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

Factsheet

Top 10 Sicherheitsmassnahmen im EPD

Der Datenschutz und die Datensicherheit (DSDS) sind beim elektronischen Patientendossier (EPD) von zentraler Bedeutung. Die technischen und organisatorischen Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften («TOZ»; Anhang 2 der EPDV-EDI) enthalten weit über hundert Anforderungen, die sich auf das Thema DSDS beziehen. Der formale Zertifizierungsprozess sorgt dafür, dass diese Anforderungen tatsächlich eingehalten werden.

Für das EPD gelten die höchsten Sicherheitsstandards, die dank ihrer Verankerung im Gesetz auch rechtlich durchgesetzt werden können. Dieses Factsheet beschreibt zehn wichtige Sicherheitsmassnahmen auf den Ebenen der Anwendung («A»), der Technik («T») und der Organisation («O»):

Sicherheitsmassnahmen zur Absicherung der **Anwendungsebene (A)**:

A1	Sichere Identifizierung und 2-Faktor-Authentifizierung aller Benutzer
A2	Patientinnen und Patienten steuern den Zugriff auf ihr EPD selber
A3	Alle Zugriffe auf ein EPD werden protokolliert
A4	Patientinnen und Patienten bestimmen selber, wie lange ihre Daten im EPD aufbewahrt werden

Sicherheitsmassnahmen für den sicheren Betrieb der **technischen Systeme und Netzwerke (T)**:

T1	Anomalie-Erkennung und automatische Alarmierung
T2	Verschlüsselte Datenaufbewahrung in der Schweiz
T3	Sichere Kommunikationsverbindungen

Organisatorische Sicherheitsmassnahmen **(O)**:

O1	Kontinuierliches Sicherheitsmanagement inklusive Meldepflicht bei Sicherheitsvorfällen
O2	Auswahl und Instruktion der Benutzer und des administrativen Personals
O3	Sicherheitsprüfungen

Diese Liste ist nicht abschliessend. Trotzdem sollte sie aufzeigen können, warum das EPD heute zu den sichersten Anwendungen überhaupt gehört und weshalb dies auch so bleiben wird.

Jede Sicherheitsvorkehrung hat ihre Grenzen und das gilt auch für das EPD. Die nachfolgende tabellarische Beschreibung der Top Ten Sicherheitsmassnahmen im EPD adressiert deshalb nicht nur ihre Sicherheitswirkung, sondern auch die jeweiligen Grenzen.

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

Schwarzenburgstrasse 157
CH-3003 Bern

www.e-health-suisse.ch

Sicherheitsmassnahmen auf der Anwendungsebene («A»)

A1	Sichere Identifizierung und 2-Faktor Authentifizierung aller Benutzer
Für die Anmeldung am EPD braucht es zusätzlich zu einem Passwort oder einem biometrischen Merkmal (Faktor «Wissen» oder «Sein») den Besitz eines sicheren Identifikationsmittels (Faktor «Haben»). Dieses Identifikationsmittel muss der (hohen) Vertrauensstufe 3 der Norm ISO/IEC 29115:2013 entsprechen und von einem zertifizierten Herausgeber (auch *Identity Provider* oder IdP genannt) ausgestellt werden.	
Sicherheits-wirkung	Die sogenannte 2-Faktor-Authentifizierung (2FA) ist eine wirksame Massnahme gegen den Identitätsdiebstahl und kann insbesondere verhindern, dass sich Hacker mit gestohlenen Anmeldedaten in das EPD einer Patientin oder eines Patienten einwählen.
Grenzen	Die Benutzer müssen selber für die sichere Aufbewahrung ihres Identifizierungsmittels sorgen und dürfen sich auch von raffinierten *Phishing* E-Mails nicht zur Preisgabe von geheimen Informationen (z.B. Passwörtern) oder zur Ausführung von Schadsoftware verleiten lassen.
Referenzen	EPDG Art. 7, EPDV Art. 9, Art. 17, Art. 23 bis Art. 27 sowie Art. 31, TOZ Ziffern 1.4, 1.6.2, 4.13.1 und 8.3

A2	Patientinnen und Patienten steuern den Zugriff auf ihr EPD selber
Vor jedem Zugriff auf ein Dokument in einem EPD wird geprüft, ob das benötigte Zugriffsrecht vorliegt. Nur die Patientinnen und Patienten haben vollen Zugriff auf ihr EPD. Sie alleine entscheiden, welche Gesundheitsfachpersonen ebenfalls Zugriff erhalten, für welche Vertraulichkeitsstufe von Dokumenten deren Zugriffsrecht jeweils gilt und ob sie es an weitere Gesundheitsfachpersonen übertragen dürfen. Andere Personengruppen (z.B. Krankenversicherer, Forscher, Behörden) sind vom EPD ausgeschlossen. Patientinnen und Patienten können ihre eigenen Berechtigungen (inklusive des Rechts zur Rechtevergabe) pauschal an einen oder mehrere Stellvertreter (z.B. Familienangehörige) delegieren, wenn sie dies wollen. Eine detailliertere Beschreibung der Zugriffsrechtevergabe findet sich auf der EPD-Webseite unter www.patientendossier.ch/de/bevoelkerung/informationen/funktionen/zugriffsrechte-erteilen.	
Sicherheits-wirkung	Das Zugriffskontrollsystem des EPD gibt den Patientinnen und Patienten das Mittel für die informationelle Selbstbestimmung über ihre Gesundheitsdaten im EPD in die Hand. Die Durchsetzung dieses Rechtes wird vom Gesetzgeber auch dadurch unterstützt, dass der missbräuchliche Zugriff auf ein EPD nach Art. 24 EPDG mit einer hohen Busse bestraft wird.
Grenzen	Gesundheitsfachpersonen müssen die zur Behandlung beigezogenen Dokumente in ihre eigenen Systeme übernehmen. Mit dem Download der behandlungsrelevanten Dokumente verlassen diese den Wirkungskreis der EPD-Zugriffskontrolle und es kommen die etablierten internen Verfahren der Gesundheitseinrichtung (Spital, Arztpraxis, …) zum Zug. Die informationelle Selbstbestimmung geht mit einer hohen Eigenverantwortung einher. Patientinnen und Patienten müssen bei der Vergabe der Zugriffsrechte die nötige Sorgfalt walten lassen und insbesondere ihren Stellvertretern vertrauen können.
Referenzen	EPDG Art. 9 und Art. 24, EPDV Art. 1 bis Art. 4, TOZ Ziffern 2.1 bis 2.3

A3	**Alle Zugriffe auf ein EPD werden protokolliert**
Jeder Zugriff auf ein Dokument in einem EPD wird protokolliert. Patientinnen und Patienten können im Patientenportal jederzeit sehen, welche Person zu welchem Zeitpunkt auf welches Dokument zugegriffen hat. Patientinnen und Patienten können sich ausserdem aktiv über Notfallzugriffe oder Veränderungen an GFP-Gruppenzugehörigkeiten informieren lassen (z.B. mittels SMS). Die Protokolldaten werden 10 Jahre aufbewahrt und können nicht gelöscht werden (auch nicht durch die Patientin oder den Patienten selber).	
Sicherheitswirkung	Die Protokollierung im EPD stellt einen sehr hohen Grad der Nachvollziehbarkeit sicher. Dies hat auch eine präventive bzw. abschreckende Wirkung, weil jede zugreifende Person damit rechnen muss, die Rechtmässigkeit des Zugriffs belegen zu müssen.
Grenzen	Dank der Protokollierung können missbräuchliche Zugriffe aufgedeckt und strafrechtlich verfolgt, nicht aber verhindert oder rückgängig gemacht werden
Referenzen	EPDG Art. 10, EPDV Art. 9 und Art. 18, TOZ Ziffern 2.10 und 9.3

A4	**Patientinnen und Patienten bestimmen selber, wie lange ihre Daten im EPD aufbewahrt werden**
Wenn eine Patientin oder ein Patient nichts anderes vorsieht, dann werden die Daten in ihrem EPD nach 20 Jahren automatisch gelöscht. Patientinnen und Patienten können ihre Daten aber auch jederzeit selber löschen oder von der automatischen Löschfrist ausnehmen.	
Sicherheitswirkung	Die Backupverfahren der (Stamm-)Gemeinschaften stellen sicher, dass Gesundheitsdaten im EPD nicht verloren gehen. Die informationelle Selbstbestimmung der Patientinnen und Patienten und insbesondere ihr «Recht auf Vergessen» werden dadurch aber nicht tangiert.
Grenzen	Gesundheitsfachpersonen müssen die zur Behandlung beigezogenen Dokumente in ihren eigenen Systemen aufbewahren. Mit dem Download der behandlungsrelevanten Dokumente verlassen diese den Rechtsrahmen des EPD und es kommen die kantonalen gesetzlichen Aufbewahrungsfristen zur Anwendung.
Referenzen	EPDV Art. 10, TOZ Ziffern 9.4.1 und 10

Sicherheitsmassnahmen auf der technischen Ebene («T»)

T1	**Anomalie-Erkennung und automatische Alarmierung**
Jede (Stamm-)Gemeinschaft verfügt über ein sogenanntes SIEM (*Security Information and Event Management*), das die Protokolldaten inklusive der technischen Ereignisprotokolle laufend überwacht. Ein Regelwerk erkennt unübliche Muster (Anomalien), die auf einen Angriff aus dem Internet oder einen missbräuchlichen Zugriff hinweisen, und löst einen entsprechenden Alarm aus. Jede (Stamm-)Gemeinschaft verfügt über einen Prozess für den Umgang mit Sicherheitsvorfällen, so dass der Alarm analysiert wird und bei Bedarf geeignete Gegenmassnahmen getroffen werden.	
Sicherheitswirkung	Die automatisierte Erkennung von potentiellen Sicherheitsvorfällen ermöglicht eine rasche Reaktion auf Angriffsversuche oder Missbräuche.
Grenzen	Die «EPD-Alarmanlage» kann einen Schaden manchmal nur begrenzen und nicht verhindern.
Referenzen	EPDV Art. 12, TOZ Ziffern 4.3 und 4.15.6

T2	**Verschlüsselte Datenaufbewahrung in der Schweiz**
Die Daten im EPD (inklusive aller Backups) sind verschlüsselt gespeichert und befinden sich in der Schweiz bei Unternehmen, die dem Schweizer Recht unterstehen. Diese Unternehmen dürfen die Daten für keine anderen Zwecke nutzen und können nicht von einer ausländischen Behörde zur Datenherausgabe gezwungen werden.	
Sicherheitswirkung	Die Verschlüsselung der gespeicherten Daten schützt wirksam gegen eine Umgehung der EPD-Zugriffskontrolle.
Grenzen	Sehr wenige namentlich bekannte Personen (im Fachjargon auch *golden key holder* genannt) können sich direkten Zugang zu den Daten verschaffen. Die TOZ definieren aber eine ganze Reihe von technischen und organisatorischen Massnahmen im Bereich der Betriebssicherheit, die das von solchen «Innentätern» ausgehende Risiko soweit möglich mitigieren.
Referenzen	EPDV Art. 10 und Art. 12, TOZ Ziffern 2.5.b, 13 bis 15 sowie 19

T3	**Sichere Kommunikationsverbindungen**
Die (Stamm-)Gemeinschaften mit den angeschlossenen Gesundheitseinrichtungen bilden einen Vertrauensraum, der mit kryptographischen Mitteln auf Basis der Protokolle von TLS (*Transport Layer Security*) vom Internet isoliert ist. Die sichere Konfiguration aller TLS-Endpunkte wird regelmässig mit Schwachstellendetektoren (sogenannte *Vulnerability Scanner*) überprüft.	
Sicherheitswirkung	Die konsequente Verwendung von MTLS (*Mutually authenticated Transport Layer Security*) verhindert, dass unerwünschte Kommunikationsverbindungen mit dem EPD-Vertrauensraum aufgebaut werden oder dass die Kommunikationsverbindungen innerhalb des EPD-Vertrauensraums abgehört werden.
Grenzen	Wirksame Kryptographie setzt voraus, dass alle Teilnehmer am EPD-Vertrauensraum ihre geheimen Kommunikationsschlüssel gemäss den gesetzlichen Vorgaben korrekt verwalten.
Referenzen	EPDV Art. 10, TOZ Ziffern 2.5.a, 4.12 und 4.15

Sicherheit auf der Organisationsebene («O»)

O1	Kontinuierliches Sicherheitsmanagement inklusive Meldepflicht bei Sicherheitsvorfällen
In jeder (Stamm-)Gemeinschaft sorgt ein DSDS-Verantwortlicher dafür, dass die Sicherheitsrisiken kontinuierlich identifiziert, bewertet und begrenzt werden. Er tauscht sich regelmässig mit den Behörden und seinen Kollegen bei den anderen (Stamm-)Gemeinschaften aus und kann im Bedarfsfall auch Sicherheitsmassnahmen anordnen, die über die gesetzlichen Bestimmungen hinausgehen. Der DSDS-Verantwortliche verantwortet auch den gesetzlich vorgeschriebenen Prozess für die unverzügliche Meldung von Datenschutz- und Datensicherheitsereignissen an das BAG.	
Sicherheitswirkung	Eine tragfähige Sicherheitsorganisation mit etablierten Prozessen schafft die unerlässliche Basis für die laufende Verbesserung des Sicherheitsdispositivs und dessen Anpassung an das sich ständig verändernde Umfeld. Mit dem EPD wird erstmalig im Gesundheitswesen eine Meldepflicht für Sicherheitsvorfälle auf nationaler Ebene eingeführt, was die Transparenz und die Steuerbarkeit der Massnahmen für Datenschutz und Datensicherheit unterstützt.
Grenzen	Eine hundertprozentige Sicherheit kann auch mit dem besten Sicherheitsmanagement nie erreicht werden.
Referenzen	EPDV Art. 12, TOZ Ziffern 4.2, 4.3.3.a und 4.11

O2	Auswahl und Instruktion der Benutzer und des administrativen Personals
Die DSDS-Schulung (*Awareness Training*) ist ein obligatorisches Element der EPD-Schulung aller Gesundheitsfachpersonen und des administrativen Personals (z.B. Supportstellen, Systembetreiber). Alle diese Personengruppen, sofern sie nicht ohnehin der ärztlichen Schweigepflicht unterstellt sind, müssen eine entsprechende Schweigepflichterklärung unterzeichnen. Zur sorgfältigen Auswahl des Personals bei den (Stamm-)Gemeinschaften und ihren Plattform-Anbietern gehört auch die obligatorische Prüfung von Betreibungsregister und Strafregister.	
Sicherheitswirkung	Alle Personen mit Zugang zum EPD sind sich bewusst, dass sie besonders schützenswerte Personendaten bearbeiten. Sie verfügen über eine Grundausbildung zum Umgang mit solchen Daten und kennen die Strafbestimmungen bei fehlbarem Verhalten, was die Wahrscheinlichkeit von bewussten oder unbewussten Regelverstössen auf ein Minimum reduziert.
Grenzen	Benutzerfehler beim Umgang mit dem EPD lassen sich nicht gänzlich verhindern.
Referenzen	TOZ Ziffern 4.2.2, 4.8, 4.9

O3	Sicherheitsprüfungen
Jede (Stamm-)Gemeinschaft verfügt über Werkzeuge und Prozesse, um Sicherheitsschwachstellen (z.B. veraltete Software, fehlende *Patches*, unsorgfältige Konfigurationen) zu entdecken und zu beheben. Nach jeder sicherheitsrelevanten Veränderung und insbesondere vor der Einführung jedes neuen Software-Releases werden ausserdem die Zugänge zum EPD von hierauf spezialisierten Firmen (sogenannte *White Hat Hacker*) auf potentielle Sicherheitsschwachstellen untersucht.	
Sicherheitswirkung	Programmfehler oder Konfigurationsfehler werden entdeckt und behoben, bevor die Anwendung aus dem Internet zugreifbar und damit angreifbar ist.
Grenzen	Auch die aktuellsten Schwachstellendetektoren (*Vulnerability Scanner*) und bestens qualifizierte *White Hat Hacker* bieten keine Garantie dafür, restlos alle Schwachstellen aufzudecken, bevor dies ein anderer tut. Gefährlich sind insbesondere neu entdeckte Schwachstellen, für die noch keine Sicherheitspatches verfügbar sind (sogenannte *Zero Day Exploits*).
Referenzen	TOZ Ziffern 3.4.1, 3.4.2, 4.4, 4.5