Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Abteilung Kommunikation und Kampagnen

Faktenblatt

Datum: 28. Juni 2023

Datensicherheit im elektronischen Patientendossier

Datenschutz und Datensicherheit sind für das elektronische Patientendossier (EPD) von zentraler Bedeutung. Das Bundesgesetz über den Datenschutz (DSG) und das Bundesgesetz über das elektronische Patientendossier (EPDG) sorgen dafür. Die EPD-Gemeinschaften wie auch die Herausgeber der Identifikationsmittel (elektronische Identität) und die Gesundheitseinrichtungen müssen strenge Auflagen erfüllen, um ihre Zertifizierung zu erhalten. Es werden regelmässig Kontrollen durchgeführt, um die Einhaltung dieser Auflagen zu überprüfen. Dies soll gewährleisten, dass die im EPD abgelegten Unterlagen vor jeglichem externen Zugriff geschützt und **sicher** archiviert sind.

Zertifizierung nach dem EPDG

Das Gesetz regelt die technischen Spezifikationen und das Sicherheitsniveau des EPD.

Nur zertifizierte EPD-Gemeinschaften dürfen das offizielle Logo verwenden. Dieses belegt, dass es sich um einen vertrauenswürdigen Anbieter handelt, der alle einschlägigen Vorschriften des Bundes einhält.

Die technischen und organisatorischen Zertifizierungskriterien für EPD-Gemeinschaften umfassen über 400 Anforderungen, von denen rund 100 den Datenschutz und die Datensicherheit betreffen. Die organisatorischen Sicherheitskriterien beziehen sich namentlich auf die Schulung des Personals und die Ernennung von Sicherheitsverantwortlichen.

Identifizierte Zugriffe

Ob Patient/-in, Gesundheitsfachperson, Hilfskraft oder Vertreter/-in: Alle am EPD beteiligten Personen müssen sich sicher und eindeutig mittels elektronischer Identität identifizieren können. Die Zwei-Faktor-Authentifizierung und das Sicherheitsniveau sind ähnlich wie beim eBanking. Die Stammgemeinschaften sind verpflichtet, die Identität der am EPD beteiligten Gesundheitsfachpersonen und ihrer Hilfskräfte zu überprüfen.

Protokollierung der Zugriffe

Alle Namen der Personen, die Unterlagen gesichtet haben, sowie die Daten, an denen sie diese Informationen abgerufen oder neue Dokumente abgespeichert haben, werden im EPD verzeichnet. Die Daten im Zugriffsprotokoll können zehn Jahre lang eingesehen werden. Während dieses Zeitraums können sie nicht gelöscht werden. Anhand des Zugriffsprotokolls können Missbräuche aufgedeckt und strafrechtlich geahndet werden.

Weitere Informationen:
Bundesamt für Gesundheit, Medien und Kommunikation, www.bag.admin.ch
Diese Publikation erscheint ebenfalls in französischer, italienischer und englischer Sprache.

Verschlüsselte Datenaufbewahrung in der Schweiz

Die Daten im EPD (inkl. aller Backups) werden verschlüsselt gespeichert und von in der Schweiz ansässigen Unternehmen aufbewahrt, die dem Schweizer Recht unterstehen. Diese Unternehmen dürfen die Daten nicht zu anderen Zwecken nutzen und können nicht von einer ausländischen Behörde zur Datenherausgabe gezwungen werden.

Gesicherte Kommunikation

Die (Stamm-)Gemeinschaften bilden zusammen mit den angeschlossenen Gesundheitseinrichtungen einen geschützten Vertrauensraum. Die Sicherheit dieses Raums wird regelmässig mit Schwachstellendetektoren überprüft. Jede EPD-Gemeinschaft verfügt über einen Prozess für das Störfallmanagement bei einer Anomalie.

Weitere Informationen:
Bundesamt für Gesundheit, Medien und Kommunikation, www.bag.admin.ch
Diese Publikation erscheint ebenfalls in französischer, italienischer und englischer Sprache.