Elektronisches Patientendossier (EPD)

Bedrohungs- und Risikoanalyse

Status *	Abgeschlossen
Projektname / Schutzobjekt	Bedrohungs- und Risikoanalyse Elektronisches Patientendossier (EPD)
Projektnummer	
Auftraggeber	Bundesamt für Gesundheit BAG
Geschäftsprozessver-antwortlicher	
Projektleiter	Reinhold Sojer
ISDSV	
Bearbeitende	Thomas Kessler und Erik Küng, beide TEMET AG
Prüfende	Reinhold Sojer und Walid Ahmed, beide BAG
Genehmigung durch Projektauftraggeber und/oder Geschäfts-prozessverantwortli-cher	
Version	1.0

* In Arbeit, In Prüfung, Abgeschlossen/Genehmigt

Änderungskontrolle, Prüfung, Genehmigung

Datum	Version	Autor(en)	Beschreibung
10.07.2015	0.1	Thomas Kessler, Erik Küng	Initialversion
31.07.2015	0.3	Thomas Kessler, Erik Küng	Big Picture, Schutzobjekte, Schadenszenarien
14.08.2015	0.5	Thomas Kessler, Erik Küng	Erste Risikoübersicht hinzugefügt
09.09.2015	0.7	Thomas Kessler, Erik Küng	Erster Massnahmenkatalog hinzugefügt
17.09.2015	0.75	Thomas Kessler	Massnahmenkatalog überarbeitet, Restrisiken beschrieben, Zusammenfassung entworfen
01.10.2015	0.80	Thomas Kessler, Erik Küng	Inhaltlich vollständiger Entwurf
20.10.2015	0.85	Thomas Kessler	Massnahmenkatalog überarbeitet: Empfehlungen zum besonderen Schutz sensibler Daten von den übrigen Massnahmen separiert.
04.11.2015	0.90	Erik Küng, Thomas Kessler	Version zur Abnahme durch BAG
09.11.2015	1.0	Erik Küng, Thomas Kessler	Abschliessende Version z.Hd. Auftraggeber

Inhaltsverzeichnis

Zusammenfassung

Das elektronische Patientendossier (EPD) ist ein komplexes System, bei dem viele Komponenten zusammenwirken und die Kommunikation zu grossen Teilen über das öffentliche Internet stattfindet. Daraus entstehen Risiken in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit.

Datenschutz und Datensicherheit sind im Grundkonzept des EPD vorgesehen und auch im Bundesgesetz über das EPD prominent adressiert. Die gesetzlichen Vorgaben definieren insbesondere die Eckpunkte in Bezug auf die sichere Identifikation, die Rechteverwaltung und die Protokollierung aller EPD-Zugriffe.

Auf Grund der vorliegenden Bedrohungs- und Risikoanalyse werden ergänzende Sicherheitsmassnahmen in Bezug auf die Organisation der (Stamm-)Gemeinschaften, die applikatorische Sicherheit sowie die technische Sicherheit der Betriebsplattformen und Systeme empfohlen:

- Bei der ***Organisation*** stehen die Klärung der Verantwortlichkeiten sowie die Etablierung von Prozessen für die Pflege der Informationssicherheit und den Umgang mit Sicherheitsereignissen im Vordergrund. Als diesbezügliche Schlüsselmassnahme wird empfohlen, von jeder (Stamm-)Gemeinschaft die Nominierung eines Informationssicherheitsbeauftragten (ISBO) einzuverlangen.
- Die Massnahmen auf der ***applikatorischen Ebene*** konzentrieren sich auf die sichere Identifikation der Benutzer und Systeme sowie die Zugriffskontrolle, wobei mehrere spezielle Vorkehrungen zum Schutz von sensiblen und geheimen Dokumenten empfohlen werden. Eine zusätzliche Bestätigung von Notfallzugriffen, analog der im e-Banking gebräuchlichen Transaktionsbestätigung, könnte zudem den Missbrauch dieser kritischen Funktion durch unberechtigte Dritte wesentlich erschweren.
- Bei den ***technischen Massnahmen*** sind die logische Isolation des EPD Vertrauensraums vom Internet sowie die netzwerktechnische Separierung der EPD Datenbestände von anderen Systemen beim Betreiber oder beim Primärsystem besonders wichtig. Ein besonderes Augenmerk gilt ausserdem dem Schutz der internen und externen Zugangsportale vor Angriffen aus dem Internet.

Trotz aller Massnahmen wird es nicht gelingen, jede unberechtigte Einsicht in das EPD von Patienten und Patientinnen auf Dauer zu verhindern. Speziell ist mit folgenden Schadenfällen zu rechnen:

- ***Missbrauch unsicherer Endgeräte von Patienten und GFP durch Dritte:*** Phishing und Social Engineering Angriffe werden dazu führen, dass Endgeräte von Patienten oder Gesundheitsfachpersonen von Dritten kontrolliert und ferngesteuert werden. Die Tragweite solcher Schadenfälle hängt von den Berechtigungen der betroffenen Personen ab sowie davon, wie rasch der Angriff entdeckt und unterbunden wird.
- ***Nachlässige Rechtevergabe durch Patienten und Fehler bei der Verwaltung von Organisationszugehörigkeiten:*** Fehler bei der Erteilung der Zugriffsrechte durch Patienten und bei der Verwaltung von Organisationszugehörigkeiten im nationalen Verzeichnis der Gesundheitsfachpersonen lassen sich nicht vollständig vermeiden. Beides kann dazu führen, dass Gesundheitsfachpersonen Zugriff auf unerwünscht viele elektronische Patientendossiers erhalten.
- ***Datendiebstahl durch Insider oder Hacker:*** Technische Zugriffe unter Umgehung der applikatorischen Rechteverwaltung können auf wenige Personen eingeschränkt aber nicht völlig unterbunden werden. Ein Datendiebstahl auf diesem Weg wäre von potentiell sehr grosser Tragweite, weshalb die Eintretenswahrscheinlichkeit auf ein absolutes Minimum begrenzt werden muss.
- ***Erfolgreiche Angriffe aus dem Internet auf ein internes oder externes Zugangsportal:*** Der sichere Betrieb einer Internet-Webapplikation stellt hohe Ansprüche an die technische und prozedurale Kompetenz des Betreibers und die Softwareentwicklung. Langjährige Erfahrung im e-Banking hat gezeigt, dass sich die entsprechende Lernkurve nicht beliebig verkürzen lässt.

Angesichts dieser Restrisiken ist es eminent wichtig, dass die für eine zeitnahe Erkennung und fachgerechte Behandlung von Sicherheitsereignissen erforderlichen Prozesse und Verantwortlichkeiten vor der Betriebsaufnahme einer (Stamm-)Gemeinschaft definiert und etabliert werden.

1 Einleitung

1.1 Ausgangslage

Das Bundesgesetz über das elektronische Patientendossier (EPDG) wurde von beiden Räten in der Schlussabstimmung vom 19. Juni 2015 verabschiedet. Die Vorbereitungen zur Ausgestaltung des Ausführungsrechts zum EPDG haben inzwischen begonnen. In der nun folgenden Phase wird für die Zertifizierungskriterien nach Art. 12 Abs. 1 Bst. b unter anderem festzulegen sein, wie der Datenschutz und die Datensicherheit zu gewährleisten sind.

Gemäss Botschaft zum Entwurf des EPDG ist es erforderlich, dass schweizweit einheitliche Regeln im Bereich des Datenschutzes und der Datensicherheit im Rahmen der Zertifizierungsvoraussetzungen definiert werden. Für die Festlegung der Zertifizierungsvoraussetzungen ist eine Bestandsaufnahme möglicher Bedrohungen, eine Analyse der betroffenen IT-Systeme sowie des potentiellen Schadens unabdingbar. Die empfohlenen technischen und organisatorischen Massnahmen müssen ausgewogen hinsichtlich der betrieblichen Produktivität und der Wirtschaftlichkeit sein.

Als Basis für die Festlegung der Zertifizierungskriterien in Bezug auf den Datenschutz und die Datensicherheit soll im 3. Quartal 2015 eine Bedrohungs- und Risikoanalyse (vorliegendes Dokument) für die wesentlichen Elemente der Informatikinfrastruktur (EIIS) von (Stamm-)Gemeinschaften und Zugangsportalen sowie der Abfragedienste und ZAS durchgeführt werden.

1.2 Zielsetzung

Bezogen auf die Zertifizierung von (Stamm-)Gemeinschaften gemäss Art. 12 Abs. 1 Bst. b des Entwurfs EPDG werden mit der Bedrohungs- und Risikoanalyse die folgenden Ziele verfolgt:

- Die wesentlichen Risiken im Gesamtsystem EPD sind identifiziert;
- Eintretenswahrscheinlichkeit und Schadensausmass sind für jedes der wesentlichen Risiken quantifiziert. Nicht-mitigierbare Risiken oder solche, die nur mit unverhältnismässig hohem Aufwand mitigiert werden können, sind explizit ausgewiesen;
- Anwendbare Normen und Standards zur Mitigation der Risiken sind evaluiert;
- Ergänzende oder weitergehende Empfehlungen sind formuliert.

1.3 Umfang (Scope)

Der Untersuchungsgegenstand ist in Kapitel 3.1 „Systemübersicht“ graphisch dargestellt. Insbesondere gehören die folgenden Elemente der Informatikinfrastruktur dazu:

- Gateway
- Master Patient Index
- Dokumenten-Register
- Dokumenten-Ablage(n) in der (Stamm-)Gemeinschaft und dedizierte bei den Primärsystemen
- System zur Steuerung der Zugriffsrechte
- Protokollierungs-System
- internes oder externes Zugangsportal
- Health Professionals Index (HPI) und Health Organisation Index (HOI)
- Community Portal Index (CPI)
- Metadaten-Index (MDI)
- Systemanbindung der Primärsysteme (eHealth-Connector)
- Identity and Access Management (IAM) System einer (Stamm-)Gemeinschaft

1.4 Abgrenzung

Soweit die Schnittstellen und internen Systeme der Gesundheitseinrichtungen der (Stamm-)Gemeinschaften betroffen sind, werden auch diese in die Analyse einbezogen. Alle weiteren internen Systeme der Gesundheitseinrichtungen wie z. B. Labor- oder Radiologie-Informations-systeme sowie deren angeschlossenen Medizingeräte sind nicht Gegenstand dieser Risiko- und Bedrohungsanalyse. Ferner sind die Zugriffsregeln für das EPD und deren Durchsetzung ebenfalls nicht Teil dieser Risiko- und Bedrohungsanalyse.

1.5 Basis Sicherheit

Vor der Durchführung dieser Bedrohungs- und Risikoanalyse wurde die Annahme getroffen, dass eine Basis Sicherheit in Bezug auf den Aufbau und Betrieb einer (Stamm-)Gemeinschaft vorhanden ist. Damit ist gemeint, dass heute allgemein bekannte, unumstrittene minimale Sicherheitsmassnahmen bereits umgesetzt sind: Es betrifft dies Bereiche wie:

- Sicherheitsschulung
- Zugriffskontrolle
- Physikalische Sicherheit
- Schutz vor Schadsoftware
- Backup
- Schwachstellen-Management, Software Updates
- Netzwerksicherheit
- Incident Management
- Business Continuity Management
- Compliance

Die getroffene Annahme beinhaltet ebenfalls Massnahmen, welche die geforderte hohe Verfügbarkeit gewährleisten sollen. Trotzdem wurden für Risiken teilweise Massnahmen aufgeführt, welche heute als allgemein bekannt und angewendet gelten. Dies um die Wichtigkeit dieser Massnahmen hervorzuheben.

1.6 Aufbau des Dokumentes

- Kapitel 2 „Systembeschreibung und Schutzobjekte„ zeigt das Gesamtsystem im Rahmen eines Big Picture und beschreibt die wichtigsten Daten, Benutzergruppen, Prozesse und Komponenten.
- Kapitel 3 „Risikoanalyse„ ist das zentrale Kapitel dieses Dokuments. Es identifiziert und bewertet die Sicherheitsrisiken nach Tragweite und Eintretenswahrscheinlichkeit.
- Kapitel 4 „Sicherheitsmassnahmen“ fasst die empfohlenen Sicherheitsmassnahmen tabellarisch in einem Massnahmenkatalog zusammen und beschreibt die verbleibenden Restrisiken.

Anhang A dokumentiert die Grundlagen der Risikoeinschätzung.

Anhang B erläutert einzelne Fachbegriffe der Informationssicherheit.

Anhang C gibt eine Übersicht der in diesem Dokument benutzen Abkürzungen.

1.7 Input-Dokumente

[Referenz] und Titel	Autor	Version	Datum
[Standards und Architektur - Erste Empfehlungen]	eHealth Suisse	-	20.08.2009
[Standards und Architektur Empfehlungen II]	eHealth Suisse	-	21.10.2010

[Referenz] und Titel	Autor	Version	Datum
[Standards und Architektur Empfehlungen III] Personenidentifikation und Berechtigungssystem	eHealth Suisse	-	27.10.2011
[Standards und Architektur Empfehlungen IV] Kommunikation zwischen (Stamm-)Gemeinschaften / Zugangsportal	eHealth Suisse	-	17.01.2013
[Standards und Architektur Empfehlungen V] Regeln für die Steuerung der Zugriffsrechte	eHealth Suisse	-	28.08.2014
[ARGE EPD-Anwendungsfälle Berechtigung] Anwendungsfälle und Metadaten für Berechtigungssteuerung	eHealth Suisse	1.0	01.07.2013
[Botschaft] zum Bundesgesetz über das elektronische Patientendossier		-	29.05.2013
[network_overview2.pdf] Beispielhafter Entwurf Architekturskizze	BAG	-	-
[Erläuterungen_Landkarte-EPD_v091.pdf] Prozesslandkarte EPD	BAG	0.91	-
IHE-ITI TF vol.2x Annex K	IHE International	11.0	23.09.2014
IHE IT Infrastructure Technical Framework, Volume 2x (ITI TF-2x): Appendices (K.1: Security Environments)	IHE International	11.0	23.09.2014
HIE Security and Privacy through IHE Profiles	IHE International	2.0	22.08.2008
Cookbook for Security Considerations (IHE Wiki)	IHE International	online	online
[ISDS_Konzept_Template_Version_2-0-d.docx] Informationssicherheits- und Datenschutzkonzept		2.0	01.03.2015
[Vorlage_Risikoanalyse_ISDS-Konzept_V2-0-d.xls] ISDS Konzept, Risikoanalyse		2.0	02.03.2015

Tabelle 1: Input-Dokumente

2 Systembeschreibung und Schutzobjekte

2.1 Systemübersicht („Big Picture“)

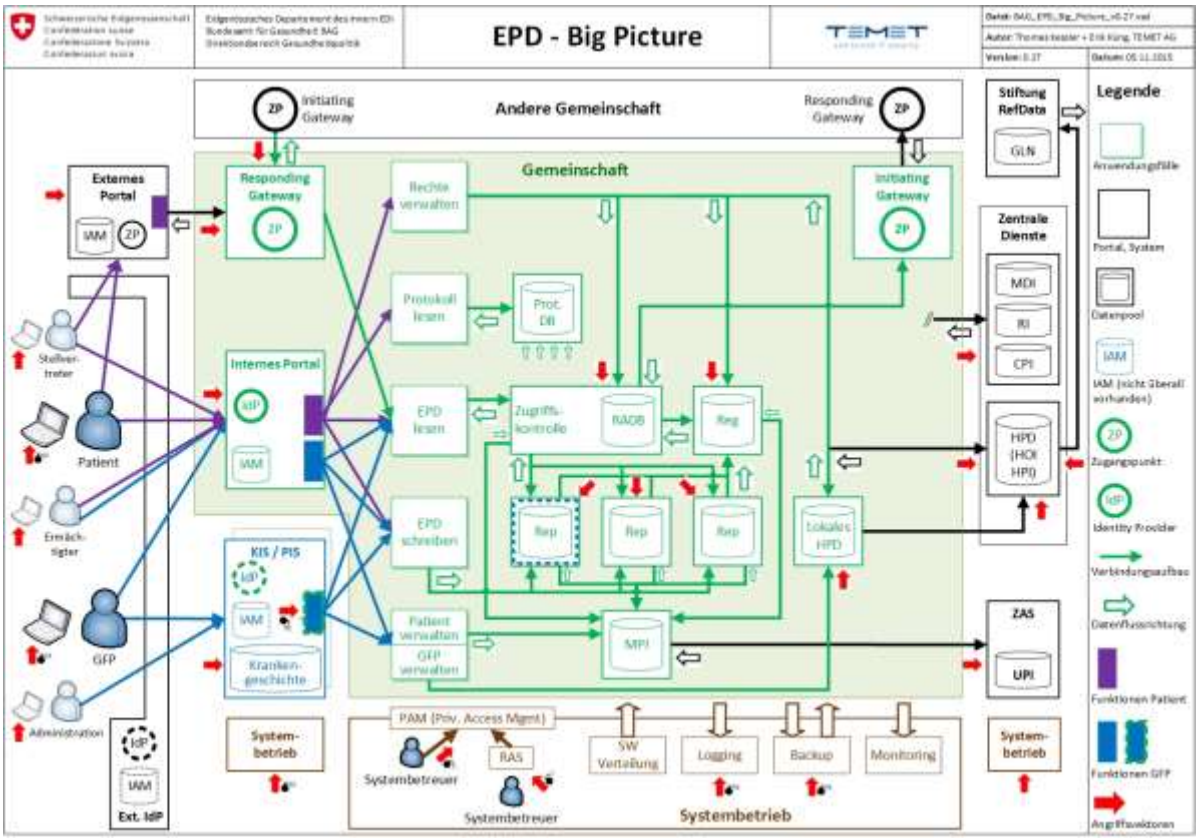


Abbildung 1: Elektronisches Patientendossier - Big Picture

Abbildung 1 zeigt die Elemente und Kommunikationsverbindungen des elektronischen Patientendossiers mit den wichtigsten Aktoren und Umsystemen in der Übersicht. Dieses „Big Picture“ bildet den Rahmen für die vorliegende Bedrohungs- und Risikoanalyse.

Der **grün** hinterlegte Bereich umfasst die wesentlichen Komponenten einer (Stamm-)Gemeinschaft und zeigt die Anwendungsfälle, die über verschiedene Schnittstellen zur Verfügung stehen. **Blau** umrandet sind die an der (Stamm-)Gemeinschaft teilnehmenden Primärsysteme wie z.B. Apotheken, Labore, Pflegeheime sowie insbesondere die Informationssysteme von Krankenhäusern (KIS) und Praxen (PIS). Die Abgrenzung zwischen der (Stamm-)Gemeinschaft und den Primärsystemen ist nicht immer offensichtlich. So bedeutet z.B. die grün-gestrichelte Umrandung des eHealth-Connectors, dass diese Softwarekomponente Teil der Zertifizierung einer (Stamm-)Gemeinschaft sein muss, obwohl sie auf dem Primärsystem betrieben wird. Die blau-gestrichelte Umrandung bei einem der Document Repositories deutet demgegenüber an, dass ein Document Repository nicht zwingend von der (Stamm-)Gemeinschaft betrieben werden muss sondern Teil eines Primärsystems sein kann.

Klarer abgegrenzt sind die auf der rechten Seite dargestellten zentralen Dienste, die von der Bundesverwaltung betrieben werden und im Big Picture **schwarz** umrandet sind. Ebenfalls schwarz umrandet sind die externen Portale, allfällige externe Identity Provider (IdP) sowie die Systeme anderer (Stamm-)Gemeinschaften, die mit der (Stamm-)Gemeinschaft über ihren Zugangspunkt kommunizieren. **Braun** umrandet sind schliesslich die Systeme des Systembetriebs. Diese tragen nicht direkt zur Funktionalität des elektronischen Patientendossiers bei, müssen in Bezug auf mögliche Sicherheitsrisiken aber einbezogen werden.

Mögliche Angriffsvektoren auf ein elektronisches Patientendossier sind mit roten Pfeilen angedeutet; ihre Analyse und Entschärfung sind das hauptsächliche Thema des vorliegenden Dokuments.

2.2 Schutzobjekte

Die Schutzobjekte sind aus dem Big Picture ersichtlich und werden wie folgt gruppiert:

- Daten
- Benutzergruppen
- Anwendungsfälle
- Systemkomponenten

2.2.1 Daten

ID	Name	Inhaber	Vertraulichkeit	Verfügbarkeit	Integrität	Nachvollziehbarkeit	Datenschutzstufe
	Elektronisches Patientendossier (EPD)	Patient	4	2	2	2	4
	Document Repositories (DocRep) einer (Stamm-) Gemeinschaft	(Stamm-) Gemeinschaft	4	2	2	2	4
	Document Registry (DocReg) einer (Stamm-)Gemeinschaft	(Stamm-) Gemeinschaft	4	2	2	2	4
	EPD Lokaler Zwischenspeicher (Cache, falls vorhanden)	(Stamm-) Gemeinschaft	4	1	2	2	4
	Protokollierungsdatenbank	(Stamm-) Gemeinschaft	4	2	2	2	4
	Rechteattributdatenbank (RADB)	(Stamm-) Gemeinschaft	4	2	2	2	4
	Master Patient Index (MPI) einer (Stamm-)Gemeinschaft	(Stamm-) Gemeinschaft	3	2	2	2	3
	Lokales HPD einer (Stamm-)Gemeinschaft (falls vorhanden)	(Stamm-) Gemeinschaft	2	2	2	2	2
	Internes Portal IAM DB	(Stamm-) Gemeinschaft	3	2	2	2	2
	Systembetrieb Datenbestände (z.B. Logs, Backup, PAM)	Betreiber	4	1	2	2	4
	Externes Portal IAM DB	Ext. Portal	3	2	2	2	2
	Krankengeschichte	Primärsystem	4	3	2	2	4
	Primärsystem IAM DB	Primärsystem	2	2	2	2	2
	Nationales Healthcare Provider Directory (HPD)	BAG	1	2	2	2	1
	Unique Person Identification Database (UPI)	ZAS	4	1	2	2	4
	RefData Database (GLN Verzeichnis)	Stiftung RefData	1	1	2	2	1

Definitionen (Quelle: ISDS Template):

- Stufen bzgl. Vertraulichkeit: 1 (nicht klassifiziert), 2 (intern), 3 (vertraulich), 4 (geheim)
- Stufen bzgl. Verfügbarkeit: 1 (Ausfalldauer mehr als einen Tag), 2 (Ausfalldauer ein Tag),

3 (Ausfalldauer weniger als ein Tag)

- Stufen bzgl. Integrität: 1 (muss nicht gewährleistet sein), 2 (muss gewährleistet sein)
- Stufen bzgl. Nachvollziehbarkeit: 1 (muss nicht gewährleistet sein), 2 (muss gewährleistet sein)
- Stufen bzgl. Datenschutz: 1 (geringer Schutzbedarf), 2 (mittlerer Schutzbedarf), 3 (hoher Schutzbedarf), 4 (sehr hoher Schutzbedarf)

Die nachfolgende Tabelle zeigt die fünf Vertraulichkeitsstufen gemäss „Standards und Architektur Empfehlungen V“ im Vergleich zu den Vertraulichkeitsstufen und der Datenschutzrelevanz gemäss ISDS Template:

<table>
<tr><th>Standards und Architektur Empfehlungen V</th><th>Speicherort</th><th>ISDS Template (Vertraulichkeit)</th><th>ISDS Template (Datenschutz)</th></tr>
<tr><td></td><td></td><td>1 (nicht klassifiziert)</td><td></td></tr>
<tr><td>Demographische Daten</td><td>Verzeichnisse</td><td>2 (intern)</td><td>1 (gering)</td></tr>
<tr><td>Nützliche Daten</td><td rowspan="4">Document Repository</td><td rowspan="2">3 (vertraulich)</td><td rowspan="2">2 (mittel)</td></tr>
<tr><td>Medizinische Daten</td></tr>
<tr><td>Sensible Daten</td><td rowspan="2">4 (geheim)</td><td>3 (hoch)</td></tr>
<tr><td>Geheime Daten</td><td>4 (sehr hoch)</td></tr>
</table>

2.2.2 Benutzergruppen

Benutzergruppe	Beschreibung	Verantwortliche Organisationseinheit
Patient	Der Patient ist einer der wesentlichen Aktoren am EPD. Das EPD soll dem Patienten einen erleichterten Einblick in seine Krankengeschichte geben und ihn befähigen, seine Eigenverantwortung besser wahrzunehmen. Der Patient steuert mittels der Berechtigungsvergabe, welche GFP wie lange auf sein EPD zugreifen kann. In die Benutzergruppe „Patient“ gehört auch ein von einem Patienten eingesetzter Stellvertreter. Dieser Stellvertreter muss selbst nicht am EPD teilnehmen, sprich kein EPD eröffnet haben.	Stammgemeinschaft
Gesundheitsfachperson (GFP) und Hilfspersonen	Die Benutzergruppe „Gesundheitsfachpersonen (GFP)“ beinhaltet alle Personen, die im Gesundheitswesen tätig und an der Behandlung des Patienten beteiligt sind. Z.B. Ärzte, Apotheker, Pfegefachpersonen aber auch Hilfspersonen wie z.B. Medizinische Praxis Assistentin (MPA). Eine GFP, die von einem Patienten als „Ermächtigter“ bestimmt wurde, kann für den Patienten die Berechtigungsverwaltung führen.	(Stamm-)Gemeinschaft
Administrative Teilnehmer[1]	Zur Benutzergruppe der „Administrativen Teilnehmer“ gehören Personen im Umfeld der Behandelnden wie z.B. Administrativpersonal, Systembetreuer oder Helpdesk. Hilfspersonen von GFP sind nicht dieser Benutzergruppe zugeteilt. Administrative Teilnehmer erhalten nur Zugriff auf administrative Daten.	(Stamm-)Gemeinschaft
Administration MPI und IAM	Personen, welche für die Datenpflege des MPI und IAM einer (Stamm-)Gemeinschaft zuständig sind. Ausser dem MPI und IAM haben sie keinen weiteren Zugriff auf Daten des EPD:	(Stamm-)Gemeinschaft

[1] Gemäss Standards und Architektur Empfehlungen III, S.19

Benutzergruppe	Beschreibung	Verantwortliche Organisationseinheit
Administration HPD	Personen, welche für die Pflege der Daten des nationalen HPD zuständig sind. Sie haben keinen Zugriff auf Daten im EPD.	(Stamm-)Gemeinschaft
Administration UPI	Personen, welche für die Datenpflege des nationalen UPI zuständig sind. Sie haben keinen Zugriff auf Daten des EPD.	(Stamm-)Gemeinschaft
Administration RefData	Personen, welche für die Datenpflege der RefData (z.B. GLN) zuständig sind. Sie haben keinen Zugriff auf die Daten des EPD.	Stiftung RefData
Betreiber (Stamm-)Gemeinschaftssystem	Zu dieser Benutzergruppe gehören Personen, welche für den Betrieb der Systeme einer (Stamm-)Gemeinschaft verantwortlich und zuständig sind. Ihr Zugriff ist auf die Systeme des EPD beschränkt. Idealerweise kommen sie mit den Daten des EPD nicht in Berührung.	(Stamm-)Gemeinschaft
Betreiber Primärsystem	Zu dieser Benutzergruppe gehören Personen, welche für den Betrieb der Systeme z.B. eines Krankenhauses oder einer Praxis verantwortlich und zuständig sind. Sie haben keinen Zugriff auf die Systeme und Daten des EPD. Jedoch haben sie u.U. in den Primärsystemen Zugriff auf Daten, welche ins EPD geladen werden oder vom EPD heruntergeladen wurden.	Krankenhaus, Praxis

2.2.3 Anwendungsfälle

SO1 EPD lesen

Im Anwendungsfall „EPD lesen“ sind alle Lesezugriffe auf das EPD zusammengefasst. Lesezugriffe können über das interne Portal erfolgen, aber auch über das externe Portal oder den Zugangspunkt (IHE Document Consumer). Mittels eHealth-Connector kann auch von einem Primärsystem (z.B. KIS / PIS) heraus ein EPD gelesen werden. Alle Lesezugriffe auf das Document Registry und Document Repository werden vorgängig durch die Zugriffskontrolle geführt.

SO2 EPD schreiben

In diesem Anwendungsfall sind alle Schreibzugriffe auf das EPD zusammengefasst. In ein EPD kann nur über eine IHE Document Source (z.B. KIS, PIS, AIS, internes Portal) geschrieben werden. Andere Schreibzugriffe in das Document Registry resp. Document Repository sind nicht vorgesehen. Im Gegensatz zu „EPD lesen“ wird bei „EPD schreiben“ keine Zugriffskontrolle durchgeführt. Eine GFP kann in alle EPD schreiben, ein Patienten resp. deren Stellvertreter nur in das eigene.

SO3 Rechte verwalten

Im Anwendungsfall „Rechte verwalten“ wird die Zugriffssteuerung auf ein EPD vorgenommen. Dabei kann der Patient anhand verschiedener Vertraulichkeitsstufen auf Dokumente sowie Zugriffsstufen für Gesundheitsfachpersonen steuern, wer auf welche Daten in seinem EPD zugreifen kann. Eine GFP muss dazu im nationalen HPD gefunden werden. Die Zugriffsrechte sind so lange gültig, bis der Patient sie wieder entzieht. Wahlweise kann - sofern die (Stamm-)Gemeinschaft dies anbietet - ein zeitlich befristetes Zugriffsrecht erteilt werden. Der Patient als Besitzer der Dokumente hat immer Zugriff auf seine Dokumente, solange er die Bedingungen für eine Teilnahme am EPD erfüllt. Über die Zugriffssteuerung kann auch eine Ausschlussliste („Blacklist“) gepflegt werden, welche einer einzelnen GFP den Zugriff auf ein EPD verwehrt, selbst wenn diese über eine Organisationszugehörigkeit

eigentlich eine Zugriffsberechtigung hätte.

SO4 Patienten verwalten

Über den Anwendungsfall „Patienten verwalten“ kann für einen Patienten, der noch nicht Teilnehmer am EPD ist, ein EPD eröffnet werden. Die Gemeinschaft, in der sein EPD eröffnet wird, wird für den Patienten zu seiner Stammgemeinschaft. Beim Eröffnen eines neuen EPD wird bei der ZAS die UPI abgefragt und im MPI mit der Patienten ID aus dem Primärsystem verknüpft sowie den lokalen IDs des Patienten in den Primärsystemen der Stammgemeinschaft.

SO5 GFP verwalten

In diesem Anwendungsfall werden Eintritte und Austritte einer GFP in eine Gesundheitseinrichtung abgebildet. Ebenfalls müssen in diesem Anwendungsfall Gruppenzugehörigkeiten von GFP nachgeführt werden, da aus unterschiedlichen Organisationszugehörigkeiten unterschiedliche Zugriffsberechtigungen resultieren können. Diese Zugehörigkeiten werden im lokalen HPD abgebildet (falls vorhanden) und von dort an das nationale HPD weitergeleitet.

SO6 Protokoll lesen

Über diesen Anwendungsfall kann ein Patient respektive ein Stellvertreter ein detailliertes Protokoll einsehen, aus dem hervorgeht, wer wann auf welche Daten in seinem EPD zugegriffen hat oder Daten in sein EPD geschrieben hat. Es ist ebenfalls ersichtlich, welche Berechtigungsvergaben und -anpassungen wann von wem vorgenommen wurden und welche Daten wann von wem für ungültig erklärt wurden.

SO7 (Stamm-)Gemeinschaftssysteme betreiben

Im Anwendungsfall „(Stamm-)Gemeinschaftssystem betreiben“ sind alle Aktivitäten zusammengefasst, welche für den sicheren Betrieb der Systeme einer (Stamm-)Gemeinschaft notwendig sind. Unter anderem sind dies Aufgaben wie die Systemadministration der Server, Betriebssysteme, Datenbanken und Applikationen aber auch der Netzwerkelemente und Sicherheitssysteme. Ebenfalls dazu gehören Softwareverteilung, zentrales Logging, Backup und Monitoring der Systemumgebung.

SO8 Zentrale Dienste betreiben

Analog zum Anwendungsfall „(Stamm-)Gemeinschaftssysteme betreiben“ sind in diesem Anwendungsfall alle Aktivitäten zusammengefasst, welche zum sicheren Betrieb der Zentralen Dienste notwendig sind.

SO9 Primärsystem (z.B. KIS / PIS) betreiben

Analog zum Anwendungsfall „(Stamm-)Gemeinschaftssysteme betreiben“ sind in diesem Anwendungsfall alle Aktivitäten zusammengefasst, welche zum sicheren Betrieb der Primärsysteme notwendig sind.

2.2.4 Systemkomponenten

Systeme einer (Stamm-)Gemeinschaft
Internes Portal
Zugangspunkt (Initiating & Responding Gateways)
Rechteattribute Datenbank
Document Registry
Document Repository
Lokales HPD (falls vorhanden)
Protokollierungs-Datenbank
MPI

Umsysteme einer (Stamm-)Gemeinschaft
Primärsysteme (z.B. KIS, PIS)
eHealth-Connector
HPD
MDI
RI
CPI
UPI
Externes Portal
Endgerät GFP
Endgerät Patient

SO10 Internes Portal

Vom Internet her zugängliches internes Zugangsportal einer (Stamm-)Gemeinschaft für Patienten. Es ermöglicht Patientinnen und Patienten einen Orts- und zeit-unabhängigen, sicheren und zurück verfolgbaren Zugang auf die Daten des eigenen EPD ohne die Hilfe von Dritten. Darüber hinaus kann der Patient den Datenzugriff mittels individueller Einwilligungen und Rechtevergabe regeln. Es ist nebst dem externen Portal die einzige Architektur-Komponente, die sich direkt an den Bürger, beziehungsweise an den Patienten wendet.

SO11 Zugangspunkt

Schnittstelle über welche eine (Stamm-)Gemeinschaft von einer anderen (Stamm-)Gemeinschaft oder einem externen Portal angefragt wird oder über welches die (Stamm-)Gemeinschaft selbst Anfragen bei anderen (Stamm-)Gemeinschaften stellt.

SO12 Rechteattribute Datenbank

Datenbank in welcher die Berechtigungen des Zugriffs auf Dokumente innerhalt eines EPD eines Patienten gespeichert sind. Die vom Patienten gewählten Zugriffsregeln werden in Form einer Rechtematrix aus der Kombination von berechtigter Person mit zugeteilter Zugriffsstufe und Vertraulichkeitsstufen der EPD-Inhalte festgehalten. Für die Entscheidung, ob ein Zugriff auf ein Dokument erteilt oder verweigert wird, müssen diese Regeln ausgewertet werden. Die berechtigten Personen (Gesundheitsfachpersonen und Patienten) haben Zugriff auf Daten eines EPD, wenn die erforderlichen Bedingungen erfüllt sind. Die Rechtematrix kann jederzeit vom Patienten angepasst werden. Die Information über einen Stellvertreter oder Ermächtigten den der Patient einsetzt wird ebenfalls in der Rechteattribute Datenbank gespeichert.

SO13 Document Registry

Datenbank in welcher beschreibende Informationen, sogenannte Dokumenten-Metadaten, sowie Verweise auf den Ablageort der Dokumente gespeichert sind.

SO14 Document Repository

Ablageort an welchem die effektiven Daten des EPD eines Patienten gespeichert sind.

SO15 Lokales HPD

Eine (Stamm-)Gemeinschaft ist verantwortlich Daten der ihr angeschlossenen Behandelnden und Gesundheitsorganisationen im nationalen HPD einzustellen. Dazu kann die (Stamm-)Gemeinschaft ein lokales HPD innerhalb der (Stamm-)Gemeinschaft aufbauen in welchem sie diese Daten pflegt und von welchem das nationale HPD aktualisiert wird. Ein lokales HPD ist jedoch nicht zwingend notwendendig.

SO16 Protokollierungs-Datenbank

Datenbank in der alle Lese und Schreib-Zugriffe auf Daten im EPD eines Patienten gespeichert werden. Änderungen an Berechtigungen werden ebenfalls dokumentiert.

SO17 MPI

Dienst für die Zusammenführung verschiedener lokaler Identifikatoren eines Patienten welche in IT-Systemen der Leistungserbringer gespeichert ist. Der Patient wird anhand eines organisationsübergreifenden Identifikators referenziert, welcher innerhalb einer (Stamm-)Gemeinschaft gültig ist. Der Dienst ermöglicht das Auffinden eines Patienten anhand vorgegebener demographischer Attribute wie Name, Vorname, Alter und Geschlecht.

SO18 Primärsysteme

Gesamtheit aller informationsverarbeitenden Systeme zur Bearbeitung medizinischer Daten in einer Klinik, Spital, Arztpraxis, Apotheke, Labor, etc. Im Primärsystem ist die Gesamtheit der Dokumente eines Patienten gespeichert, welche während dessen Behandlung in einer Organisation erstellt wurden. Für den weiteren Behandlungsverlauf oder für die Zukunft relevante Dokumente können in das EPD des Patienten kopiert werden.

SO19 eHealth-Connector

Schnittstelle zwischen Primärsystem und (Stamm-)Gemeinschaftssystem, über welche Daten in das EPD geschrieben werden oder Daten aus dem EPD abgefragt werden können.

SO20 HPD

Dienst, welcher das Verzeichnis der Behandelnden (HPI-S) und Gesundheitsorganisationen (HOI-S) bereitstellt. Dieser Dienst ist als eigener zentraler Service verfügbar.

SO21 MDI

Zentraler Metadaten Index-Service (MDI-S). Bietet das Verzeichnis der Dokumenten-Metadaten an.

SO22 RI

Zentraler Dienst, welcher das Verzeichnis der Rollen (RI-S) bereitstellt.

SO23 CPI

Verzeichnisdienst welcher zentral eine Übersicht der (Stamm-)Gemeinschaften und externen Zugangsportale anbietet.

SO24 UPI

Verzeichnisdienst des zentralen Versichertenregisters der AHV für die Personenidentifikation bei der Zuordnung und der Verwaltung der AHV-Nummer (AHVN13).

SO25 Externes Portal

Vom Internet her zugängliches externes Zugangsportal einer (Stamm-)Gemeinschaft. Ermöglicht Behandelnden, welche nicht oder noch nicht Mitglied einer (Stamm-)Gemeinschaft sind, einen einfachen und sicheren Zugang zum EPD. Damit besteht grundsätzlich eine technische Möglichkeit des lesenden Zugriffs für den Behandelnden als weiterer Benutzer eines externen Zugangsportals, solange der Patient diesen explizit gewährt hat.

SO26 Endgerät GFP

Endgerät mit welchem eine GFP lesend oder schreibend auf das EPD zugreift. Kann ein PC oder Notebook sein, zunehmend aber auch Tablet. Es sind aber auch Apps auf Smartphone denkbar.

SO27 Endgerät Patient

Endgerät mit welchem ein Patient lesend oder schreibend auf das EPD zugreift. Üblicherweise PC, Notebook, oder Tablet. Es sind aber auch Apps auf Smartphone denkbar.

3 Risikoanalyse

3.1 Bedrohungskatalog

Generische Bedrohungen gemäss [ISDS Template]:

Ref	Bedrohung
Höhere Gewalt	
G1	Personenausfall
G2	Systemausfall, Netzausfall (WAN), Klimaanlage, Heizung
G3	Feuer, Wasser, Blitz, Lawinen, Sturm, Temperatur, Feuchtigkeit, Staub
G4	Technische Katastrophe, benachbarte Gebäude, KKW Unfall, Magnetfelder, Licht
G5	Grossveranstaltungen, Demonstrationen, Krawalle
Organisatorische Mängel	
G6	Fehlende Betriebsmittel
G7	Fehlende Kontrollen, Tests, Auswertungen
G8	Fehlende oder unzureichende Schulung, Komplexität von Systemen und Komponenten
G9	Fehlende Regelungen oder Prozesse
G10	Mangelhaftes Management bei Änderungen
G11	Prozess wird nicht gelebt oder Verstoss gegen gültige Regelungen
G12	Unbefugter oder schlecht geschützter Zutritt
Menschliche Fehlhandlungen	
G13	Fahrlässigkeit, unbeabsichtigte Beschädigung
G14	Fehlerhafte Administration
G15	Fehlverhalten Benutzer
G16	Gefährdung durch Fremdpersonal
G17	Nichtbeachtung von Vorschriften
Technisches Versagen	
G18	Ausfall von Sicherheitskomponenten / nicht funktionierende Sicherheitskomponenten
G19	Datenverlust
G20	Hardwaredefekt
G21	Softwareschwachstelle
G22	Versorgungsausfall oder Beeinträchtigung durch Netzausfall, DB Ausfall, Stromausfall usw.
Vorsätzliche Handlungen	
G23	Abhören, Auswerten, Analysen, Hacken, Spoofing
G24	Bösartige Software, Trojanische Pferde und Viren
G25	Gefälschte Daten, Integritäts- und Vertraulichkeitsverlust
G26	Manipulieren, kompromittieren, vortäuschen
G27	Missbrauchen von Konten, Zutritten, Berechtigungen usw., Erpressen von Mitarbeitern
G28	Schwachstellen ausnutzen
G29	Unberechtigte Handlungen, Diebstahl (auch z.B. defekte HD), Betrug
G30	Vandalismus, Anschläge, Sabotagen

Tabelle 2: Generischer Bedrohungskatalog

3.2 Schadenszenarien

Nachfolgend sind typische Schadenszenarien beschrieben, die im Zusammenhang mit dem EPD

eintreten können, und in Bezug auf ihre Tragweite / Schadensausmass bewertet. Die Einstufung des Schadensausmasses erfolgt gemäss Template ISDS Konzept (siehe Anhang A).

Massgebend für die Einstufung ist der Schutzbedarf der betroffenen Daten gemäss Kapitel 2.2.1.

3.2.1 Verlust der Vertraulichkeit

Tabelle 3 identifiziert und bewertet Schadenfälle in Bezug auf unberechtigte Einsicht in EPD Daten. Dabei spielen nicht nur Art und Umfang der eingesehenen Daten eine Rolle sondern auch der Personenkreis, der unberechtigterweise Einsicht erhält.

Ref.	Szenario	Umfang der Information	Unberechtigt einsehende Person	Auswirkung / Tragweite	Stufe
C1a	Patientendossiers werden durch Unberechtigte eingesehen bzw. kopiert	Systematisch in grosser Menge	Unerkannter Dritter (z.B. Krimineller)	Worst Case Szenario, das die Akzeptanz des EPD ist in seiner Gesamtheit gefährdet. Die gestohlenen Daten können im grossen Stil missbraucht werden, z.B. für Erpressung.	**4 Katastrophal**
C1b			Identifizierbarer Systembenutzer (z.B. Patient)	Das EPD mit seinen (Stamm-)Gemeinschaften und Einrichtungen kann in seinem Ruf geschädigt werden, z.B. durch Presseberichte über Sicherheitsmängel.	3 kritisch
C1c			GFP mit Schweigepflicht (z.B. Arzt)	Das EPD mit seinen (Stamm-)Gemeinschaften und Einrichtungen kann in seinem Ruf geschädigt werden, z.B. durch Presseberichte über Sicherheitsmängel.	3 kritisch
C1d		Gezielt bezogen auf einzelne Personen oder Dokumententypen	Unerkannter Dritter (z.B. Krimineller)	Exponierte Personen (z.B. VIP aus Sport oder Politik) oder Einrichtungen (z.B. Psychiatrie) können systematisch erpresst und massiv im Ruf geschädigt werden.	**4 Katastrophal**
C1e			Identifizierbarer Systembenutzer (z.B. Patient)	Exponierte Personen (z.B. VIP aus Sport oder Politik) oder Einrichtungen (z.B. Psychiatrie) können in ihrem Ruf geschädigt werden, z.B. durch Presseberichte.	3 kritisch
C1f			GFP mit Schweigepflicht (z.B. Arzt)	Auswirkung ist vernachlässigbar, da nicht anzunehmen ist, dass eine Person mit Schweigepflicht Daten missbraucht.	1
C1g		Zufällige einzelne Dossiers oder Dokumente	Unerkannter Dritter (z.B. Krimineller)	Einzelne Patienten oder GFP können in ihrem Ruf geschädigt werden, wobei aber meistens keine sensiblen Daten dabei sind (da zufällige Dossiers betroffen sind).	2 marginal
C1h			Identifizierbarer Systembenutzer (z.B. Patient)	Imageschaden für das EPD, z.B. durch Berichte in der Presse.	2 marginal
C1i			GFP mit Schweigepflicht (z.B. Arzt)	Auswirkung ist vernachlässigbar, da nicht anzunehmen ist, dass eine Person mit Schweigepflicht Daten missbraucht.	1
C2a	Beziehung von Patienten zu GFP mit typischerweise sensiblen Daten (z.B. Psychiater, Onkologen) wird aufgedeckt	Systematisch in grosser Menge	Exponierte Personen (z.B. VIP aus Sport oder Politik) oder Einrichtungen (z.B. Psychiatrie) können erpresst oder massiv in ihrem Ruf geschädigt werden.		**4 Katastrophal**
C2b		Für alle Patienten einer GFP	Die geschädigte GFP (z.B. ein Psychiater) kann zur Berufsaufgabe gezwungen sein.		3 kritisch
C2c		Für einzelne Patienten	Der geschädigte Patient kann seine Stelle verlieren und andere Gesellschaftliche Nachteile erleiden.		3 kritisch
C3a	EPD-Datenbestand einer einzelnen (Stamm-)Gemeinschaft oder Einrichtung wird kompromittiert	Mit sensiblen oder geheimen Daten	Die betroffene (Stamm-)Gemeinschaft oder Einrichtung kann mit Existenzbedrohenden Rechts- und Bussenfolgen konfrontiert sein.		**4 Katastrophal**
C3b		Ohne sensible oder geheime Daten	Die betroffene (Stamm-)Gemeinschaft oder Einrichtung kann einen Imageschaden erleiden.		2 marginal

Ref.	Szenario	Umfang der Information	Unberechtigt einsehende Person	Auswirkung / Tragweite	Stufe
C4a	Interne Dokumente werden unbeabsichtigt in ein Patientendossier eingestellt	In grosser Menge	Der Patient und die von ihm berechtigten GFP erhalten Einsicht in interne Dokumente einer Einrichtung (z.B. Reklamationsmanagement oder interne Aktennotizen), was zu einem Imageverlust und/oder Reklamationen führen oder das Vertrauensverhältnis nachhaltig belasten kann.		3 kritisch
C4b		Einzelne Dokumente			1

Tabelle 3: Schadenszenarien „Vertraulichkeitsverlust“

3.2.2 Verlust der Integrität

Tabelle 4 identifiziert und bewertet Schadenfälle in Bezug auf die (absichtliche oder unabsichtliche) Veränderung von Daten im Elektronischen Patientendossier.

Hinweis: Beim Verlust der Integrität wird beim Schadensausmass nur der direkte Schaden bewertet. Ein aus dem Integritätsverlust (z.B. von Berechtigungsdaten) eventuell resultierender Verlust von Vertraulichkeit oder Verfügbarkeit ist ein anderes Schadenszenario, das separat aufgelistet ist.

Ref.	Szenario	Umfang der Dokumente	Auswirkungen / Tragweite	Stufe
I1a	Dokumente in Patientendossiers werden verändert	Systematisch in grosser Menge	Das EPD in seiner Gesamtheit kann bzw. darf nicht mehr genutzt werden, bis alle Dossiers richtiggestellt sind.	**4 Katastrophal**
I1b		Gezielt bezogen auf einzelne Personen oder Dokumententypen	Gezielt eingestellte Falschinformationen (z.B. Medikationslisten) können zu fehlerhafter Behandlung und zur Gefährdung von Leib und Leben des Geschädigten führen.	3 kritisch
I1c		Zufällige einzelne Dossiers oder Dokumente	Zufällige fehlerhafte Informationen werden im Normalfall festgestellt und können mit gewissem Aufwand korrigiert werden.	2 marginal
I2a	Daten der Zentralen Dienste werden verändert	Systematisch in grosser Menge	Das EPD in seiner Gesamtheit arbeitet nicht mehr zuverlässig. Bei einer Suche werden z.B. nicht mehr alle Dokumente angezeigt. Oder es werden Dossiers von Patienten eingesehen für die die GFP eigentlich keine Berechtigung hat.	3 kritisch
I2b		Gezielt bezogen auf einzelne Daten	Gezielt veränderte Informationen führen dazu, dass das EPD für eine GFP oder einen Patienten nicht mehr benutzbar ist.	3 kritisch
I2c		Zufällige einzelne Daten	Zufällig veränderte Informationen führen dazu, dass das EPD für eine GFP oder einen Patienten nicht mehr benutzbar ist.	2 marginal

Tabelle 4: Schadenszenarien „Integritätsverlust“

3.2.3 Verlust der Verfügbarkeit

Tabelle 5 identifiziert und bewertet Schadenfälle beim Ausfall von Services für das Lesen, Schreiben und Verwalten von EPD Daten. Für die Bewertung des Schadens ist neben der Art und der Menge der betroffenen Daten insbesondere die Dauer des Ausfalles wesentlich.

Ref.	Szenario	Art und Umfang der Information	Dauer der Nichtverfügbarkeit	Auswirkung / Tragweite	Stufe
A1a	Patientendossiers können nicht eingesehen werden	Dossiers aller oder vieler Patienten	Tagelang	Das EPD in seiner Gesamtheit erleidet einen substanziellen Imageverlust.	3 kritisch
A1b			Stundenlang	Es muss vorübergehend auf alternative Kommunikationskanäle (Telefon, Fax, Brief, Secure Mail,…) zurückgegriffen werden.	2 marginal
A1c		Dossiers einzelner Patienten	Tagelang	Es muss im Einzelfall auf alternative Kommunikationskanäle (Telefon, Mail,…) zurückgegriffen werden.	2 marginal
A1d			Stundenlang	Auswirkung ist vernachlässigbar.	1
A2a	Datenbestand einer einzelnen (Stamm-)	Mit notfallrelevanten Daten	Tagelang	Wichtige Daten können in Notfallsituation fehlen bzw. müssen neu erfasst werden.	3 kritisch

Ref.	Szenario	Art und Umfang der Information	Dauer der Nicht-verfügbarkeit	Auswirkung / Tragweite	Stufe
A2b	Gemeinschaft oder Einrichtung kann nicht im EPD eingesehen werden		Stundenlang	Wichtige Daten können in Notfallsituation fehlen bzw. müssen neu erfasst werden.	2 marginal
A2c		Ohne notfallrelevante Daten	Tagelang	Auswirkung ist vernachlässigbar.	1
A2d			Stundenlang	Auswirkung ist vernachlässigbar.	1
A3a	Protokollierungsdaten können nicht eingesehen werden		Tagelang	Reklamationen und Abklärungen	2 marginal
A3b			Stundenlang	Auswirkung ist vernachlässigbar.	1
A4a	Patientendossiers können nicht ergänzt / aktualisiert werden		Tagelang	Veraltete Informationen können zu fehlerhafter Behandlung führen.	3 kritisch
A4b			Stundenlang	Auswirkung ist vernachlässigbar.	1
A5a	Es können keine neuen Patientendossiers eröffnet und keine GFP erfasst werden		Tagelang	Auswirkung ist vernachlässigbar.	1
A5b			Stundenlang	Auswirkung ist vernachlässigbar.	1
A6a	Benutzerdaten von Patienten oder GFP können nicht mutiert werden		Tagelang	Mutationswünsche von Patienten und Stellenwechsel von GFP können nicht zeitnah nachgeführt werden.	3 kritisch
A6b			Stundenlang	Auswirkung ist vernachlässigbar.	1

Tabelle 5: Schadenszenarien „Verfügbarkeitsverlust“

3.2.4 Verlust der Nachvollziehbarkeit

Tabelle 6 identifiziert und bewertet Schadenfälle bei fehlenden Protokollierungsdaten.

Ref.	Szenario	Umfang der Dokumente	Auswirkungen / Tragweite	Stufe
N1a	Zugriffe auf Patientendossiers können nicht nachvollzogen werden	Lesezugriffe	Die gesetzliche Verpflichtung wird verletzt.	3 kritisch
N1b		Schreibzugriffe	Es kann nicht nachvollzogen werden, wer ein ggf. fehlerhaftes Dokument in ein Patientendossier eingestellt hat.	3 kritisch
N2a	Verwaltungshandlungen können nicht nachvollzogen werden	Rechteverwaltung	Es kann nicht nachvollzogen werden, wer spezifische Zugriffsrechte vergeben oder entzogen hat.	2 marginal
N2b		Benutzerverwaltung	Es kann nicht nachvollzogen werden, wer einen Patienten oder eine GFP im System eröffnet oder mutiert hat.	2 marginal
N2c		Verwaltung von Metadaten (z.B. Klassifizierungsstufe)	Es kann nicht nachvollzogen werden, wer Metadaten zu einem Dokument erfasst oder mutiert hat.	2 marginal
N2d		Verwaltung der Systemkonfiguration	Es kann nicht nachvollzogen werden, wer eine Veränderung der Systemkonfiguration vorgenommen hat.	2 marginal

Tabelle 6: Schadenszenarien „Nachvollziehbarkeitsverlust“

3.3 Schwachstellenanalyse

Relevante Risiken entstehen dort, wo eine allgemeine Bedrohung (z.B. Bösartige Software, Trojanische Pferde und Viren) auf Grund einer Schwachstelle (z.B. GFP-Schreibrecht auf alle Dossiers) zu einem Schadenszenario (z.B. unbemerkter Diebstahl von vielen Patientendossiers) führen kann.

Schwachstellen stehen immer im Zusammenhang mit einem Anwendungsfall oder einer Systemkomponente, weshalb die Schwachstellenanalyse entlang dieser Schutzobjekte erfolgt.

Die Tragweite leitet sich jeweils direkt aus den Schadenszenarien ab. Die Eintretenswahrscheinlichkeit muss auf Grund von Erfahrungswerten und Expertenwissen geschätzt werden und ist mit einer bedeutenden Unschärfe behaftet.

Hinweis: Risiken, welche die Verfügbarkeit gefährden, werden nur aufgeführt, soweit es sich um Angriffe unbekannter Dritter handelt. Es wird davon ausgegangen, dass Risiken wie z.B. Unterbruch der Stromversorgung, Ausfall einer Harddisk, Unterbruch der Netzwerkverbindung u.ä. bereits durch geeignete Massnahmen begrenzt sind.

3.3.1 Anwendungsfälle

SO1 EPD lesen

R1 Daten werden fälschlicherweise über das EPD zugänglich gemacht

Über die Infrastruktur des Elektronischen Patientendossiers werden Daten der Primärsysteme zugänglich gemacht, die in kein EPD gehören, z.B. die Krankengeschichte von Patienten, die kein EPD eröffnet haben, oder interne Dokumente, die nicht zur externen Einsichtnahme gedacht sind.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R1	G8, G9	C4a	3 (kritisch)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

O5 Inventar und Ownership der Repositories

SO2 EPD schreiben

R2 Datenspezifische Sicherheitsvorkehrungen im Primärsystem werden von der (Stamm-) Gemeinschaft nicht eingehalten

In das EPD geschriebene Daten verlassen das Hoheitsgebiet des Datenerstellers. Allfällige spezielle Sicherheitsvorkehrungen im Primärsystem für sensible Daten (z.B. Datenverschlüsselung einer auf Psychiatrie spezialisierten Klinik) werden eventuell von der (Stamm-)Gemeinschaftslösung nicht unterstützt. Dadurch sind Daten in der (Stamm-)Gemeinschaft schlechter geschützt als im Primärsystem.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R2	G9, G10, G14	C1c, C1i	3 (kritisch)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

O5 Inventar und Ownership der Repositories

R3 Dateien mit Schadsoftware werden ins EPD geschrieben

Eine GFP (seine Hilfsperson) oder ein Patient selbst schreibt eine mit einem trojanischen Pferd infizierte PDF Datei in das Dossier des Patienten oder in alle Dossiers einer (Stamm-)Gemeinschaft. Sobald eine berechtigte Person diese Datei anschaut, wird das trojanische Pferd auf dem PC dieser Person aktiv, greift über die offene Benutzersession auf das EPD zu und schickt Teile oder das gesamte Dossier an eine konfigurierte Webseite oder Mailadresse.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R3	G24, G29	C1g, C2c	3 (kritisch)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

T12 Virenschutz

SO3 Rechte verwalten

R4 Sensible Daten sind falsch klassifiziert wegen Standard-Grundeinstellung

Ein psychiatrisches Gutachten wird gemäss Standard-Grundeinstellung als „medizinische Daten“ klassifiziert und der Patient vergisst, ihre Klassifizierung manuell auf „sensible Daten“ anzupassen. Das Dokument wird daraufhin von Personen eingesehen, die der Patient nicht beabsichtigt hat.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R4	G8, G15	C1h, C1i	2 (marginal)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

O6 Awareness aller Patienten

O7 Awareness aller Gesundheitsfachpersonen

R5 Erschleichen der Rolle „Stellvertreter“

Ein Hacker schafft es mittels Social Engineering oder Phishing, dass er von einem am EPD teilnehmenden Patienten als Stellvertreter eingetragen wird.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R5	G15, G24, G26, G29	C1d, C1g	4 (katastrophal)	3 (möglich)	Rot (Hoch)

Sicherheitsmassnahmen:

O6 Awareness aller Patienten

E8 Besondere Sorgfaltspflichten bei PEP

R6 Nachlässige Berechtigungsadministration

Nachlässige Berechtigungsadministration seitens eines Patienten oder dessen Ermächtigten führen dazu, dass sensible Daten von GFP eingesehen werden, die dazu aus Sicht des Patienten gar nicht befugt wären, was zu nachträglichen Reklamationen und einem Imageschaden führt.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R6	G8, G15	C1i, C2c	3 (kritisch)	3 (möglich)	Rot (Hoch)

Sicherheitsmassnahmen:

O6 Awareness aller Patienten

E8 Besondere Sorgfaltspflichten bei PEP

SO4 Patienten verwalten

Derzeit kein spezifisches Risiko identifiziert

SO5 GFP verwalten

R7 Berufsaufgabe einer GFP wird nicht nachgeführt

Ein Arzt oder Apotheker wird pensioniert oder gibt seine Praxis oder Apotheke aus anderen Gründen ab, sein Eintrag im HPD wird aber nicht (zeitnah) gelöscht. Er behält deshalb seine Zugriffsrechte auf Patientendossiers.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R7	G7, G11, G14	C1c, C2b	3 (kritisch)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z4 IAM HPD

R8 Mutation des Anstellungsverhältnisses einer GFP wird nicht konsequent nachgeführt

Ein Assistenzarzt wird nach Beendigung eines Stage in der psychiatrischen Abteilung des Spitals im HPD nicht aus der entsprechenden Gruppe gelöscht. Nach dem Stage behält er den Zugriff auf alle Dossiers, die für diese Abteilung freigegeben sind, auch wenn er in anderen Abteilungen des Spitals tätig ist.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R8	G7, G11, G14	C1c, C2b	3 (kritisch)	3 (möglich)	Rot (Hoch)

Sicherheitsmassnahmen:

Z4 IAM HPD

R9 Fehlende oder mangelhafte Trennung von Aufgabenbereichen

Eine GFP trägt ihre GLN unberechtigterweise in viele Organisations-Gruppen des lokalen HPD ein und erhält dadurch unberechtigten Zugriff auf Dossiers, die für sie eigentlich nicht einsehbar wären.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R9	G9, G27, G29	C1b, C2c	3 (kritisch)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z4 IAM HPD

SO6 Protokoll lesen

R10 GFP Hilfspersonen sind nicht im nationalen HPD erfasst

Die Ehefrau eines praktizierenden Arztes wird von diesem in der Nutzung des EPD instruiert und als seine Hilfsperson im lokalen HPD erfasst. Da für sie keine GLN ausgestellt ist kann sie im nationalen HPD nicht erfasst werden. Der Patient einer anderen (Stamm-)Gemeinschaft stellt im Zugriffsprotokoll den Lesezugriff dieser Hilfsperson fest, kann im HPD aber keine weiteren Angaben zu dieser Person entnehmen und ist auch nicht in der Lage, diese Hilfsperson auf die Sperrliste zu setzen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R10	G9	N1a	3 (kritisch)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z3 Eintrag aller GFP im HPD

SO7 (Stamm-)Gemeinschaftssysteme betreiben

R11 Betrügerischer System-Administrator

Ein betrügerischer System-Administrator kopiert alle Patientendossiers der von ihm betreuten (Stamm-)Gemeinschaft und verkauft diese an den Meistbietenden.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R11	G7, G27, G29	C1b, C2a, C3a	4 (katastrophal)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

T11 Zusätzliche Evidenz für sicheren Systembetrieb

R12 Sub-Unternehmer eines Betreibers einer (Stamm-)Gemeinschaft hat tieferes Sicherheitsniveau als Betreiber einer (Stamm-)Gemeinschaft

Ein Betreiber einer (Stamm-)Gemeinschaft vergibt z.B. das komplette Backup an einen Sub-Unternehmer, welcher nicht die gleich hohen Sicherheitsanforderungen erfüllt wie der Betreiber einer (Stamm-)Gemeinschaft selbst und deshalb verwundbar ist.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R12	G16	C1a, C1g, C3a	4 (katastrophal)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

T11 Zusätzliche Evidenz für sicheren Systembetrieb

R13 Informationsabfluss an unautorisierte Dritte, z.B. geheimdienstliche Ausspähung

Ein Betreiber einer (Stamm-)Gemeinschaft speichert Daten im Ausland oder setzt zu Analysezwecken anstelle lokaler Tools webbasierte Dienste ein (z.B. Google Analytics). Es ist dadurch möglich, dass sensible Informationen an eine am EPD nicht beteiligte Drittfirma oder ausländische Geheimdienste gelangen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R13	G9	C2a	4 (katastrophal)	2 (selten)	Rot (Hoch)

Sicherheitsmassnahmen:

T9 EP Datenbleiben in der Schweiz

T11 Zusätzliche Evidenz für sicheren Systembetrieb

R14 Front-end, Back-end oder anderes System mit einer möglichen Kommunikationsbeziehung zu einem System einer (Stamm-)Gemeinschaft wird gehackt

Ein Front-end, Back-end oder anderes System, von welchem eine Kommunikation mit einem System der (Stamm-)Gemeinschaft möglich ist, wird gehackt. Der Hacker arbeitet sich Schritt für Schritt bis ins EPD vor.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R14	G12, G14, G21, G28	C1a, C1g, C3a	4 (katastrophal)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

T1 Logische Isolation des EPD Vertrauensraums vom Internet

T2 ATNA Profil als Standard

T3 Inventar der angebundenen eHealth-Connectors

T7 Isolation der IHE-Services von anderen Systemen

T8 Isolation der EPD-Daten von anderen Systemen

R15 Mangelhafte Sicherheitsorganisation

Unklare Verantwortlichkeiten innerhalb der (Stamm-)Gemeinschaft führen dazu, dass dringende Entscheide (z.B. Bewertung und Bearbeitung aktueller Schwachstellen, bis hin zur Notabschaltung) nicht zeitgerecht gefällt werden.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R15	G9	C1a, I1a, N1b	4 (katastrophal)	2 (selten)	Rot (Hoch)

Sicherheitsmassnahmen:

O1 ISMS

O2 SIEM

SO8 Zentrale Dienste betreiben

Für das Schutzobjekt „SO8 Zentrale Dienste betreiben„ treffen im Grundsatz dieselben Risiken zu wie

für das Schutzobjekt „SO7 (Stamm-)Gemeinschaftssysteme betreiben„. Aus diesem Grund werden für dieses Schutzobjekt die Risiken nicht wieder aufgeführt.

SO9 Primärsystem (z.B. KIS / PIS) betreiben

Für das Schutzobjekt „SO9 Primärsystem (z.B. KIS / PIS) betreiben„ treffen im Grundsatz dieselben Risiken zu wie für das Schutzobjekt „SO7 (Stamm-)Gemeinschaftssysteme betreiben„. Aus diesem Grund werden für dieses Schutzobjekt die Risiken nicht wieder aufgeführt.

3.3.2 Systemkomponenten

SO10 Internes Portal

R16 Schwachstelle im internen Portal

Ein Hacker dringt über eine Schwachstelle in das interne Portal ein, von dort auf weitere Systeme und kann dadurch auf einzelne oder alle Dossiers dieser (Stamm-)Gemeinschaft zugreifen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R16	G10, G18, G21, G23, G28, G29	C1a, C2a, C3a	4 (katastrophal)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

T4 „Swiss banking level security“ des internen Portals

T5 Dokumentierte Sicherheit des internen Portals

T6 Penetration Testing aller aus dem Internet ansprechbaren Systeme

R17 Übernahme der Identität eines Patienten am internen Portal

Ein Hacker stiehlt mittels Phishing die Login Daten eines beliebigen Patienten und benutzt diese, um über das interne Portal auf das EPD dieses Patienten zuzugreifen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R17	G8, G15, G23, G26, G29	C1g	2 (marginal)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

O6 Awareness aller Patienten

E8 Besondere Sorgfaltspflichten bei PEP

A1 2-FA von Patienten

A3 Session Timeout

R18 Übernahme der Identität einer GFP am internen Portal

Ein Hacker stiehlt mittels Phishing die Login Daten einer hoch berechtigten GFP und benutzt diese, um über das interne Portal auf alle Dossiers zuzugreifen, für welche diese GFP berechtigt ist. Zusätzlich kann über den Notfallzugriff gezielt auf beliebige Dossiers zugegriffen werden.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R18	G8, G15, G23, G26, G29	C1a	4 (katastrophal)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

O7 Awareness aller Gesundheitsfachpersonen

A2 2-FA von GFP

A3 Session Timeout

A7 „Tx-Bestätigung“ beim Notfallzugriff

R19 Denial-of-Service Attacke auf das interne Portal einer (Stamm-)Gemeinschaft

Das interne Portal einer (Stamm-)Gemeinschaft wird mittels einer koordinierten Denial-of-Service (DoS) Attacke aus dem Internet ausser Betrieb gesetzt. Lese- und Schreibzugriffe für Patienten sind nicht mehr möglich.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R19	G18, G30	A2b	2 (marginal)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

T6 Penetration Testing aller aus dem Internet ansprechbaren Systeme

T14 Anti-DoS

SO11 Zugangspunkt

R20 Denial-of-Service Attacke auf den Zugangspunkt einer (Stamm-)Gemeinschaft

Der Zugangspunkt einer (Stamm-)Gemeinschaft wird mittels einer koordinierten Denial-of-Service Attacke aus dem Internet ausser Betrieb gesetzt. Lesezugriffe aus anderen (Stamm-)Gemeinschaften führen zu unvollständigen Resultaten. (Stamm-)Gemeinschaftsinterne Abfragen sind ebenfalls betroffen, soweit sie über den Zugangspunkt erfolgen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R20	G18, G30	A2b	2 (marginal)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

T14 Anti-DoS

SO12 Rechteattribute Datenbank

Keine besonderen zusätzlichen Risiken identifiziert

SO13 Document Registry

Keine besonderen zusätzlichen Risiken identifiziert

SO14 Document Repository

Keine besonderen zusätzlichen Risiken identifiziert

SO15 Lokales HPD

Keine besonderen zusätzlichen Risiken identifiziert

SO16 Protokollierungs-Datenbank

Keine besonderen zusätzlichen Risiken identifiziert

SO17 MPI

Keine besonderen zusätzlichen Risiken identifiziert

SO18 Primärsysteme

R21 Übernahme der KIS / PIS Identität einer GFP

Das (gegebenenfalls schwach authentisierte) KIS / PIS Login einer GFP wird durch eine andere GFP oder einen betrügerischen Dritten missbraucht, um gezielt auf die EPD deren Patienten zuzugreifen. Über den Notfallzugriff können beliebige Dossiers gezielt attackiert werden.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R21	G11, G12, G15, G29	C1d, C2c	4 (katastrophal)	2 (selten)	Rot (Hoch)

Sicherheitsmassnahmen:

A4 Sichere Identity Propagation (1)

A5 Sichere Identity Propagation (2)

A6 XUA Profil als Standard

SO19 eHealth-Connector

R22 Kompromittierter eHealth-Connector

Ein Hacker verwendet einen falschen oder kompromittierten eHealth-Connector und sammelt Patientendossiers. Da er den eHealth-Connector kontrolliert, kann er im Request beliebige GLN (weltweit oder zumindest dieser (Stamm-)Gemeinschaft) einsetzen und somit eine grosse Anzahl Dossiers einsehen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R22	G10, G18, G21, G28, G29	C1a, C2a, C3a	4 (katastrophal)	2 (selten)	Rot (Hoch)

Sicherheitsmassnahmen:

A4 Sichere Identity Propagation (1)

A5 Sichere Identity Propagation (2)

A6 XUA Profil als Standard

T3 Inventar der angebundenen eHealth-Connectors

SO20_HPD

R23 HPD-Anfragen werden umgeleitet und von unberechtigter Stelle beantwortet

Ein Hacker leitet HPD Anfragen auf ein falsches Verzeichnis um. In diesem gefälschten Verzeichnis sind GFPs in falschen Organisationen eingetragen. Die Integrität des HPD ist nicht mehr gewährleistet. Dadurch können GFPs nicht mehr auf EPDs zugreifen welche sie eigentlich sehen sollten und zudem können GFPs auf Dossiers zugreifen für welche sie eigentlich nicht berechtigt sind.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R23	G21, G23, G25, G30	I2a	3 (kritisch)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z1 Teilnahme am EPD Vertrauensraum

R24 Denial-of-Service Attacke auf das nationale HPD

Das nationale HPD wird mittels einer koordinierten Denial-of-Service Attacke aus dem Internet ausser Betrieb gesetzt. Die Rechteadministration für GFP ist nicht mehr möglich (z.B. GFP kann durch Patient nicht auf Sperrliste gesetzt werden, Abteilungswechsel kann nicht nachgeführt werden).

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R24	G18, G30	A1b	2 (marginal)	2 (selten)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z2 Penetration Testing der Zentralen Dienste

SO21_MDI

R25 MDI-Anfragen werden umgeleitet und von unberechtigter Stelle beantwortet

Ein Hacker leitet MDI-Anfragen auf ein falsches Verzeichnis um. In diesem gefälschten Verzeichnis wird das Metadatum „sensibel“ auf „nützlich“ umbenannt, womit alle sensiblen Daten nicht mehr ausreichend geschützt sind.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R25	G21, G23, G25, G30	I2a	3 (kritisch)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z2 Penetration Testing der Zentralen Dienste

Z5 Integritätsschutz für CPI Daten

SO22_RI

Keine besonderen Risiken identifiziert

SO23_CPI

R26 CPI nicht ausreichend gegen Manipulationen geschützt

Eine politisch motivierte Gruppierung installiert auf ihren eigenen Systemen eine Gemeinschafts-Software nach IHE inklusive einem SAML Identity Provider. Mittels Social Engineering gelingt es, den Zugangspunkt und den SAML IdP im nationalen CPI-Service zu konfigurieren. Dieser falsche Zugangspunkt kann nun unter der Identität beliebiger Gesundheitsfachpersonen Suchanfragen zu beliebigen Patientendossiers in allen (Stamm-)Gemeinschaften durchführen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R26	G25	C2c, I2b	4 (katastrophal)	1 (unwahrscheinlich)	Gelb (Mittel)

Sicherheitsmassnahmen:

Z2 Penetration Testing der Zentralen Dienste

Z5 Integritätsschutz für CPI Daten

SO24_UPI

Keine besonderen Risiken identifiziert

SO24_Externes Portal

Keine besonderen Risiken identifiziert

SO26_Endgerät GFP

R27 Übernahme der Kontrolle eines Endgerätes (PC, Laptop, Tablet, etc.) einer GFP

Mittels Trojanischem Pferd wird die Identität einer hochberechtigten GFP und die Kontrolle über deren Endgerät (PC, Laptop, Tablet, etc.) übernommen, um damit gezielt ein EPD oder alle EPDs zu lesen, für welche diese GFP berechtigt ist, resp. die eventuell lokal gespeicherten Daten zu kopieren oder auch falsche Daten (z.B. in Bezug auf Medikamentenverträglichkeit) ins EPD zu schreiben..

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R27	G23, G24, G26, G28, G29	C1a, C1d, I1b	4 (katastrophal)	2 (selten)	Rot (Hoch)

Sicherheitsmassnahmen:

O7 Awareness aller Gesundheitsfachpersonen

A7 „Tx-Bestätigung“ beim Notfallzugriff

E7 Kein Download sensibler Daten

A11 Sicherer EPD-Browser

A12 Sichere EPD-App

A13 Digitale Signatur für Daten im EPD

T13 Sichere Endgeräte für GFP

SO27 Endgerät Patient

R28 Übernahme der Kontrolle eines Endgerätes (PC, Laptop, Tablet, etc.) eines Patienten

Mittels Trojanischem Pferd wird die Identität eines Patienten und die Kontrolle über dessen Endgerät (PC, Laptop, Tablet, etc.) übernommen um damit auf dessen EPD zuzugreifen.

Risikobeurteilung:

Ref.	Bedrohungen	Szenarien	Max. Tragweite	Wahrscheinlichkeit	Risikostufe
R28	G23, G24, G26, G28, G29	C1g	2 (marginal)	3 (möglich)	Gelb (Mittel)

Sicherheitsmassnahmen:

A6 Awareness aller Patienten

E8 Besondere Sorgfaltspflichten bei PEP

A11 Sicherer EPD-Browser

A12 Sichere EPD-App

3.4 Risikoübersicht

Die identifizierten Risiken sind in der untenstehenden Tabelle summarisch aufgeführt:

	(1) vernachlässigbar	(2) marginal	(3) kritisch	(4) katastrophal
(5) häufig fast jeden Tag				
(4) wahrscheinlich alle 10 Tage				
(3) gelegentlich alle 100 Tage		R28	R6, R8	R5
(2) selten alle 1'000 Tage		R4, R17, R19, R20, R24	R3, R7, R10	R13, R15, R21, R22, R27
(1) unwahrscheinlich alle 10'000 Tage			R1, R2, R9, R23, R25	R11, R12, R14, R16, R18, R26

3.5 Bedrohungsübersicht

Ref	SO1	SO2	SO3	SO4	SO5	SO6	SO7	SO8	SO9	SO10	SO11	SO12	SO13	SO14	SO15	SO16	SO17	SO18	SO19	SO20	SO21	SO22	SO23	SO24	SO25	SO26	SO27
Höhere Gewalt																											
G1																											
G2																											
G3																											
G4																											
G5																											
Organisatorische Mängel																											
G6																											
G7					R7 **R8**		R11																				
G8	R1		R4 **R6**							R17 R18																	
G9	R1	R2			R9	R10	**R13** **R15**																				
G10		R2								R16									**R22**								
G11					R7 **R8**													**R21**									
G12							R14											**R21**									
Menschliche Fehlhandlungen																											
G13																											
G14		R2			R7 **R8**		R14																				
G15			R4 **R5** **R6**							R17 R18								**R21**									
G16							R12																				
G17																											
Technisches Versagen																											
G18										R16 R19	R20								**R22**	R24							
G19																											
G20																											
G21							R14			R16									**R22**	R23	R25						
G22																											
Vorsätzliche Handlungen																											
G23										R16 R17 R18										R23	R25					**R27**	R28
G24		R3	**R5**																							**R27**	R28
G25																				R23	R25		R26				
G26			**R5**							R17 R18																**R27**	R28
G27					R9		R11																				
G28							R14			R16									**R22**							**R27**	R28
G29		R3	**R5**		R9		R11			R16 R17 R18								**R21**	**R22**							**R27**	R28
G30										R19	R20									R23 R24	R25						

4 Sicherheitsmassnahmen

In diesem Kapitel sind organisatorische, applikatorische und technische Sicherheitsmassnahmen zur Begrenzung der identifizierten Sicherheitsrisiken aufgeführt und beschrieben (Massnahmenkatalog).

Für jede Massnahme ist aufgeführt:

- Welche Risiken mit der Massnahme adressiert werden
- Welchen „Controls“ gemäss ISO 27002:2013 die Massnahme zugeordnet ist
- Der für die Umsetzung zu erwartende Aufwand „A“ (gross / mittel / klein)
- Der durch Risikominderung zu erzielende Nutzen „N“ (gross / mittel / klein)
- Die aktuelle Priorisierung der Massnahme (MUSS / SOLL / KANN)

4.1 Organisatorische Sicherheitsmassnahmen

Ref	Massnahme	Beschreibung	Risi-ken	ISO	A/N	Prio.
O1	ISMS	Jede zertifizierte (Stamm-)Gemeinschaft betreibt ein Information Security Management System (ISMS) für die nachhaltige Pflege der Informationssicherheit. Das ISMS berücksichtigt Komplexität und Grösse der (Stamm-)Gemeinschaft, umfasst aber im Minimum: • Die Nominierung eines Informationssicherheitsbeauftragten (ISBO) für die (Stamm-)Gemeinschaft; • Einen vom ISBO beurteilten Risikokatalog (Risk Register); • Einen Risikobehandlungsplan (Risk Treatment Plan); • Einen mindestens jährlich stattfindenden Management Review, bei dem die Geschäftsleitung der (Stamm-) Gemeinschaft über den Risikokatalog und den Risikobehandlungsplan befindet. *Hinweis:* Hilfsmittel (z.B. ISBO Stellenbeschreibung, Template für Risikokatalog) sollten zentral von eHealth Suisse bereitgestellt werden.	alle	6.1.1	M/G	MUSS
O2	SIEM	Jede zertifizierte (Stamm-)Gemeinschaft betreibt ein Security Information and Event Management (SIEM), das Anomalien im System erkennt und sicherstellt, dass diese angemessen adressiert werden (organisatorisch und technisch). Das SIEM wird (Stamm-)Gemeinschaftsspezifisch aufgebaut, erkennt und adressiert aber im Minimum die folgenden Muster: • Angriffe aus dem Internet auf das interne Portal oder auf den Zugangspunkt (insb. Responding Gateway); • Eine unübliche Häufung von schreibenden oder lesenden Zugriffen auf Repositories, Registry oder MPI, die auf eine automatisierte Attacke hinweist; • Ungewöhnliche und kritische Mutationen von Berechtigungsdaten in RADB, IAM oder HPD. Das SIEM umfasst Prozesse für den Umgang mit Sicherheitsereignissen und definiert mindestens die folgenden Notfallprozesse: • Wie und unter welchen Bedingungen wird die (Stamm-) Gemeinschaft vom EPD Vertrauensraum isoliert (Sperren des Zugangspunktes); • Wie und unter welchen Bedingungen wird die (Stamm-) Gemeinschaft vom Internet isoliert (z.B. Sperren des internen Portals); • Wie und unter welchen Bedingungen wird die (Stamm-) Gemeinschaft von einem angebundenen Primärsystem isoliert (z.B. Sperren eHealth-Connector).	R15	16.1.x	M/G	MUSS

Ref	Massnahme	Beschreibung	Risiken	ISO	A/N	Prio.
O3	Meldepflicht für Sicherheits-vorfälle	Jede zertifizierte (Stamm-)Gemeinschaft ist verpflichtet, Sicherheitsvorfälle an eine nationale zentrale Stelle zu melden. *Hinweis*: Die Melde- und Analysestelle Informationssicherung (MELANI) stellt grundsätzlich die Möglichkeit solcher geschlossener Benutzerkreise zur Verfügung.	alle	16.1.2	K/M	MUSS
O4	EPD ISBO-Gremium	Unter Leitung von eHealth Suisse wird ein Schweiz-weites Gremium etabliert, in dem die ISBO aller zertifizierten (Stamm-) Gemeinschaften vertreten sind. In diesem Gremium werden insbesondere die folgenden Themen behandelt: • Peer Review der Risikokataloge und Risk Treatment Plans der zertifizierten (Stamm-)Gemeinschaften; • Gemeldete Sicherheitsereignisse und deren Bewältigung; • Aktuelle Themen bezüglich Risikoexposition und Risikobegrenzung.	alle	6.1.3 6.1.4	M/M	SOLL
O5	Inventar und Ownership der Repositories	Jedes an einer zertifizierten (Stamm-)Gemeinschaft teilnehmende Primärsystem verfügt über eine Regelung dafür, welche Datenbestände als Kopie über die EPD-Infrastruktur zugänglich gemacht werden dürfen. Jede zertifizierte (Stamm-)Gemeinschaft verfügt über ein Inventar aller eigenen Repositories. Dieses Inventar: • Identifiziert pro Repository einen Dateneigner („Owner“); • Dokumentiert das Einverständnis des Dateneigners, dass das Repository Teil des EPD Vertrauensraums ist; • Wird mindestens jährlich nachgeführt.	R1 R2	8.1.1 8.1.2 13.2.1 13.2.2	T/M	MUSS
O6	Awareness aller Patienten	Patienten werden vor der Eröffnung eines Patientendossiers auf die damit verbundenen Sicherheitsrisiken und die empfohlenen Sicherheitsmassnahmen hingewiesen. Themen sind insbesondere: • Der Umgang mit Authentisierungsmitteln • Die Prinzipien der Berechtigungsvergabe • Die sichere Nutzung von Endgeräten (PC, Smartphone,…) • Das Verhalten in Bezug auf Social Engineering, Phishing, Hoaxes, etc.	R5 R6 R17 R28	7.2.2	M/G	MUSS
O7	Awareness aller Gesundheits-fachpersonen	Gesundheitsfachpersonen werden vor der Registrierung im nationalen HPD auf die mit dem Patientendossier verbundenen Sicherheitsrisiken und die einzuhaltenden Sicherheitsmassnahmen hingewiesen. Themen sind insbesondere: • Der Umgang mit Authentisierungsmitteln • Die Prinzipien der Dokumentenklassifizierung • Die sichere Nutzung von Endgeräten (PC, Smartphone,…) • Das Verhalten in Bezug auf „Social Engineering“, Phishing, Hoaxes, etc. • Information über die Verantwortlichkeiten beim Einsatz von Hilfspersonen.	R18 R27	7.2.2	M/G	MUSS

Tabelle 7: Organisatorische Sicherheitsmassnahmen

4.2 Applikatorische Sicherheitsmassnahmen

Ref	Massnahme	Beschreibung	Risiken	ISO	A/N	Prio.
A1	2-FA von Patienten	Patienten werden vor dem Zugriff auf das elektronische Patientendossier mit mindestens zwei Faktoren aus den Kategorien „Wissen“, „Haben“ oder „Sein“ authentisiert. • Die 2-Faktor Authentisierung wird vom internen Portal oder einem vorgelagerten Authentisierungsservice (z.B. (Stamm-)Gemeinschafts-externer IdP) durchgeführt. • Die Authentisierung muss mittels eines vom BAG für Patienten zugelassenen Authentisierungsverfahrens erfolgen. • Bei der Ausstellung des Authentisierungsmittels muss der Patient persönlich anhand von offiziellen Ausweispapieren (ID, Pass, Versichertenkarte) identifiziert werden spätestens anlässlich der Eröffnung des Patientendossiers. *Hinweis*: Die 2-Faktor Authentisierung von Patienten entspricht damit dem NIST Level 3 gemäss „Electronic Authentication Guideline“ (NIST Special Publication 800-63-2, August 2013).	R17	9.4.2	G/G	MUSS
A2	2-FA von GFP	Gesundheitsfachpersonen werden vor dem Zugriff auf das elektronische Patientendossier mit mindestens zwei Faktoren aus den Kategorien „Wissen“, „Haben“ oder „Sein“ authentisiert. Dabei muss mindestens einer der Faktoren auf nicht kopierbarer kryptographischer Hardware beruhen. • Die 2-Faktor Authentisierung gilt für alle Zugriffspfade, insbesondere auch für Zugriffe über das KIS/PIS. • Die 2-Faktor Authentisierung wird vom internen Portal oder einem vorgelagerten Authentisierungsservice (z.B. (Stamm-)Gemeinschafts-externer IdP oder KIS Authentisierungssystem) durchgeführt. • Die Authentisierung muss mittels eines vom BAG für GFP zugelassenen Authentisierungsverfahrens erfolgen. • Die Verwaltungsprozesse für die Ausstellung des Authentisierungsmittels müssen dokumentiert und mit der Benutzerverwaltung abgestimmt sein (z.B. Eintritt, Austritt). *Hinweis*: Die 2-Faktor Authentisierung von GFP entspricht damit dem NIST Level 4 gemäss „Electronic Authentication Guideline“ (NIST Special Publication 800-63-2, August 2013).	R18	9.4.2	G/G	MUSS
A3	Session Timeout	Erfolgt über mehr als max. 30 Minuten (bei Patienten) beziehungsweise max. 2 Stunden (Gesundheitsfachpersonen) keine Interaktion des Benutzers mit dem Elektronischen Patientendossier, so muss die 2-Faktor Authentisierung vor dem nächsten Zugriff erneut durchgeführt werden.	R17 R18	9.4.2	K/M	MUSS
A4	Sichere Identity Propagation (1)	Für die Weitergabe der authentisierten Benutzeridentität in der (Stamm-)Gemeinschafts-übergreifenden Kommunikation wird das IHE:XUA Profil eingesetzt. • Der X-Assertion Provider muss von einer national anerkannten CA zertifiziert sein. • Die Integrität des öffentlichen Schlüssels des X-Assertion Providers wird durch ein X.509 Zertifikat gewährleistet, ausgestellt von einer nationalen EPD Certification Authority.	R21 R22	9.4.2	M/G	MUSS
A5	Sichere Identity Propagation (2)	Der Missbrauch (z.B. Manipulation und Replay) von X-Assertions wird verhindert. Dabei gilt mindestens: • Die Lebensdauer von X-Assertions ist auf maximal 5 Minuten begrenzt. X-Assertions können erneuert werden, solange eine aktive Session zwischen dem X-Assertion Provider und dem Benutzer besteht; • Für die Signatur der X-Assertions wird ein privater Schlüssel mit einer Länge von mindestens 2048 Bit eingesetzt; • X-Assertions werden von X-Service User und X-Service Provider nicht gespeichert und/oder gegenüber der Applikation exponiert; • X-Service Provider validieren bei jedem Aufruf mindestens die Signatur, die Certificate Chain des X-Service Providers sowie die Gültigkeitsperiode der X-Assertion.	R21 R22	9.4.2	M/G	MUSS

Ref	Massnahme	Beschreibung	Risiken	ISO	A/N	Prio.
A6	XUA Profil als Standard	Wird für die Weitergabe der authentisierten Benutzeridentität innerhalb einer (Stamm-)Gemeinschaft ein anderes Verfahren als das IHE:XUA Profil (gem. IHE ITI Technical Framework Rev. 11.0 vom 23.09.2014) eingesetzt, so muss dessen sicherheitstechnische Äquivalenz nachgewiesen werden.	R21 R22	9.4.2	K/G	MUSS
A7	„Tx-Bestätigung“ beim Notfallzugriff	Ein Notfallzugriff muss von der Gesundheitsfachperson bestätigt werden, bevor er vom System ausgeführt wird. • Die Bestätigung umfasst zwingend eine manuelle Interaktion der GFP, beispielsweise die Eingabe eines Einmalpasswortes (ab Streichliste gelesen oder per SMS empfangen) oder die PIN-Eingabe an einem lokalen Token (z.B. Smartcard). *Hinweis*: Solche „Transaktionsbestätigungen“ für kritische Funktionen sind aus dem e-Banking bekannt und haben sich als Massnahme gegen „man-in-the-client“ Angriffe bewährt.	R18 R27	9.4.2	M/G	MUSS
A8	Datenklassifizierung anhand der Berufsgruppe ermöglichen	Der Patient kann als Erweiterung der vom Gesetz verlangten Möglichkeiten die Grundeinstellung so definieren, dass Dokumente definierter Berufsgruppen (z.B. Psychiatrie, Onkologie, Strafverfolgung) bei der Aufnahme ins Patientendossier als „sensible Daten“ oder „geheime Daten“ klassifiziert werden. • Die Klassifizierung kann z.B. auf dem „healthcareFacilityType“ Attribut von datenerzeugenden Organisationen sowie passenden Attributen von Gesundheitsfachpersonen basieren.	R4 R6	8.2.3	K/M	SOLL
A9	Verschlüsselte Daten-speicherung	Im EPD abgelegte Daten werden verschlüsselt gespeichert, im Minimum Document Registry und Document Repository.	R11 R12 R14	8.2.3 10.1.1 10.1.2	G/G	MUSS
A10	Kein Caching von Daten	Im EPD abgelegte Daten werden nicht ausserhalb der Document Repositories persistent gespeichert. Insbesondere keine Vorratsdatenspeicherung ohne explizite Willensäusserung durch den Anwender (GFP oder Patient). • *Hinweis*: Dies gilt insbesondere auch für Daten, die aus einer anderen (Stamm-)Gemeinschaft bezogen werden.	R14	8.2.3	K/M	MUSS
A11	Sicherer EPD-Browser	Allen Patienten und Gesundheitsfachpersonen wird ein sicher konfigurierter Browser zur Verfügung gestellt, der missbräuchliche EPD-Zugriffe durch lokale Schadsoftware („man-in-the-client“) nach Möglichkeit unterbindet: • Einschränkung des Zugriffes auf die internen Portale der zertifizierten (Stamm-)Gemeinschaften durch restriktive Konfiguration der TLS Serverauthentisierung; • Kontrollierte und statisch konfigurierte Laufzeitumgebung; • Laufende Aktualisierung der Software, um bekannt werdende Schwachstellen zu eliminieren.	R27 R28	11.2.6 12.2.1	M/G	SOLL
A12	Sichere EPD-App	Allen Patienten und Gesundheitsfachpersonen wird eine sicher konfigurierte Smartphone App zur Verfügung gestellt, die missbräuchliche EPD-Zugriffe durch lokale Schadsoftware („man-in-the-client“) nach Möglichkeit unterbindet: • Einschränkung des Zugriffes auf die internen Portale der zertifizierten (Stamm-)Gemeinschaften durch restriktive Konfiguration der TLS Serverauthentisierung; • Kontrollierte und von anderen Apps separierte Laufzeitumgebung; • Laufende Aktualisierung der Software, um bekannt werdende Schwachstellen zu eliminieren.	R27 R28	11.2.6 12.2.1	M/G	SOLL
A13	Digital signierte EPD-Dokumente	Dokumente werden bei der Registrierung im EPD digital signiert, so dass jede nachträgliche Manipulation der Dokumente festgestellt werden kann.	R27	8.2.3 10.1.1 10.1.2	G/M	KANN

Tabelle 8: Applikatorische Sicherheitsmassnahmen

4.3 Technische Sicherheitsmassnahmen

Ref	Massnahme	Beschreibung	Risiken	ISO	A/N	Prio.

T1	Logische Isolation des EPD Vertrauensraums vom Internet	IHE-Services einer (Stamm-)Gemeinschaft sind durch Firewalls geschützt und können nur von Systemen aufgerufen werden, die zu einer zertifizierten (Stamm-)Gemeinschaft gehören.
		• Alle Systeme, die über das Internet auf einen IHE-Service zugreifen, authentisieren den IHE-Service mittels TLS Serverauthentisierung.
		  ○ Für interne und externe Portale sowie Responding Gateways werden hierfür öffentliche Extended Validation (EV) TLS Zertifikate eingesetzt.
		  ○ Für andere IHE-Services werden hierfür öffentliche Extended Validation (EV) TLS Zertifikate eingesetzt oder TLS Zertifikate, die nur innerhalb der Gemeinschaft gültig sind.
		• Alle IHE-Services, die aus dem Internet aufrufbar sind, authentisieren das aufrufende System mittels TLS Client Authentication:
		  ○ Responding Gateways lassen den Verbindungsaufbau nur zu, wenn das aufrufende System zu einer zertifizierten (Stamm-)Gemeinschaft oder einem zertifizierten Portal gehört.
		  ○ Alle übrigen IHE-Services lassen den Verbindungsaufbau nur zu, wenn das aufrufende System zur eigenen zertifizierten (Stamm-)Gemeinschaft gehört.
			R14	9.1.2
				13.1.3
					M/G	MUSS

T2	ATNA Profil als Standard	Wird für die gegenseitige Authentisierung von Systemen über öffentliche Netze innerhalb einer (Stamm-)Gemeinschaft ein anderes Verfahren als das IHE:ATNA Profil eingesetzt, so ist dessen sicherheitstechnische Äquivalenz nachzuweisen.	R14	9.4.2	K/G	MUSS
T3	Inventar der angebundenen eHealth-Connectors	Jede zertifizierte (Stamm-)Gemeinschaft führt ein Inventar, in dem alle zur (Stamm-)Gemeinschaft gehörigen IHE-Aktoren (Document Source resp. Document Consumer) explizit registriert sind. Das Inventar umfasst mindestens: • Das TLS Clientzertifikat des IHE-Aktors; • Die für den IHE-Aktor verantwortliche Person; • Das Datum der letzten Bestätigung durch den ISBO. Der Verbindungsaufbau mit einem IHE-Service wird nur zugelassen, wenn der IHE-Aktor im Inventar registriert ist. Der Sicherheitsbeauftragte der (Stamm-)Gemeinschaft (ISBO) muss der Registrierung zustimmen und das Inventar der eHealth-Connectors mindestens jährlich überprüfen.	R14 R22	9.1.2 13.1.3	M/G	MUSS
T4	„Swiss banking level security“ des internen Portals	Das interne Portal einer (Stamm-)Gemeinschaft ist mit speziellen Sicherheitsmassnahmen gegen Angriffe aus dem Internet geschützt. Das Niveau der Sicherheitsmassnahmen entspricht mindestens den *best practices* im Schweizer Bankenumfeld. Wesentliche Sicherheitselemente sind beispielsweise: • Eine dem internen Portal vorgelagerte Web Application Firewall als sicherer TLS-Endpunkt, Authentication Enforcement Point, Access Control Enforcement Point sowie Filter für Angriffe auf Protokoll- oder Datenebene; • Die Nutzung von Extended Validation (EV) TLS Zertifikaten; • Betriebsprozesse, die eine laufende Erkennung von Angriffen sowie eine sehr rasche Behebung von bekanntgewordenen Schwachstellen sicherstellen. *Hinweis zur Umsetzung*: • „Best practices im Schweizer Bankenumfeld“ haben sich in bald 20 Jahren des Schweizer Internet-Bankings durch gegenseitigen Erfahrungsaustausch informell etabliert, sind allerdings weder formal definiert noch dokumentiert. • Bei spezifischen Fragestellungen (z.B. zugelassene Token, minimale Passwortregeln, session timeout, …) könnte die Best Practice beigezogen werden, indem die aktuelle Implementierung bei 5 Referenz-Banken in Erfahrung gebracht und als Entscheidungsgrundlage verwendet wird	R16	14.1.2	G/G	SOLL

Ref	Massnahme	Beschreibung	Risiken	ISO	A/N	Prio.
T5	Dokumentierte Sicherheit des internen Portals	Jede zertifizierte (Stamm-)Gemeinschaft dokumentiert das zum Schutz des internen Portals implementierte Sicherheitsdispositiv zu Handen der Zertifizierungsstelle. Die Dokumentation umfasst mindestens: • Die Systemtopologie der DMZ; • Die auf WAF und Webserver eingesetzte Software (inklusive Version und Release-Stand); • Vorkehrungen für die Erkennung und Behandlung von Angriffen und Schwachstellen.	R16	14.1.2	K/M	MUSS
T6	Penetration Testing aller aus dem Internet ansprechbaren Systeme	Alle aus dem Internet erreichbaren Systeme werden im Rahmen der Zertifizierung von einer hierauf spezialisierten unabhängigen Stelle auf Schwachstellen überprüft. Der Scope dieses Penetration Testing umfasst mindestens: • Das interne Portal • Den Zugangspunkt (insb. Responding Gateway) • Andere IHE-Services, die über das Internet aufrufbar sind Die Prüfung des internen Portals umfasst mindestens: • Angriffe auf der Applikationsebene („manual hacking“); • Angriffe auf der Protokollebene; • Die Konfiguration von Plattform und Applikationsserver. Die Prüfung der Zugangspunkte umfasst mindestens: • Prüfung, dass nur von Initiating Gateways zertifizierter (Stamm-)Gemeinschaften und zertifizierter externer Portale eine Verbindung aufgebaut werden kann; Die Prüfung aller übrigen aus dem Internet aufrufbaren IHE-Services umfasst mindestens: • Prüfung, dass nur von Systemen der eigenen (Stamm-) Gemeinschaft eine Verbindung aufgebaut werden kann; • Prüfung, dass aufrufende eHealth-Connectors gemäss Massnahme T3 korrekt inventarisiert sind.	R16 R19	12.6.1 14.1.2 18.2.1	M/G	MUSS
T7	Isolation der IHE-Services von anderen Systemen	Auch IHE-Services, die nicht aus dem Internet aufgerufen werden können, lassen den Verbindungsaufbau nur von hierzu vom ISBO der (Stamm-)Gemeinschaft akzeptierten Systemen zu. • Jede zertifizierte (Stamm-)Gemeinschaft dokumentiert das hierzu eingesetzte Verfahren (z.B. IP-Filter auf Firewalls) zu Handen der Zertifizierungsstelle.	R14	13.1.3	K/M	MUSS
T8	Isolation der EPD-Daten von anderen Systemen	Systeme mit persistent gespeicherten EPD-Daten (dies sind insb. alle Repositories sowie Registry, RADB und MPI der (Stamm-)Gemeinschaft) sind netzwerktechnisch von allen Systemen separiert, die ein tieferes Sicherheitsniveau aufweisen. • Jede zertifizierte (Stamm-)Gemeinschaft dokumentiert das hierzu eingesetzte Verfahren (z.B. Netzwerksegmentierung mittels Firewalls) zu Handen der Zertifizierungsstelle.	R14	13.1.3	M/M	MUSS
T9	EPD-Daten bleiben in der Schweiz	Datenspeicher und Datenleitungen im EPD Vertrauensraum werden zu keinem Zeitpunkt ausserhalb der Schweizer Rechtshoheit gespeichert.	R13	18.1.4	M/G	MUSS
T10	Zertifizierte Betreiber der EPD-Systeme	Alle Betreiber von Systemen einer zertifizierten (Stamm-)Gemeinschaft verfügen über eine anerkannte Zertifizierung nach ISO 27001. Diese Zertifizierung bietet eine gewisse Gewähr dafür, dass der Betreiber die Informationssicherheit nachhaltig und gemäss dokumentierten Prozessen sicherstellt, macht aber keine Aussage in Bezug auf EPD-spezifische Sicherheitsmassnahmen.	Alle	18.2.1	M/M	SOLL

Ref	Massnahme	Beschreibung	Risiken	ISO	A/N	Prio.
T11	Zusätzliche Evidenz für sicheren Systembetrieb	Für ISO 27002 Controls, die für den sicheren Betrieb des EPD von besonderer Relevanz sind, wird im Rahmen der Zertifizierung zusätzliche Evidenz verlangt und überprüft. Die von jedem Betreiber (inklusive der Betreiber aller Repositories) zu liefernde zusätzliche Evidenz umfasst insbesondere: • Nachweis, dass externe Zugriffe auf die Betriebsumgebung entweder unterbunden oder angemessen geschützt sind. Externe Zugriffe erfordern eine 2-Faktor Authentisierung, dürfen nur befristet bei Bedarf aktiviert werden und dürfen keinen Export von Patientendaten ermöglichen (ISO Control 6.2.2); • Nachweis, dass Betriebspersonal mit Zugriff auf Patientendaten sorgfältig ausgewählt wird und der ärztlichen Schweigepflicht untersteht (7.1.2); • Nachweis, dass Datenträger mit Patientendaten korrekt entsorgt und vorgängig alle Daten gelöscht werden (8.3.2); • Eine vom ISBO der (Stamm-)Gemeinschaft visierte Liste aller Personen, die unabhängig von der RADB Rechteverwaltung Zugriff auf Patientendaten haben („Liste der Schlüsselpersonen“) (9.2.3); • Nachweis, dass privilegierte Zugriffe von OS-, DB- und Applikations-Administratoren auf die Betriebsumgebung angemessen geschützt sind. Privilegierte Zugriffe erfordern eine 2-Faktor Authentisierung, müssen überwacht werden und dürfen keinen Export von Patientendaten ermöglichen (ISO Control 9.2.3); • Nachweis, dass diese Schlüsselpersonen eine Personensicherheitsprüfung (PSP) nach Militärgesetz durchlaufen haben (7.1.1); • Nachweis, dass Entwicklung, Test und Inbetriebnahme neuer Systeme nach einem kontrollierten Prozess abläuft (12.1.2); • Nachweis, dass die EPD Produktionsumgebung von den Entwicklungs- und Testumgebungen isoliert ist (12.1.4); • Nachweis, dass vollständige Backups gemacht werden und dass diese verschlüsselt sind (12.3.1); • Nachweis, dass die technischen Logs keine unverschlüsselten Patientendaten enthalten (12.4.2); • Nachweis, dass die Systemuhren mit einer externen Zeitquelle abgeglichen sind (12.4.4); • Nachweis, dass die Installation von Software auf EPD Produktionssystemen nach einem kontrollierten Prozess abläuft (12.5.1); • Nachweis, dass alle EPD Produktionssysteme regelmässig auf Sicherheitsschwachstellen überprüft und die erkannten Schwachstellen im Rahmen eines kontrollierten Patch Management Prozesses behoben werden (12.6.1); • Nachweis, dass die EPD Produktionssysteme von anderen Systemen des Betreibers isoliert sind (13.1.3); • Nachweis, dass neue Software vor der Inbetriebnahme einem kontrollierten Abnahmetest unterliegt (14.2.9); • Nachweis, dass sich in unzureichend geschützten Testumgebungen keine Patientendaten befinden (14.3.1); • Eine vom ISBO der (Stamm-)Gemeinschaft visierte Liste und Risikobewertung aller am Betrieb beteiligten Sub-Unternehmen (15.2.1).	R11 R12 R13	6.2.2 7.1.1 7.1.2 8.3.2 9.2.3 12.1.2 12.1.4 12.3.1 12.4.2 12.4.4 12.5.1 12.6.1 13.1.3 14.2.9 14.3.1 15.2.1	M/G	MUSS
T12	Virenschutz	Alle im EPD abgelegten Dateien werden auf Schadsoftware gescannt. Solche Scans finden statt: • Vor jedem schreiben in ein Repository; • Entweder bei jedem lesen aus einem Repository oder periodisch mindestens halbjährlich für gespeicherte Dateien.	R3	12.2.1	K/M	MUSS
T13	Sichere Endgeräte für GFP	Alle Betreiber von Endgeräten, die von Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier genutzt werden, stellen eine sichere Konfiguration der Geräte sicher. Diese umfasst mindestens: • Ein regelmässig aktualisierter lokaler Virenschutz • Kein lokales Administrationsrecht für normale Benutzer • Regelmässige Softwareaktualisierungen	R27	11.2.4	M/M	MUSS

Ref	Massnahme	Beschreibung	Risi-ken	ISO	A/N	Prio.
T14	Anti-DoS	Alle vom Internet erreichbaren Schnittstellen wie z.B. internes Portal, externes Portal, Zugangspunkt (Gateway) sind gegen Denial-of-Service (DoS) Angriffe aus dem Internet geschützt.	R19 R20	11.2.4	M/M	MUSS

Tabelle 9: Technische Sicherheitsmassnahmen

4.4 Sicherheitsmassnahmen für Zentrale Dienste

Ref	Massnahme	Beschreibung	Risi-ken	ISO	A/N	Prio.
Z1	Teilnahme am EPD Vertrauens-raum	Beim Aufruf eines zentralen EPD-Dienstes (CPI-Service, HPD-Service, MDI-Service, RI-Service sowie UPI-Service der ZAS) authentisieren sich Client und Server gegenseitig. Wird beim Aufruf eines zentralen EPD-Dienstes für die gegen-seitige Authentisierung ein anderes Verfahren als das IHE:ATNA Profil eingesetzt, so muss dessen sicherheitstechni-sche Äquivalenz nachgewiesen werden.	R23	9.1.2 13.1.3	K/G	MUSS
Z2	Penetration Testing der Zentralen Dienste	Die zentralen Dienste (CPI-Service, HPD-Service, MDI-Service, RI-Service sowie UPI-Service der ZAS) werden vor der Be-triebsaufnahme von einer hierauf spezialisierten unabhängigen Firma auf Schwachstellen überprüft. Die Prüfung der Zentralen Dienste umfasst mindestens: • Angriffe auf der Applikationsebene („manual hacking“); • Angriffe auf der Protokollebene; • Die Konfiguration von Plattform und Applikationsserver.	R24 R25 R26	12.6.1 14.1.2 18.2.1	M/G	MUSS
Z3	Eintrag aller GFP im HPD	Alle Gesundheitsfachpersonen, die für den Zugriff auf ein Pati-entendossier berechtigt werden können, werden vorgängig im nationalen Verzeichnis der GFP (HPD) registriert. Dies umfasst insbesondere auch alle Hilfspersonen.	R10	9.2.1	K/M	SOLL
Z4	IAM HPD	Die Prozesse und Verantwortlichkeiten für die Verwaltung der Gesundheitsfachpersonen und Organisationseinheiten im zent-ralen Verzeichnisdienst HPD-S sind etabliert. Das IAM HPD umfasst im Minimum: • Für jede im HPD registrierte Gesundheitsfachperson und Organisationseinheit sind die für den Eintrag verantwortliche (Stamm-)Gemeinschaft und eine von der (Stamm-) Gemeinschaft beauftragte verantwortliche Person identifi-ziert; • Für jede im HPD registrierte Gesundheitsfachperson wird mindestens halbjährlich geprüft und bestätigt, dass der Ein-trag gerechtfertigt und die eingetragenen Daten korrekt sind; • Für jede im HPD registrierte Organisationseinheit wird min-destens vierteljährlich geprüft und bestätigt, dass die einge-tragenen Gruppenzugehörigkeiten korrekt sind.	R7 R8 R9	7.3.1 9.2.1 9.2.2 9.2.5 9.2.6	M/G	MUSS
Z5	Integritätsschutz für CPI Daten	Einträge und Mutationen an sicherheitskritischen Einträgen im Verzeichnisservice für die (Stamm-)Gemeinschaften (CPI-S) sind mit speziellen Massnahmen gegen Missbrauch geschützt: • Mutationen werden nur vom BAG vorgenommen; • Die sicherheitskritischen Einträge sind kryptographisch (z.B. durch einen Hashwert) gegen unbemerkte Manipulation geschützt.	R25 R26	12.1.2	K/M	MUSS

Tabelle 10: Sicherheitsmassnahmen für Zentrale Dienste

4.5 Empfehlungen zum besonderen Schutz sensibler Daten

Die nachfolgende Betrachtung adressiert eine von den Autoren empfohlene Erweiterung des grundlegenden Konzeptes der Zugriffsregelung nach EPDG. Die zusätzlichen Sicherheitsmassnahmen, die sich daraus ergeben, sind für die Zertifizierung von (Stamm-)Gemeinschaften bis auf weiteres nicht relevant.

Grundlegendes Konzept der Zugriffsregelung:

Nach Datenschutzgesetzgebung sind alle medizinischen Daten besonders schützenswerte Daten, weshalb bei den vorgeschriebenen Sicherheitsmassnahmen keine Unterscheidung zwischen medizinischen und sensiblen Daten gemacht wird. Die Vertraulichkeitsstufen sind gemäss diesem Konzept primär dazu gedacht, dass der Patient entsprechend seiner individuellen Beurteilung der Dokumenten-Vertraulichkeit den Kreis der zugreifenden Personen (GFPs) steuern kann.

Empfohlene Erweiterung zum besonderen Schutz sensibler Daten:

Auf Grund der Risikobetrachtung sehen wir zwischen medizinischen Daten und sensiblen Daten einen Unterschied in Bezug auf die Tragweite eines typischen bzw. durchschnittlichen Schadenfalls: Wenn der Patient gewisse Dokumente als sensibel klassifiziert, dann müssen wir davon ausgehen, dass er bei einer unberechtigten Einsicht in diese Dokumente einen besonders grossen finanziellen oder persönlichen Schaden erwartet. Aus dieser grösseren erwarteten Tragweite resultiert ein entsprechend grösseres Risiko. Dies rechtfertigt aus unserer Sicht die Anwendung zusätzlicher Sicherheitsmassnahmen für sensible Daten, deren Anwendung auf die grosse Masse der medizinischen Daten ggf. nicht praktikabel oder zu einschränkend wäre.

In Erweiterung des grundlegenden Konzeptes der Zugriffsregelung zielen diese zusätzlichen Massnahmen darauf ab, den Kreis der potentiell Zugreifenden weiter zu limitieren. Der Kreis der potentiell Zugreifenden umfasst in dieser erweiterten Sicht aber nicht nur die Gesundheitsfachpersonen sondern vor allem auch Zugriffe, die ausserhalb der Applikation erfolgen (z.B. durch Systemadministratoren, Hacker, Trojanische Pferde oder Festplatten-Diebe).

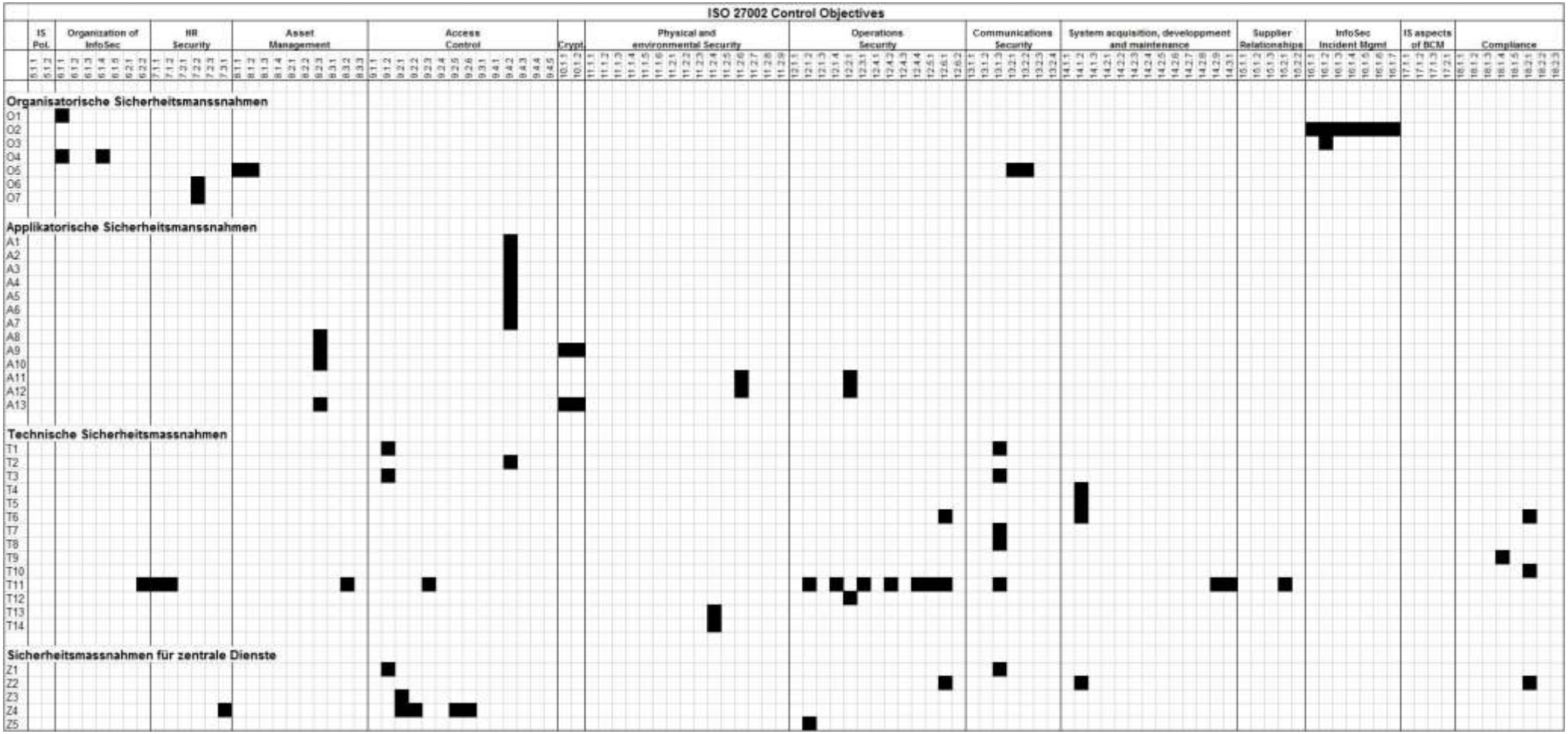
Ref	Erweiterte Massnahme	Beschreibung	Risiken	ISO	A/N
E1	Dokumentierter Schutz sensibler und geheimer Daten	Für sensible und geheime Daten gilt ein besonderer Schutz. • Jede zertifizierte (Stamm-)Gemeinschaft dokumentiert, ob bzw. welche speziellen Sicherheitsmassnahmen für sensible und geheime Daten implementiert sind. • Für die Anwendbarkeit der besonderen Massnahmen ist die Klassifizierung gemäss Metadatum des Registry-Eintrags massgebend unabhängig davon, wer diese Klassifizierung aus welchen Gründen vorgenommen hat.	R4 R6	8.2.1 8.2.2 8.2.3	K/M
E2	Besondere Sorgfaltspflichten bei Nutzern sensibler Dokumente	Bei Gesundheitsfachpersonen, die auf Grund ihrer beruflichen Tätigkeit häufig mit sensiblen Daten in Berührung kommen, gelten besondere Sorgfaltspflichten bei der Schulung. Vertieft zu behandelnde Themen sind (vgl. Massnahme O9): • Der Umgang mit Authentisierungsmitteln • Die Prinzipien der Dokumentenklassifizierung • Die sichere Nutzung von Endgeräten (PC, Smartphone, …) • Das Verhalten in Bezug auf „Social Engineering“ • Information über die Verantwortlichkeiten beim Einsatz von Hilfspersonen. Insbesondere werden diese dahingehend instruiert, sensible Daten beim Schreiben ins EPD als solche zu klassifizieren.	R18 R27	7.2.2	M/M

Ref	Erweiterte Massnahme	Beschreibung	Risiken	ISO	A/N
E3	Datenklassifizierung anhand der Berufsgruppe ermöglichen	Der Patient kann als Erweiterung der vom Gesetz verlangten Möglichkeiten die Grundeinstellung so definieren, dass Dokumente definierter Berufsgruppen (z.B. Psychiatrie, Onkologie, Strafverfolgung) bei der Aufnahme ins Patientendossier als „sensible Daten“ oder „geheime Daten“ klassifiziert werden. • Die Klassifizierung kann z.B. auf dem „healthcareFacilityType“ Attribut von datenerzeugenden Organisationen sowie passenden Attributen von Gesundheitsfachpersonen basieren.	R4 R6	8.2.3	K/M
E4	Applikatorische Verschlüsselung sensibler und geheimer Daten	Daten der Klassifizierungsstufen „geheim“ und „sensibel“ werden verschlüsselt gespeichert. Verschlüsselung und Schlüsselverwaltung sind so implementiert, dass weder die OS-Administratoren (z.B. „root“) noch die DB-Administratoren (z.B. „DBA“) des Document Repository bzw. Document Registry die verschlüsselten Daten lesen können.	R11 R12 R14	8.2.3 10.1.1 10.1.2	G/G
E5	Attribut-basierte Zugriffskontrolle für sensible Daten	Beim Lesen von Daten der Klassifizierungsstufe „sensibel“ wird zusätzlich zur RADB-Autorisierung geprüft, ob die Gesundheitsfachperson über die erforderliche Qualifikation verfügt, erkennbar über entsprechende Attribute im HPD-Eintrag der Gesundheitsfachperson. • Der Patient hat die Möglichkeit, diese zusätzliche Zugriffskontrolle im Rahmen der Grundeinstellungen zu aktivieren oder zu deaktivieren; • Der Patient hat die Möglichkeit, diese zusätzliche Zugriffskontrolle nur für solche Zugriffe zu aktivieren, die über eine Gruppenberechtigung erfolgen; • Der Patient hat die Möglichkeit, diese zusätzliche Zugriffskontrolle nur für Notfallzugriffe zu aktivieren.	R6	8.2.3	K/M
E6	Kein Caching von sensiblen und geheimen Daten	Im EPD abgelegte Daten der Klassifizierungsstufen „geheim“ und „sensibel“ werden nicht ausserhalb der Document Repositories persistent gespeichert. *Hinweis*: Dies gilt insbesondere auch für geheime und sensible Daten, die aus einer anderen (Stamm-)Gemeinschaft bezogen werden.	R14	8.2.3	K/M
E7	Kein Download sensibler Daten	Beim Lesen von Daten der Klassifizierungsstufe „sensibel“ wird das Erstellen einer dezentralen Kopie technisch möglichst verhindert, indem: • Das interne Portal für diese Daten keine Download-Möglichkeit anbietet; • Sensible Daten über einen eHealth-Connector nicht gelesen werden können. ***Wichtiger Hinweis***: Weil gemäss heutiger Praxis die Gesundheitsfachpersonen in der Lage sein müssen, eine lokale Kopie der eingesehenen Daten zu erstellen, ist die Umsetzung dieser Massnahme zum heutigen Zeitpunkt nicht möglich.	R27 R28	8.2.3	G/G
E8	Besondere Sorgfaltspflichten bei PEP	Bei politisch exponierten Personen (PEP) gelten besondere Sorgfaltspflichten in Bezug auf die Eröffnung eines Patientendossiers. Für die Definition von PEP kann beispielsweise auf die Geldwäschereiverordnung der FINMA abgestützt werden. Als PEP werden dort Personen bezeichnet • mit prominenten öffentlichen Funktionen im Ausland (wie „Staats- und Regierungschefinnen und -chefs, hohe Politikerinnen und Politiker auf nationaler Ebene, hohe Funktionärinnen und Funktionäre in Verwaltung, Justiz, Militär und Parteien auf nationaler Ebene, die obersten Organe staatlicher Unternehmen von nationaler Bedeutung“) sowie • „Unternehmen und Personen, die den genannten Personen aus familiären, persönlichen oder geschäftlichen Gründen erkennbar nahe stehen“. *Quelle*: „Sorgfaltspflichten der Schweizer Banken im Umgang mit Vermögenswerten von „politisch exponierten Personen“„ (FINMA Kurzbericht, 11.3.2011, Kapitel 2.3)	R5 R6 R17 R28	7.2.2	K/M

Ref	Erweiterte Massnahme	Beschreibung	Risi-ken	ISO	A/N
E9	„PEP Flag“	Politisch exponierten Personen (PEP) werden im MPI als solche gekennzeichnet, damit (Stamm-)Gemeinschaften bei Bedarf spezifische Sicherheitsmassnahmen (z.B. bei der Rechteverwaltung, Rechteüberprüfung oder Zugriffsüberwachung im SIEM) zur Anwendung bringen können.	tbd	8.2.2	K/M

4.6 Massnahmenübersicht

Auf der nachfolgenden Seite wird aufgezeigt welche ISO 27001 Controls (resp. ISO 27002 Control Objectives) mit den in den Kapitel 4.1 bis 4.4 aufgeführten Massnahmen (ohne erweiterte Massnahmen in Kapitel 4.5) adressiert werden.


ISO 27002 Control Objectives
IS Pol.
Organization of InfoSec
HR Security
Asset Management
Access Control
Crypt.
Physical and environmental Security
Operations Security
Communications Security
System acquisition, development and maintenance
Supplier Relationships
InfoSec Incident Mgmt
IS aspects of BCM
Compliance
Organisatorische Sicherheitsmanssnahmen
O1
O2
O3
O4
O5
O6
O7
Applikatorische Sicherheitsmanssnahmen
A1
A2
A3
A4
A5
A6
A7
A8
A9
A10
A11
A12
A13
Technische Sicherheitsmassnahmen
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
T12
T13
T14
Sicherheitsmassnahmen für zentrale Dienste
Z1
Z2
Z3
Z4
Z5

4.7 Restrisiken nach Massnahmenumsetzung

Auch nach Umsetzung aller beschriebenen Massnahmen verbleiben Restrisiken, die mit vertretbarem Aufwand nicht weiter reduziert werden können und deshalb getragen werden müssen. Diese Restrisiken sind nachfolgend zusammenfassend beschrieben:

Unsichere Endgeräte von Patienten und Gesundheitsfachpersonen (Risiken R27, R28):

- Die Erfahrung der letzten Jahre zeigt, dass privat genutzte Endgeräte nur unzureichend gegen Schadsoftware geschützt werden können. Es muss deshalb davon ausgegangen werden, dass unberechtigte Dritte durch Fernsteuerung von Endgeräten von Patienten in den Besitz von Patientendossiers gelangen werden. Weil typische Phishing-Attacken ungezielt erfolgen, ist die durchschnittliche Tragweite solcher Attacken allerdings relativ gering.
- Die Endgeräte von Gesundheitsfachpersonen werden professioneller betrieben und sind insgesamt besser geschützt, wobei allerdings eine sehr grosse Bandbreite anzunehmen ist. Die reduzierte Eintrittswahrscheinlichkeit eines Schadenfalls wird allerdings kompensiert durch die deutlich grössere Tragweite des Schadens, wenn ein Dritter unberechtigte Einsicht in alle für eine GFP sichtbaren Patientendossiers erhält.

Nachlässige Rechtevergabe durch Patienten und (Stamm-)Gemeinschaften (Risiken R6, R8):

- Die vom Patienten teilweise selber vorzunehmende Berechtigungsverwaltung erfordert ein Sicherheitsbewusstsein und eine Sorgfalt, die heute nicht in der gesamten Bevölkerung gegeben ist. Dies wird in einzelnen Fällen zu Fehlern führen, deren Tragweite aber auf ein einzelnes Patientendossier begrenzt bleibt.
- Die langjährige Erfahrung mit dem Identity and Access Management in grösseren und kleineren Betrieben zeigt, dass bei personellen Mutationen eine vollständig fehlerfreie zeitnahe Administration von Organisationszugehörigkeiten nie vollständig gelingen kann. In Verbindung mit den auf Organisationseinheiten abstützenden Gruppenberechtigungen wird dies ebenfalls zu Fehlern bei der Zugriffssteuerung führen, deren potentielle Tragweite allerdings erheblich ist.

Datendiebstahl durch Insider oder Hacker (Risiken R11, R12, R14):

- Es ist nicht praktikabel, alle in den Repositories gespeicherten Daten so zu verschlüsseln, dass sie nur über die gesicherten IHE-Services gelesen werden können. Systemadministratoren oder unberechtigte Dritte, die sich Systemadministrationsrechte verschaffen, können deshalb unter Umgehung der applikatorischen Rechteverwaltung auf Daten in potentiell grosser Menge zugreifen und diese an interessierte Dritte weitergeben.
- Ein Datendiebstahl auf diesem Weg wäre von potentiell sehr grosser Tragweite, weshalb die Eintretenswahrscheinlichkeit eines solchen Ereignisses auf ein absolutes Minimum begrenzt werden muss.

Erfolgreiche Angriffe aus dem Internet auf ein internes Portal (Risiko R16):

- Der sichere Betrieb einer Internet-Webapplikation stellt sehr hohe Ansprüche an die technische und prozedurale Kompetenz des Betreibers. Der Betrieb von Internet Banking Lösungen hat über die letzten bald 20 Jahre eine Lernkurve durchlaufen, die voraussichtlich nicht von allen Betreibern interner EPD-Portale zeitgerecht aufgeholt werden kann.
- Angesichts der grossen Visibilität und politischen Exponiertheit des elektronischen Patientenportals ist davon auszugehen, dass sich erfolgreiche Angriffe aus dem Internet nicht vollständig verhindern lassen und zu tatsächlichen oder vermeintlichen Schadenfällen führen werden, auf die mit der erforderlichen Geschwindigkeit und Sorgfalt reagiert werden muss.

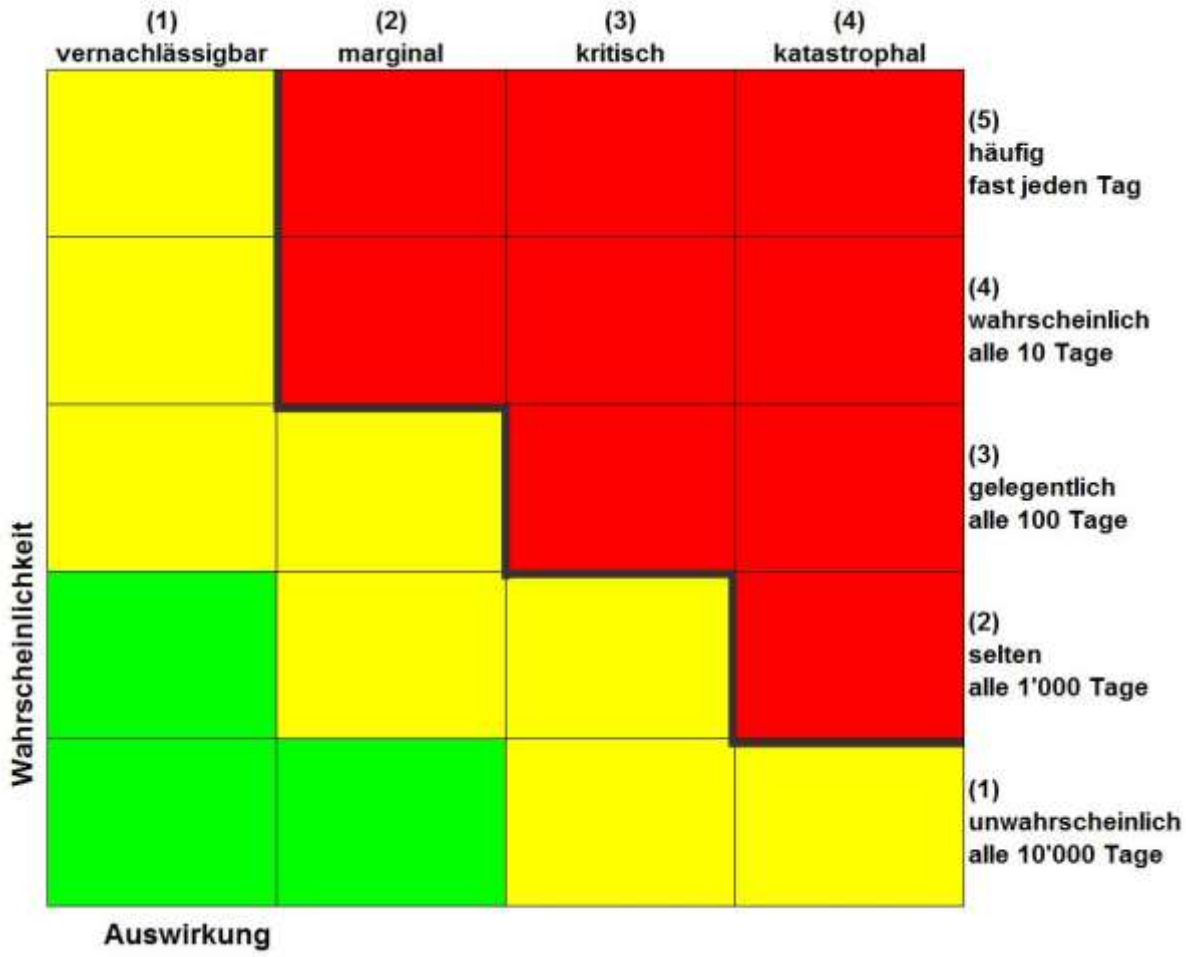
Anhang A: Grundlagen der Risikoeinschätzung

Die vorliegenden Grundlagen

- Risikomatrix
- Einstufung der Eintretenswahrscheinlichkeit
- Einstufung des Schadensausmasses

basieren auf dem [Template ISDS Konzept], V.2.0 vom 1. März 2015

Risikomatrix



Einstufung der Eintretenswahrscheinlichkeit

Stufe	Bemerkung	Beschreibung
1	**Unwahrscheinlich**	• Möglich aber eher unwahrscheinlich • Tritt sehr unwahrscheinlich im Lebenslauf eines Objektes ein • Mehr als alle 10 000 Tage (> 27 Jahre)
2	**Selten**	• Tritt selten ein, aber man muss mit Eintritt rechnen • Unwahrscheinlich aber gut möglich im Lebenslauf eines Objektes • Alle 1000 bis 10 000 Tage (3 - 27 Jahre)
3	**Möglich**	• Tritt gelegentlich ein • Geschieht mehrmals im Lebenslauf eines Objekt • Alle 100 bis 1000 Tage (1/4 - 3 Jahre)
4	**Wahrscheinlich**	• Kommt oft vor • Geschieht manchmal im Lebenslauf eines Objekts • Alle 10 bis 100 Tage
5	**sehr wahrscheinlich**	• Kommt laufend vor • Geschieht oft im Lebenslauf eines Objekts • Häufiger als alle 10 Tage

Einstufung des Schadensausmasses

Stufe	Auswirkung	Beurteilungskriterien
1	**Vernachlässigbar**	• Finanzieller Schaden kleiner als 10'000 CHF • Die Einhaltung gesetzlicher und vertraglicher Pflichten ist nicht gefährdet • Die Aufgabenerfüllung wird höchstens geringfügig beeinträchtigt • Persönlichkeitsrechte sind nicht gefährdet • Umweltschäden sind minimal • Unfälle oder Krankheiten ohne Arbeitsabwesenheiten • Kein Imageschaden für die BVerw
2	**Marginal**	• Finanzieller Schaden zwischen 10'000 und 200'000 CHF • Die Einhaltung gesetzlicher und vertraglicher Pflichten ist gefährdet oder die Erfüllung wesentlicher Aufgaben ist beeinträchtigt. • Persönlichkeitsrechte sind gefährdet • Umweltschäden, welche wieder gut gemacht werden können Unfälle oder Krankheiten mit mehreren verlorenen Arbeitstagen aber ohne bleibende Schäden sind möglich • Imageschaden für die BVerw ist klein und von kurzer Dauer (kein Fernsehen und höchstens Kurzmeldung in der Presse)
3	**Kritisch**	• Finanzieller Schaden zwischen 200'000 und 1‘000'000 CHF • Die Einhaltung gesetzlicher und vertraglicher Pflichten stark eingeschränkt oder die Erfüllung wesentlicher Aufgaben verunmöglicht • Persönlichkeitsrechte sind in hohem Masse gefährdet • Umweltschäden, welche wieder gut gemacht werden können • Unfälle oder Krankheiten mit Hospitalisierung und bleibenden Schäden (Teil-Invalidität) • Grösserer Imageschaden für die BVerw (Artikel in Presse, aber nicht Seite 1 - kein Fernsehen)
4	**Katastrophal**	• Finanzieller Schaden > 1'000'000 CHF • Einhaltung gesetzlicher und vertraglicher Pflichten bzw. die Erfüllung wesentlicher Aufgaben verunmöglicht • Verletzung der Persönlichkeitsrechte • Leib und Leben sind gefährdet • Umweltschäden entstehen • Grosser Imageschaden für BVerw (Seite 1-Meldung in Presse und Fernsehen)

Anhang B: Fachbegriffe der Informationssicherheit

Fachbegriff	Beschreibung [1)]
Denial-of-Service Attacke (DoS)	DoS Attacke ist der Oberbegriff für Angriffe auf die Verfügbarkeit von Netzwerkdiensten, meist Internet-Dienste, wie z.B. Web- oder DNS-Server. Die häufigsten DoS-Attacken sind: a) E-Mail-Bombing; Versenden einer grossen Anzahl von E-Mails an einen Empfänger. Ziele der Attacke sind der Empfänger, durch sehr lange Wartezeiten, bzw. Absturz seines Systems und der E-Mail-Server, durch erhöhte Last, bzw. Absturz des E-Mail-Systems). b) E-Mail-List Bombing; das Abonnieren zahlreicher Mailinglisten auf eine fremde E-Mail-Adresse. c) Distributed DoS (DDoS); DoS-Attacke, die von vielen Systemen synchronisiert durchgeführt wird. In der Regel werden schlecht geschützte Systeme mit direkter Internet-Verbindung und grosser Bandbreite für solche Attacken genutzt. Kleine Programme, so genannte Agents, werden auf diesen Systemen implementiert und von zentraler Stelle über so genannte Handler koordiniert.
Hacker	Person, welche sich unberechtigt Zugang zu Systemen beschafft. Früher wurde unter dem Begriff Hacker ein Tüftler verstanden, welcher aus Neugierde an der Technik Schwachstellen sucht um in IT Systeme einzudringen. Heute wird unter Hacker eher ein böswilliger Angreifer verstanden, welcher durch seinen Aktivitäten einen persönlichen Nutzen erzielen will indem er z.B. eine Web-Seite mit ihm genehmen Inhalt ersetzt oder Daten stiehlt, welche er verkaufen oder anderweitig einsetzen kann.
Malware	Malware (= bösartige Software) ist der Überbegriff für Schadprogramme, welche vom Benutzer unbemerkt im Hintergrund laufen und Daten abgreifen oder manipulieren sowie weitere für Kriminelle wertvolle Funktionen ausführen. Zu Malware gehören insbesondere Viren, Würmer und Trojaner.
Phishing	Unter Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.
Social Engineering	Social Engineering ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Um an vertrauliche Informationen zu gelangen, wird sehr oft die Gutgläubigkeit und die Hilfsbereitschaft aber auch die Unsicherheit einer Person ausgenutzt. Von fingierten Telefonanrufen, über Personen die sich als jemand anderes ausgeben, bis hin zu Phishing-Attacken, ist alles möglich.
Trojanisches Pferd	Als Trojanisches Pferd, im EDV-Jargon auch kurz „Trojaner“ genannt, bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. Ein Trojanisches Pferd zählt zur Familie unerwünschter bzw. schädlicher Programme, der so genannten Malware.

[1)] Teilweise von https://www.swiss-isa.ch/de/glossar

Anhang C: Abkürzungen

Begriff / Abkürzung	Bedeutung
CPI	Community / Portal Index, Verzeichnis der (Stamm-)Gemeinschaften und externe Zugangsportale
DSG	Eidgenössisches Datenschutzgesetz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EPD	Elektronisches Patientendossier
GFP	Gesundheitsfachperson
GLN	Global Location Number
HOI-S	Healthcare Organization Index, Verzeichnis der Gesundheitsorganisationen
HPC	Health Professional Card
HPD	Healthcare Provider Directory
HPI-S	Healthcare Professional Index, Verzeichnis der Behandelnden
IAM	Identity and Access Management, Identitäts- und Berechtigungsverwaltung
IdP	Identity Provider
ISBO	Informationssicherheitsbeauftragter einer Organisation
ISDSV	Informationssicherheits- und Datenschutzverantwortlicher im Rahmen des Projekts, gemäss HERMES
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
MDI	Metadaten-Index, Verzeichnis der Dokumenten Metadaten
OID	Objekt Identifikatoren
PAM	Privileged Access Management, Verwaltung privilegierter Zugriffsrechte von Systembetreuern
RADB	Rechteattribute Datenbank
RAS	Remote Access, Fernzugriff
RI	Rollen-Index, Verzeichnis der Rollen
UPI	Unique Person Identification
VDSG	Verordnung zum Datenschutzgesetz
VK	Versichertenkarte
ZAS	Zentrale Ausgleichsstelle
ZP	Zugangspunkt