Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Faktenblatt

Erfassung medizinischer Daten im EPD durch einen technischen Benutzer

Vor allem in grösseren Gesundheitseinrichtungen werden die medizinischen Daten aus dem eigentlichen Primärsystem (z. B. Klinikinformationssystem; KIS) zunächst in ein so genanntes (Universal-)Archiv überführt. Die Bereitstellung für das elektronische Patientendossier (EPD) in Gesundheitseinrichtungen, die einer EPD-(Stamm-)Gemeinschaft angeschlossen sind, soll dann – in der Rolle des IHE-Akteurs *Document Source* – aus diesem Archiv heraus und zwar automatisch, d.h. ohne dass eine Gesundheitsfachperson mit dem System interagiert, erfolgen. Dieser Anwendungsfall ist neben den Spitälern auch für andere EPD-Architekturen relevant. Es handelt sich also um eine «Dokumentenbereitstellung durch einen technischen Benutzer».

Das vorliegende Faktenblatt zeigt auf, welche Voraussetzungen bei der Dokumentenbereitstellung durch technische Benutzer (Rolle *technical user*; «TCU») zu berücksichtigen sind, damit das Verfahren mit den rechtlichen Vorgaben konform ist. Grundsätzlich gilt, dass folgende Voraussetzungen analog zur Bereitstellung medizinischer Dokumente durch Gesundheitsfachpersonen selbst zu erfüllen sind:

- Die inhaltliche Verantwortung von bereitgestellten medizinischen Dokumenten muss zurechenbar *(accountability*) und darf nicht abstreitbar sein (*non repudiation*);
- Die Verantwortung für die Selektion/Bereitstellung von medizinischen Dokumenten muss zurechenbar (*accountability*) und darf nicht abstreitbar sein (*non repudiation*) (vgl. Art. 10 Abs. 1 Bst. b EPDG). Falls eine Selektion und Bereitstellung aufgrund vordefinierter Selektionskriterien automatisch erfolgt, muss die für die Definition und Aktivierung der Kriterien verantwortliche Person zweifelsfrei identifiziert werden, was eine starke Authentifizierung mit zwei Faktoren für diese Person bedingt.
- Patientinnen und Patienten müssen die Möglichkeit haben, der vermuteten Einwilligung zur Bereitstellung medizinischer Dokumente im Einzelfall widersprechen zu können (vgl. Art. 3 Abs. 2 EPDG und Art. 10 Abs. 2 Bst. a EPDV).

Die Einhaltung dieser Vorgaben wird im Rahmen der Zertifizierung überprüft.

Authentifizierung bei der Erfassung medizinischer Daten im EPD durch technische Benutzer

Auch bei der Dokumentenbereitstellung im EPD durch einen technischen Benutzter gilt die Anforderung, dass vor der Datenbearbeitung (in diesem Falle der Erfassung medizinischer Daten) geprüft werden muss, ob es sich um einen korrekt authentifizierten und auch autorisierten Nutzer handelt. Die (Stamm-)Gemeinschaft muss daher sicherstellen, dass die Datenbereitstellung von einem dazu autorisierten und entsprechend authentifizierten System (IHE-Akteur in der Rolle *Document Source*) einer

Version 1.1
14.10.2019

Schwarzenburgstrasse 157
CH-3003 Berne

www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

angeschlossenen Gesundheitseinrichtung stammt (vgl. Ziff. 4.6.2 Bst. j und Ziff. 4.6.3 des Anhangs 2 der EPDV-EDI).

Da auch für den Anwendungsfall «Erfassung durch technische Benutzer» der Autorisierungsentscheid (*CH:ADR*) anhand der Berechtigungskonfiguration *(«policy stack»; CH:PPQ*) ermittelt werden muss, wird für die weitere Kommunikation der *Document Source* – wie bei natürlichen Benutzern – eine vom *X-Assertion Provider* signierte *CH:XUA User Assertion* (*User Authorization Token*) benötigt. Ein technischer Benutzer kann sich jedoch nicht gegen einen *Identity Provider (User Authentication Provider; IdP*) authentifizieren, da dies nur für natürliche Personen mit einer 2-Faktor-Authentifizierung möglich ist.

Um den technischen Benutzer (d. h. das bereitstellende System oder die Applikation) eindeutig und sicher zu identifizieren, muss dieser durch ein *CH:XUA User Authentication Token* (technisch eine *SAML 2 Identity Assertion*) authentifiziert sein. Die vom TCU selbst zu erzeugende *SAML 2 Identity Assertion* muss dabei mit einem gültigen und in der (Stamm-)Gemeinschaft registrierten Zertifikat (z. B. X-509) signiert werden. Das Zertifikat muss gültig sein und dem TCU eineindeutig und sicher zugeordnet sein. Die korrekte Verwaltung dieser Zertifikate, der Zuordnungen zu Systemen und damit die Vertrauenswürdigkeit der behaupteten Identitäten der Systeme in der Rolle TCU liegt in der Verantwortung des Datenschutz- und Datensicherheits-Verantwortlichen der jeweiligen (Stamm-)Gemeinschaft.

Um das für die Berechtigungssteuerung nötige *CH:XUA User Authorization Token* vom X-Assertion Provider zu erhalten, muss das zuvor erstellte und selbst-signierte *User Authentication Token* vom *X-Assertion Provider* bzgl. Validität, Authentizität und Integrität validiert werden. Kann der *X-Assertion Provider* die Validität, Integrität und Authentizität des *User Authentication Tokens* vom TCU bestätigen, darf dieser das von der Berechtigungssteuerung benötigte *CH:XUA User Authorization Token* generieren. Das vom *X-Assertion Provider* generierte *CH:XUA User Authorization Token* enthält die Rolle «TCU» im Attribut («*subject role*») für die zugreifende Person. Der technische Benutzer agiert im System – rechtlich gesehen analog einer Hilfsperson – «im Auftrag» einer realen Gesundheitsfachperson. Diese verantwortliche Gesundheitsfachperson wird im Attribut für die verantwortliche Person («*principal name*») aufgeführt. Im Gegensatz zu der inhaltlichen Verantwortlichkeit (s. u.) geht es hier um die Verantwortlichkeit für die Bereitstellung selbst. Im Fall von regelbasiert automatisiert bereitstellenden TCU ist hier die Person zu referenzieren, welche die rechtliche Verantwortung für die definierten Regeln übernimmt. Die rechtliche Verantwortung kann nur von Gesundheitsfachpersonen übernommen werden, die am EPD teilnehmen und entsprechend im HPD erfasst sind.

Metadaten bei der Erfassung medizinischer Daten im EPD durch technische Benutzer

Auch bei der Dokumentenbereitstellung durch technische Benutzer muss sichergestellt sein, dass für autorisierte Benutzer jederzeit – und zwar sowohl bei der Einsichtnahme ins EPD (*Document Registry*) wie auch beim Abruf der Protokolldaten (*CH:ATC*) – ersichtlich wird, wer oder welche Organisationseinheit für die Autorenschaft der jeweiligen medizinischen Daten im EPD verantwortlich ist. Dazu muss in den Metadaten im Minimum erfasst werden, in welcher Abteilung oder Klinik innerhalb der Gesundheitseinrichtung die medizinischen Daten erstellt wurden. Die für die fachliche Richtigkeit der medizinischen Daten verantwortliche Gesundheitsfachperson muss aus den Metadaten des Dokuments ersichtlich sein (z. B. Attribut *authorPerson* enthält GLN und Klarnamen des Autors) oder zur Not über die Angaben zum Autor im Dokument selbst (Informationen ersichtlich, wenn Dokument geöffnet wird). Ob die relevanten Metadaten bereits aus dem Primärsystem in das Archivsystem geliefert werden, oder erst dort ermittelt und angereichert werden, ist den jeweiligen Implementierungen überlassen.

Umsetzung des Widerspruchs zur vermuteten Zustimmung bei der Erfassung medizinischer Daten im EPD durch technische Benutzer

Das von der Gemeinschaft und Stammgemeinschaft gewählte organisatorische (oder technische) Verfahren, das dann zur Anwendung gelangt, wenn ein Patient oder eine Patientin nicht will, dass im Behandlungsfall bestimmte medizinische Daten im EPD erfasst werden, muss auch für die Erfassung medizinischer Daten durch technische Benutzter anwendbar sein.

Frist für Erfassung medizinischer Daten im EPD

Es gibt bislang keine rechtlichen Vorgaben zur Frist, innert der behandlungsrelevante Daten im EPD erfasst werden müssen. Somit ist es den Gemeinschaften und Stammgemeinschaften überlassen, eine interne Richtlinie für das Erfassen von Daten im EPD zu erarbeiten und die Gesundheitseinrichtungen vertraglich zu deren Einhaltung zu verpflichten, sofern nicht übergeordnete Bestimmungen (z. B. kantonale Gesetze) dies konkret fordern. Dabei gilt es zu berücksichtigen, dass die Fristen so gewählt werden, dass sie den Zwecken des EPD (Unterstützung der Behandlungsprozesse, Förderung der Patientensicherheit, Verbesserung der Behandlungsqualität etc.) nicht entgegenlaufen. Allenfalls sind auch spezielle Regelungen für das Erfassen sensibler Daten, die der Patient oder die Patientin nicht ohne begleitendes Gespräch durch eine Gesundheitsfachperson einsehen sollte, vorzusehen. Diese Richtlinie muss sowohl für die Erfassung medizinischer Daten durch Gesundheitsfachpersonen als auch durch technische Benutzer gelten.

Neue Versionen von Metadaten und/oder Dokumenten

Da die beschriebenen *Document Sources* in der Rolle TCU keine Zugriffsrechte zum Lesen von medizinischen Daten erhalten können, ist es grundsätzlich nicht möglich, bereits bereitgestellte Daten zu aktualisieren (d. h. neue Versionen von Dokumenten oder Metadaten bereitzustellen). Technisch wäre dies zwar noch solange möglich, bis sich die, dem TCU durch die Bereitstellung bekannte, *UUID* des Metadatensatzes wieder geändert hat. Ist zwischenzeitlich ein neuer Metadatensatz mit neuer *UUID* erzeugt worden – z. B. weil der Patient oder die Patientin die Vertraulichkeitsstufe geändert hat – wird die Transaktion nicht erfolgreich sein. Es wird daher empfohlen keine nachträglichen Aktualisierungen der Metadaten nach der einmal erfolgten Bereitstellung durch einen TCU durchzuführen. Gegebenenfalls wird diese Möglichkeit durch eine technisch-normative Vorgabe (z. B. keine Autorisierung für *XDS Metadata Update* in der Rolle TCU) ausgeschlossen werden.