Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Departement des Innern EDI

Bern, 1. Juni 2023

Änderung der Verordnung des EDI über das elektronische Patientendossier

Jahresrevision 2023 (Anhänge 2–5, einschliesslich der Ergänzungen 1 und 2.1–2.3 zu Anhang 5, 8 und 9)

Erläuterungen

BK-D-BF8A3401/507

1 Ausgangslage

Das Parlament hat das Bundesgesetz über das elektronische Patientendossier (EPDG, SR 816.1, BBl 2015 4865) am 19. Juni 2015 verabschiedet. Als Rahmengesetz regelt das EPDG die Voraussetzungen für die Bearbeitung der Daten des elektronischen Patientendossiers (EPD).

Der Bundesrat hat das EPDG und dessen Ausführungsrecht mit Beschluss vom 22. März 2017 auf den 15. April 2017 in Kraft gesetzt. Die Verordnung vom 22. März 2017 über das elektronische Patientendossier (EPDV, SR 816.11) delegiert gewisse Rechtssetzungskompetenzen zur Festlegung der Einzelheiten für die Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften sowie für Herausgeber von Identifikationsmittel an das EDI.

2 Revisionsbedarf

Die vorliegende Revision der Anhänge 2, 3, 4, 5, 8 und 9 sowie der Ergänzungen 1, 2.1, 2.2 und 2.3 zu Anhang 5 der EPDV-EDI erfolgt zur Präzisierung von technischen Unklarheiten und zur Berichtigung von Fehlern in den jeweiligen Vorgaben, die im Rahmen der laufenden Zertifizierungsverfahren zu Tage getreten sind oder den technischen Spezialistinnen und Spezialisten von Plattform- und Primärsystemanbietern aufgefallen sind.

2.1 Medication Card Document

Die Verfügbarkeit und der Austausch von Medikationsdaten stellt für alle Patientinnen und Patienten und involvierten Gesundheitsfachpersonen eine der häufigsten und wichtigsten Informationen im Rahmen des EPD dar. Patientinnen, Patienten und Gesundheitsfachpersonen sollten im Rahmen des EPD jederzeit Zugang zu einem möglichst aktuellen Stand der Medikation haben. Zudem fordert die Motion Stöckli 18.3512 «Recht auf einen Medikationsplan zur Stärkung der Patientensicherheit» dem Parlament eine Rechtsgrundlage zu unterbreiten, die ein Anrecht für Patientinnen und Patienten schafft, einen elektronischen oder gedruckten Medikationsplan zu erhalten, sofern sie drei oder mehr Arzneimittel gleichzeitig einnehmen.

Das Medication Card Document ermöglicht eine möglichst vollständige Übersicht über die aktuelle Medikation einer Patientin oder eines Patienten. Zudem dient es auch als Grundlage für eine optimale Medikationsanamnese und vollständige Interaktionskontrolle. Für die Patientin bzw. den Patienten bietet das Medication Card Document eine Übersicht, wann sie bzw. er welche Arzneimittel wie einnehmen soll und was bei der Einnahme der Medikamente zu beachten ist.

2.2 OpenID Connect

Das Protokoll OpenID Connect (OIDC) ist ein moderner Standard, der die Kommunikation zwischen verschiedenen Anwendungen ermöglicht. OIDC ist insbesondere dafür geeignet, eine Benutzerin oder einen Benutzer nach einmaliger Authentisierung auf einem zentralen System auf mehreren weiteren Servicesystemen anzumelden. Dies wird auch als *Identity Federation* bezeichnet. Für die Benutzerin bzw. den Benutzer vereinfacht dieser auch als *Single-Sign-On (SSO)* bezeichnete Ansatz die Verwendung eines Systems erheblich, weil nicht mehr für jedes System individuelle Anmeldeparameter verwaltet werden müssen, sondern nur noch an einem System eine Anmeldung erfolgen muss.

Damit bietet OIDC eine Alternative zu der bereits etablierten Security Assertion Markup Language (SAML), die bei gleichem Sicherheitsniveau die gleichen Funktionen wie SAML abdeckt, aber heute im Markt weiter verbreitet ist. Namentlich ist die Integration von OIDC in Primärsystemen gegenüber SAML einfacher und kann so potenziell mehr Leistungserbringer zu einer tiefen Integration ihrer Primärsysteme motivieren.

Um beim Einsatz von OIDC die Sicherheit des Datenverkehrs zu gewährleisten, sind Massnahmen bei der Umsetzung des Protokolls erforderlich. Wichtige Massnahmen sind das kryptographische Signieren der Nachrichten, die von den teilnehmenden Systemen ausgetauscht werden und die Verifikation der Signatur durch die Empfängerin bzw. den Empfänger einer solchen Nachricht. Diese Massnahmen wurden in der vorliegenden Version von Anhang 8 festgehalten.

Die Implementierung von OIDC ist aufwändig, unter Berücksichtigung und im Dialog mit den Identity Providern wird deshalb die Implementierung von OIDC in der vorliegenden Ausgabe als optional eingestuft.

3 Erläuterungen zu einzelnen Artikeln

3.1 Anhang 2: Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften

Ziff. 2.3.2 Durchsetzen der Zugriffsentscheidung

Die Ziffer wird gestrichen. Die Überprüfung der Korrektheit der Zugriffsentscheide ist bereits genügend abgedeckt durch die Anforderungen in Anhang 5 in den entsprechenden technischen Profilen und mit den daher eingehenden SIAS und Tests der komplexen Anwendungsfälle.

Ziff. 2.6 Vernichtung von Daten

Anstelle von «Löschen» wird neu von «Vernichtung» gesprochen. An den Anforderungen ändert sich dadurch nichts.

Ziff. 2.9 *Vorgaben für die Verwaltung und die Übertragung der Daten des elektronischen Patientendossiers*

Viele der Ziffern in diesem Kapitel wurden gestrichen, da sie mit dem Verweis auf Anhang 5 der EPDV-EDI bereits genügend abgedeckt sind. Folgende Ziffern wurden dabei gestrichen: 2.9.4, 2.9.5, 2.9.5*a*, 2.9.6, 2.9.7, 2.9.7*b*, 2.9.7*c*, 2.9.8, 2.9.9, 2.9.10, 2.9.11, 2.9.12, 2.9.13, 2.9.13*a*, 2.9.14, 2.9.15, 2.9.16, 2.9.16*a*, 2.9.17, 2.9.18, 2.9.19, 2.9.19*a*, 2.9.20, 2.9.21, 2.9.22, 2.9.23, 2.9.24, 2.9.25, 2.9.27 und 2.9.28.

Ziff. 2.9.3 *IHE-Integrationsprofile, nationale Anpassungen der IHE-Integrationsprofile und nationale Integrationsprofile*

Neu wird neben den Profilen auch explizit auf die Akteure und Transaktionen in Anhang 5 der EPDV-EDI verwiesen.

Ziff. 2.9.7a *Kommunikation beglaubigter Identitäten*

Die Ziffer wird gestrichen, da die Anforderungen neu in Anhang 5 Ergänzung 1 aufgenommen werden.

Ziff. 2.9.26a *Authentisierung mit gültigen Zertifikaten*

Neu wird nur noch von Zugangspunkten und nicht mehr von Endpunkten gesprochen. An den Anforderungen ändert sich dadurch nichts.

Ziff. 2.10 *Protokolldaten*

Um Klarheit zu schaffen wird explizit erwähnt, dass es sich bei den hier beschriebenen Protokolldaten, um die Protokollierung nach den Profilen ATNA und CH:ATC gemäss Anhang 5 der EPDV-EDI handelt. In der Vergangenheit war jeweils nicht ganz klar, ob dies auch für die Systemlogs gilt.

Ziff. 2.10.5 *Protokolldaten*

Die Ziffer wird gestrichen, da in Anhang 5 bereits der genaue Umfang der Protokollierung umschrieben ist.

Ziff. 2.10.7 *Protokolldaten*

In *Buchstabe a* wurde klargestellt, dass es sich hier um Protokolldaten nach dem Profil CH:ATC handelt. In *Buchstabe e* wird anstelle von Systemadministratoren nun von administrativen Nutzern gesprochen. Dies schliesst die Systemadministratoren mit ein aber auch alle sonstigen Nutzer, die administrative Arbeiten für eine Gemeinschaft erledigen.

Ziff. 3.1b *Vertrauensstellung von Zugangsportalen*

Diese Ausnahmeregelung wird entfernt, da sie bisher von keiner Gemeinschaft umgesetzt wird. Berechtigungsrelevante Behauptungen müssen also immer bei einer vertrauenswürdigen Datenquelle überprüft werden. Die Sicherheit der EPD-Infrastruktur wird damit verstärkt.

Ziff. 3.4.2 *Technische Anforderungen*

Die Ziffer wird gestrichen und die Anforderung neu in Ziffer 4.4.3 Buchstabe d aufgenommen.

Ziff. 4.2.1 *Datenschutz- und Datensicherheitsmanagementsystem*

Die Referenz auf die Norm ISO/IEC 27002, Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Massnahmen wird von der Version 2017-06 auf die Version 2022 aktualisiert.

Ziff. 4.4.3 *Umgang mit Sicherheitsschwachstellen*

Buchstabe c wird so umformuliert, dass nicht nur ein spezifisches Angriffsszenario erwähnt wird, sondern alle gängigen Angriffs- und Kompromittierungstypen. Dies soll zusammen mit dem neu hinzugefügten *Buchstaben d* auch die gestrichenen Ziffern 3.4.2, 4.18 Buchstabe f und 9.6.2 umfassen.

Ziff. 4.6.2 *Verwaltung schützenswerter Informatikmittel und Datensammlungen*

Auf die Auflistung der entsprechenden IHE-Akteure wird neu verzichtet. An den Anforderungen ändert sich dadurch nichts.

Ziff. 4.6.5 *Verwaltung schützenswerter Informatikmittel und Datensammlungen*

Es wird präzisiert, dass das «Inventar der Informatikinfrastruktur» bei der Überprüfung auch aktualisiert werden muss.

Ziff. 4.7.1. *Datenschutz- und Datensicherheitsanforderungen an die angeschlossenen Gesundheitseinrichtungen und deren Gesundheitsfachpersonen sowie an deren Endgeräte*

Es wird neu verlangt, dass die Verpflichtung der Gesundheitseinrichtungen durch Gemeinschaften und Stammgemeinschaften zur Einhaltung von Datenschutz- und Datensicherheitsanforderungen schriftlich zu erfolgen hat.

Ziff. 4.18 *Verfügbarkeit*

Mit *Buchstabe a^{bis}* wird eine neue Anforderung eingeführt, gemäss der die Daten auch dann noch verfügbar sein sollen, wenn eine Gemeinschaft ihren Betrieb einstellt. Der neue *Buchstabe a^{ter}* fordert bei einer Migration der Daten, dass die Metadaten und insbesondere die Rolle des Bereitstellers erhalten bleiben. *Buchstabe f* wird an dieser Stelle gestrichen und die Anforderung neu unter Ziffer 4.4.3 Buchstabe d geführt.

Ziff. 8.2.1 *Identifikation der Patientinnen und Patienten*

Die Vorgaben der Ziffer 8.2.1 der bisherigen Fassung des Anhangs 2 werden neu in den Ziffern 8.2.1–8.2.1*b* geführt. Die Ziffer 8.2.1 enthält neu ausschliesslich die Möglichkeiten der Identifizierung von Personen, die gestützt auf Artikel 17 Absatz 1 Buchstabe b EPDV ein EPD eröffnen möchten. Darüber hinaus wird der Verweis auf Artikel 24 EPDV in Buchstabe a aufgelöst und durch eine explizite Aufzählung der anerkannten Mittel zur Identifikation im Eröffnungsprozess für ein EPD ersetzt.

In materieller Hinsicht wurden die Anforderungen an die Identifikation um zwei Tatbestände erweitert. Nach *Buchstabe d* sind neu auch abgelaufene Schweizer Reisepässe und Schweizer Identitätskarten für die Identifikation anerkannt, sofern sie mit weiteren Unterlagen oder mittels der Erklärung der Identifikation durch Angehörige oder durch eine Behörde ergänzt werden. Der abgelaufene Reisepass oder Identitätskarte muss in Kombination mit den weiteren Unterlagen oder der Erklärung eine zuverlässige Identifikation ermöglichen. Als weitere Unterlagen kommen beispielsweise die Krankenversicherungskarte, ein Niederlassungsausweis und Bankkarten in Betracht. Die Stammgemeinschaften sind nach wie vor zuständig, die Einzelheiten und den Prozess für die Identifikation von Personen festzulegen. Dazu gehört insbesondere auch, welche weiteren Unterlagen sie verlangen muss, um eine sichere Identifikation durchzuführen. Mit dieser Anpassung soll insbesondere die Eröffnung eines EPD für Personen erleichtert werden, die nur einen erschwerten Zugang zu einem gültigen Ausweis haben (beispielsweise Bettlägerige in Alters- und Pflegeheimen).

Nach *Buchstabe m* kann neu mit einer ausländischen Identitätskarte ein EPD eröffnet werden, sofern die Identitätskarte zur Einreise in die Schweiz berechtigt und die Inhaberin oder der Inhaber gegenüber der Stammgemeinschaft nachweisen kann, dass sie mit einer Person in einem gemeinsamen Haushalt lebt, die Inhaberin oder Inhaber einer Legitimationskarte nach Artikel 17 der Gaststaatverordnung ist.

Ziff. 8.2.1a *Identifikation der Patientinnen und Patienten (Kinder bis zum zwölften Lebensjahr)*

Mit der Ziffer 8.2.1*a* wird eine Spezialregelung für die Identifikation von Kindern bis zum vollendeten zwölften Lebensjahr eingeführt. Gestützt auf diese Bestimmung kann eine Identifikation von Kindern anhand einer Krankenversicherungskarte einer schweizerischen Krankenversicherung in Kombination mit der Geburtsurkunde oder anderen für die Identifikation geeignete Unterlagen erfolgen. Die Formulierung wurde bewusst offen gewählt, damit die Stammgemeinschaften, wie bei der Identifikation mit einem abgelaufenen Schweizer Reisepass oder mit einer abgelaufenen Schweizer Identitätskarte, selbst die genauen Anforderungen festlegen und insofern den Ansprüchen aus der Praxis gerecht werden können.

Ziff. 8.2.1b *Identifikation der Patientinnen und Patienten (weitere Prozesse)*

In der Ziffer 8.2.1*b* werden die übrigen Anforderungen an den Identifikationsprozess geregelt, die vormals in der Ziffer 8.2.1 Buchstaben b–e enthalten waren.

Ziff. 8.6.3 *Berechtigungssteuerung*

In *Buchstabe c* wird präzisiert, dass die Information über Eintritte von Gesundheitsfachpersonen in berechtigte Gruppen nur auf Verlangen der Patientinnen oder Patienten erfolgen muss.

Ziff. 9.1a *Vertrauensstellung von Zugangsportalen*

Diese Ausnahmeregelung wird entfernt, da sie bisher von keiner Gemeinschaft umgesetzt wird. Berechtigungsrelevante Behauptungen müssen also immer bei einer vertrauenswürdigen Datenquelle überprüft werden, was die Sicherheit erhöht.

Ziff. 9.6.2 *Technische Anforderungen*

Die Ziffer wird gestrichen und die Anforderung neu in Ziffer 4.4.3 Buchstabe d aufgenommen.

3.2 Anhang 3: Metadaten für den Austausch medizinischer Daten

Ziff. 1.1 *Zuordnung der Metadaten-Attribute nach Anhang 3 zu den Metadaten-Attributen der Integrationsprofile nach Anhang 5*

Der Name des Metadatenattributs «Fachrichtung der Autorin oder des Autors» wird an das IHE IT Infrastructure Handbook Version 2.1 angepasst.

Ziff. 2.2 *Fachrichtung der Autorin oder des Autors*

Die Änderung in Ziffer 1.1 (s. oben) bedingt auch eine Anpassung der Ziffer 2.2. Ausserdem erfolgt eine Präzisierung einzelner Begriffe sowie die Berichtigung der Gross- und Kleinschreibung.

Ziff. 2.3 *Organisatorischer Typ der Gesundheitseinrichtung*

Eine neue Gesundheitseinrichtung wird hinzugefügt: Free-standing birthing center (environment).

Ziff. 2.4 *Fachrichtung der Gesundheitseinrichtung*

Vier neue Fachrichtungen werden hinzugefügt: Obstetrics (qualifier value), Vascular surgery (qualifier value), Emergency medicine (qualifier value) und Dentistry (qualifier value).

Ziff. 2.6 *Dokumententyp*

Ein neuer Dokumententyp wird hinzugefügt: Digital representation of specimen (record artifact). Zudem werden verschiedene Rechtschreibefehler korrigiert.

Ziff. 2.7 *Zulässige Dokumententypen nach Dokumentenklasse*

Die Änderung gemäss Ziffer 2.6 wird in dieser Ziffer entsprechend für das Mapping von Dokumententyp nach Dokumentenklasse übernommen. Zudem wurden verschiedene Rechtschreibefehler korrigiert.

Ziff. 2.12 *Detailliertes technisches Format*

Für die Medication Card document wird ein neues technisches Format hinzugefügt: CH EMED Medication Card document.

3.3 Anhang 4: Austauschformate

Ziff. 3 *Administrative Informationen*

In Ziffer 3 wird die Version von CH Core von 2.1.0 auf 3.0.0 angepasst. Die Änderungen beinhalten technische Anpassungen am Standard. Dies umfasst z. B. die Überprüfung der GLN-Nummer, die höchstens 13 Ziffern lang sein darf. Weiter wurden Anpassungen an der Spezifikation vorgenommen, um deren Lesbarkeit zu verbessern.

Ziff. 4 *Austauschformat eImpfung (CH VACD)*

In Ziffer 4 wird die Version des Austauschformates CH VACD von 2.1.0 auf 3.0.0 angepasst. Mit der neuen Version wurden technische Anpassungen am Austauschformat vorgenommen.

Die Version der Value Sets wird von 2.1.0 auf 3.0.0 angehoben. Die Änderungen beinhalten Ergänzungen von Impfungen wie zum Beispiel Mpox und Korrekturen von Schreibfehlern.

Ziff. 5 *Austauschformat eMedikation (CH EMED)*

Das Austauschformat eMedikation ermöglicht die Erfassung, Verwaltung und Darstellung der Medikationsdaten einer Patientin oder eines Patienten. Die technische Umsetzung hat gemäss der Detailspezifikation CH EMED (Ziff. 5) für FHIR Dokumente zu erfolgen. Zunächst wird das Dokument Medikationsplan (Ziff. 5.1) vom Austauschformat eMedikation eingeführt. Zum Medikationsplan sind die zu vergebenden Metadaten definiert, die zwingend vergeben werden müssen (Ziff. 5.1.1). Die Metadaten ermöglichen u.a. die Erkennung der Dokumente.

3.4 Anhang 5: Integrationsprofile

Die EPDV-EDI hält in Anhang 5 fest, welche Integrationsprofile im Kontext des EPD zu verwenden sind. In der Ergänzung 1 zu Anhang 5 werden die nationalen Anpassungen zu Standard IHE-Profilen beschrieben. Die Ergänzung 2.1 enthält die nationalen Integrationsprofile CH:ADR und CH:PPQ, in der Ergänzung 2.2 werden die nationalen Integrationsprofile CH:ATC geführt und das nationale Integrationsprofil CH:CPI ist in der Ergänzung 2.3 festgehalten. Diese Vorgaben sind an den Stand der Technik anzupassen.

3.4.1 Anhang 5 (amtlich publizierter Teil)

Ziff. 1 und 2 *IHE Integrationsprofile und Nationale Integrationsprofile*

Am 10. März 2022 wurde die Revision 20.0 des IHE Radiology Technical Framework und am 17. Juni 2022 die Revision 19 des IHE IT Infrastructure Technical Framework veröffentlicht. In der neuen Version finden sich neue Profile, aber auch für das EPD relevante und von uns eingebrachte Change Proposals zu Restricted Metadata Update (RMU) und Healthcare Provider Directory (HPD).

In den Tabellen der Integrationsprofile in Anhang 5 (Ziff. 1 und Ziff. 2), wie auch in der Ergänzung 1 zu Anhang 5 werden die Referenzen gemäss den obengenannten IHE Technical Frameworks angepasst.

3.4.2 Ergänzung 1 zu Anhang 5: Nationale Anpassungen der Integrationsprofile nach Artikel 5 Absatz 1 Buchstabe b EPDV-EDI

Ziff. 1.3 Requirements on XDS-I.b

Die Anbindung von radiologischen Bildarchiven an das EPD ist seit Inkrafttreten des EPDG im 2017 vorgesehen. Damit die Zugriffe auf die DICOM-Studien in den radiologischen Bildarchiven in den Spitälern korrekt über die Infrastruktur des EPD erfolgen und Missbrauch verhindert werden kann, wird die Verordnung präzisiert. Insbesondere ist es nun nur noch dem Technischen Benutzer erlaubt, DICOM Key Object Selection (KOS) Objekte im EPD bereitzustellen. Dadurch wird verhindert, dass Patientinnen bzw. Patienten und Gesundheitsfachpersonal manipulierte KOS-Objekte im EPD ablegen und so unberechtigten Zugang zu Studien anderer Patientinnen und Patienten erlangen. Diese Gefahr bestand in der Praxis jedoch nicht, da es bisher keine Anbindung von radiologischen Bildarchivsystemen gibt.

Ziff. 1.5.1 Precisions on Authenticate Node [ITI-19]

Mit der neuen Version der IHE ITI Technical Framework (siehe Kapitel 3.4.1) gibt es bei der Transaktion Authenticate Node [ITI-19] mehrere Optionen bezüglich TLS Version. Es wird präzisiert, dass mindestens TLS Version 1.2 (STX: TLS 1.2 floor using BCP195 Option) zu verwenden ist. Hierzu wurden die Ziffer 1.5.1 und Ziffer 1.5.2 neu hinzugefügt.

Ziff. 1.6.2 Actors / Transactions

IHE-Akteure sind Softwarekomponenten, welche miteinander über standardisierte Schnittstellen kommunizieren (Transaktionen). Nach der IHE-Konvention können Akteure gruppiert werden, was bedeutet, dass immer alle Transaktionen der gruppierten Akteure implementiert werden müssen. Die bestehenden Gruppierungen haben zur Pflicht der Implementation von unnötigen Transaktionen geführt. Mit der vorliegenden Änderung wird die Gruppierung der Akteure neu festgelegt, was einer Anpassung an die Realität entspricht.

Ziff. 1.6.3 Actor Grouping

Die Änderung in Ziffer 1.6.2 (s. oben) bedingt auch eine Anpassung der Ziffer 1.6.3: Die Tabelle 7 wird mit den korrekten Gruppierungen der Akteure ergänzt.

Ziff. 1.6.4 Transactions

In der Ausgabe 3 zu Anhang 8 EPDV-EDI wird zusätzlich zu SAML neu OpenID Connect rechtlich verankert, damit die Anbindung von mobilen Geräten via mobile Schnittstellen ans EPD möglich wird.

Damit OpenID Connect auch bei den (Stamm-)Gemeinschaften und Primärsystemen funktioniert, wird OpenID Connect beim XUA-Profil (Unterziffern von Ziffer 1.6.4) als Option ergänzt.

Ziff. 1.6.4.3.4.2 Message Semantics

Bei den Vorgaben zur Transaktion Provide X-User Assertion im XUA Profil, welche z.B. zur Suche nach Dokumenten benötigt wird, um die Zugriffsrechte zu ermitteln, werden die Vorgaben zur Strukturierung der Attribute der «organization» und «organization-id» korrigiert. Diese Präzisierung soll falsche Implementierungen verhindern und fördert so Interoperabilität.

Ziff. 1.11.5.1.2 Attribute

Die Schweizer Vorgaben zum Health-Provider-Directory (HPD) -Profil werden dahingehend präzisiert, dass beim «prefix» die Assigning Authority die (Stamm-)Gemeinschaft ist und insgesamt nur ein Doppelpunkt verwendet werden darf, um den ISO 21091 Standard nicht zu verletzen. Darüber hinaus sind im HPD für das UID-Feld nur noch folgende Zeichen erlaubt: Alphanumerische Zeichen, Minus "-", Doppelpunkt ":", Ausrufezeichen "!", Senkrechter Strich "|", Unterstrich "_", Punkt ".". Bisher konnte es zu Problemen aufgrund von unzulässigen Zeichen kommen, d.h. dass ein HPD-Eintrag bei einer Suche nicht gefunden wurde.

Ziff. 1.14 Requirements on Medication Card document

Die Ziffern 1.13 und 1.14 beinhalten die Beschreibung der IHE-Akteure, die zur Anzeige und Validierung der Medication Card document erforderlich sind. Hierfür werden die entsprechenden IHE-Akteure Content Consumer und Content Creator in der Ergänzung 1 zu Anhang 5 EPDV-EDI aufgenommen.

3.4.3 Ergänzung 2.1 zu Anhang 5: Nationale Integrationsprofile nach Artikel 5 Absatz 1 Buchstabe c EPDV-EDI – Authorization Decision Request (CH:ADR) and Privacy Policy Query (CH:PPQ)

Diese Ergänzung spezifiziert die technischen Vorgaben zur Berechtigungssteuerung des EPD. Die Vorgaben haben sich historisch entwickelt und werden komplett überarbeitet und bereinigt. Hintergrund sind Erkenntnisse aus der Praxis, die kontinuierlich gesammelt und nun für verbindlich erklärt werden, was sich positiv auf die Sicherheit und den Datenschutz auswirken wird. Dabei werden insbesondere die Vorgaben in der Ergänzung auf das Wesentliche gekürzt und die enthaltenen Code-Beispiele aus dem Dokument ausgelagert. Zudem werden XML-Schemas für die Definition von Zugriffsrechten auf das EPD weiterentwickelt und die Pflicht, diese zu verwenden, normativ verankert, was bisher nicht der Fall war. In diesem Zusammenhang wird auch ein Prüfschema entwickelt und im Anhang referenziert (Ziff. 4.1). Mit der Einführung dieser

Vorgaben soll verhindert werden, dass bei der Erteilung oder Änderung von Zugriffsrechten unerlaubte Angaben gemacht werden.

Weiter werden die Detailbestimmungen zur Anbindung von Bildarchiven an die EPD-Infrastruktur einer (Stamm-)Gemeinschaft präzisiert. Damit ist sichergestellt, dass nur autorisierte EPD Benutzer Inhalte aus den Bildarchiven über das EPD freigeben können. Insbesondere ist es nun nur noch dem Technischen Benutzer erlaubt, DICOM Key Object Selection (KOS) Objekte im EPD bereitzustellen. Dadurch wird verhindert, dass Patientinnen und Patienten und Gesundheitsfachpersonal manipulierte KOS-Objekte im EPD ablegen und so unberechtigten Zugang zu Studien anderer Patientinnen und Patienten erlangen.

Schliesslich werden viele kleinere Änderungen vorgenommen, um beispielsweise unnötige Komplexität aus dem System zu entfernen oder ein besseres Fehlermanagement zu ermöglichen. Die folgende Konkordanztabelle gibt einen Überblick über die Neustrukturierung der Ergänzung 2.1 zu Anhang 5:

Kapitel	**Ziffer in Ausgabe 4**	**Entsprechung in Ausgabe 5**
Introduction	1	1
Definitions of terms	1.1	-
EPR circle of trust	1.1.1	-
Patient Identifiers (EPR-SPID, MPI-PID)	1.1.2	-
Terminology	1.1.3	-
Volume 1 - Integration Profiles	2	2
Overview	2.1	-
Authorization Decision Request (CH:ADR)	2.2	2.1
Motivation	2.2.1	-
Objectives and Constraints	2.2.2	-
Actors / Transactions	2.2.3	-
Privacy Policy Query (CH:PPQ)	2.3	2.2
Motivation	2.3.1	-
Objectives and Constraints	2.3.2	-
Actors / Transactions	2.3.3	-
Volume 2 - Transactions	3	3
Bezeichnung bisher: Authorization Decision Request (CH:ADR) *Bezeichnung neu:* Authorization Decision Request [CH:ADR]	3.1	3.1
Scope	3.1.1	3.1.1
Referenced Standards	3.1.2	3.1.2
Neues Kapitel: XML Namespaces	-	3.1.3
Interaction Diagram	3.1.3	3.1.4
Bezeichnung bisher: XACMLAuthzDecisionQuery Request *Bezeichnung neu:* CH:ADR Request	3.1.4	3.1.5
Trigger Events	3.1.5	
Message Semantics	3.1.6	-
Expected Actions	3.1.7	-
Bezeichnung bisher: XACMLAuthzDecision Response *Bezeichnung neu:* CH:ADR Response	3.1.8	3.1.6
Neues Kapitel: Indirect decision queries	-	3.1.7
Trigger Events	3.1.9	-
Message Semantics	3.1.10	-
Expected Actions	3.1.11	-
Enforcement of XDS Retrieve Document Set transactions	3.1.12	-
Enforcement of XDS-I.b "Imaging Retrieve" transactions	3.1.13	-
Security Considerations	3.1.14	3.1.8
Authorization Decision Consumer Audit Message	3.1.15	-
Authorization Decision Provider Audit Message	3.1.16	-
Cross-Community Authorization Decision Request (CH:XADR)	3.2	-
Bezeichnung bisher: Privacy Policy Feed (PPQ-1) *Bezeichnung neu:* Privacy Policy Feed [PPQ-1]	3.3	3.2
Scope	3.3.1	3.2.1

Kapitel	Ziffer in Ausgabe 4	Entsprechung in Ausgabe 5
Use Case Roles	3.3.2	-
Referenced Standards	3.3.3	3.2.2
Neues Kapitel: XML Namespaces	-	3.2.3
Interaction Diagrams	3.3.4	3.2.4
Message Semantics	3.3.5	-
Bezeichnung bisher: EPR AddPolicyRequest and EPR UpdatePolicyRequest *Bezeichnung neu:* AddPolicyRequest and UpdatePolicyRequest	3.3.6	3.2.5
Bezeichnung bisher: EPR AddPolicyRequest Response and EPR UpdatePolicyRequest Response *Bezeichnung neu:* AddPolicyRequest Response and UpdatePolicyRequest Response	3.3.7	3.2.6
Bezeichnung bisher: EPR DeletePolicyRequest *Bezeichnung neu:* DeletePolicyRequest	3.3.8	3.2.7
Bezeichnung bisher: EPR DeletePolicyRequest Response *Bezeichnung neu:* DeletePolicyRequest Response	3.3.9	3.2.8
Security Considerations	3.3.10	3.2.9
Bezeichnung bisher: Privacy Policy Retrieve (PPQ-2) *Bezeichnung neu:* Privacy Policy Retrieve [PPQ-2]	3.4	3.3
Scope	3.4.1	3.3.1
Use Case Roles	3.4.2	-
Referenced Standards	3.4.3	3.3.2
Neues Kapitel: XML Namespaces	-	3.3.3
Interaction Diagrams	3.4.4	3.3.4
Bezeichnung bisher: XACMLPolicyQuery *Bezeichnung neu:* Policy Query Request	3.4.5	3.3.5
Bezeichnung bisher: XACMLPolicyQuery Response *Bezeichnung neu:* Policy Query Response	3.4.6	3.3.6
Security Considerations	3.4.7	3.3.7
Volume 3 - Content Profiles	4	4
XACML EPR Access Policies	4.1	-
EPR Access Policy Stack	4.2	-
Entry Policies for the Evaluation of Access Decisions	4.2.1	-
Access Constraints	4.3	-
Read and Write Access Rights Overview	4.4	-
Enforcement of EPR transactions	4.4.1	-
Read EPR	4.4.2	-
Write EPR	4.4.3	-
Detailed Privacy Policy Format definitions	4.4.4	-
Value-Sets	4.4.5	-
Neues Kapitel: Submission Rules for Policies and Policy Sets	-	4.1
Neues Kapitel: Base Policies and Base Policy Sets	-	4.1.1
Neues Kapitel: Patient Bootstrap Policy Sets and Patient User Assignment Policy Sets	-	4.1.2
Figures	5	5
Tables	6	6
Listings	7	-

3.4.4 Ergänzung 2.2 zu Anhang 5: Nationale Integrationsprofile nach Artikel 5 Absatz 1 Buchstabe c EPDV-EDI – Audit Trail Consumption (CH:ATC)

Das CH:ATC Profil, welches für die Protokolldaten im Patientenportal verwendet wird, wird von *Fast Healthcare Interoperability Resources* (FHIR) STU3 auf FHIR Release 4 angehoben. Da kommende Austauschformate auch auf FHIR Release 4 publiziert werden, würde das Beibehalten einer alten Version das System unnötig komplex machen und es müssten zwei Versionen gepflegt werden. Die Änderung wirkt sich auf das gesamte Dokument aus.

Ziff. 1.1 Definitions of terms

Die Ziffer 1.1 wird gestrichen, da sie mit den entsprechenden Ziffern in der Ergänzung 1 zu Anhang 5 identisch ist.

Ziff. 3.1.4 Security Considerations

In der aktuellen Revision 2.1 des IHE IUA Supplement hat sich das Attribut «Token-Typ» im HTTP Header «Authorization» geändert und wurde im CH:ATC Profile nachgezogen: Im HTTP-Header «Authorization» wird als Tokentyp «Bearer» und nicht mehr «IHE-SAML» angegeben. Dies dient der Anpassung an internationale Standards, wobei das Sicherheitsniveau dadurch nicht verändert wird.

Ziff. 4.1 Audit Trail Consumption Event Types

Die Suche nach Dokumenten in einem EPD wird in den technischen Protokolldaten (ATNA) registriert, jedoch nicht in den Protokolldaten im Patientenportal angezeigt. Um die Rückverfolgbarkeit zu verbessern, wird durch diese Anpassung nun auch die Suche nach Dokumenten in den Protokolldaten im Patientenportal gespeichert. Zudem wird so auch ein Notfallzugriff ohne anschliessenden Abruf von Dokumenten klar in den Protokolldaten im Patientenportal angezeigt.

Der Artikel 9 Absatz 2 Buchstabe f EPDV legt fest, dass Gemeinschaften die Patientinnen und Patienten auf deren Verlangen über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen informieren müssen. Die Gemeinschaften wünschen, dass diese Ereignisse zur einfacheren Nachvollziehbarkeit zusätzlich in den Protokolldaten im Patientenportal gespeichert werden. Hierfür werden die Ziffern 4.5 und 4.5.1, die technische Spezifikationen und Beispiele enthalten, neu hinzugefügt.

Ziff. 4.2 Document Audit Event Content Profile

Beim Abruf oder der Bearbeitung von Dokumenten oder deren Metadaten wird neu im ATC-Log neben der wenig aussagekräftigen ID auch der Titel angezeigt.

Ziff. 4.2.1 Example of a Document Audit Event: Document upload

Beim Beispiel in Ziffer 4.2.1 zum ATC-Log Eintrag wird der Titel des betreffenden Dokuments ergänzt.

3.4.5 Ergänzung 2.3 zu Anhang 5: Nationales Integrationsprofil nach Artikel 5 Absatz 1 Buchstabe c EPDV-EDI – Community Portal Index (CH:CPI)

Ziff. 1.1 Definitions of terms

Die Ziffer 1.1 wird gestrichen, da sie mit den entsprechenden Ziffern in der Ergänzung 1 zu Anhang 5 identisch ist.

Ziff. 3.1.4.2 Message Semantics

Es ist eine Anforderung der EPD-Plattformanbieter, dass alle notwendigen Informationen aus dem CH:CPI ausgelesen werden können, damit eine zertifizierte Gemeinschaft sich mit allen anderen zertifizierten Gemeinschaften im CH:CPI automatisch mit allen Gateways verbinden kann. Nun wird das Datenmodell des CH:CPI um den *CH:ATC Patient Audit Consumer* erweitert, da diese relevante Information bisher noch fehlte. Insofern müssen nun Zertifikate nicht mehr ausserhalb des Vertrauensraum ausgetauscht werden, was die Sicherheit verbessert. Dies betrifft auch die Ziffern 3.1.5.2.3, 4.1.3.2 und 4.1.3.3.9, die die technische Spezifikation enthalten. Des Weiteren werden Rechtschreibfehler korrigiert.

Ziff. 3.1.8 Security Considerations

Mit der neuen Version der IHE ITI Technical Framework (siehe Kapitel 3.4.1) gibt es bei der Transaktion Authenticate Node [ITI-19] mehrere Optionen bezüglich TLS Version. Es wird präzisiert, dass mindestens TLS Version 1.2 (STX: TLS 1.2 floor using BCP195 Option) zu verwenden ist.

3.5 Anhang 8: Technische und organisatorische Zertifizierungsvoraussetzungen für Identifikationsmittel und deren Herausgeber (Schutzprofil für Identifikationsmittel)

Anhang 8 wurde in zwei Schritten wie folgt bearbeitet:

In einem ersten Schritt wurde Anhang 8 neu strukturiert. Die Notwendigkeit der Neustrukturierung ergab sich aus der Tatsache, dass in Anhang 8 Ausgabe 2.1 die notwendigen Änderungen und Erweiterungen zur Berücksichtigung des Feedbacks der Zertifizierungsstelle und der Identitätsanbieter sowie für die geplante Erweiterung um OpenID Connect nicht oder nur mit unangemessen hohem Aufwand hätten eingepflegt werden können. Im ersten Schritt wurden in Anhang 8 keine inhaltlichen Änderungen vorgenommen, sondern die Kapitel lediglich neu strukturiert, wobei Inkonsistenzen bereinigt und Unklarheiten beseitigt wurden.

Nach der Restrukturierung ist Anhang 8 wie folgt gegliedert:

1. Einleitung,

2. Anforderungen an die Dienstleistung gegenüber den Benutzern (Patienten und Patientinnen, Gesundheitsfach- und Hilfspersonen),
3. Anforderungen an den operativen Betrieb durch den Identitätsanbieter,
4. Technische Anforderungen an die Schnittstelle und Protokolle.

Alle Änderungen zur Restrukturierung, sowie zur Bereinigung von Inkonsistenzen und Unklarheiten wurden in einer temporären Begleitgruppe (AG Identifikationsmittel, mit Vertretern der Gemeinschaften, Plattformen, der Zertifizierungsstelle und der Identitätsanbieter) vorgestellt und diskutiert. Die Änderungen der Restrukturierung, sowie zur Bereinigung von Inkonsistenzen und Unklarheiten wurden von der Begleitgruppe abschliessend bewertet, begrüsst und unterstützt. Die folgende Konkordanztabelle gibt einen Überblick über die Neustrukturierung des Anhangs 8:

Kapitel	**Ziffer in Ausgabe 2.1**	**Entsprechung in Ausgabe 3**
PP Reference	1	3
TOE Definition	1.2.1	3.1.1
Operational Environment	1.3	3.1.1
Physical Protection of the TOE	1.4	3.1.3
Assets	1.5	3.1.4
External Entities and Subjects	1.6	3.1.5
Conformance Claims	2	obsolet
Security Problem Definition	3	3.2
Assumptions	3.1	3.2.1
Organizational Security Policies	3.2	3.2.2
Threats	3.3	3.2.3
Security Objectives	4	3.3
Security Objectives for the TOE	4.1	3.3.1
Security Objectives for the operational environment	4.2	3.3.2
Security Objectives rationale	4.3	3.3.3
Countering the threats	4.3.2	3.3.3.1
Security Requirements	5	3.4
Overview	5.1	3.4.1
Security Functional Requirements for the TOE	5.2	3.4.2
Security Requirements rationale	5.3	3.4.3
Security Assurance Requirements Rationale	5.4	3.5
Appendix	6	5
Identity Proofing Requirements	**6.1**	**2.5**
Authentication Sequences (v2), SAML2.0 Binding (v3)	6.2	4.1
SAML Assertion Renewal	Tab. 12	4.1.1.2
Logout Sequence	6.2a	v.1.1.3
SAML Recommendations (v2), Protocol Requirements (v3)	6.3	4.1.2/.3
OpenID Connect	**n/a**	**4.2**
Protocol Requirements for OpenID Connect (v3)	**n/a**	**4.2.2**
WS Trust Recommendations	6.4	4.1.3.6, 4.1.3.7

Im zweiten Schritt der Überarbeitung wurden die folgenden Anforderungen präzisiert bzw. hinzugefügt:

1. Abstimmung der Anforderungen an die X.509 Zertifikate von Relying Party Systemen (d.h. Portale und Primärsysteme) für die Authentifizierung und Verschlüsselung auf dem TLS-Transportlayer mit den technischen und organisatorischen Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (Anhang 2 zur EPDV-EDI).
2. Präzisierung der Anforderungen an die für die digitale Signatur des Nachrichtenaustauschs eingesetzten X.509 Zertifikate zwischen Identitätsanbieter und Relying Parties (Portale und Primärsysteme).

3. Um die Integration von verschiedenen Service Providern (beispielsweise die Registrierungsseite für neue Mitglieder der Stammgemeinschaft oder das EPD Zugangsportal) innerhalb einer (Stamm-)Gemeinschaft zu ermöglichen, wurde die Verwendung der NameID (*Ziff. 4.1.3.5*) und des Subject Identifier (*Ziff. 4.2.3.5*) bei Services, die unter der Autorität der (Stamm-)Gemeinschaft stehen, zugelassen, sofern die eingesetzten Service Provider aufgelistet werden.

Schliesslich erfolgt mit der vorliegenden Änderung eine Berichtigung der formellen Elemente an unterschiedlichen Stellen (Vereinheitlichung und Ergänzung von Verweisen und Quellenangaben).

3.6 Anhang 9: Metadaten für den Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen

Ziff. 2.2 *Spezialisierung der Gesundheitsfachperson*

Die Berichtigung der Gross- und Kleinschreibung bei der Ziffer 2.2 in Anhang 3 EPDV-EDI bedingt auch eine Anpassung der Ziffer 2.2.

Beilagen

- Entwurf Änderungserlass EPDV-EDI (SR *816.111*)
- Entwurf Anhang 2 zur EPDV-EDI, Ausgabe 6
- Entwurf Anhang 3 zur EPDV-EDI, Ausgabe 5
- Entwurf Anhang 4 zur EPDV-EDI, Ausgabe 2
- Entwurf Anhang 5 Ergänzung 1 zur EPDV-EDI, Ausgabe 6
- Entwurf Anhang 5 Ergänzung 2.1 zur EPDV-EDI, Ausgabe 5
- Entwurf Anhang 5 Ergänzung 2.2 zur EPDV-EDI, Ausgabe 4
- Entwurf Anhang 5 Ergänzung 2.3 zur EPDV-EDI, Ausgabe 5
- Entwurf Anhang 8 zur EPDV-EDI, Ausgabe 3
- Entwurf Anhang 9 zur EPDV-EDI, Ausgabe 3
- Begleitschreiben