlinien müssen sicherstellen, dass:

1.5.2.1 die Zusammensetzung der Gruppen für Patientinnen und Patienten jederzeit nachvollziehbar ist;

1.5.2.2 die Patientinnen und Patienten über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen informiert werden können;

1.5.2.3 die Grössen von Gruppen verhältnismässig bleiben;

1.5.2.4 die Daten im Abfragedienstes der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV aktualisiert werden.

# 2 Datenhaltung und Datenübertragung (Art. 9 EPDV)

### 2.1 Löschen von Daten (Abs. 1 Bst. a und b)

2.1.1 Gemeinschaften müssen Verfahren vorsehen, die sicherstellen, dass:

2.1.1.1 die bei ihnen von den Gesundheitsfachpersonen im elektronischen Patientendossier erfassten Daten nach 10 Jahren vernichtet werden;

2.1.1.2 bei einer Aufhebung des elektronischen Patientendossiers gemäss Artikel 20 Absatz 1 sämtliche Daten vernichtet werden; dabei sind die Daten mindestens aus folgenden

abfragbaren Systemen zu vernichten:

2.1.1.2.1 Dokumentenregister;
2.1.1.2.2 Dokumentenablagen;
2.1.1.2.3 Patientenindex;
2.1.1.2.4 Berechtigungssteuerung;
2.1.1.2.5 internes Zugangsportal.

### 2.2 Dokumentenablage (Abs. 1 Bst. c)

2.2.1 Gemeinschaften müssen Verfahren vorsehen, die sicherstellen, dass:

2.2.1.1 Dokumente des elektronischen Patientendossiers nur in ausschliesslich für diesen Zweck vorgesehenen Dokumentenablagen gespeichert werden;

2.2.1.2 in den Dokumentenablagen nur die gemäss Anhang 3 der EPDV-EDI zugelassenen Dateiformate gespeichert werden;

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

2.2.1.4 als Kodierung von Zeichen in abrufbaren Daten und Dokumenten Unicode UTF-8 verwendet wird.

### 2.3 Verwaltung auf Wunsch der Patienten (Abs. 2)

2.3.1.1 Gemeinschaften müssen Verfahren vorsehen, damit auf Wunsch der Patientin oder des Patienten bestimmte auf diese oder diesen bezogene Daten (Abs. 2):

2.3.1.1.1 nicht im elektronischen Patientendossier erfasst werden;
2.3.1.1.2 nach Artikel 9 Absatz 1 Buchstabe a weitere 10 Jahre verfügbar bleiben;
2.3.1.1.3 aus dem elektronischen Patientendossier vernichtet werden;

2.3.2 Von den Vorgaben nach Artikel 9 Absätze 1 und 2 EPDV auszunehmen sind Protokolldaten und Daten in den nicht abfragbaren Primärsystemen sowie in Datensicherungen.

### 2.4 Umsetzung der Vertraulichkeitsstufen (Abs. 3 Bst. a)

2.4.1 Gemeinschaften müssen sicherstellen, dass:

2.4.1.1 die Patientin oder der Patient Daten des elektronischen Patientendossiers den Vertraulichkeitsstufen nach den Vorgaben von Artikel 1 EPDV zuordnen kann. Dies indem die von der Patientin oder dem Patienten über das Zugangsportal der Stammgemeinschaft vorgenommene Zuordnung von Daten des elektronischen Patientendossiers zu einer der vier Vertraulichkeitsstufen, für die jeweiligen bei ihr gespeicherten Dokumente übernommen wird;

2.4.1.2 neu eingestellten Daten die Vertraulichkeitsstufe gemäss Artikel 1 Absatz 2 oder entsprechend der Festlegung des Patienten oder der Patienten nach Artikel 3 Buchstabe c EPDV zugewiesen wird;

2.4.1.3 Gesundheitsfachpersonen neu eingestellten Daten die Vertraulichkeitsstufe «sensible Daten» zuweisen können.

### 2.5 Durchsetzen der Zugriffsentscheidung (Abs. 3 Bst. a)

2.5.1.1 Gemeinschaften müssen sicherstellen, dass Zugriffe auf Daten ihrer Dokumentenablagen und Dokumentenregister nur gemäss der zuvor eingeholten Zugriffsentscheidung der Stammgemeinschaft erfolgen können.

### 2.6 Notfallzugriff (Abs. 3 Bst. a)

2.6.1 Hinsichtlich Zugriff in medizinischen Notfallsituationen (Art. 2 Abs. 5 EPDV) müssen Gemeinschaften sicherstellen, dass:

2.6.1.1 vorgängig eine Begründung für den Notfallzugriff angegeben werden muss;

2.6.1.2 ein Notfallzugriff nur nach einer nochmaligen Bestätigung, mittels einer nicht automatisiert reproduzierbaren, manuellen Interaktion der Gesundheitsfachperson möglich ist.

2.6.1.3 die Patientin oder der Patient darüber unverzüglich informiert wird (*Art. 9 Abs. 5 EPDG*);

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

### 2.7 Überprüfung der Berechtigungssteuerung (Abs. 3 Bst. a)

2.7.1.1 Die Berechtigungssteuerung muss die Möglichkeit bieten, dass im Rahmen automatisierter Testszenarien die Korrektheit der Funktionalitäten und Regelauswertungen überprüft werden können.

### 2.8 Metadaten (Abs. 3 Bst. b)

2.8.1 Gemeinschaften müssen sicherstellen, dass für die Beschreibung der bereitgestellten Dokumente die Metadaten nach Anhang 4 der EPDV-EDI verwendet werden.

### 2.9 Integrationsprofile (Abs. 3 Bst. d)

**Standardschnittstelle zur Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS)**

2.9.1 Die Zugangspunkte der Gemeinschaften müssen sicherstellen, dass sie die von der Zentralen Ausgleichsstelle (ZAS) angebotenen technischen Schnittstellen zur Identifikationsdatenbank (UPI) 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 gemäss dem Bearbeitungsreglement der ZAS einzuhalten.

**Integrationsprofile, nationale Anpassungen der Integrationsprofile und nationale Integrationsprofile**

2.9.3 Die Gemeinschaften müssen für die Informationsübertragung die Integrationsprofile nach Artikel 5 Buchstaben a bis c (Integrationsprofile, nationale Anpassungen der Integrationsprofile und nationale Integrationsprofile) im Anhang 5 der EPDV-EDI verwenden.

**Akteure und Transaktionen der Integrationsprofile – 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:

2.9.4.1 Cross Gateway Query [ITI-38]

2.9.4.2 Cross Gateway Retrieve [ITI-39]

2.9.4.3 Cross Gateway Patient Discovery [ITI-55]

2.9.4.4 Patient Location Query [ITI-56]

**Akteure und Transaktionen der Integrationsprofile – Kommunikation beglaubigter Identitäten**

2.9.5 Die Gruppierung anderer Akteure mit den IHE-Akteuren *X-Service Provider* und *X-Service User* des IHE-Integrationsprofils IHE XUA richtet sich nach den Vorgaben der nationalen Integrationsprofile und Anpassungen der Integrationsprofile gemäss Anhang 5 der EPDV-EDI und ist dem entsprechend sicherzustellen.

2.9.6 Die IHE-Akteure *X-Service* Provider und *X-Service User* müssen folgende Transaktion des Integrationsprofils IHE XUA in der Version nach Anhang 5 der EPDV-EDI unterstützen:

2.9.6.1 Provide X-User Assertion [ITI-40]

**Akteure und Transaktionen der Integrationsprofile – Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen**

2.9.7 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:

2.9.7.1 Provider Information Query [ITI-58]

2.9.7.2 Provider Information Feed [ITI-59]

**Akteure und Transaktionen der Integrationsprofile – Dokumente abrufen**

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

2.9.8.1 Registry Stored Query [ITI-18]

2.9.8.2 Retrieve Document Set [ITI-43 ]

**Akteure und Transaktionen der Integrationsprofile – Dokumente bereitstellen**

2.9.9 Der IHE Akteur *Document Source* muss folgende Transaktionen des Integrationsprofils IHE XDS in der Version nach Anhang 5 der EPDV-EDI unterstützen:

2.9.9.1 Provide and Register Document Set-b [ITI-41]

2.9.9.2 Retrieve Document Set [ITI-43]

**Akteure und Transaktionen der Integrationsprofile – Dokumenten-Metadaten mutieren**

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

2.9.10.1 Update Document Set [ITI-57]

2.9.10.2 Delete Document Set [ITI-62]

**Akteure und Transaktionen der Integrationsprofile – Dokumentenregister**

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

2.9.11.1 Register Document Set-b [ITI-42]

2.9.11.2 Register Stored Query [ITI-18]

2.9.11.3 Update Document Set [ITI-57]

2.9.11.4 Delete Document Set [ITI-62]

**Akteure und Transaktionen der Integrationsprofile – Dokumentenablage**

2.9.12 Der IHE-Akteur *Document Repository* muss folgenden Transaktionen des Integrationsprofils IHE XDS in der Version gemäss Anhang 5 der EPDV-EDI unterstützen:
2.9.12.1 Provide and Register Document Set-b [ITI-41]
2.9.12.2 Retrieve Document Set [ITI-43]

**Akteure und Transaktionen der Integrationsprofile – Daten für den Patientenindex bereitstellen**

2.9.13 Der IHE-Akteur *Patient Identity Source* muss die folgende Transaktion der Integrationsprofile PIX V3 in den Versionen gemäss Anhang 5 der EPDV-EDI unterstützen:
2.9.13.1 Patient Identity Feed HL7 v3 [ITI-44]

**Akteure und Transaktionen der Integrationsprofile – Patientenindex bereitstellen und abfragen**

2.9.14 Die IHE-Akteure *Patient Demographics Supplier* und *Patient Demographics Consumer* muss die folgende Transaktion des Integrationsprofils PDQ V3 in den Versionen nach Anhang 5 der EPDV-EDI unterstützen:
2.9.14.1 Patient Demographics Query V3 [ITI-47]

**Akteure und Transaktionen der Integrationsprofile – Patientenindex verwalten**

2.9.15 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:
2.9.15.1 Patient Identity Feed HL7 V3 [ITI-44]
2.9.15.2 PIX V3 Query [ITI-45]
2.9.15.3 PIX V3 Update Notification [ITI-46]

**Akteure und Transaktionen der Integrationsprofile – Authentisierung von Systemen und Protokollierung von IHE-Transaktionen**

2.9.16 Die Gruppierung anderer Akteure mit den IHE-Akteuren *Secure Application* und *Secure Node grouped with Any IHE Actor* des Integrationsprofils IHE ATNA (resp. der nationalen Anpassung dazu) richtet sich nach den Vorgaben der IHE-Integrationsprofile, der nationalen Integrationsprofile sowie der Anpassungen der Integrationsprofile und ist dem entsprechend sicherzustellen.

2.9.17 Die Akteure in der Rolle *Secure Node grouped with Any IHE Actor* müssen die folgenden Transaktionen des Integrationsprofils IHE ATNA und seiner nationalen Anpassung gemäss Anhang 5 der EPDV-EDI unterstützen:
2.9.17.1 Maintain Time [ITI-1]
2.9.17.2 Authenticate Node [ITI-19]

2.9.18 Die Akteure in der Rolle *Secure Application* müssen die folgende Transaktion des Integrationsprofils IHE ATNA und seiner nationalen Anpassung gemäss Anhang 5 der EPDV-EDI unterstützen:
2.9.18.1 Record Audit Event [ITI-20]

**Akteure und Transaktionen der nationalen Integrationsprofile – Autorisierungsentscheid abfragen**

2.9.19 Die Gruppierung anderer Akteure mit dem Akteur *Authorization Decision Consumer* des nationalen Integrationsprofils CH:ADR richtet sich nach den dort spezifizierten Vorgaben und ist dem entsprechend sicherzustellen.

2.9.20 Die Akteure *Authorization Decision Provider*, *Authorization Decision Consumer* und *Policy Repository* müssen die Transaktionen des nationalen Integrationsprofils CH:ADR gemäss den technischen Spezifikationen nach Anhang 5 der EPDV-EDI unterstützen.

**Akteure und Transaktionen der nationalen Integrationsprofile – Berechtigungskonfiguration managen**

2.9.21 Die Akteure *Policy Repository* und *Policy Manager* müssen die Transaktion des nationalen Integrationsprofils CH:PPQ gemäss der technischen Spezifikation nach Anhang 5 der EPDV-EDI unterstützen.

**Authentisierung mit gültigen Zertifikaten**

2.9.22 Gemeinschaften müssen über ein gültiges elektronisches Zertifikat verfügen, das bei einer nach dem Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur anerkannten Anbieterin von Zertifikatsdiensten bezogen wurde, für:

2.9.22.1 die gegenseitige Authentisierung ihrer Zugangspunkte;

2.9.22.2 die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber den Abfragediensten nach Artikel 38 Absatz 1 Buchstaben a bis c EPDV;

2.9.22.3 die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber gegenüber der Identifikationsdatenbank der ZAS.

2.9.23 Gemeinschaften müssen für den Datenaustausch mit den Abfragediensten nach Artikel 38 Absatz 1 Buchstabe a die Transaktionen des Integrationsprofils IHE ATNA verwenden.

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

**Konsistente Zeit der Schweiz**

2.9.25 Für Zeitstempel in der Kommunikation und Protokollierung ist die gesetzliche Zeit der Schweiz der METAS zu verwenden. Die Uhren aller relevanten informationsverarbeitenden Systeme müssen mit der gesetzlichen Zeit der Schweiz synchronisiert sein.

### 2.10 Protokolldaten (Abs. 3 Bst. e)

**Anforderungen an das Protokollierungssystem:**

2.10.1 Jede Bearbeitung von Daten des elektronischen Patientendossiers ist zu protokollieren und mit Zeitstempel zu versehen.

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

2.10.3 Es gelten folgende Anforderungen:

2.10.3.1 vorgesehene Protokollierungen dürfen nicht umgangen werden können;

2.10.3.2 eine nachträgliche Veränderung von Protokolldaten darf nicht möglich sein;
2.10.3.3 bei der Protokollierung muss unterschieden werden zwischen Zugriffen, die aus der Nutzung des elektronischen Patientendossiers resultieren und für Patientinnen und Patienten einsehbar sein müssen sowie technisch-administrativen Zugriffen im Rahmen des Systembetriebs;
2.10.3.4 für Systemadministratoren darf keine Möglichkeit bestehen, die Protokollierung ihrer eigenen Aktivitäten zu löschen oder zu deaktivieren.

2.10.4 Protokolleinträge für die Einsichtnahme durch den Patienten oder die Patientin sind jedes Mal dann zu erzeugen, wenn
2.10.4.1 folgende Daten bearbeitet werden:
2.10.4.1.1 die Dokumente in den Dokumentenablagen;
2.10.4.1.2 die Einträge im Dokumentenregister;
2.10.4.1.3 die Konfiguration der Berechtigungssteuerung;
2.10.4.1.4 die Daten des Patientenindex.
2.10.4.2 folgende Ereignisse auftreten:
2.10.4.2.1 die Authentifizierung am System (Login/Logout);
2.10.4.2.2 erfolgreiche und abgewiesene Versuche auf das System zuzugreifen;
2.10.4.2.3 die Suche nach dem Patientendossier;
2.10.4.2.4 die Suche nach Dokumenten eines Patientendossiers;
2.10.4.2.5 ein erfolgter Notfallzugriff;
2.10.4.2.6 erfolgreiche und abgewiesene Versuche auf Dokumente zuzugreifen;
2.10.4.2.7 die Registrierung eines neuen Identifikationsmittels.

2.10.5 Bei Aufruf einer Suchfunktion muss das Protokoll mindestens enthalten:
2.10.5.1 verwendete Such- bzw. Abfragekriterien (z. B. verwendete Identifikatoren, Name, Geburtsdatum, etc.);
2.10.5.2 Angaben zum Ergebnis der Abfrage (z. B. Anzahl Ergebnisse);
2.10.5.3 etwaige Folgeaktionen (z. B. Auswahl eines Datensatzes aus einer Trefferliste, Druck, Datenexport).

2.10.6 Die Protokolldaten sind 10 Jahre aufzubewahren.

2.10.7 Der Abruf und die Darstellung der Protokollinformationen für die Einsichtnahme durch den Patienten oder die Patientin richtet sich nach den nationalen Anpassungen zum IHE-Integrationsprofil ATNA («Audit Trail Consumption») und dem dort enthaltenen technischen Austauschformat für Protokollinformationen in Anhang 5 der EPDV-EDI.

### 2.11 Verknüpfung der Patientenidentifikationsnummer mit Dokumenten (Abs. 3)

2.11.1 Gemeinschaften müssen sicherstellen, dass die Patientenidentifikationsnummer der ZAS nicht persistent in den Dokumentenablagen oder Dokumentenregistern gespeichert wird und in den Primärsystemen nicht direkt und dauerhaft mit Dokumenten der Patientinnen und Patienten verknüpft wird.

# 3 Zugangsportal für Gesundheitsfachpersonen (Art. 10 EPDV)

### 3.1 Konformität mit gesetzlichen Bestimmungen

3.1.1 Das Zugangsportal für Gesundheitsfachpersonen muss den einschlägigen rechtlichen Anforderungen entsprechen.

### 3.2 Darstellung

3.2.1 Die Darstellung auf den Benutzeroberflächen des Zugangsportals muss korrekt und vollständig sein und klar erkennen lassen:
3.2.1.1 ob ein Dokument durch eine oder durch den Patienten oder die Patientin selbst bereitgestellt wurde;
3.2.1.2 welche Dokumente von der zugreifenden Gesundheitsfachperson selbst bereitgestellt wurden;
3.2.1.3 welche Dokumente annulliert wurden;
3.2.1.4 welche Versionen eines Dokumentes gegebenenfalls auch vorhanden sind

### 3.3 Barrierefreiheit

3.3.1 Das Zugangsportal muss:
3.3.1.1 so ausgestaltet sein, dass behinderte oder ältere Gesundheitsfachpersonen dieses barrierefrei nutzen können;
3.3.1.2 den Konformitätsbedingungen gemäss Web Content Accessibility Guidelines (WCAG) 2.0 entsprechen und die Konformitätsstufe AA erreichen.

### 3.4 Dateiformate: Bereitstellung

3.4.1 Das Zugangsportal muss:
3.4.1.1 die Möglichkeit bieten, die gemäss Anhang 3 der EPDV-EDI zugelassenen Dateiformate bereitzustellen;
3.4.1.2 die Dateien anderer Formate vor dem Abspeichern in der Dokumentenablage in ein zugelassenes Format umwandeln.

### 3.5 Dateiformate: Abruf

3.5.1 Das Zugangsportal muss:
3.5.1.1 die Möglichkeit bieten, die gemäss Anhang 3 der EPDV-EDI zugelassenen Dateiformate abzurufen;
3.5.1.2 den Abruf von Dateien zum Abspeichern im Primärsystem unterstützen («Download»);
3.5.1.3 die Möglichkeit bieten, ausgewählte Dokumente nicht nur einzeln, sondern auch gesammelt («bulk download») herunterzuladen;
3.5.1.4 strukturierte Daten menschenlesbar, korrekt und vollständig darstellen;
3.5.1.5 die Möglichkeit bieten, dass strukturierte Daten sowohl im Originalformat, als auch als menschenlesbares Format heruntergeladen werden können.

3.5.2 Für den Abruf von Dokumenten zur Darstellung oder zum Abspeichern sind zulässige Obergrenzen für die erlaube Anzahl von Dokumenten pro Zeiteinheit («rate limits») zu definieren, welche beim Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen auslösen.

# 4 Datenschutz und Datensicherheit (Art. 11 EPDV)

### 4.1 Anforderungen an Dritte

4.1.1 Die Sicherstellung der Anforderungen dieses Kapitels (Datenschutz und Datensicherheit) liegt auch dann in der Verantwortung der Gemeinschaften, wenn sie Leistungen durch Dritte (Betriebsorganisationen) erbringen lassen.

### 4.2 Datenschutz- und Datensicherheitsmanagementsystem (Abs. 1)

4.2.1 Gemeinschaften müssen ein Datenschutz- und Datensicherheitsmanagementsystem, wie in der Norm ISO/IEC 27001:2013 definiert, betreiben, dass:

4.2.1.1 alle einzuhaltenden gesetzlichen Anforderungen an die besonders schützenswerten Datenbestände ausdrücklich definiert und auf aktuellem Stand hält;

4.2.1.2 die zur deren Erfüllung notwendigen spezifischen Massnahmen und die für deren Überwachung verantwortlichen Personen festlegt;

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

4.2.2 Das Datenschutz- und Datensicherheitsmanagementsystem muss mindestens umfassen:

4.2.2.1 einen von der oder dem Datenschutz- und Datensicherheitsverantwortlichen (vgl. Kap. 4.3) beurteilten Risikokatalog;

4.2.2.2 einen Risikobehandlungsplan;

4.2.2.3 ein aktuell gehaltenes Inventar der folgenden Betriebsmittel (vgl. Kap. 4.8):

4.2.2.3.1 Hardware;

4.2.2.3.2 Software;

4.2.2.3.3 Datenbestände;

4.2.2.3.4 Aufbauorganisation;

4.2.2.3.5 Prozesse.

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

4.2.4 Mindestens jährlich ist ein Management Review durchzuführen, bei dem die Geschäftsleitung der Gemeinschaft über den Risikokatalog und den Risikobehandlungsplan befindet.

### 4.3 Datenschutz- und Datensicherheitsverantwortlicher (Abs. 1 Bst. a)

4.3.1 Für das Führen des Datenschutz- und Datensicherheitsmanagementsystems der Gemeinschaft ist ein Datenschutz- und Datensicherheitsverantwortlicher zu benennen und dessen Aufgabenprofil zu definieren, der die Einhaltung der Datenschutz- und Datensicherheitsvorschriften überwacht und:

4.3.1.1 seine Funktion fachlich unabhängig ausüben kann;

4.3.1.2 über die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen verfügt;

### 4.4 Erkennen von Sicherheitsvorfällen (SIEM) (Abs. 1 Bst. b)

4.4.1 Gemeinschaften müssen:

4.4.1.1 ein System zur Erkennung von und zum Umgang mit Sicherheitsvorfällen (*Security Information and Event Management System* [SIEM]) betreiben, das alle relevanten Systeme der gemeinschaftsinternen Informatikinfrastruktur risikogerecht überwacht, Anomalien im System erkennt und Datenschutz- und Datensicherheitsereignisse aufzeichnet.

4.4.1.2 diese Aufzeichnungen vor Veränderungen und Löschungen schützen.

4.4.1.3 sicherstellen, dass Datenschutz- und Datensicherheitsereignisse angemessen organisatorisch und technisch gemäss Kap. 4.5 adressiert werden.

4.4.2 Das SIEM muss gemeinschaftsspezifisch aufgebaut werden und mindestens die folgenden Muster erkennen und adressieren:

4.4.2.1 Angriffe aus dem Internet auf das Zugangsportal oder auf den Zugangspunkt der Gemeinschaft;

4.4.2.2 unübliche Häufungen schreibender oder lesender Zugriffe auf die Dokumentenablagen, das Dokumentenregister oder den Patientenindex, welche auf eine missbräuchliche Nutzung oder automatisierte Attacke hinweisen;

4.4.2.3 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, analog dem Abfragedienst für Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 40 EPDV («lokaler HPD»).

### 4.5 Umgang mit Sicherheitsvorfällen (SIEM) (Abs. 1 Bst. b)

4.5.1 Gemeinschaften müssen:

4.5.1.1 formale Verfahren für das unverzügliche Melden von Datenschutz- oder Datensicherheitsereignissen an die vorgegebenen Stellen und für die Eskalation (Meldung an BAG und Zertifizerungsstelle nach Art. 11 Abs. 2) definiert haben sowie deren Einhaltung einfordern und kontrollieren;

4.5.1.2 sicherstellen, dass diese Verfahren und die daraus resultierenden Verpflichtungen allen betroffenen Mitarbeitenden der Gesundheitseinrichtungen sowie der Betriebsorganisationen bekannt sind.

4.5.2 Das SIEM:

4.5.2.1 umfasst Prozesse für den Umgang mit Sicherheitsereignissen;

4.5.2.2 definiert bei sicherheitskritischen Ereignisse einer definierten Stufe mindestens die folgenden Notfallprozesse zur sofortigen Unterbindung sämtlicher Kommunikation:

4.5.2.2.1 wie und unter welchen Bedingungen die Gemeinschaft durch das Sperren des Zugangspunktes der Gemeinschaft von der Bearbeitung von Daten des elektronischen Patientendossiers isoliert wird;

4.5.2.2.2 wie und unter welchen Bedingungen die Gemeinschaft vom Internet isoliert wird;

4.5.2.2.3 wie und unter welchen Bedingungen die Gemeinschaft von einem angebundenen Primärsystem isoliert wird.

### 4.6 Schutz vor Schadcode (Abs. 1 Bst. b)

4.6.1 Gemeinschaften müssen sicherstellen, dass
4.6.1.1 sie Massnahmen, Verfahren und Systeme zum Schutz bzw. zum Erkennen und Entfernen von Schadsoftware und zur Überwachung von mobilem Programmcode (z. B. Viren) festlegen und umsetzen, respektive einsetzen;
4.6.1.2 die Systemverantwortlichen die Aktualität der eingesetzten Software zur Erkennung und Entfernung von Schadsoftware regelmässig überprüfen.

### 4.7 Umgang mit Sicherheitsschwachstellen (Abs. 1 Bst. b)

4.7.1 Gemeinschaften müssen über ein Sicherheitsschwachstellenmanagement verfügen, welches Informationen über technische Sicherheitsschwachstellen von verwendeten Informationssystemen rechtzeitig einholt, die Anfälligkeit der Organisation für eine Ausnutzung solcher Sicherheitsschwachstellen bewertet und angemessene Massnahmen für den Umgang mit den damit einhergehenden Risiken ergreift.

4.7.2 Software-Aktualisierungen zur Beseitigung von Sicherheitsschwachstellen (sog. «*Patches*») müssen vor der Installation getestet und auf allfällige unerwünschte Wirkungen hin beurteilt werden.

4.7.3 Steht für die Beseitigung einer Sicherheitsschwachstelle noch kein «*Patch*» zur Verfügung, müssen alternative Sicherheitsmassnahmen in Betracht gezogen werden (z. B. Anpassung der Zugriffskontrollen oder Einschränkung des Netzwerkverkehrs).

### 4.8 Verwaltung schützenswerter Daten und Systeme (Abs. 1 Bst. c und d)

4.8.1 Gemeinschaften müssen sicherstellen, dass die angeschlossenen Gesundheitseinrichtungen über Regelungen verfügen, dass nur behandlungsrelevante Daten aus der Krankengeschichte der Patientin oder des Patienten im elektronischen Patientendossier zugänglich gemacht werden dürfen.

4.8.2 Gemeinschaften müssen sicherstellen, dass alle schützenswerten Daten, Systeme und Einrichtungen des elektronischen Patientendossiers eindeutig identifiziert, klassifiziert und in einem Inventar erfasst werden.

4.8.3 Im Inventar müssen mindestens folgende Systeme erfasst und verwaltet werden:
4.8.3.1 die Dokumentenablagen;
4.8.3.2 das Dokumentenregister;
4.8.3.3 die Protokollierungssysteme;
4.8.3.4 das System zur Berechtigungssteuerung;
4.8.3.5 das Identitäts- und Zugangsmanagement-System (IAM);
4.8.3.6 der Patientenindex;
4.8.3.7 die datenschutz- oder datensicherheitsrelevanten Datenbestände des Systembetriebs (z.B. Logs, Backups, privilegiertes Zugangs Management für Systemadministratoren).
4.8.3.8 die Primärsysteme mit den Rollen (IHE-Aktoren) *Document Source* und *Document Consumer*. Das Inventar umfasst für diese Elemente zusätzlich mindestens:
4.8.3.8.1 das TLS-Clientzertifikat für die Transportschichtsicherheit (TLS) des jeweiligen IHE-Aktors.

4.8.4 Zu jedem Element im Inventar muss:
4.8.4.1 ein verantwortlicher Eigentümer zugeordnet werden;

4.8.4.2 die ursprüngliche Quelle der enthaltenen Daten ersichtlich sein;
4.8.4.3 das Datum der letzten Bestätigung durch den oder die Datenschutz- und Datensicherheitsverantwortliche geführt werden.

4.8.5 Der oder die Datenschutz- und Datensicherheitsverantwortliche muss das Inventar mindestens jährlich überprüfen.

### 4.9 Datenschutz- und Datensicherheitsanforderungen für die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen, sowie Endgeräte (Bst. e)

4.9.1 Gemeinschaften müssen Datenschutz- und Datensicherheitsvorgaben für Gesundheitseinrichtungen und deren Gesundheitsfachpersonen vorsehen, die sicherstellen, dass:
4.9.1.1 die Gesundheitseinrichtungen auf die einzuhaltenden Sicherheitsmassnahmen (vgl. Kapitel 1.1.2.1) hingewiesen werden;
4.9.1.2 die Gesundheitseinrichtungen dazu verpflichten, ihre auf das elektronische Patientendossier zugreifenden Gesundheitsfachpersonen über die Aufgaben, Rechte und Pflichten im Zusammenhang mit der Bearbeitung von Daten des elektronischen Patientendossiers sowie Risiken und Massnahmen bezüglich Datenschutz und Datensicherheit zu informieren und zur Einhaltung der geforderten Massnahmen zu verpflichten. Die Verpflichtung und Information muss mindestens folgende Punkte umfassen:
4.9.1.2.1 den sicheren Umgang mit Identifikationsmitteln und Zugangsdaten;
4.9.1.2.2 die Prinzipien der Beschreibung von bereitzustellenden Dokumenten mit Metadaten;
4.9.1.2.3 die Massnahmen zur sicheren Nutzung von Endgeräten (PC, Smartphone, Tablet, etc.);
4.9.1.2.4 das Verhalten zur Abwehr von an Gesundheitsfachpersonen gerichtete Bedrohungen wie z. B. «Social Engineering», «Phishing», Umgang mit externen Speichermedien, etc.;
4.9.1.2.5 die Kontaktstellen und Verfahren zur Meldung von Datenschutz- und Datensicherheitsvorfällen;
4.9.1.2.6 die Verantwortlichkeiten beim Einsatz von Hilfspersonen.

**Sichere Endgeräte für Gesundheitsfachpersonen**

4.9.2 Gemeinschaften verpflichten die angeschlossenen Gesundheitseinrichtungen dazu, eine sichere Konfiguration derjenigen Endgeräte sicherzustellen, die von den Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier genutzt werden.

4.9.3 Die Konfiguration der Endgeräte muss mindestens umfassen:
4.9.3.1 den Einsatz einer regelmässig aktualisierten Software gegen Schadprogramme;
4.9.3.2 den Einsatz netzwerktechnischer Schutzsysteme (z. B. Firewalls);
4.9.3.3 eine restriktive Handhabung von Systemadministratorrechten für normale Endsystem-Benutzer;
4.9.3.4 eine regelmässige Aktualisierung des Betriebssystems und sicherheitskritischer Software-Komponenten (z. B. Laufzeitumgebungen wie Java, .Net, etc.).

### 4.10 Datenschutz- und Datensicherheitsanforderungen an das Personal (Abs. 1 Bst. f)

4.10.1 Gemeinschaften müssen über ein Regelwerk verfügen, in dem die Regeln zur Zugriffskontrolle und Berechtigungen für jeden Benutzer oder jede Benutzergruppe klar

festgelegt und in den entsprechenden informationsverarbeitenden Systemen und Netzwerkdiensten umgesetzt sind.

4.10.2 Gemeinschaften müssen sicherstellen, dass:

4.10.2.1 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 bewusst nachkommen;

4.10.2.2 Anforderungen für den Gebrauch geheimer Authentisierungsinformationen, wie z. B. Passwörter, erstellt und kommuniziert werden;

4.10.2.3 Personen, die Zugang zu Daten des elektronischen Patientendossier erlangen könnten, einer der ärztlichen Schweigepflicht analogen Verpflichtungen unterliegen;

4.10.2.4 definierte Prozesse für das Personalmanagement definiert umgesetzt und eingehalten werden.

4.10.3 Gemeinschaften müssen:

4.10.3.1 eine von dem oder der Datenschutz- und Datensicherheitsverantwortlichen der Gemeinschaft visierte Liste aller Personen führen, die – unabhängig von der Rechteverwaltung im elektronischen Patientendossier – Zugriff auf Patientendaten haben («Liste der Schlüsselpersonen»);

4.10.3.2 diese Personen eine Personensicherheitsprüfung (PSP) nach Militärgesetz durchlaufen haben;

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

### 4.11 Datenschutz- und Datensicherheitsanforderungen an Dritte (Abs. 1 Bst. f)

4.11.1 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 IT-Infrastrukturkomponenten dafür bereitstellen.

4.11.2 Gemeinschaften müssen sicherstellen, kein Datenzugriff durch Intermediäre erfolgt und dass «Dritte», die unter Umständen im Rahmen der Bereitstellung von Dienstleistungen oder Infrastrukturkomponenten auf Daten des elektronischen Patientendossiers zugreifen könnten, dies nur zum Zwecke der Leistungserbringung für die Gemeinschaften tun und Daten des elektronischen Patientendossiers keinesfalls für andere Zwecke weiter verarbeiten oder weitergeben.

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

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

4.11.5 Die Liefervereinbarungen müssen mindestens folgende Bestimmungen umfassen:

4.11.5.1 Verpflichtungen des Lieferanten, die relevanten Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft beim Einsatz oder der Bereitstellung von Informations- und Kommunikationstechnologie-Produkten, Personal und/oder Dienstleistungen einzuhalten.

4.11.5.2 Anforderungen und Verfahren für den Umgang mit Datenschutz- und Datensicherheitsvorfällen;
4.11.5.3 die Angabe von Kontaktpersonen für Fragen und bei Vorkommnissen im Bereich Datenschutz- und Datensicherheit;
4.11.5.4 das Recht zur regelmässigen Überprüfung der Lieferantenprozesse und Kontrollmassnahmen im Zusammenhang mit dem Vertrag;
4.11.5.5 die Verpflichtung zur Einhaltung der Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft innerhalb der gesamten Lieferkette weiterzuverpflichten für den Fall, dass die Lieferanten Unterlieferanten beauftragen;
4.11.5.6 die Vorschriften und Kontrollmassnahmen für Unterverträge;
4.11.5.7 die Verpflichtung, die Gemeinschaft über jedwede Änderung in den Vertragsbeziehungen zu involvierten Unterlieferanten zu informieren.

### 4.12 Überwachung und Überprüfung von Dienstleistungen (Abs. 1 Bst. f)

4.12.1 Die von Dritten und allfälligen Unterlieferanten gelieferten Dienstleistungen, Berichte und Aufzeichnungen müssen von den Gemeinschaften regelmässig überwacht und überprüft werden, so dass sichergestellt ist, dass:
4.12.1.1 die vertraglich festgelegten Bedingungen für den Datenschutz- und die Datensicherheit eingehalten wurden;
4.12.1.2 Datenschutz- und Datensicherheitsvorfälle und -probleme angemessen bearbeitet wurden;
4.12.1.3 Änderungen der Dienstleistungen einem gelenkten Änderungsmanagement unterliegen.

### 4.13 Meldepflicht für Sicherheitsvorfälle (Abs. 2)

4.13.1 Gemeinschaften müssen formale Verfahren für das unverzügliche Melden von, gemäss dem Datenschutz- und Datensicherheitsmanagementsystem als sicherheitsrelevant eingestuften Vorfällen, an die Zertifizierungsstelle und das BAG definiert haben, sowie deren Einhaltung einfordern und kontrollieren.

### 4.14 Betriebssicherheit (Abs. 3)

4.14.1 Gemeinschaften müssen sicherstellen, dass:
4.14.1.1 Privilegierte Zugriffe auf die produktive Betriebsumgebung z. B. durch Betriebssystem-, Datenbank- und Applikations-Administratoren:
4.14.1.1.1 eine starke 2-Faktor Authentisierung erfordern;
4.14.1.1.2 durch ein unabhängig administriertes überwacht und protokolliert werden;
4.14.1.1.3 keinen Export von Patientendaten ermöglichen.
4.14.1.2 externe Zugriffe durch Dritte und Nachauftragnehmer und insbesondere privilegierte externe Zugriffe auf die produktive Betriebsumgebung zusätzlich:
4.14.1.2.1 entweder unterbunden oder angemessen geschützt sind;
4.14.1.2.2 überwacht und protokolliert werden;
4.14.1.2.3 nur befristet und bei Bedarf aktiviert werden.
4.14.1.3 Entwicklungs-, Test- und Inbetriebnahme-Aktivitäten neuer Systeme in ihren Umgebungen nachvollziehbar dokumentiert und nach einem kontrollierten Prozess ablaufen;
4.14.1.4 vollständige Backups gemacht werden und dass diese verschlüsselt sind;
4.14.1.5 das Schlüsselmaterial für die Verwaltung der Backups dem 4-Augenprinzip unterliegt;

4.14.1.6 Backups mit einem Zeitstempel versehen werden;
4.14.1.7 Backups integritätsgeschützt auf einem separaten Speicher gespeichert werden und diese nach dem Kopieren vom Netzwerk getrennt werden;
4.14.1.8 die Verfahren zur Systemwiederherstellung ausreichend dokumentiert sind und regelmässig erprobt werden;
4.14.1.9 die technischen Logs keine unverschlüsselten Patientendaten enthalten;
4.14.1.10 Logfiles mit einem Zeitstempel versehen werden und integritätsgeschützt gespeichert werden;
4.14.1.11 Datenträger mit Patientendaten stets korrekt entsorgt und vorgängig alle Daten gelöscht werden;
4.14.1.12 die Systemuhren mit der gesetzlichen Zeit der Schweiz abgeglichen sind;

4.14.2 Die Produktivumgebung der gemeinschaftsinternen Informatikinfrastruktur des elektronischen Patientendossiers muss:
4.14.2.1 von anderen Umgebungen (z. B. Entwicklungs-, Abnahme- und Testumgebungen) isoliert sein;
4.14.2.2 ausschliesslich im Rahmen kontrolliert ablaufender Prozesse mit neuer Software versorgt werden;
4.14.2.3 regelmässig auf Sicherheitsschwachstellen überprüft werden.
4.14.2.4 die erkannten Sicherheitsschwachstellen im Rahmen eines kontrollierten Patch-Management-Prozesses beheben;
4.14.2.5 von anderen Systemen des Betreibers mittels eigener Netwerkzonierung isoliert sein;

4.14.3 Neben der Bearbeitung von Daten des elektronischen Patientendossiers durch Gesundheitsfachpersonen sowie Patienten und Patientinnen sind mindestens folgende Informationen von Ereignissen, die im Rahmen des Systembetriebs auftreten, aufzuzeichnen:
4.14.3.1 Datum, Zeit und Details von Schlüssel-Ereignissen (z. B. Login und Logout);
4.14.3.2 erfolgreiche und abgewiesene Versuche auf das System zuzugreifen;
4.14.3.3 erfolgreiche und abgewiesene Versuche auf Daten oder Dokumente zuzugreifen;
4.14.3.4 Veränderungen an der Systemkonfiguration;
4.14.3.5 die Verwendung von privilegierten Zugriffsrechten;
4.14.3.6 Netzwerkadressen und -protokolle;
4.14.3.7 die Aktivierung und Deaktivierung von Schutz- oder Authentisierungs-Systemen;
4.14.3.8 die Modifikation von Systemberechtigungen und Zugängen;
4.14.3.9 das Anlegen, die Modifikation oder das Löschen von Benutzerkonten («Accounts»);
4.14.3.10 das Kopieren oder Ausdrucken von besonders schützenswerten Informationen.

### 4.15 Anschaffung, Entwicklung und Instandhaltung von Systemen (Abs. 3)

4.15.1 Gemeinschaften müssen den Datenschutz und die Datensicherheit über den gesamten Lebenszyklus der Systeme des elektronischen Patientendossiers sicherstellen. Dazu müssen formale Prozesse definiert, eingeführt und eingehalten werden für die Dokumentation, die Spezifikation, das Testen, die Qualitätskontrolle und die kontrollierte Umsetzung bei:
4.15.1.1 der Einführung oder der Entwicklung neuer Systeme;
4.15.1.2 grösseren Änderungen oder Entwicklungen an bestehenden Systemen;
4.15.1.3 dem Wechsel der Betriebsplattformen.

4.15.2 Mindestens ist nachzuweisen, dass innerhalb jedes Entwicklungszyklus:
4.15.2.1 Sicherheitsanforderungen bereits in der Planung mittels einer strukturierten Anforderungsanalyse noch vor allfälligen Entwicklungsaufträgen oder Erweiterungen von bestehenden Informationssystemen definiert werden;
4.15.2.2 Änderungen an Systemen einem formalen, dokumentierten Verfahren zur Änderungskontrolle unterliegen;

4.15.2.3 der Zugriff auf den Software-Quellcode beschränkt, kontrolliert und protokolliert wird;
4.15.2.4 Leitlinien für die sichere Entwicklung, auch bei ausgelagerten Systementwicklungstätigkeiten vorhanden sind und im Entwicklungszyklus angewandt und umgesetzt werden;
4.15.2.5 sich in Testumgebungen keine Patientendaten befinden;
4.15.2.6 ausgelagerte Softwareentwicklung durch die Betriebsorganisation überwacht und beaufsichtigt werden.

### 4.16 Verschlüsselung in der Kommunikation (Abs. 3)

4.16.1 Gemeinschaften müssen sicherstellen, dass jegliche Übertragung von Daten des elektronischen Patientendossiers innerhalb der Gemeinschaft wie auch zwischen Gemeinschaften durch geeignete und dem Stand der Technik entsprechende kryptographische Massnahmen gegen den Verlust der Vertraulichkeit, Authentizität und Integrität abgesichert werden.

### 4.17 Verschlüsselte Datenspeicherung (Abs. 3)

4.17.1 Besonders schützenswerte Daten des elektronischen Patientendossiers müssen mit geeigneten und dem Stand der Technik entsprechenden kryptographischen Massnahmen verschlüsselt und integritätsgeschützt gespeichert werden.

### 4.18 Verwaltung kryptographischer Schlüssel (Abs. 3)

4.18.1 Gemeinschaften müssen sicherstellen, dass:
4.18.1.1 Verfahren für die Erzeugung, die Verteilung, die Aktivierung, die Aktualisierung, den Widerruf oder Deaktivierung und die Löschung von kryptographischen Schlüsseln definiert, umgesetzt und kontrolliert werden;
4.18.1.2 die verwendeten kryptographischen Schlüssel gegen Veränderung und Verlust geschützt werden;
4.18.1.3 geheime und private Schlüssel vor unbefugter Benutzung und Offenlegung geschützt werden;
4.18.1.4 Einrichtungen zur Erzeugung, Speicherung und Archivierung von Schlüsseln physisch geschützt werden.

### 4.19 Kommunikationssicherheit: Verwaltung von Netzwerken (Abs. 3)

4.19.1 Gemeinschaften müssen sicherstellen, dass:
4.19.1.1 Richtlinien zur Netzwerksicherheit definiert, eingehalten und kontrolliert werden;
4.19.1.2 Netzwerke so verwaltet werden, dass Daten des elektronischen Patientendossiers in Anwendungen und Systemen vor unautorisierten Zugriffen geschützt sind;
4.19.1.3 Regelungen der Zuständigkeiten für die Verwaltung von Netzwerken innerhalb einer Gemeinschaft definiert, eingehalten und kontrolliert werden.

### 4.20 Kommunikationssicherheit: Netzwerkdienste (Abs. 3)

4.20.1 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, indem:

4.20.1.1 geeignete sichere Netzwerkstrukturen festgelegt, durch Netzwerkpläne dargestellt und umgesetzt werden, wodurch dedizierte Gruppen von Informationsdiensten, Benutzern und Informationssystemen in Netzwerken voneinander getrennt gehalten werden können. Insbesondere müssen Firewalls, Router, Switches, etc. und technologische Umsetzungen für Netzwerkdienste derart konfiguriert sein, dass:

4.20.1.1.1 die technischen Schnittstellen der gemeinschaftsinternen Informatikinfrastruktur einer Gemeinschaft («IHE-Services») nur von Systemen aufgerufen werden dürfen, die zu einer zertifizierten Gemeinschaft gehören;

4.20.1.1.2 Systeme, die über das Internet auf einen IHE-Service zugreifen, sich gegenüber den IHE-Services mittels TLS-Serverauthentisierung mit einem gültigen elektronischen Zertifikat authentisieren. Dabei müssen:

4.20.1.1.2.1 für Zugangsportale sowie *Responding Gateways* mindestens öffentliche *Extended-Validation*-TLS-Zertifikate eingesetzt werden;

4.20.1.1.2.2 für andere IHE-Services entweder mindestens öffentliche *Extended-Validation*-TLS-Zertifikate eingesetzt werden oder TLS-Zertifikate, die nur innerhalb der Gemeinschaft gültig sind.

4.20.1.1.3 alle IHE-Services, die aus dem Internet aufrufbar sind, das aufrufende System mittels *TLS-Client-Authentication* authentisieren;

4.20.1.1.4 *Responding Gateways* den Verbindungsaufbau nur zulassen, wenn das aufrufende System zu einer zertifizierten Gemeinschaft gehört;

4.20.1.1.5 alle gemeinschaftsinternen IHE-Services, die nicht aus dem Internet aufgerufen werden können, den Verbindungsaufbau nur zulassen, wenn das aufrufende System zur eigenen zertifizierten Gemeinschaft gehört und im Inventar der eigenen Gemeinschaft registriert und vom ISBO der Gemeinschaft akzeptiert wurde;

4.20.1.2 die hierzu eingesetzten Verfahren (z. B. Client-Server-Zertifikate, IP- oder MAC-Adress-Filter) dokumentiert werden.

4.20.2 Gemeinschaften müssen:

4.20.2.1 alle Systeme mit persistent gespeicherten Daten des elektronischen Patientendossiers der Gemeinschaft (namentlich Dokumentenregister, Dokumentenablage, Berechtigungssteuerung und Patientenindex) netzwerktechnisch von allen anderen Systemen separieren, die ein tieferes Sicherheitsniveau aufweisen;

4.20.2.2 die hierzu eingesetzten Verfahren (z. B. Netzwerksegmentierung mittels Firewalls) dokumentieren.

4.20.3 Gemeinschaften müssen insbesondere das zum Schutz des Zugangsportals implementierte Sicherheitsdispositiv dokumentieren. Die Dokumentation umfasst mindestens:

4.20.3.1 die Netzwerktopologie und das Ausweisen der sog. «demilitarisierten Zone» (DMZ);

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

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

### 4.21 Ablauf von Netzwerk-Sitzungen («*Session timeout*») (Abs. 3)

4.21.1 Inaktive Netzwerk-Sitzungen müssen nach einer definierten Inaktivitätsperiode (20 Minuten bei Patienten, 2 Stunden bei Gesundheitsfachpersonen) beendet werden.

4.21.2 Die Authentisierung auf den Zugangsportalen und Endgeräten muss vor dem nächsten Zugriff erneut durchgeführt werden, wenn während 20 Minuten bei Patienten, beziehungsweise 2 Stunden bei Gesundheitsfachpersonen keine Interaktion des Benutzers mit dem elektronischen Patientendossier stattfand.

### 4.22 Zwischenspeicher (Abs. 3)

4.22.1 Elemente der gemeinschaftsinternen Informatikinfrastruktur, die der Übermittlung von Dokumenten des elektronischen Patientendossiers dienen (namentlich die Zugangspunkte), dürfen diese nicht persistent speichern.

### 4.23 Verfügbarkeit (Abs. 3)

4.23.1 Gemeinschaften müssen sicherstellen, dass:

4.23.1.1 die technischen Dienste zur Nutzung des elektronischen Patientendossiers vor Unterbrechungen geschützt sind, so dass grössere Störungen nur eingeschränkte und vertraglich vereinbarte Auswirkungen auf die Informationsverarbeitungssysteme haben und eine rechtzeitige Wiederaufnahme sämtlicher Dienste sichergestellt werden kann;

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

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

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

### 4.24 Datenspeicher unter Schweizer Rechtshoheit (Abs. 4)

4.24.1 Die Gemeinschaft muss sicherstellen, dass der Betrieb der gemeinschaftsinternen Datenspeicher des elektronischen Patientendossiers (insbesondere Dokumentenablagen, Dokumentenregister, Patientenindex) von juristischen Personen erbracht wird, die:

4.24.1.1 unter Schweizer Recht sind;

4.24.1.2 für die Erbringung der Leistung ausschliesslich unter Schweizer Recht handeln;

4.24.1.3 sich zur Mehrheit in Schweizer Eigentum befinden;

4.24.1.4 die Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erbringen.

# 5 Kontaktstelle für Gesundheitsfachpersonen (Art. 12 EPDV)

5.1.1 Die Gemeinschaften müssen für die Gesundheitsfachpersonen eine Kontaktstelle («*Service-Desk*») bezeichnen, die diese im Umgang mit dem elektronischen Patientendossier unterstützt.

5.1.2 Gemeinschaften müssen mindestens sicherstellen, dass:

5.1.2.1 die Mitarbeitenden des «Service-Desk» ihre Aufgaben, Rechte und Pflichten sowie die Risiken und die Massnahmen bezüglich Datenschutz und Datensicherheit kennen;

5.1.2.2 die Mitarbeitenden mit Zugriff auf Daten des elektronischen Patientendossiers sorgfältig ausgewählt werden und einer der ärztlichen Schweigepflicht analogen Verpflichtung unterstehen;

5.1.2.3 die Einwilligung der Mitarbeitenden zu den spezifischen Richtlinien der Gemeinschaft dokumentiert wird;

5.1.2.4 Remote-Zugriffe für Support-Tätigkeiten auf die Endgeräte der Gesundheitsfachpersonen ausschliesslich mit Kenntnis und Einwilligung der jeweiligen Gesundheitsfachperson erfolgen können und automatisch dokumentiert werden.

# Zusätzliche Anforderungen für Stammgemeinschaften

## 6 Information der Patientin oder des Patienten (Art. 14 EPDV)

**6.1 Die Information der Patientin oder des Patienten nach Artikel 14 EPDV muss mindestens folgende Punkte umfassen:**

6.1.1 Informationen über den Zweck des elektronischen Patientendossiers.

6.1.2 Informationen zu den Grundzügen der Datenbearbeitung, mindestens über:
6.1.2.1 den Verbleib der Dokumente in den Primärsystemen und Dokumentenablagen;
6.1.2.2 das Recht auf Widerruf der vermuteten Einwilligung zur Bereitstellung von Dokumenten im Behandlungsfall sowie auf die Löschung bestimmter Dokumente;
6.1.2.3 die Möglichkeiten und Funktionen des Zugangsportals für Patientinnen und Patienten;
6.1.2.4 die Möglichkeit zur Einsichtnahme in die Protokollinformationen;
6.1.2.5 die Möglichkeit, einen Stellvertreter oder eine Stellvertreterin zu benennen;
6.1.2.6 die Möglichkeit, Gesundheitsfachpersonen nach Artikel 3 Buchstabe h EPDV zur Weitergabe von Zugriffsrechten zu ermächtigen.

6.1.3 Informationen zu den Folgen der Einwilligung und der Möglichkeit des Widerrufs, mindestens über:
6.1.3.1 die Freiwilligkeit der Einwilligung;
6.1.3.2 die Tatsache, dass nur ein Patientendossier gleichzeitig geführt werden kann;
6.1.3.3 die Modalitäten der Vergabe und Verwendung der Patientenidentifikationsnummer;
6.1.3.4 die Möglichkeit, die Stammgemeinschaft zu wechseln und die damit verbundenen Konsequenzen für den Datenverbleib sowie für allfällige Stellvertretungen und ermächtigte Gesundheitsfachpersonen;
6.1.3.5 die Möglichkeit des formlosen Widerrufs ohne Angabe von Gründen;
6.1.3.6 die Möglichkeit, nach einem Widerruf erneut ein elektronisches Patientendossier eröffnen zu können, dem eine neue Patientenidentifikationsnummer zugeordnet wird;

6.1.4 Informationen zu den Möglichkeiten der Erteilung von Zugriffsrechten nach den Artikeln 1 bis 3 EPDV, mindestens über:
6.1.4.1 die nach der Eröffnung geltenden Einstellungen für Zugriffsrechte von Gesundheitsfachpersonen und der Vertraulichkeitsstufe von Dokumenten;
6.1.4.2 die Möglichkeiten der Vergabe, Anpassung und des Entzugs von Zugriffsrechten an Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen;
6.1.4.3 die Möglichkeit, dass auch von den Gesundheitsfachpersonen registrierte Hilfspersonen mit dem Zugriffsrecht der verantwortlichen Gesundheitsfachperson zugreifen können;
6.1.4.4 die Möglichkeit des Zugriffs von Gesundheitsfachpersonen in medizinischen Notfallsituationen und die Möglichkeit, den Zugriff in medizinischen Notfallsituationen einzuschränken, zu erweitern oder ganz auszuschliessen;
6.1.4.5 die Möglichkeit einzelne Gesundheitsfachpersonen vollständig vom Zugriff auszuschliessen (Ausschlussliste);
6.1.4.6 die Möglichkeit für Mitarbeitende des «Service-Desks» Remote-Zugriffe auf die Endgeräte der Patienten oder der Patientin durchzuführen, sofern er oder sie die Einwilligung dazu

erteilt hat.

6.1.5 Informationen zu den empfohlenen Datenschutz- und Datensicherheitsmassnahmen, mindestens über:

6.1.5.1 die möglichen Restrisiken und die vorgesehenen Massnahmen bezüglich Datenschutz und Datensicherheit;

6.1.5.2 die sichere Authentisierung und den Umgang mit Identifikationsmitteln und Zugangsdaten;

6.1.5.3 die Prinzipien der Beschreibung von bereitzustellenden Dokumenten mit Metadaten;

6.1.5.4 die Massnahmen für eine sichere Nutzung von Endgeräten (PC, Smartphone, Tablet, etc.);

6.1.5.5 die Verhaltensempfehlungen zur Abwehr von patientengerichteten Bedrohungen wie z. B. «*Social Engineering*», «Phishing», etc.

# 7 Einwilligung (Art. 15 EPDV)

### 7.1 Die Prozesse für die Erstellung eines elektronischen Patientendossiers müssen definiert, dokumentiert, umgesetzt und eingehalten werden.

7.1.1 Der Prozess zur Erstellung eines elektronischen Patientendossiers muss sicherstellen, dass eine Einwilligung zur Eröffnung eines elektronischen Patientendossiers mit einer eigenhändigen Unterschrift des Patienten oder der Patientin eingeholt wird.

# 8 Verwaltung (Art. 16 EPDV)

### 8.1 Eintritt und Austritt von Patientinnen und Patienten (Abs. 1 Bst. a)

8.1.1 Die Prozesse für die Verwaltung von Patientinnen und Patienten müssen definiert, dokumentiert, umgesetzt und eingehalten werden. Die Prozesse müssen insbesondere sicherstellen, dass:

8.1.1.1 die jeweiligen Prozesse zur Sicherstellung Vorgaben nach den Buchstaben b–e definiert, dokumentiert, umgesetzt und eingehalten werden.

### 8.2 Identifikation der Patientinnen und Patienten (Abs. 1 Bst. b)

8.2.1 Die Prozesse zur Identifikation der Patientinnen und Patienten müssen definiert, dokumentiert, umgesetzt und eingehalten werden.

8.2.2 Der Prozess zur Identifikation einer Patientin oder eines Patienten muss sicherstellen, dass:

8.2.2.1 die Identifikation des Patienten oder der Patientin (Bst. b):

8.2.2.1.1 anhand des Identifikationsmittels eines nach Artikel 30 zertifizierten Herausgebers erfolgt, oder

8.2.2.1.2 den Anforderungen nach Artikel 23 Absatz 1 EPDV entspricht;

8.2.2.2 ein elektronisches Patientendossier nur dann neu erstellt wird, wenn zuvor sichergestellt wurde, dass zu der betreffenden Person nicht bereits ein elektronisches Patientendossier besteht;

8.2.2.3 der Patient oder die Patientin im Patientenindex der Stammgemeinschaft angelegt wird;

8.2.2.4 das Identifikationsmittel des Patienten oder der Patientin eindeutig mit seinem oder ihrem

elektronischen Patientendossier verknüpft wird (Bst. c);

8.2.2.5 eine Patientenidentifikationsnummer nach den Vorgaben der Artikel 5 und 6 EPDV angefordert und dem zu erstellenden elektronischen Patientendossiers korrekt zugeordnet wird (Bst. d);

8.2.2.6 die demographischen Daten der Identifikationsdatenbank der zentralen Ausgleichsstelle (ZAS) in den Patientenindex der Stammgemeinschaft übernommen werden (Bst. d);

### 8.3 Identifikation und Authentisierung (Abs. 1 Bst. c)

8.3.1 Für den Zugriff von Patientinnen und Patienten auf das elektronische Patientendossier dürfen nur gültige Identifikationsmittel verwendet werden, die von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurden.

8.3.2 Gemeinschaften müssen sicherstellen, dass die eindeutigen Identifikatoren der Identifikationsmittel von Patientinnen und Patienten sowie deren allfälligen Stellvertreterinnen und Stellvertretern zuverlässig mit der registrierten Identität der jeweiligen Person in der Gemeinschaft verbunden wird.

8.3.3 Gemeinschaften müssen sicherstellen, dass die Zugangsportale:

8.3.3.1 ein starkes Authentifizierungsverfahren nach aktuellem Stand der Technik mit mindestens zwei Authentifizierungsfaktoren als Voraussetzung für die Bearbeitung von Daten des elektronischen Patientendossiers unterstützen.

8.3.3.2 einen vertrauenswürdigen Endpunkt für die sichere Kommunikation mit dem Identitätsdienstleister (Herausgeber des Identifikationsmittels) gemäss Kapitel 3.2 (*P.TrustedCommunityEndpoint*) des Schutzprofils nach Art. 8 EPDV-EDI zur Verfügung stellen.

### 8.4 Wechsel der Stammgemeinschaft (Bst. e)

8.4.1 Die Prozesse zum Wechsel der Stammgemeinschaft durch einen Patienten oder eine Patientin müssen definiert, dokumentiert, umgesetzt und eingehalten werden.

8.4.2 Der Prozess zum Wechsel der Stammgemeinschaft muss sicherstellen, dass:

8.4.2.1 die individuelle Konfiguration der Berechtigungssteuerung in die neue Stammgemeinschaft überführt und von dieser übernommen werden kann. Dabei sind die Vorgaben zum technischen Format im nationalen Integrationsprofil CH:PPQ gemäss Anhang 5 der EPDV-EDI einzuhalten;

8.4.2.2 die Ermächtigung einer Gesundheitsfachpersonen gemäss Artikel 3 Buchstabe h EPDV aufgehoben wird;

8.4.2.3 die Möglichkeiten des Zugriff durch allfällige Stellvertreter oder Stellvertreterinnen eines Patienten oder einer Patientin aufgehoben wird.

### 8.5 Durchsetzen der Zugriffsentscheidung zur Bearbeitung der Berechtigungskonfiguration (Abs. 2): Zugriffsrechte (Art. 2 EPDV Abs. 1) und Optionen der Patientinnen und Patienten (Art. 3 EPDV)

**8.5.1** Stammgemeinschaften müssen sicherstellen, dass eine Bearbeitung der Konfiguration der Berechtigungssteuerung nur gemäss der zuvor eingeholten Zugriffssentscheidung erfolgen kann.

### 8.6 Berechtigungssteuerung (Abs. 2): Zugriffsrechte (Art. 2 EPDV Abs. 1 bis 4)

8.6.1 Patientinnen und Patienten müssen die Möglichkeit haben, die Zugriffsrechte für Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen zu vergeben und anzupassen. Dabei sind die Vorgaben von Artikel 2 Absätze 1 bis 4 EPDV einzuhalten.

8.6.2 Die einzuhaltenden Vorgaben betreffen insbesondere:
8.6.2.1 die Möglichkeit Zugriffsrechte einzelnen Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen Zugriffsrechte nach Artikel 1 Absatz 1 zuzuweisen;
8.6.2.2 die Gültigkeit der vergebenen Zugriffsrechte bis zum Entzug durch die Patientin oder den Patienten;
8.6.2.3 die korrekte Umsetzung der mit dem Ein- oder Austritt einer Gesundheitsfachperson in eine Gruppe von Gesundheitsfachpersonen verbundenen Veränderungen der Zugriffsrechte nach Artikel 2 Absatz 4 EPDV, inklusive der Berücksichtigung allfälliger an sie individuell erteilter Zugriffsrechte;

### 8.7 Optionen der Patientinnen und Patienten (Art. 3 EPDV)

8.7.1 Stammgemeinschaften müssen sicherstellen, dass:
8.7.1.1 Patientinnen und Patienten die Optionen nach den Vorgaben von Artikel 3 EPDV nutzen können;
8.7.1.2 die Vorgaben von Artikel 3 korrekt umgesetzt werden.

8.7.2 Die einzuhaltenden Vorgaben betreffen die korrekte Umsetzung:
8.7.2.1 von zeitlich beschränkten Zugriffsrechten nach Artikel 3 Buchstabe a EPDV;
8.7.2.2 der Einschränkung, der Erweiterung und des Ausschlusses von Notfallzugriffen;
8.7.2.3 der Festlegung welche Vertraulichkeitsstufe neu eingestellten Daten zugewiesen wird;
8.7.2.4 des Ausschlusses einzelner Gesundheitsfachpersonen vom Zugriff auf das elektronische Patientendossier;
8.7.2.5 der Deaktivierung der Information nach Artikel 8 Buchstabe f;
8.7.2.6 der Festlegung, dass Gesundheitsfachpersonen, die in eine Gruppe von Gesundheitsfachpersonen eintreten, nicht automatisch das mit der Gruppe verbundene Zugriffsrecht erhalten;
8.7.2.7 der Benennung einer Stellvertretung;
8.7.2.8 der Ermächtigung von Gesundheitsfachpersonen zur Weitergabe ihrer Zugriffsrechte nach Massgabe von Buchstabe h EPDV;
8.7.2.9 die korrekte Auswertung der geltenden Berechtigungsregeln.

### 8.8 Stellvertretung (Art. 16 Abs. 3)

8.8.1 Stammgemeinschaften müssen der Patientin oder dem Patienten die Möglichkeit bieten, eine Stellvertretung zu benennen.

8.8.2 Die Stellvertreterin oder der Stellvertreter muss mittels eigenem Identifikationsmittel, das von einem nach Artikel 30 zertifizierten Herausgeber herausgegeben wurde, auf das elektronische Patientendossier der vertretenen Person zugreifen.

8.8.3 Die Stammgemeinschaft muss sicherstellen, dass:
8.8.3.1 die Identifikation des Stellvertreters oder der Stellvertreterin

8.8.3.1.1 anhand des Identifikationsmittels eines nach Artikel 30 zertifizierten Herausgebers erfolgt, oder
8.8.3.1.2 den Anforderungen nach Artikel 23 Absatz 1 EPDV entspricht;
8.8.3.2 die rechtlichen Voraussetzungen für die Wahrnehmung der Stellvertretung erfüllt sind;
8.8.3.3 die Stellvertretung nach Artikel 14 EPDV über die Grundzüge der Datenbearbeitung sowie die Möglichkeiten, Rechte und Pflichten im Zusammenhang mit der Nutzung des elektronischen Patientendossiers informiert wird;
8.8.3.4 das Identifikationsmittel der Stellvertretung, das von einem nach Artikel 30 EPDV zertifizierten Herausgebers herausgegeben wurde, eindeutig und korrekt mit dem elektronischen Patientendossier der vertretenen Person verknüpft wird;
8.8.3.5 dass der Zugang des Stellvertreters oder der Stellvertreterin zum elektronischen Patientendossier nur für die Dauer der Stellvertretung besteht.

# 9 Zugangsportal für Patientinnen und Patienten (Art. 17 EPDV)

## 9.1 Konformität mit gesetzlichen Bestimmungen

9.1.1 Das Zugangsportal für Patientinnen und Patienten muss den einschlägigen rechtlichen Anforderungen entsprechen.

9.1.2 Das Zugangsportal muss Patientinnen und Patienten und den nach Artikel 3 Buchstabe h EPDV ermächtigten Gesundheitsfachpersonen die Möglichkeit bieten, die Berechtigungssteuerung unter Einhaltung der Vorgaben von Artikel 1 bis 3 EPDV umzusetzen.

9.1.3 Das Zugangsportal muss hinsichtlich der Verwendung von Patientendaten mindestens folgende Rahmenbedingungen erfüllen:
9.1.3.1 die von den Patienten in Bereichen ausserhalb des elektronischen Patientendossiers bereitgestellten Daten dürfen nur dann im elektronische Patientendossier erfasst werden, wenn die Patientin oder der Patient dazu ihre oder seine Einwilligung erteilt hat;
9.1.3.2 die vom Patienten oder von der Patientin selbst bereitgestellte Daten müssen immer direkt, d.h. ohne Verwendung intermediärer Speicher im elektronischen Patientendossier erfasst werden können;
9.1.3.3 die Daten des elektronischen Patientendossiers dürfen nicht automatisch und nicht ohne explizite Einwilligung des Patienten oder der Patientin in funktionelle Bereiche «ausserhalb» des elektronischen Patientendossiers überführt werden.

## 9.2 Darstellung

9.2.1 Die Darstellung auf der Benutzeroberfläche des Zugangsportals muss korrekt und vollständig sein und klar erkennen lassen:
9.2.1.1 ob ein Dokument durch eine Gesundheitsfachpersonen oder durch den Patienten oder die Patientin selbst bereitgestellt wurde;
9.2.1.2 welche Dokumente von der Patientin oder dem Patienten selbst bereitgestellt wurden;
9.2.1.3 welche Dokumente annulliert wurden;
9.2.1.4 welche Versionen eines Dokumentes gegebenenfalls auch vorhanden sind.
9.2.1.5 welche Gesundheitsfachpersonen über welche Zugriffsrechten verfügen;
9.2.1.6 welche Dokumente welcher Vertraulichkeitsstufe zugeordnet sind;

9.2.2 Für die Darstellung der in Anhang 3 der EPDV-EDI vorgegebenen Metadaten auf der Benutzeroberfläche des Zugangsportals sind die dort vorgegebenen Begriffe («defined terms») gemäss gewählter Spracheinstellung zu verwenden.

### 9.3 Barrierefreiheit

9.3.1 Das interne Zugangsportal muss:
9.3.1.1 so ausgestaltet sein, dass behinderte oder ältere Patientinnen und Patienten dieses barrierefrei nutzen können;
9.3.1.2 den Konformitätsbedingungen gemäss Web Content Accessibility Guidelines (WCAG) 2.0 entsprechen und die Konformitätsstufe AA erreichen.

### 9.4 Dateiformate: Bereitstellung

9.4.1 Das Zugangsportal muss:
9.4.1.1 die Möglichkeit bieten, die gemäss Anhang 3 der EPDV-EDI zugelassenen Dateiformate bereitzustellen;
9.4.1.2 die Dateien anderer Formate vor dem Abspeichern in der Dokumentenablage in ein zugelassenes Format umwandeln.

### 9.5 Dateiformate: Abruf

9.5.1 Das Zugangsportal muss:
9.5.1.1 die Möglichkeit bieten, die gemäss Anhang 3 der EPDV-EDI zugelassenen Dateiformate abzurufen;
9.5.1.2 den Abruf von Dateien zum Abspeichern im Primärsystem unterstützen («Download»);
9.5.1.3 die Möglichkeit bieten, ausgewählte Dokumente nicht nur einzeln, sondern auch gesammelt («bulk download») herunterzuladen;
9.5.1.4 strukturierte Daten menschenlesbar, korrekt und vollständig darstellen;
9.5.1.5 die Möglichkeit bieten, dass strukturierte Daten sowohl im Originalformat, als auch als menschenlesbares Format heruntergeladen werden können.

9.5.2 Für den Abruf von Dokumenten zur Darstellung oder zum Abspeichern sind zulässige Obergrenzen pro Zeiteinheit («rate limits») zu definieren, welche beim Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen auslösen.

### 9.6 Protokolldaten (Bst. c)

*9.6.1* Patientinnen und Patienten müssen die Möglichkeit haben, Protokolldaten für ihr oder sein elektronisches Pateientendossier aus allen Gemeinschaften und Stammgemeinschaften in einer für sie lesbaren Form einzusehen.

# 10 Verfügbarkeit der von Patientinnen oder Patienten erfassten Daten (Art. 18 EPDV)

### 10.1 Dokumentenablagen für Dokumente von Patientinnen und Patienten

10.1.1 Stammgemeinschaften müssen dedizierte gemeinschaftsinterne Dokumentenablagen für die durch Patientinnen oder Patienten selbst erfassten Dokumente bereitstellen.

10.1.2 Die Dokumente dürfen keiner Löschungsfrist unterliegen.

10.1.3 Der dafür vorgesehene Speicherplatz muss mindestens 2 Gigabyte umfassen.

10.1.4 Stammgemeinschaften müssen ein Kapazitätsmanagement für den verfügbaren Speicherplatz für die durch Patientinnen und Patienten erfassten Dokumente führen.

### 10.2 Offline-Archivierung von Dokumenten und Metadaten

10.2.1 Patientenbezogene Daten und deren Metadaten müssen den Patientinnen und Patienten in einem interoperablen gängigen elektronischen Format zur Verfügung gestellt werden können.

10.2.2 Dabei sind Verfahren vorzusehen, die es ermöglichen festzustellen, ob die Daten seit der Verfügungsstellung verändert wurden.

10.2.3 Stammgemeinschaften müssen sicherstellen, dass Daten, die erneut im elektronischen Patientendossier verfügbar gemacht werden sollen, unverändert geblieben sind.

# 11 Kontaktstelle für Patientinnen und Patienten (Art. 19 EPDV)

11.1.1 Stammgemeinschaften müssen für die Patientinnen und Patienten eine Kontaktstelle («*Service-Desk*») bezeichnen, die sie im Umgang mit dem elektronischen Patientendossier unterstützt.

11.1.2 Stammgemeinschaften müssen mindestens sicherstellen, dass:

11.1.2.1 die Mitarbeitenden des «Service-Desk» ihre Aufgaben, Rechte und Pflichten sowie die Risiken und die Massnahmen bezüglich Datenschutz und Datensicherheit kennen;

11.1.2.2 die Mitarbeitenden mit Zugriff auf Daten des elektronischen Patientendossiers sorgfältig ausgewählt werden und einer der ärztlichen Schweigepflicht analogen Vereinbarung unterstehen;

11.1.2.3 die Einwilligung der Mitarbeitenden des Service-Desk zu den spezifischen Richtlinien der Stammgemeinschaft dokumentiert wird;

11.1.2.4 Remote-Zugriffe für Support-Tätigkeiten auf die Endgeräte der Patientinnen und Patienten ausschliesslich mit Kenntnis und Einwilligung der jeweiligen Gesundheitsfachperson erfolgen können und automatisch dokumentiert werden.

# 12 Aufhebung des elektronischen Patientendossiers (Art. 20 EPDV)

12.1.1 Stammgemeinschaften müssen Prozesse zur Aufhebung des elektronischen Patientendossiers aufgrund von Widerruf, Nichtgebrauch und Tod der Patientin oder des Patienten definiert, dokumentiert, umgesetzt und eingehalten haben.

## 12.2 Bedingungen zur Aufhebung des elektronischen Patientendossiers (Abs. 1)

12.2.1 Der Prozess zur Aufhebung des elektronischen Patientendossiers muss ausgelöst werden, wenn:
12.2.1.1 die Patientin oder der Patient die Einwilligung zu dessen Führung widerruft;
12.2.1.2 während 10 Jahren niemand darauf zugreift; oder
12.2.1.3 die Patientin oder der Patient verstorben ist.

## 12.3 Aufhebung des elektronischen Patientendossiers (Abs. 2)

12.3.1 Der Prozess zur Aufhebung des elektronischen Patientendossiers muss sicherstellen, dass:
12.3.1.1 das aufzuhebende elektronische Patientendossier korrekt identifiziert wird;
12.3.1.2 sämtliche Zugriffsrechte auf das entsprechende Patientendossier unverzüglich entzogen werden;
12.3.1.3 sämtliche Daten des entsprechenden Patientendossiers nach Artikel 9 Absatz 1 Buchstabe b vernichtet werden;
12.3.1.4 alle Gemeinschaften und Stammgemeinschaften innert angemessener Frist über die Aufhebung des elektronischen Patientendossiers informiert werden;
12.3.1.5 die ZAS innert angemessener Frist über die Aufhebung des elektronischen Patientendossiers informiert wird.

## 12.4 Widerruf der Einwilligung zur Führung eines elektronischen Patientendossiers (Abs. 2 Bst. a)

12.4.1 Der Prozess zur Aufhebung des elektronischen Patientendossiers aufgrund Widerruf muss, in Ergänzung zu Kap. 12.3, zudem sicherstellen, dass:
12.4.1.1 der Widerruf rechtsgültig dokumentiert wird;
12.4.1.2 die Widerrufserklärung während zehn Jahren aufbewahrt wird.

12.4.2 Es muss sichergestellt werden, dass:
12.4.2.1 die Identifikation der widerrufenden Person
12.4.2.1.1 anhand des Identifikationsmittels eines nach Artikel 30 zertifizierten Herausgebers erfolgt, oder
12.4.2.1.2 den Anforderungen nach Artikel 23 Absatz 1 EPDV entspricht;
12.4.2.2 die widerrufende Person über die Folgen des Widerrufs informiert wurde;

### 12.5 Schliessen bei Nichtgebrauch (Abs. 2 Bst. b)

12.5.1 Der Prozess zur Aufhebung des elektronischen Patientendossiers aufgrund Nichtgebrauch nach Artikel 20 Absatz 1 Buchstabe b muss, in Ergänzung zu Kap. 12.3, zudem sicherstellen, dass:

12.5.1.1 die Patientin oder der Patient drei Monate vor der Aufhebung darüber informiert wird.