Datenschutz- und Datensicherheitsrichtlinie (DSDS-Richtlinie) der XAD-SG

Version / Datum	Freigegeben durch
V1.32 / 25.02.2020	GL-axsana

XAD-Stammgemeinschaft

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Zielsetzung

Die DSDS-Richtlinie basiert auf der DSDS-Policy der XAD-Stammgemeinschaft (XAD-SG) und definiert Mindestanforderungen an den Datenschutz und die Datensicherheit, um ein gutes Sicherheitsniveau der Daten aufzubauen und aufrechtzuerhalten, die Gesetzeskonformität sicherzustellen (s. 1.8 Mitgeltende Dokumente) sowie die DSDS-Policy zu implementieren.

Die Mindestanforderungen leiten sich einerseits aus der Verordnung über das elektronischen Patientendossier (EPDV) und den Anhang 2 der Verordnung des Eidgenössischen Departements des Innern über das elektronische Patientendossier (EPDV-EDI) zu den technischen und organisatorischen Zertifizierungsvoraussetzungen (TOZ) ab und orientieren sich an der internationalen Informationssicherheitsnorm ISO/IEC 27000x.

Die Ableitung ist folgendermassen zu verstehen: die DSDS-Richtlinie konkretisiert die TOZ, sofern dafür eine Notwendigkeit besteht. Sie hat nicht zum Ziel, bestehende Vorgaben aus den TOZ ohne weitere Konkretisierung erneut aufzuführen. Daraus folgt, dass zur Erreichung der Gesetzeskonformität betreffend Datenschutz und die Datensicherheit sämtliche relevanten Gesetze und Verordnungen zu berücksichtigen sind (s. 1.8 Mitgeltende Dokumente).

1.2 Geltungsbereich

Der Geltungsbereich wird nachfolgend aus organisatorischer und technischer Perspektive festgelegt. Das Kriterium, ob ein System, eine Organisation oder deren Prozesse zum Geltungsbereich zählen, ist die Bearbeitung von EPD-Daten gemäss Art. 3 DSG durch die Organisation oder ein System.

1.2.1 Organisatorischer Geltungsbereich

Der Geltungsbereich der DSDS-Richtlinie umfasst die XAD-SG, das heisst, die Zentralen Dienste und die ihr angeschlossenen Gesundheitseinrichtungen sowie Lieferanten, Dienstleister oder Partner, die unter Dritte zusammengefasst (EPD-Beteiligte) werden.

XAD-SG	Dritte
Zentrale Dienste	Technik Provider
Angeschlossene Gesundheitseinrichtungen, deren Tochter- und Beteiligungsgesellschaften	Identity Provider
	weitere Lieferanten, Dienstleister oder Partner

Tabelle 1: Geltungsbereich DSDS-Richtlinie

Der Geltungsbereich der DSDS-Richtlinie sowie der gesetzlichen Bestimmungen der Verordnung zum elektronischen Patientendossier des Bundes (EPDV) und des Eidgenössischen Departement des Innern (EPDV-EDI) einschliesslich dessen Anhang 2 betreffend die technischen- und organisatorischen Zertifizierungsvoraussetzungen (TOZ) erstreckt sich

- auf alle EPD-Beteiligte der Tabelle 1: Geltungsbereich DSDS-Richtlinie die EPD-Daten bearbeiten (im Sinne des Art. 3 DSG) und somit auf diese zugreifen können und
- auf sämtliche Prozesse, bei denen EPD-Daten bearbeitet (im Sinne des Art. 3 DSG) oder im Zusammenhang mit dem EPD stehen.

1.2.2 Geltungsbereich technisch

Der Geltungsbereich der DSDS-Richtlinie umfasst technisch

- die gesamten nach EPDV definierten EPD-Systemen, welche EPD-Daten bearbeiten (im Sinne des Art. 3 DSG) oder mit denen auf EPD-Daten zugegriffen werden kann,
- die Schnittstellen zu Primärsystemen der Gesundheitseinrichtungen, bei denen EPD-Daten übertragen werden und
- weiter unterstützende Systeme, über die EPD-Daten bearbeitet (im Sinne des Art. 3 DSG) werden oder mit denen die Berechtigungsregeln der GFPs und HPs verändert werden können.

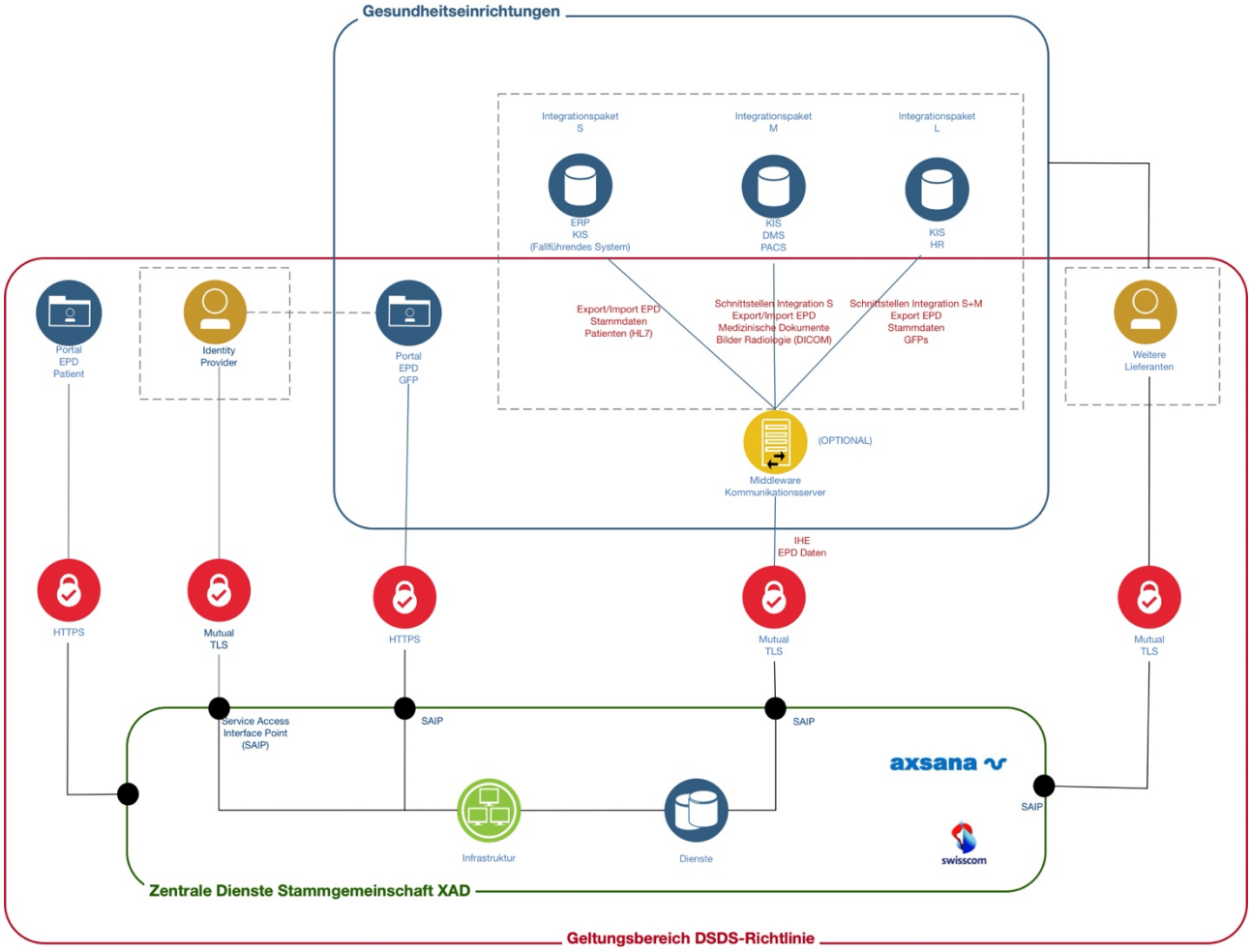

Abbildung 1: Geltungsbereich DSDS-Richtlinie der XAD-SG

1.3 Integrationspakete

Im Zusammenhang mit dem elektronischen Patientendossier werden die Integrationspakete vom webbasierten Zugangsportal für Gesundheitsfachpersonen unterschieden. Die Integrationslösungen haben eine in das Krankenhausinformationssystem oder Patienteninformationssystem integrierte Schnittstelle zum elektronischen Patientendossier. Es werden drei Integrationspakete S, M und L unterschieden, die sich in Bezug auf die Tiefe der Integration unterscheiden.

Anbindungslösung	Beschreibung
Portal (A-Portal)	Der Anschluss via Portal (Standard) ermöglicht der Stammgemeinschaft den Zugang zum EPD. Der Zugang erfolgt über das Gesundheitsfachpersonenportal. Die Gesundheitseinrichtung kann sich auf der EPD-Plattform registrieren sowie die initiale Freischaltung von Gesundheitsfachpersonen (GFP), Hilfspersonen (HIP) und Gruppen durch die zentralen Dienste beauftragen. Der Login erfolgt mit dem Identifikationsmittel eines nach EPDG zertifizierten Herausgebers.
Integrationspaket S	Der Anschluss «Integriert S» ermöglicht der Stammgemeinschaft den Zugang zum EPD, der über das Gesundheitsfachpersonenportal erfolgt. Es können die folgenden Funktionen über das Primärsystem der Gesundheitseinrichtung ausgeführt werden: ▪ Verwaltung von Patientendaten Der Login erfolgt mit dem Identifikationsmittel eines nach EPDG zertifizierten Herausgebers.
Integrationspaket M	Der Anschluss «Integriert M» ermöglicht der Stammgemeinschaft den Zugang zum EPD, der über das Gesundheitsfachpersonenportal erfolgt. Es können die folgenden Funktionen über das Primärsystem der Gesundheitseinrichtung ausgeführt werden: ▪ Verwaltung von Patientendaten ▪ Abruf und die Übermittelung von Dokumenten aus dem Primärsystem der Gesundheitseinrichtung Der Login erfolgt mit dem Identifikationsmittel eines nach EPDG zertifizierten Herausgebers.
Integrationspaket L	Der Anschluss «Integriert L» ermöglicht der Stammgemeinschaft den Zugang zum EPD, der über das Gesundheitsfachpersonenportal erfolgt. Es können die folgenden Funktionen über das Primärsystem der Gesundheitseinrichtung ausgeführt werden: ▪ Verwaltung von Patientendaten ▪ Abruf und die Übermittelung von Dokumenten aus dem Primärsystem der Gesundheitseinrichtung ▪ Verwaltung von Gesundheitsfachpersonen, Hilfspersonen und Gruppen Der Login erfolgt mit dem Identifikationsmittel eines nach EPDG zertifizierten Herausgebers.

Tabelle 2: Integrationspakete

1.4 DSDS relevante Übersicht für Gesundheitseinrichtungen

Nachfolgend eine Übersicht mit allen Kapiteln, welche relevant sind für Gesundheitseinrichtungen.

DSDS-Richtlinie Kapitel	Relevante Unterpunkte
Einleitung	Alles
Organisation	2.2 Datenschutz- und Datensicherheitsverantwortung GE
	2.4 Sicherheitsprozesse
	2.5 Vorgehen bei Verstössen
Daten des elektronischen Patientendossiers	3.1 Definition behandlungsrelevante Daten
	3.2 Verschlüsselung
	3.5 Protokolldaten und Protokollierung
	3.6 Umgang mit Testdaten
	3.7 Gruppen GFP
Komponenten und Systeme	4.1 Sichere Konfiguration Endgeräte
	4.2 Schutz vor Schadsoftware
	4.3 Authentisierung und Autorisierung
	4.4 Zertifikate
	4.5 Lebenszyklus von Systemen
Netzwerk	Alles
Sensibilisierung	Alles
Berichtwesen und Dokumentation	7.1 Nachweispflicht Gesundheitseinrichtungen
Anhang	8.4 Geltungsbereich

Tabelle 2: Relevante Punkte für GEs

Weitere Einzelheiten sind im Geltungsbereich im Kapitel 8.4 zu finden.

1.5 Abgrenzungen

Das Dokument unterliegt folgenden Abgrenzungen:

- Die Vorgaben der DSDS-Richtlinie beziehen sich gemäss der EPDV-EDI ausschliesslich auf die Informationen und Daten im Kontext des elektronischen Patientendossiers.
- Die Vorgaben der DSDS-Richtlinie beziehen sich gemäss der EPDV-EDI ausschliesslich auf die EPD-Systeme im Kontext des elektronischen Patientendossiers.
- Die Vorgaben der DSDS-Richtlinie beziehen sich gemäss der EPDV-EDI ausschliesslich auf die Prozesse und organisationale Strukturen im Kontext des elektronischen Patientendossiers.
- Sämtliche Informationen, Daten, Informatik- und Kommunikationsmittel, Prozesse und Akteure, welche keine Verbindung zum EPD haben, unterliegen nicht den Vorgaben, Richtwerten und Standards der DSDS-Richtlinie.
- Sämtliche Primärsysteme innerhalb einer Gesundheitseinrichtung (KIS, ERP, PACS, HR, usw.) unterliegen nicht den Vorgaben, Richtwerten und Standards der DSDS-Richtlinie.

- Sämtliche Vorgaben zur physischen Sicherheit der Systeme werden nicht in der DSDS-Richtlinie beschrieben.

1.6 Änderungen

Änderungen an der DSDS-Richtlinie richten sich nach den folgenden Bestimmungen.

- Änderungen an der DSDS-Richtlinie der XAD-SG können durch die Gesamtverantwortung XAD-SG und die Datenschutz- und Datensicherheitsverantwortung XAD-SG (DSDS-V XAD-SG) beantragt werden.
- Änderungsanträge werden durch die DSDS-V XAD-SG (DSDS-V XAD-SG) beurteilt, mit der DSDS-Expertengruppe diskutiert und durch die Gesamtverantwortung XAD-SG abgenommen. Bei positivem Entscheid wird die Änderung in die bestehende Dokumentation eingearbeitet.
- Die DSDS-Richtlinie der XAD-SG wird nach Inkrafttreten und nach jeder Änderung den EPD-Beteiligten gemäss Kapitel 1.2 Geltungsbereich zur Kenntnis gebracht. Das Verfahren richtet sich dabei nach den relevanten Bestimmungen des Anschlussvertrages.

1.7 Kontrolle

Die Kontrolle soll sicherstellen, dass die DSDS-Richtlinie der XAD-SG einerseits stets dem aktuellen Stand der Technik, den geltenden Best-Practice Ansätzen und anderseits den gesetzlichen Grundlagen (s. Kapitel 1.8 Mitgeltende Dokumente) sowie Änderungen an der DSDS-Policy berücksichtigt werden. Dadurch soll ein bestmöglicher Schutz gewährleistet werden. Die Kontrolle der DSDS-Richtlinie richtet sich nach dem folgenden Vorgehen.

- Die DSDS-Richtlinie wird mindestens einmal jährlich durch die DSDS-V XAD-SG auf Zweckmässigkeit und Aktualität überprüft.
- Verbesserungsvorschläge werden der Gesamtverantwortung XAD-SG zur Evaluierung und Genehmigung präsentiert.
- Nach der erfolgten Genehmigung werden sie gemäss dem in Kapitel 1.6 beschriebenen Prozess beantragt.

1.8 Mitgeltende Dokumente

Typ	Name	Beschreibung
Gesetz	Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG)	Das EPDG ist seit dem 15. April 2015 in Kraft und regelt die Rahmenbedingungen für die Einführung und Verbreitung des EPD.
	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)	Das DSG regelt gestützt auf die Artikel 95, 122 und 173 Absatz 2 der Bundesverfassung, die geltenden Anforderungen sowie Rechte und Pflichten von privaten Personen und Bundesorganen im Umgang mit Personendaten.
Verordnung	Verordnung vom 22. März 2017 über das elektronische Patientendossier (EPDV)	Die EPDV regelt, gestützt auf das Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier, die im Rahmen der EPD Anwendung findenden Vertraulichkeitsstufen und Zugriffsrechte, die Patientenidentifikationsnummer, die Aufgaben von Gemeinschaften und Stammgemeinschaften, die einzusetzenden Identifikationsmittel, die Akkreditierung, die Zertifizierung sowie die Abfragedienste.
	Verordnung vom 22. März 2017 des Eidgenössischen Departements des Innern	Die EPDV-EDI regelt die Patientenidentifikationsnummer (Anhang 1), technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (Anhang 2), Metadaten (Anhang 3), Austauschformate (Anhang 4), Integrationsprofile (Anhang 5),

	über das elektronische Patientendossier (EPDV-EDI)	Evaluation und Forschung (Anhang 6), Mindestanforderungen an das Personal sowie technische und organisatorische Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln (Anhang 7 und Anhang 8).
	Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier. Ausgabe 2 / 24. Juni 2019	Der Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier regelt die gesetzlich vorgeschriebenen Anforderungen, welche von Stamm-gemeinschaften und Gemeinschaften erfüllt werden müssen, um sich als Anbieter des EPD für Gesundheitseinrichtungen zu qualifizieren.
Hilfsdokument	Umsetzungshilfe Datenschutz und Datensicherheit im EPD vom 27. Juni 2017	Die gesetzlich vorgeschriebenen Anforderungen sind als die geltenden Minimalanforderungen zu verstehen. Eine detaillierte Hilfestellung zur möglichen Umsetzung dieser Anforderungen sowie zum Aufbau des benötigten Datenschutz- und Datensicherheitsmanagementsystems bietet die «Umsetzungshilfe Datenschutz und Datensicherheit im EPD» von eHealth-Suisse.
Basisdokument	Datenschutz- und Datensicherheits-Policy (DSDS-Policy) der XAD-SG	Die DSDS-Policy bildet das Fundament des Datenschutz- und Datensicherheitsmanagementsystem und gibt den Rahmen sowie die Grundlagen der DSDS-Richtlinie vor.

Tabelle 3: Mitgeltende Dokumente

1.9 Inkrafttreten

Die DSDS-Richtlinie der XAD-SG tritt per 26.09.2019 in Kraft.

2 Organisation

2.1 Datenschutz- und Datensicherheitsverantwortung XAD

Relevante TOZ

4.2.1 Gemeinschaften müssen ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem nach Art der Norm DIN EN ISO/IEC 27001:2017-06 einrichten, aufrechterhalten, regelmässig überprüfen sowie dessen Eignung, Angemessenheit und Wirksamkeit laufend verbessern, so dass:

a) geeignete Massnahmen, insbesondere Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen zur Erfüllung der Anforderungen definiert, die den hier aufgestellten Bestimmungen entsprechen;

b) die allgemeinen und spezifischen Verantwortlichkeiten für das Management von Datenschutz und Datensicherheit auf definierte Funktionen festlegt und den dafür verantwortlichen Personen zuordnet.

4.11.1 Für das Führen des Datenschutz- und Datensicherheitsmanagementsystems der Gemeinschaft ist eine Datenschutz- und Datensicherheitsverantwortliche oder ein Datenschutz- und Datensicherheitsverantwortlicher zu benennen und dessen Aufgabenprofil zu definieren.

4.11.2 Der oder die Datenschutz- und Datensicherheitsverantwortliche muss:

a) die Einhaltung der Datenschutz- und Datensicherheitsvorschriften durch die Gemeinschaft, durch die angeschlossenen Gesundheitseinrichtungen sowie durch Dritte (vgl. Ziff. 4.1) überwachen;

b) seine oder ihre Funktion fachlich unabhängig ausüben können;

c) über die zur Erfüllung seiner oder ihrer Aufgaben erforderlichen fachlichen Kompetenzen und Ressourcen verfügen;

d) die Kommunikation an die verantwortlichen Entscheidungsträger und weitere zu informierende Stellen sicherstellen.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

Vorgaben XAD

2.1.1 Die DSDS-V XAD-SG nimmt folgende Verantwortlichkeiten wahr:

- Führung, Unterhalt und laufende Optimierung des Datenschutz- und Datensicherheitsmanagementsystems (DSDS-MS)
- Überwachung der Einhaltung der Datenschutz- und Datensicherheitsvorschriften
- Erlass von Vorgaben und Umsetzungsempfehlungen

2.1.2 Die Führung, den Unterhalt und die laufende Optimierung des Datenschutz- und Datensicherheitsmanagementsystems umfassen die nachfolgenden Aufgaben:

- die Erarbeitung und Aktualisierung der Sicherheitsvorgaben der XAD-SG
- das Aussprechen der Umsetzungsempfehlungen für alle beteiligten Organisationen im Rahmen des EPD
- die Identifikation, Klassifikation und Beurteilung der Risiken im Umfeld der Schutzobjekte (Informationen, Daten, Anwendungen, Systeme und Prozesse)

- die Beurteilung der Konformität von Vorhaben mit den Sicherheitsvorgaben der XAD-SG
- die Bearbeitung von Sicherheitsvorfällen
- die Sensibilisierung der Mitarbeitenden der Zentralen Dienste zum Thema Datenschutz und Datensicherheit im Kontext des EPD
- die Zusammenarbeit mit den Sicherheitsverantwortlichen von anderen Gemeinschaften, den Gesundheitseinrichtungen sowie beauftragten Dritten
- die Verfügbarkeit für sicherheitsrelevante Fragenstellungen
- die Prüfung der eingereichten Nachweise durch Gesundheitseinrichtungen und beauftragten Dritten
- die Sicherstellung der Kommunikation betreffend Überwachung der Einhaltung der Datenschutz- und Datensicherheitsanforderungen der XAD-SG (Kontrollbericht)
- die jährliche Prüfung des Inventars der Informatikinfrastruktur

2.1.3 Die DSDS-V XAD-SG bringt nachfolgende Kompetenzen mit:

- Technische und betriebswirtschaftliche Grundausbildung
- Erfahrungen im Aufbau und Unterhalt eines Managementsystems
- Kenntnisse des Schweizer Datenschutzgesetzes
- Kenntnisse der ISO/IEC Standardreihe 2700x
- (Empfohlen) IT-Security Zertifizierungen wie CISA, CISSP oder ähnliches

2.2 Datenschutz- und Datensicherheitsverantwortung GE

4.2.1	Gemeinschaften müssen ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem nach Art der Norm DIN EN ISO/IEC 27001:2017-06 einrichten, aufrechterhalten, regelmässig überprüfen sowie dessen Eignung, Angemessenheit und Wirksamkeit laufend verbessern, so dass: a) geeignete Massnahmen, insbesondere Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen zur Erfüllung der Anforderungen definiert, die den hier aufgestellten Bestimmungen entsprechen; b) die allgemeinen und spezifischen Verantwortlichkeiten für das Management von Datenschutz und Datensicherheit auf definierte Funktionen festlegt und den dafür verantwortlichen Personen zuordnet	**Relevante TOZ**

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

2.2.1 Die DSDS-V GE nimmt folgende Verantwortlichkeiten wahr: **Vorgaben XAD**

- Umsetzung der Sicherheitsvorgaben der XAD-SG
- Sicherstellung der Einhaltung von Sicherheitsvorgaben der XAD-SG
- Ansprechpartner für sicherheitsrelevante Themen

2.2.2 Die Umsetzung und Sicherstellung der Einhaltung der Datenschutz- und Datensicherheitsanforderung der Stammgemeinschaft umfassen die nachfolgenden Aufgaben:

- Erarbeitung von Sicherheitsvorgaben und Aussprechen von Umsetzungsempfehlungen für die eigene Gesundheitseinrichtung
- Überwachung der Einhaltung der Datenschutz- und Datensicherheitsvorschriften in der Gesundheitseinrichtung
- Entwicklung und Implementierung von Instandhaltungsplänen für die EPD-relevanten Systeme
- Aktualisierung des Katalogs der Schutzobjekte
- Lieferung der Nachweise zur Kontrolle der Einhaltung der Datenschutz- und Datensicherheitsanforderungen
- Meldung und Meldestelle von/für Risiken, Schwachstellen und Sicherheitsvorfälle/n
- Lieferung der erforderlichen Nachweise zur Kontrolle der Einhaltung der Datenschutz- und Datensicherheitsanforderungen der XAD-SG

2.2.3 Es wird empfohlen, dass die DSDS-V GE nachfolgende fachliche Voraussetzungen mit sich bringt:

- Technische und betriebswirtschaftliche Grundausbildung
- Erfahrung im Aufbau und Unterhalt eines Managementsystems
- Kenntnisse des Schweizer Datenschutzgesetztes
- Kenntnisse der ISO/IEC Standardreihe 2700x

2.2.4 Die Datenschutz- und Datensicherheitsverantwortung GE fungiert als Ansprechpartner für die DSDS-V XAD-SG.

2.3 Datenschutz- und Datensicherheitsverantwortung von Lieferanten und Dienstleistungserbringern

Relevante TOZ

4.9.1 Gemeinschaften müssen eine von dem oder der Datenschutz- und Datensicherheitsverantwortlichen visierte Liste mit allen Lieferanten und Dienstleistungserbringern («Dritte») führen, die unter Umständen auf Daten des elektronischen Patientendossiers zugreifen, sie verarbeiten, speichern, weitergeben oder Informatikinfrastrukturkomponenten dafür bereitstellen.

4.9.2 Mit Dritten müssen alle relevanten Datenschutz- und Datensicherheitsanforderungen formal festgelegt und in Liefervereinbarungen vereinbart werden.

4.9.3 Die Liefervereinbarungen müssen unmissverständlich die Verpflichtungen und Verantwortlichkeiten zur Erfüllung der relevanten Anforderungen an den Datenschutz und die Datensicherheit festhalten.

4.9.4 Sie müssen mindestens folgende Bestimmungen umfassen:

a) Verpflichtungen des Lieferanten, die relevanten Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft beim Einsatz oder der Bereitstellung von Informatikmitteln, Personal oder Dienstleistungen jederzeit einzuhalten;

b) Anforderungen und Verfahren für den Umgang mit Datenschutz- und Datensicherheitsvorfällen;

c) die Angabe von Kontaktpersonen für Fragen und bei Vorkommnissen im Bereich Datenschutz- und Datensicherheit;

d) das Recht zur regelmässigen Überprüfung der Lieferantenprozesse und Kontrollmassnahmen im Zusammenhang mit dem Vertrag;

e) die Verpflichtung zur Einhaltung der Datenschutz- und Datensicherheitsanforderungen der Gemeinschaft innerhalb der gesamten Lieferkette sowie Beauftragung zur Weiterverpflichtung der Unterlieferanten (sofern vorhanden);

f) die Vorschriften und Kontrollmassnahmen für Unterverträge;

g) die Verpflichtung, die Gemeinschaft über jede Änderung in den Vertragsbeziehungen zu involvierten Unterlieferanten zu informieren.

2.4 b Gemeinschaften müssen sicherstellen, dass:

b) die medizinischen Daten des elektronischen Patientendossiers in den Dokumentenablagen so getrennt von anderen Datenbeständen gespeichert werden, dass sie gegen unzulässige Verwendung geschützt sind.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

Vorgaben XAD

2.3.1 Dritte (Lieferanten und Leistungserbringer, Technik Provider, Identity Provider) haben eine Datenschutz- und Datensicherheitsverantwortlichen zu bestimmen.

2.3.2 Die Datenschutz- und Datensicherheitsverantwortung oder eine definierte Ansprechpartnerstelle nimmt folgende Verantwortlichkeiten war:

- Umsetzung und Einhaltung der Datenschutz- und Datensicherheitsanforderungen der XAD-SG
- Aktualisierung des Katalogs der Schutzobjekte
- Meldung und Meldestelle von/für Risiken, Schwachstellen und Sicherheitsvorfälle/n
- Lieferung der erforderlichen Nachweise zur Kontrolle der Einhaltung der Datenschutz- und Datensicherheitsanforderungen der XAD-SG
- Lieferung der Nachweise zur Kontrolle der Einhaltung der Datenschutz- und Datensicherheitsanforderungen
- Lieferung eines Konzepts für die Regelung von Dokumentenablage für EPD-Daten. Das Dokument soll klar definierte Vorgaben über die Trennung von EPD-Daten mit anderen Datenbeständen vorweisen, um eine unzulässige Nutzung zu vermeiden.

2.3.3 Die Datenschutz- und Datensicherheitsverantwortung von Dritten oder eine definierte Ansprechpartnerstelle ist Ansprechpartner für den DSDS-V XAD-SG.

2.4 Sicherheitsprozesse

4.2.1	Gemeinschaften müssen ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem nach Art der Norm DIN EN ISO/IEC 27001:2017-06 einrichten, aufrechterhalten, regelmässig überprüfen sowie dessen Eignung, Angemessenheit und Wirksamkeit laufend verbessern, so dass: a) geeignete Massnahmen, insbesondere Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen zur Erfüllung der Anforderungen definiert, die den hier aufgestellten Bestimmungen entsprechen; b) die allgemeinen und spezifischen Verantwortlichkeiten für das Management von Datenschutz und Datensicherheit auf definierte Funktionen festlegt und den dafür verantwortlichen Personen zuordnet; c) alle relevanten Aufzeichnungen im Einklang mit den gesetzlichen Anforderungen vor Verlust, Zerstörung und Fälschung schützt.	**Relevante TOZ**
4.3.3	Gemeinschaften müssen zu den unter Ziffer 4.3.1 beschriebenen Massnahmen: a) Verfahren vorsehen für das unverzügliche Melden von Datenschutz- und Datensicherheitsereignissen an die vorgegebenen Stellen der Gemeinschaft und an das BAG (Art. 12 Abs. 3 EPDV); b) Prozesse vorsehen zur raschen Reaktion auf Ereignisse und zur Behandlung von Ursachen, die den Datenschutz oder die Datensicherheit gefährden; c) für sicherheitskritische Ereignisse einer definierten Stufe geeignete Notfallprozesse zur Eindämmung von Schadwirkungen vorsehen, insbesondere wie und unter welchen Bedingungen sicherheitskritische Systeme der Gemeinschaft von gefährdenden Zugriffen von aussen oder innen zu isolieren sind.	

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

2.4 a	Die DSDS-V XAD-SG definiert die Sicherheitsprozesse und geben diese an die Gesundheitseinrichtungen und beauftragten Dritten bekannt.	**Vorgaben XAD**

2.4.1 Sicherheitsvorfällen, Schwachstellen und Risiken

2.4.1.1	Die DSDS-V XAD-SG stellt eine Checkliste, mit möglichen Sicherheitsvorfällen, welche das EPD tangieren, zur Verfügung.	**Vorgaben XAD**
2.4.1.2	Die Mitarbeitenden der GE, der Zentralen Dienste und von Dritten sollen hinsichtlich der Erkennung und den Prozessen zur Meldung von Sicherheitsvorfällen, Schwachstellen und Risiken regelmässig sensibilisiert und geschult werden. Damit soll jeder Mitarbeitende innerhalb der GE eine Meldung eines Sicherheitsvorfalls bei der DSDS-V GE deponieren können.	
2.4.1.3	Die DSDS-V XAD-SG soll die Rolle der Meldestelle innerhalb der Zentralen Dienste für Sicherheitsvorfälle übernehmen. Somit müssen Incident Handling und Definition der Kommunikationspfade seitens DSDS-V XAD-SG geregelt werden.	

2.4.1.4 Die DSDS-V GE muss Sicherheitsvorfälle der Meldestelle der Zentralen Dienste melden. Ein Sicherheitsvorfall kann sich in den folgenden Bereichen einer Gemeinschaft ereignen:

- Physische Sicherheit
- Vorhandene ICT-Umgebung
- Benutzer und Anspruchsgruppen
- Applikationen und Systeme

Für alle vorgenannten Bereiche müssen demnach Vorkehrungen und Massnahmen zur Erkennung und Behandlung von Sicherheitsvorfällen definiert und umgesetzt werden.

Dabei müssen mindestens folgende Szenarien berücksichtigt werden:

- Phishing
- Kritische Schwachstellen in Hard- oder Software
- DDoS-Angriff auf ein Zugangsportal
- Schadsoftware (z.B. Ransomware)
- Unerlaubte Dateneinsicht
- Datenabfluss
- Kompromittierter kryptografischer Schlüssel
- Individuelles Fehlverhalten von Zugriffsberechtigten

2.4.1.5 Wurde ein Sicherheitsvorfall, bei welchem EPD-Daten (Dokument) an eine falsche Person zugeordnet wurde, innerhalb einer GE festgestellt, muss die DSDS-V GE die DSDS-V XAD-SG und die betroffenen Patienten umgehend, jedoch spätestens innerhalb der nächsten 24 Stunden gemäss Prozess der XAD-SG, informieren.

2.4.1.6 Wurde ein Sicherheitsvorfall, bei welchem EPD-Daten betroffen sind, innerhalb der Zentralen Dienste oder durch Dritte der XAD-SG festgestellt, muss die DSDS-V XAD-SG die betroffene GE und die betroffenen Patienten umgehend, jedoch spätestens innerhalb der nächsten 24 Stunden, informieren.

2.4.1.7 Wurde ein Sicherheitsvorfall seitens DSDS-V XAD-SG festgestellt, muss sie das BAG innerhalb der nächsten 72 Stunden informieren, sofern die Meldepflicht gemäss der Checkliste Sicherheitsvorfälle gegeben ist.

2.4.1.8 Wurde ein Sicherheitsvorfall seitens DSDS-V XAD-SG (Datenschutzverletzung) festgestellt, ist das EDÖB innerhalb der nächsten 72 Stunden zu informieren, sofern die Meldepflicht gemäss der Checkliste Sicherheitsvorfälle gegeben ist.

2.4.1.9 Wurde ein Sicherheitsvorfall beim Technik Provider, Identity Provider oder weiteren Lieferanten, Dienstleister und Partner festgestellt, ist die DSDS-V XAD-SG umgehend zu informieren.

2.4.1.10 Schwachstellen, die einen CVSS Score von 8.5 oder höher haben, sind innert drei Arbeitstagen zu melden und zu beheben.

2.4.2 Notfallprozess

2.4.2.1 Folgende Kriterien können den Notfallprozess auslösen: **Vorgaben XAD**

- Ein Sicherheitsvorfall, bei dem mindestens 10% der Patientendaten betroffen sind

- Ein Sicherheitsvorfall mit einem hohen Impact auf Patientendaten (Bspw. Datenmanipulation möglich)
- Performance einer Plattform, so dass diese nicht mehr funktionsfähig ist

2.4.2.2 Die Gesamtverantwortung XAD-SG entscheidet über die Auslösung des Notfallprozesses.

2.4.2.3 Die Gesamtverantwortung XAD-SG entscheidet über im Rahmen des Notfallprozesses über die Ausserbetriebnahme der EPD-Plattform.

2.5 Vorgehen bei Verstössen

Die Vorgehensweise sowie Konsequenzen bei Verstössen gegen die nachfolgenden Richtlinien bezüglich des Datenschutzes und der Datensicherheit durch die Gesundheitseinrichtungen sind im Nutzungsvertrag festgehalten.

Im Fall eines Verstosses wird die DSDS-V XAD-SG das Thema eskalieren. Entscheidungen über die Konsequenzen und das weitere Vorgehen werden durch die Gesamtverantwortung XAD-SG getroffen.

3 Daten des elektronischen Patientendossiers

3.1 Definition behandlungsrelevante Daten

2.4	Gemeinschaften müssen sicherstellen, dass: a) die angeschlossenen Gesundheitseinrichtungen über Regelungen verfügen, wonach nur behandlungsrelevante Daten aus der Krankengeschichte der Patientin oder des Patienten im elektronischen Patientendossier bereitgestellt werden; b) die medizinischen Daten des elektronischen Patientendossiers in den Dokumentenablagen so getrennt von anderen Datenbeständen gespeichert werden, dass sie gegen unzulässige Verwendung geschützt sind;	**Relevante TOZ**

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.1.1 Die Gesundheitseinrichtungen verfügen über eine schriftliche Definition der behandlungsrelevanten Daten (Nachweis N01 – Definition behandlungsrelevante Daten) und verfügen über organisatorische oder technische Kontrollen, die sicherstellen, dass nur Daten, die der Definition entsprechen, in das EPD hochgeladen werden. **Vorgaben XAD**

Behandlungsrelevanten Daten dürfen folgende Inhalte nicht beinhalten:

- Administrativen Daten (Rechnungen, Mahnungen, usw.)
- Aufgebote
- Leistungsdaten und Kodierungsdaten (Abrechnung)

3.1.2 Alle EPD-Daten sind isoliert von sonstigen Datenbeständen aufzubewahren. Mindestens einer der folgenden Datentrennungsverfahren ist zu verwenden:

- Physische Datentrennung

- Logische Datentrennung
- Kryptografische Trennung

3.2 Verschlüsselung

2.5	Gemeinschaften müssen sicherstellen, dass Daten des elektronischen Patientendossiers mit geeigneten und dem aktuellen Stand der Technik entsprechenden kryptografischen Massnahmen und unter Berücksichtigung der Vorgaben von Ziffer 4.12: a) bei jeglicher Übertragung gegen Verlust der Vertraulichkeit, Authentizität und Integrität abgesichert werden; b) verschlüsselt gespeichert werden und gegen unzulässige oder unbemerkte Veränderungen geschützt werden.	**Relevante TOZ**
4.12	Gemeinschaften müssen sicherstellen, dass: a) nach dem Stand der Technik sichere Verfahren für die Erzeugung, die Verteilung, die Aktivierung, die Aktualisierung, den Widerruf oder die Deaktivierung und die Löschung von kryptografischen Schlüsseln eingesetzt werden; b) die verwendeten kryptografischen Schlüssel gegen Veränderung und Verlust geschützt werden; c) geheime und private Schlüssel vor unbefugter Benutzung und Offenlegung geschützt werden; d) Einrichtungen zur Erzeugung, Speicherung und Archivierung von Schlüsseln angemessen geschützt werden.	
4.13.1 d	Gemeinschaften müssen sicherstellen, dass: d) vollständige Backups gemacht werden und die enthaltenen Daten verschlüsselt sind;	

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.2.2	Es sind mindestens die nachfolgenden Verfahren oder bessere Verfahren erlaubt: ▪ Symmetrische Verschlüsselung: AES-256 oder höher ▪ Blockverschlüsselung: Das Verfahren Cypher Block Chaining (CBC) ist zu verwenden. Sofern eine Authentifizierung notwendig ist, ist die Galois Counter Mode (GCM) zu verwenden. ▪ Stromverschlüsselung: Die Counter Mode (CTR) ist zu verwenden. ▪ Asymmetrische Verschlüsselung: Es ist RSA-4096 oder höher zu verwenden. ▪ Sofern ein Initialisierungsvektor (IV) eingesetzt werden muss, ist sicherzustellen, dass dieser für jede Verschlüsselung neu generiert wird.	**Vorgaben XAD**
3.2.3	Es sind mindestens folgende Hashing-Verfahren oder bessere Hashing-Verfahren erlaubt: ▪ ARGON 2 oder PBKDF2 mit Salz ▪ SHA-512 oder SHA3-512	

Zum Speichern von Passwörtern und ähnlichem sind ARGON 2 oder PBKDF2 zu bevorzugen, da diese deutlich resistenter auf Bruteforce-Attacken sind als die SHA-Varianten, welche auf Geschwindigkeit optimiert sind.

3.2.4 Sofern die Verschlüsselungsverfahren von der nachfolgenden Auswahl abweichen, ist der Standard FIPS-140-2[1] zu berücksichtigen und einzuhalten.

3.2.5 Der Austausch von kryptographischen Schlüsseln muss über eine gesicherte Verbindung oder in verschlüsselter Form, beispielsweise durch die Anwendung von asymmetrischen Verfahren, erfolgen.

3.2.6 Zur Generierung von Schlüsseln sind, wenn immer möglich, kryptographische Module (eingesetztes Set bestehend aus Hardware, Software und Firmware) einzusetzen, die mit dem Standard FIPS-140-2 konform sind.

3.2.7 Im Zusammenhang der Aufbewahrung von kryptografischen Schlüsseln sind die nachfolgenden Bestimmungen relevant:

- Die Aufbewahrung von kryptografischen Schlüsseln auf einem Datenträger, Zwischenträger und/oder in einer Applikation im Klartext ist unzulässig.
- Der Speicherort ist nur dem notwendigen Benutzerkreis bekannt zu machen.
- Die gespeicherten, kryptografischen Schlüssel auf Datenträgern, Zwischenspeicher und/oder in Applikationen sind durch kryptografische Module, die konform mit dem FIPS-140-2 sind, zu schützen.
- Zur Aufbewahrung von kryptografischen Schlüsseln sind kryptografische Tresore, beispielsweise Hardware-Sicherheitsmodul (HSM) oder isolierte kryptografische Services zu verwenden.
- Kryptografische Schlüssel, die in einer Datenbank aufbewahrt werden, müssen vor dem Transport auf einen Datenträger mit Key Encryption Keys verschlüsselt werden. Diese Keys müssen mindestens die gleiche Stärke aufweisen wie die Schlüssel selbst.
- Der Schlüsselzugriff, die Ver- und Entschlüsselung sowie das Signieren sollten in einem geschützten Tresor stattfinden.

3.2.8 Gespeicherte Schlüssel müssen in einem adäquaten Backup gesichert werden. Dieses muss mindestens nach FIPS 140-2 Level 2 geschützt sein.

3.2.9 Zur Übertragung von Daten ist mindestens der Standard TLS 1.2 zu verwenden.

3.2.10 Beim E-Mailversand aus dem EPD müssen folgende Vorgaben erfüllt sein:

- E-Mails müssen signiert werden, sodass der Absender verifizierbar ist.
- Der Transport (nicht Inhalt) muss verschlüsselt erfolgen.

3.3 Demographische Patientensuche

2.9.19	Der IHE-Akteur *Patient Identifier Cross-reference Manager* muss die folgenden Transaktionen des Integrationsprofils IHE PIX V3 in den Versionen nach Anhang 5 der EPDV-EDI unterstützen: a) Patient Identity Feed HL7 V3 [ITI-44]; b) PIX V3 Query [ITI-45];	**Relevante TOZ**

[1] FIPS-140-2 https://csrc.nist.gov/publications/fips#140-2

c) PIX V3 Update Notification [ITI-46].

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.3.1 Die maximale Anzahl der dargestellten Treffer bei einer Patientensuche im Master Patient Index ist auf fünf zu beschränken. **Vorgaben XAD**

Sind nach einer Suche mehr als fünf Treffer vorhanden, sollen Ergebnisse nicht dargestellt werden, sondern eine Meldung, welche den Benutzer signalisiert, dass zu viele Ergebnisse mit diesen Suchkriterien vorhanden sind, angezeigt werden. Ebenfalls soll die Meldung hinweisen, dass weitere Suchkriterien notwendig sind, um die Anzahl der Ergebnisse einzuschränken.

3.4 Erkennung von Anomalien

3.3 f **Abruf und Medientypen von medizinischen Daten** **Relevante TOZ**

Das Zugangsportal muss:

f) für den Abruf von medizinischen Daten zur Darstellung oder zum Abspeichern zulässige Obergrenzen für die erlaubte Anzahl von medizinischen Daten pro Zeiteinheit vorsehen, bei deren Überschreiten geeignete Sperr- oder zusätzliche Sicherheitsmassnahmen ausgelöst werden.

4.3.2 Die Verfahren zur Erkennung von Anomalien und Sicherheitsvorfällen sowie zur Analyse und Berichterstattung darüber müssen risikogerecht und gemeinschaftsspezifisch definiert sein und mindestens die folgenden Anomalien erkennen und adressieren:

a) Angriffe aus dem Internet auf Zugangsportale oder auf den Zugangspunkt der Gemeinschaft;

b) unübliche Muster schreibender oder lesender Zugriffe auf die Dokumentenablagen, das Dokumentenregister oder den Patientenindex, die auf eine missbräuchliche Nutzung oder automatisierte Attacke hinweisen;

c) ungewöhnliche und kritische Mutationen von Berechtigungsdaten in der Berechtigungssteuerung, dem Identitäts- und Zugangsmanagement-System (IAM) oder, sofern vorhanden, dem gemeinschaftsinternen Dienst zur Verwaltung von Gesundheitseinrichtungen und Gesundheitsfachpersonen.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.4.1 Bei einer ungewöhnlich hohen Anzahl von Abfragen (Queries) oder Anpassungen von Metadaten innerhalb einer Minute mit einem gleichen Benutzerkonto soll der Account gesperrt werden. **Vorgaben XAD**

3.4.2 Bei einer ungewöhnlich hohen Anzahl von Abfragen innerhalb einer Minute bei medizinischen Dokumenten soll der Account gesperrt werden.

3.4.3 Folgende Anomalien sind zu erkennen und Gegenmassnahmen zu definieren:

- SQL Injection EPD-Plattform

- Denial of Service EPD-Plattform
- Bruteforce EPD-Plattform
- Enumeration EPD-Plattform
- Document Access Anomaly EPD-Plattform
- Access Provisioning Anomaly EPD-Plattform
- Unpatched Vulnerability EPD-Infrastructure
- Excessive Login Attempts EPD-Infrastructure
- Excessive Data Access EPD-Infrastructure
- System Configuration Changes EPD-Infrastructure
- High Privileged Access EPD-Infrastructure

3.5 Protokolldaten und Protokollierung

2.10	**Protokolldaten (Art. 10 Abs. 3 Bst. d EPDV)**	**Relevante TOZ**
2.10.1	Jede Bearbeitung von Daten des elektronischen Patientendossiers ist zu protokollieren und mit einem aktuellen Zeitstempel zu versehen.	
2.10.2	Die Bearbeitung folgender Daten ist sowohl für erfolgreiche als auch für abgewiesene Versuche zu protokollieren: a) der medizinischen Daten in den Dokumentenablagen; b) der Einträge im Dokumentenregister; c) der Konfiguration der Berechtigungssteuerung; d) der Daten des Patientenindex.	
2.10.3	Zudem sind folgende Ereignisse zu protokollieren: a) Authentifizierungen am System (Login/Logout); b) gemeinschaftsübergreifende Transaktionen über die Zugangspunkte der Gemeinschaften; c) die Suche nach einer Patientin oder einem Patienten; d) die Suche nach medizinischen Daten eines elektronischen Patientendossiers; e) ein Notfallzugriff auf ein elektronisches Patientendossier; f) Zugriffe und Zugriffsversuche auf medizinische Daten eines elektronischen Patientendossiers.	
2.10.4	Mindestens zu protokollieren ist in jedem Fall: a) das Ereignis selbst («Event Identification») und der Kontext, in dem es eingetreten ist (Normalbetrieb, Notfallzugriff, Verwendung von privilegierten Sonderzugriffsrechten); b) der Zeitpunkt des Ereignisses («Event Timestamp»); c) die Person, die das Ereignis ausgelöst hat («Active Participant Identification»); d) der Ort, an dem das Ereignis ausgelöst wurde («Network Access Point Identification»); e) die Ursache des Ereignisses («Audit Source Identification»); f) die betroffenen Datensätze («Participant Object Identification»);	

g) das Resultat des Ereignisses («Event Outcome Indicator»).

2.10.5 Bei einer Suche müssen mindestens die Suchkriterien protokolliert werden.

2.10.6 Die Protokolldaten sind auf das erforderliche Mass zu beschränken und dürfen keine Dokumente enthalten.

2.10.7 Die Protokollierung muss folgende Anforderungen erfüllen:

a) Zusätzlich zu den Identifikatoren muss auch ein menschenlesbarer Text protokolliert werden, der die referenzierte Entität zum Zeitpunkt der Protokollierung namentlich bezeichnet.

b) Vorgeschriebene Protokollierungen dürfen nicht umgangen werden können.

c) Eine nachträgliche Veränderung von Protokolldaten muss erkennbar und nachvollziehbar sein.

d) Bei der Protokollierung muss unterschieden werden zwischen Zugriffen, die aus der Nutzung des elektronischen Patientendossiers resultieren, und technisch-administrativen Zugriffen im Rahmen des Systembetriebs.

e) Für Systemadministratoren darf keine Möglichkeit bestehen, die Protokollierung ihrer eigenen Aktivitäten zu löschen oder zu deaktivieren.

2.10.8 Die Protokolldaten nach den Ziffern 2.10.1 bis 2.10.3 sind 10 Jahre aufzubewahren und dann zu vernichten.

2.10.9 Der Abruf und die Darstellung von Protokollinformationen für die Einsichtnahme durch die Patientin oder den Patienten richten sich nach dem nationalen Integrationsprofil CH:ATC gemäss Anhang 5 der EPDV-EDI.

2.10.10 Gemeinschaften müssen sicherstellen, dass Datenbearbeitungen derart protokolliert werden, dass die Daten für die Evaluation gemäss Artikel 6 der EPDV-EDI zur Verfügung gestellt werden können.

4.2.1 c Gemeinschaften müssen ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem nach Art der Norm DIN EN ISO/IEC 27001:2017-06 einrichten, aufrechterhalten, regelmässig überprüfen sowie dessen Eignung, Angemessenheit und Wirksamkeit laufend verbessern, so dass:

c) alle relevanten Aufzeichnungen im Einklang mit den gesetzlichen Anforderungen vor Verlust, Zerstörung und Fälschung geschützt sind.

4.13.3 Neben Ereignissen aufgrund der Bearbeitung von Daten des elektronischen Patientendossiers durch Gesundheitsfachpersonen sowie Patientinnen und Patienten nach Ziffer 2.10 sind mindestens folgende Ereignisse, die im Rahmen des Systembetriebs auftreten, aufzuzeichnen:

a) Login und Logout;

b) erfolgreiche und abgewiesene Versuche, auf das System zuzugreifen;

c) erfolgreiche und abgewiesene Versuche, auf Daten zuzugreifen;

d) Veränderungen an der Systemkonfiguration;

e) die Verwendung privilegierter Sonderzugriffsrechte;

f) Netzwerkadressen und -protokolle;

g) die Aktivierung und Deaktivierung von Schutz- oder Authentisierungs-Systemen;

h) die Modifikation von Systemberechtigungen und Zugängen;

i) das Anlegen, die Modifikation oder das Löschen von Benutzerkonten;

j) das Kopieren als schützenswert eingestufter Daten.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.5.1 Protokollierung von folgenden Ereignissen müssen im Fall vom Integrationspaket S gewährleistet und bei Bedarf bereitgestellt werden: **Vorgaben XAD**

- Login-und Logoutaktivitäten beim Abruf oder Hochladen von Patientendaten innerhalb des KIS oder ERP (Primärsystem) über Schnittstellen oder die Middleware
- Erfolgreiche und abgewiesene Anmeldungsversuche zum Primärsystem
- Verwendung von Admin-bzw. Notfallzugriffrechten für EPD Schnittstellen Software (Middleware oder Kommunikationsserver)
- Veränderungen bei Schnittstellen-Systemberechtigungen
- Erstellung, Modifikation oder Löschen von Benutzerkonten innerhalb vom Schnittstellensystem

3.5.2 Beim Integrationspaket M sollen zusätzlich zu den Vorgaben von Integrationspaket S Schnittstellen der folgenden Systeme protokolliert werden:

- KIS, PACS, DMS und/oder DMS: Quelle der medizinischen Daten.

3.5.3 Beim Integrationspaket L sollen zusätzlich zu den Vorgaben von Integrationspaket M Schnittstellen der folgenden Systeme protokolliert werden:

- KIS, PEP oder HR Modul: Quelle der GFP-Stammdaten.

3.5.4 Bearbeitung oder gescheiterte Versuche folgender Daten sind zu protokollieren:

- medizinische Daten in den Dokumentenablagen;
- Einträge im Dokumentenregister;
- die Konfiguration der Berechtigungssteuerung;
- die Daten des Patientenindex;
- gemeinschaftsübergreifende Transaktionen über die Zugangspunkte der Gemeinschaften;
- die Suche nach einer Patientin oder einem Patienten;
- die Suche nach medizinischen Daten eines elektronischen Patientendossiers;
- ein Notfallzugriff auf ein elektronisches Patientendossier;
- Zugriffe und Zugriffsversuche auf medizinische Daten eines elektronischen Patientendossiers.

3.5.5 Alle Logfiles und Protokolle müssen einen Zeitstempel gemäss offizieller Schweizer Uhrzeit haben. Die Speicherung hat so zu erfolgen, so dass eine nachträgliche Veränderung oder Löschung der Logs oder Protokolle nicht möglich ist. Der Zugriff ist auf den notwendigen Personenkreis zu beschränken.

3.6 Umgang mit Testdaten

4.14.2 e Mindestens ist nachzuweisen, dass innerhalb jedes Entwicklungszyklus: **Relevante TOZ**

e) sich in Testumgebungen keine produktiven Daten, insbesondere keine besonders schützenswerten Daten befinden.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.6.1	Bei vorgelagerten und nicht produktiven Umgebungen (z.B.: Entwicklung, Test, Schulung, Integration) dürfen zu keinem Zeitpunkt Daten aus einer produktiven Umgebung ohne vorgenommene Anonymisierung verwendet werden.	**Vorgaben XAD**
3.6.2	Die Anonymisierung hat so zu erfolgen, dass keine Rückschlüsse auf die ursprüngliche Person mehr möglich sind.	

3.7 Gruppen GFP

1.5	**Verwaltung von Gruppen von Gesundheitsfachpersonen (Art. 9 Abs. 2 Bst. a, c, d und f EPDV)** Gemeinschaften sind für die Verwaltung der Gruppen von Gesundheitsfachpersonen verantwortlich. Sie legen den Prozess zu deren Verwaltung fest. Der Prozess muss sicherstellen, dass: a) für Gruppen von Gesundheitsfachpersonen ein OID vergeben wird, der auf dem OID der Gesundheitseinrichtung basiert; b) die Daten im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen nach Artikel 41 EPDV aktualisiert werden; c) die Patientinnen und Patienten auf deren Verlangen über Eintritte von Gesundheitsfachpersonen in Gruppen von Gesundheitsfachpersonen informiert werden.	**Relevante TOZ**
8.6.1	Patientinnen und Patienten müssen die Möglichkeit haben, Gesundheitsfachpersonen und Gruppen von Gesundheitsfachpersonen Zugriffsrechte zu erteilen, diese Zugriffsrechte anzupassen und zu entziehen. Dabei sind die Vorgaben der Artikel 2 und 3 EPDV einzuhalten.	

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.7.1	Gesundheitseinrichtungen, welche zwischen 1 und 20 GFP anmelden, ist die Gruppenbildung optional.	**Vorgaben XAD**
3.7.2	Gesundheitseinrichtungen, welche zwischen 21 und 100 GFP anmelden, haben mindestens 2 Gruppen zu erstellen.	
3.7.3	Gesundheitseinrichtungen, welche über 100 GFP anmelden, haben mindestens 4 Gruppen zu erstellen.	
3.7.4	Eine Gruppe muss aus mindestens 2 GFP bestehen und darf maximal 200 Personen beinhalten.	

3.8 Katalog der Schutzobjekte

4.6.1	Gemeinschaften müssen sicherstellen, dass alle schützenswerten Daten, Systeme und Einrichtungen des elektronischen Patientendossiers eindeutig identifiziert, klassifiziert und in einem «Inventar der Informatikinfrastruktur» erfasst und aktuell gehalten werden.	**Relevante TOZ**

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

3.8.1 Der Katalog der Schutzobjekte ist Bestandteil des Inventars der Informatikinfrastruktur und umfasst sicherheitsrelevante Elemente. Der Katalog wird durch die DSDS-V XAD-SG geführt. **Vorgaben XAD**

3.8.2 Der Katalog der Schutzobjekte muss mindestens beinhalten:

- Alle Datenobjekte, welche dem EPDG oder DSG unterliegen
- Alle EPD-relevanten IHE-Akteure
- Beide Portale: Gesundheitsfachpersonen und Patienten
- Das Identitäts- und Zugangsmanagement-System (IAM)
- Alle Systeme, die EPD-Daten verarbeiten, den Zugriff auf EPD-Daten ermöglichen oder die Berechtigungen im Zusammenhang mit Zugriffen auf EPD-Daten verändern können

Folgende Attribute werden bei den Elementen des Katalogs erfasst:

- Typ
- Owner
- Bezeichnung des Elements
- Inhaltliche Beschreibung vom Element
- Attribute für das Risikomanagement:
- Business Impact – Confidentiality
- Business Impact – Availability
- Business Impact – Integrity

3.8.3 Der Katalog wird mindestens jährlich gesamt auf Korrektheit und Aktualität geprüft. Die Überprüfung erfolgt durch die DSDS-V XAD-SG.

4 Komponenten und Systeme

4.1 Sichere Konfiguration Endgeräte

2.2 a	Gemeinschaften müssen bei Zugriffen in medizinischen Notfallsituationen sicherstellen, dass: a) die zugreifende Gesundheitsfachperson den Zugriff auf eine Weise bestätigen muss, die den Missbrauch insbesondere durch eine auf dem Endgerät installierte Schadsoftware wirksam verhindert;	**Relevante TOZ**
4.4.3	Gemeinschaften müssen sicherstellen, dass: a) die Angriffsfläche der Informatikmittel minimiert wird («Härtung» der Systeme). Sie müssen die dazu notwendigen Verfahren definieren und deren Durchführung und Kontrolle sicherstellen; b) nicht benötigte Funktionen und Schnittstellen deaktiviert werden; c) die Informatikmittel gegen Angriffe und Kompromittierungen durch XML-Dateien und Nachrichten geschützt werden.	
4.5	Gemeinschaften müssen die regelmässige Durchführung von Massnahmen zum Schutz vor Schadsoftware planen und deren effektive Ausführung regelmässig überprüfen. Insbesondere müssen sie: a) Massnahmen zum Schutz, insbesondere der schützenswerten Elemente der Informatikinfrastruktur der Ziffern 4.6.2 Buchstaben a–i und k-l, vor Schadsoftware treffen, die es insbesondere erlauben, solche Software zeitgerecht zu erkennen und zu entfernen; b) die eingesetzte Software zur Erkennung und Entfernung von Schadsoftware regelmässig überprüfen und deren Aktualität sicherstellen.	
4.7.1 c	Gemeinschaften müssen die Gesundheitseinrichtungen: c) dazu verpflichten, eine sichere Konfiguration der Endgeräte sicherzustellen, die von den Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier genutzt werden.	
4.7.2	Die Vorgaben zur Konfiguration der Endgeräte müssen mindestens umfassen: a) den Einsatz einer regelmässig aktualisierten Software gegen Schadprogramme; b) den Einsatz netzwerktechnischer Schutzsysteme; c) eine regelmässige Aktualisierung des Betriebssystems und der sicherheitskritischen Software-Komponenten; d) eine restriktive Handhabung von Systemadministratorrechten.	
4.7.3	Gemeinschaften müssen sicherstellen, dass Endgeräte mit nicht als sicher eingestuften Konfigurationen keine Daten des elektronischen Patientendossiers bearbeiten.	

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

4.1.1	Endgeräte, welche die Vorgaben an die sichere Konfiguration nicht erfüllen, dürfen weder für den Zugriff auf die Daten des EPD noch zu dessen Bearbeitung benutzt	**Vorgaben**

werden. Die Gesundheitseinrichtungen stellen organisatorisch sicher, dass diese Vorgaben bekannt gemacht und eingehalten werden.

4.1.2 Es sind persönliche Benutzerkonten für jede Gesundheitsfachpersonen, Hilfspersonen und jeden Administrator einzurichten. Die Benutzerkonten haben limitierte Berechtigungen auf dem System. Der Gast-Benutzer ist zu deaktivieren.

4.1.3 Bei der Erstinstallation von Systemen sind vordefinierten Benutzerkonten, Initialpasswörter oder Zugriffsrechte sofort zu kontrollieren und allenfalls zu löschen, oder anzupassen.

4.1.4 Die Konfiguration von Endgeräten ist auf eine Weise zu schützen, so dass kein Benutzer sicherheitsrelevante Änderungen an den Einstellungen des Virenschutzprogramms vornehmen kann. Insbesondere muss sichergestellt werden, dass die Benutzer die Virenschutzprogramme nicht deaktivieren können. Zudem sollen netzwerktechnische Schutzsysteme verwendet werden (z.B. Firewalls).

4.1.5 Die Konfiguration, die Deinstallation oder die Deaktivierung der Sicherheitseinstellungen darf nur autorisiert erfolgen.

4.1.6 Systemadministratorenkonten und -rechte sind restriktiv und nur an Personen, welche die Funktion eines Systemadministrators wahrnehmen zu vergeben.

4.1.7 Das BIOS/UEFI, welches für das Starten des Betriebssystems zuständig ist, muss mit einem Kennwort abgesichert werden.

4.2 Schutz vor Schadsoftware

4.5.1	Gemeinschaften müssen die regelmässige Durchführung von Massnahmen zum Schutz vor Schadsoftware planen und deren effektive Ausführung regelmässig überprüfen. Insbesondere müssen sie: a) Massnahmen zum Schutz, insbesondere der schützenswerten Elemente der Informatikinfrastruktur der Ziffern 4.6.2 Buchstaben a–i und k-l, vor Schadsoftware treffen, die es insbesondere erlauben, solche Software zeitgerecht zu erkennen und zu entfernen; b) die eingesetzte Software zur Erkennung und Entfernung von Schadsoftware regelmässig überprüfen und deren Aktualität sicherstellen.	**Relevante TOZ**

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

4.2.1 Sowohl Clients als auch Serversysteme müssen mit einem aktivierten Virenschutzprogramm ausgestattet sein. **Vorgaben XAD**

4.2.2 Sicherheitsrelevante Aktualisierungen (Patches) des Betriebssystems oder installierter Zusatzsoftware müssen mindestens monatlich vorgenommen werden.

4.2.3 Die Signaturen der Virenschutzprogramme sind mindestens täglich zu aktualisieren.

4.2.4 Für sämtliche Informatikmittel mit lokaler Datenablage ist mindestens einmal wöchentlich ein Full-Scan durchzuführen.

4.3 Authentisierung und Autorisierung

Relevante TOZ

2.2 Gemeinschaften müssen bei Zugriffen in medizinischen Notfallsituationen sicherstellen, dass:

a) die zugreifende Gesundheitsfachperson den Zugriff auf eine Weise bestätigen muss, die den Missbrauch insbesondere durch eine auf dem Endgerät installierte Schadsoftware wirksam verhindert;

b) die Patientin oder der Patient innert angemessener Frist informiert wird;

c) die Information über einen Notfallzugriff, sofern sie ausserhalb des elektronischen Patientendossiers elektronisch (z. B. SMS, E-Mail) übermittelt wird, keine besonders schützenswerten Daten enthält.

4.8.1 Für den Zugang und die Bearbeitung der Daten des elektronischen Patientendossiers durch das technische und administrative Personal der Gemeinschaften, müssen diese Vorgaben erlassen und die zu deren Einhaltung notwendigen technischen und organisatorischen Vorkehrungen treffen.

4.8.2 b Gemeinschaften müssen sicherstellen, dass:

b) die Verwendung von geheimen Authentifizierungsdaten über einen formellen Verwaltungsprozess kontrolliert wird und Anforderungen an den sicheren Gebrauch (z. B. Vertraulichkeit, Passwortlänge, Gültigkeit) gefordert werden und bekannt sind.

4.8.2 c Gemeinschaften müssen sicherstellen, dass:

c) Personen, die Zugang zu Daten des elektronischen Patientendossiers erlangen könnten, entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet werden.

5.1.2 c Gemeinschaften müssen mindestens sicherstellen, dass:

c) Zugriffe der Mitarbeitenden der Kontaktstelle auf die Endgeräte der Gesundheitsfachpersonen ausschliesslich mit Einwilligung der jeweiligen Gesundheitsfachperson erfolgen und dokumentiert werden.

11.1.2 c Stammgemeinschaften müssen mindestens sicherstellen, dass:

c) die Mitarbeitenden der Kontaktstelle ausschliesslich mit Einwilligung auf die Endgeräte der Patientinnen und Patienten der jeweiligen Patientin oder des Patienten zugreifen können und die Zugriffe dokumentiert werden.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

4.3.1 Authentisierung

Vorgaben XAD

4.3.1.1 Für den Zugriff auf das elektronische Patientendossier mit besonderen Benutzerrechten muss immer eine Zweifaktorenauthentifizierung (2FA) gemäss dem aktuellen Stand der Technik erfolgen. Der Prozess soll regelmässig überwacht und entsprechend protokolliert werden.

4.3.1.2 Die Verwendung des Notfallzugriffes erfordert eine erneute Authentifizierung mit dem zweiten Faktor der 2FA gemäss dem aktuellen Stand der Technik. Eine erneute Authentifikation mit dem zweiten Faktor der 2FA ist beim Verlassen der Notfall-Session nicht notwendig, solange die Notfall-Session noch nicht abgelaufen ist.

Wenn ein Notfallzugriff stattgefunden hat, müssen Patienten innerhalb von 24 Stunden benachrichtigt werden.

4.3.2 Autorisierung

4.3.2.1	Die Gesundheitseinrichtungen erstellen und pflegen ein spezifisches Rollenkonzept für alle GFP/HIP.	**Vorgaben XAD**
4.3.2.2	Die Gesundheitseinrichtungen haben die Verantwortlichkeiten für die Bewilligung und die Vergabe von Zugriffsrechten für das EPD zu trennen und im Rollenkonzept zu dokumentieren.	
4.3.2.3	Mitarbeitende der Kontaktstelle dürfen nur mit einer expliziten Einwilligung der jeweiligen GFP bzw. deren HIP auf ein GFP-Endgerät Zugriff haben. Zugriffe sowie Aktionen seitens der Kontaktstelle, welche Einfluss auf EPD-Prozesse haben, sind vollständig und nachvollziehbar zu dokumentieren.	

4.3.3 Passwörter Portal

4.3.3.1	Länge von Passwörtern ▪ Benutzerpasswort: mindestens 8 Zeichen ▪ Administratorenpasswort: mindestens 12 Zeichen	**Vorgaben XAD**
4.3.3.2	Zusammensetzung von Passwörtern ▪ Das Passwort enthält mindestens Gross-, Kleinbuchstaben, Zahlen und Sonderzeichen ▪ Trivialpasswörter wie zum Beispiel Benutzer-ID, Name, Vorname, Geburtsdatum oder Wörter des Duden-Wörterbuches dürfen nicht verwendet werden. ▪ Im Passwort sind weder Zahlen- noch Buchstabenfolgen wie zum Beispiel «abcdef», «abcba», «123456» oder «12121» erlaubt. ▪ Die Zusammensetzung ist soweit technisch realisierbar zu erzwingen. ▪ Das Initialpasswort muss nach dem erstmaligen Login auf dem EPD-Portal geändert werden.	
4.3.3.3	Umgang mit Passwörtern ▪ Das Passwort hat eine maximale Gültigkeit von zwei Jahren. Der Passwortwechsel ist technisch zu forcieren. Sofern die technische Umsetzbarkeit des Passwortwechsels nicht möglich ist, muss dieser auf organisatorische Weise sichergestellt werden. ▪ Passwörter sind persönlich und dürfen nicht weitergegeben werden. ▪ Die Logindaten für das Zugangsportal für Gesundheitsfachpersonen dürfen nicht im Internetbrowser gespeichert werden.	

4.4 Zertifikate

2.9.26	Gemeinschaften müssen über ein gültiges elektronisches Zertifikat verfügen, das bei einer nach dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur	**Relevante TOZ**

(ZertES; SR 943.03) anerkannten Anbieterin von Zertifikatsdiensten bezogen wurde, für:

a) die gegenseitige Authentisierung ihrer gemeinschaftsübergreifend kommunizierenden Endpunkte und Zugangspunkte;

b) die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber den Abfragediensten nach Artikel 39 Buchstaben a bis c EPDV;

c) die gegenseitige Authentisierung ihrer Zugangspunkte gegenüber der Identifikationsdatenbank der ZAS.

2.9.26 a Gemeinschaften müssen sicherstellen, dass:

a) der gemeinschaftsübergreifende Datenaustausch nur mit gemäss Ziffer 2.9.26 Buch- stabe a authentifizierten Endpunkten erfolgt, die im Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 Absatz 1 EPDV geführt sind.

b) die Überprüfung, welche Endpunkte als vertrauenswürdige Kommunikationspartner im Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften geführt werden, regelmässig durchgeführt wird, so dass jegliche Kommunikation mit nicht mehr vertrauenswürdigen Endpunkten rasch unterbunden werden kann (vgl. Art. 37 Abs. 1 Bst. a EPDV).

4.15.4 Die Netzwerkstrukturen müssen folgende Anforderungen erfüllen:

a) Für Zugangsportale sowie Zugangspunkte werden TLS-Zertifikate der Zertifikatsklasse 2 oder höher (gem. eCH-0048 PKI-Zertifikatsklassen, Version 2.0 vom 28.11.2018) eingesetzt, für andere Dienste entweder TLS-Zertifikate mindestens der Zertifikatsklasse 2 oder TLS-Zertifikate, die nur innerhalb der Gemeinschaft gültig sind.

b) Alle Dienste, die aus dem Internet aufrufbar sind, müssen das aufrufende System mittels *TLS-Client-Authentication* authentisieren.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

Vorgaben XAD

4.4.1 Die maximale Gültigkeitsdauer für die Verwendung eines Zertifikates ist auf zwei Jahre und drei Monate beschränkt.

4.4.2 Es sollten Zertifikate verwendet werden, welche alle benötigten Domain-Namen unterstützen (z.B. https://www.example.ch und https://example.ch). In der Subject Alternative Names (SAN) muss die Domain-Name oder -Namen eingetragen werden.

4.4.3 Es sollen nur Fully Qualified Domain Name (FQDN) eingetragen werden.

4.4.4 Es dürfen keine Wildcards in Zertifikaten verwendet werden.

4.4.5 Zertifikate müssen eine minimale Schlüssellänge von 4096 Bit aufweisen.

4.4.6 Alle eingesetzten Zertifikate, ausser dem der Root Certification Authority (CA), müssen einen SHA-256 oder besseren Fingerprint enthalten.

4.4.7 Bei öffentlichen Zertifikaten (Public Certificate) müssen zudem folgenden Voraussetzungen erfüllt sein:

- Nur bekannte und vertrauenswürdige CAs dürfen verwendet werden.

4.4.8 Für Dienste, welche ausschliesslich intern (Machine-to-Machine) verwendet werden, sollten Zertifikate eingesetzt werden, welche von einer eigenen CA abgeleitet sind und die auf allen Geräten entsprechend konfiguriert ist.

4.5 Lebenszyklus von Systemen

Relevante TOZ

4.14.1 Gemeinschaften müssen den Datenschutz und die Datensicherheit über den gesamten Lebenszyklus der Systeme des elektronischen Patientendossiers sicherstellen. Dazu müssen sie Prozesse festlegen für die Dokumentation, das Design, die Spezifikation, das Testen, die Qualitätskontrolle und die kontrollierte Umsetzung bei:

a) der Einführung oder der Entwicklung neuer Systeme;

b) grösseren Änderungen oder Entwicklungen an bestehenden Systemen;

c) dem Wechsel der Betriebsplattformen.

9.6.1 Zusätzlich zu den Anforderungen an Datenschutz und Datensicherheit nach Ziffer 4 muss das Zugangsportal:

a) mindestens nach jeder sicherheitsrelevanten Veränderung der Informatikmittel des Zugangsportals aktiv durch Penetrationstests auf Sicherheitsschwachstellen überprüft werden;

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

Vorgaben XAD

4.5.1 Eine Release-Roadmap soll erstellt und kontinuierlich aktualisiert werden. Hier sollen Major geplante Releases mindestens für die kommenden zwölf Monaten dargestellt werden.

4.5.2 Ein Change-Management-Prozess ist zu etablieren. Alle Changes sind sorgfältig zu dokumentieren.

4.5.3 Qualitätssicherung der Systeme soll immer gewährleistet werden. Dafür sind regelmässige Massnahmen bei Changes/neue Releases wie Qualitätsrunden einzuplanen.

4.5.4 Testkonzepte/Testszenarien sind zu definieren. Diese müssen regelmässig geprüft und wenn nötig aktualisiert werden.

4.5.5 Jeder Release muss durch Penetrationstests auf Schwachstellen überprüft werden. Folgende Vorgaben sollen berücksichtigt werden:

- Scope: Exponierte Systeme und Systeme mit erhöhten Risiken → Zugangsportal Patient und Gesundheitsfachperson
- Dokumentation: Testkonzept soll immer erstellt werden
- Frequenz: Bei sicherheitsrelevanten Änderungen (TOZ 9.6.1a) → jeder Release
- Testtyp: Greybox (gültige Zugangsdaten / limitierte Informationen über das System). Angriffsvektor «Internet».
- Testumfang: Gemäss OWASP Top 10 und Testing Guide (v4)

- Testmethodik: Manuelle und automatisierte Tests gemäss Penetration Testing Execution Standard (PTES)
- Berichterstattung: Bericht pro durchgeführter Penetration Test soll erstellt werden
- Eingesetzte Tools: Nessus Vulnerability Scanner, Burp Suite, Nmap, Sqlmap

4.6 Entsorgung von Hardware

4.17	Elemente der gemeinschaftsinternen Informatikinfrastruktur, die der Übermittlung von medizinischen Daten des elektronischen Patientendossiers dienen, namentlich die Zugangspunkte, dürfen diese nicht dauerhaft, sondern nur für die Dauer der Transaktion speichern.	**Relevante TOZ**

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

4.6.1	Dossiereröffnungsstellen mit Hardware, welche Daten des elektronischen Patientendossiers zwischenspeichern, stellen die ordnungsgemässe Entsorgung sicher. Hardware (z.B. Computer und Drucker), welche Daten des elektronischen Patientendossier bearbeiten und Speichermedien beinhalten, sind vor der Entsorgung oder Wiederverwendung zu prüfen. Daten des elektronischen Patientendossier sind zu entfernen oder sicher zu überschreiben.	**Vorgaben XAD**

5 Netzwerk

4.15.1	Gemeinschaften müssen Richtlinien zur Netzwerksicherheit vorsehen und die Zuständigkeiten für die Verwaltung von Netzwerken innerhalb einer Gemeinschaft festlegen.	**Relevante TOZ**
4.15.2	Gemeinschaften müssen sicherstellen, dass durch ein geeignetes Design des Netzwerks und seiner Komponenten sowie durch den geeigneten Aufbau und die Konfiguration der Netzwerkdienste, die Daten des elektronischen Patientendossiers in Anwendungen und Systemen geschützt sind.	
4.15.3	Sie müssen dazu sichere Netzwerkstrukturen festlegen, durch Netzwerkpläne darstellen und umsetzen, die es erlauben, Gruppen von Informationsdiensten, Benutzern und Informationssystemen in Netzwerken voneinander getrennt zu halten; insbesondere müssen sie Firewalls, Router, Switches, etc. und technologische Umsetzungen für Netzwerkdienste so konfigurieren, dass: a) die technischen Schnittstellen der gemeinschaftsinternen Informatikinfrastruktur einer Gemeinschaft («Services») nur von Systemen aufgerufen werden können, die zu einer zertifizierten Gemeinschaft gehören und den auf sie anwendbaren Anforderungen genügen (z. B. gem. Ziff. 3.4, 4.5.1, 4.7.2 und 4.7.3); b) Systeme, die über das Internet auf einen Dienst zugreifen, sich diesem gegenüber mittels Transportschichtsicherheit (TLS) mit einem gültigen elektronischen Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority, CA) nach dem Stand der Technik authentisieren.	
4.15.4	Die Netzwerkstrukturen müssen folgende Anforderungen erfüllen: a) Für Zugangsportale sowie Zugangspunkte werden TLS-Zertifikate der Zertifikatsklasse 2 oder höher (gem. eCH-0048 PKI-Zertifikatsklassen, Version 2.0 vom 28.11.2018) eingesetzt, für andere Dienste entweder TLS-Zertifikate mindestens der Zertifikatsklasse 2 oder TLS-Zertifikate, die nur innerhalb der Gemeinschaft gültig sind. b) Alle Dienste, die aus dem Internet aufrufbar sind, müssen das aufrufende System mittels *TLS-Client-Authentication* authentisieren. c) Antwortende Zugangspunkte (*Responding Gateways*) oder andere für die gemeinschaftsübergreifende Kommunikation erreichbaren Endpunkte dürfen den Verbindungsaufbau nur zulassen, wenn das aufrufende System zu einer zertifizierten Gemeinschaft gehört und im zentralen Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften nach Artikel 40 EPDV geführt wird. d) Alle gemeinschaftsinternen Dienste, die nicht aus dem Internet aufgerufen werden können, dürfen den Verbindungsaufbau nur zulassen, wenn das aufrufende System zur eigenen zertifizierten Gemeinschaft gehört und im Inventar der eigenen Gemeinschaft registriert und vom Datenschutz- und Datensicherheitsverantwortlichen akzeptiert wurde. e) Die eingesetzten Verfahren müssen dokumentiert werden.	
4.15.5	Gemeinschaften müssen: a) alle Datenspeicher mit Patientendaten des elektronischen Patientendossiers der Gemeinschaft (darunter die Elemente aus dem «Inventar der	

Informatikinfrastruktur» nach Ziff. 4.8) netzwerktechnisch von allen anderen Systemen trennen, die ein tieferes Sicherheitsniveau aufweisen;

b) die hierzu eingesetzten Verfahren dokumentieren.

4.16.1 Inaktive Netzwerk-Sitzungen müssen nach einer von dem oder der Datenschutz- und Datensicherheitsverantwortlichen der Gemeinschaft vorgegebenen Inaktivitätsperiode automatisch beendet werden.

4.16.2 Die Authentisierung auf den Zugangsportalen und Endgeräten muss vor dem nächsten Zugriff erneut durchgeführt werden, wenn bis zum Ablauf einer vorgegebenen Zeitspanne keine Interaktion des Benutzers oder der Benutzerin mit dem elektronischen Patientendossier stattfand.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

Vorgaben XAD

5.1.1 Der Technik-Provider setzt im entsprechenden EPD-Systemkomponenten sämtliche Vorgaben gemäss TOZ 4.15 und 4.16 um.

5.1.2 Die Gesundheitseinrichtungen mit Integrationslösungen setzen folgende Massnahmen zum Schutz und zur Sicherheit der Netzwerkkomponenten um:

- Netzwerkkomponenten müssen vor Angriffen und unberechtigten Zugriffen geschützt werden. Die getroffenen Schutzmassnahmen sind zu dokumentieren.
- Der Zugriff auf Netzwerkkomponenten durch Netzwerkadministratoren muss mittels einer 2-Faktor-Authentifizierung erfolgen.
- Änderungen an der Konfiguration aktiver Netzwerkkomponenten müssen einem Prozess zum Konfigurations- bzw. Änderungsmanagement folgen.
- Ungeschützte Schnittstellen müssen deaktiviert werden.
- Das Netzwerk ist durch eine Monitoring-Lösung zu überwachen.
- Zur Überwachung des Netzwerkes sind Einbruchserkennungs- und Einbruchsverhinderungslösungen einzusetzen (IDS oder IPS).
- Konzeption, Planung und Aufbau der Netzwerkstrukturen, sowie deren Konfiguration sollen Anwendungen, Systemen und EPD-Daten schützen.
- Die Umsetzung ist entsprechend zu dokumentieren und bei Bedarf der XAD-SG bereitzustellen.

5.1.3 Alle Anforderungen betreffend Zertifikate werden im Kapitel 4.4 behandelt.

5.1.4 Es gelten die folgenden maximalen Timeouts für Netzwerksitzungen auf den Portalen:

Artefakt	Parameter	Wert
IdP Session Patientenportal	Max. Session Lifetime	2 h
	Session Idle Timeout	15 min
Session Patientenportal	Max. Session Lifetime	1 h
	Session Idle Timeout	15 min
Session Administrationsmodul Patientenportal	Max. Session Lifetime	60 min
	Session Idle Timeout	15 min
IdP Session GFP-Portal	Max. Session Lifetime	2 h
	Session Idle Timeout	15 min
Session GFP-Portal und Notfallzugriff	Max. Session Lifetime	60 min
	Session Idle Timeout	15 min
SAML Assertion (Authentication Token, X-User-Assertion (XUA) für GFP/HIP)	Max. Session Lifetime	5 min
Session MPI's administration Userinterface	Max. Session Lifetime	-
	Session Idle Timeout	15 min
Session Swisscom Health's Admin-Cockpit	Max. Session Lifetime	60 min
	Session Idle Timeout	15 min

5.1.5 Die laufende Session muss terminiert werden, sobald der Benutzer bei einer der obengenannten Portale eine zweite Session eröffnet.

5.1.6 Die Netzwerksitzungen sind nach dem Ablauf der vorgegebenen Inaktivitätsperiode automatisch zu terminieren, so dass sich der Benutzer erneut authentifizieren muss.

6 Sensibilisierung

4.2.2	Das Datenschutz- und Datensicherheitsmanagementsystem muss innerhalb der Gemeinschaft allen Gesundheitseinrichtungen und den Gesundheitsfachpersonen bekannt gemacht werden. Für die Gesundheitsfachpersonen müssen insbesondere Schulungen betreffend der für sie relevanten Vorgaben durchgeführt, diese dokumentiert und kritische Abläufe trainiert werden.	**Relevante TOZ**
4.8.2	Gemeinschaften müssen sicherstellen, dass: a) Personen, die mit Daten oder Systemen des elektronischen Patientendossiers umgehen, für die vorgesehenen Aufgaben kompetent genug sind und ihre Verantwortlichkeiten wahrnehmen können sowie dem Datenschutz und der Datensicherheit sorgfältig nachkommen; b) Personen, die Zugang zu Daten des elektronischen Patientendossiers erlangen könnten, entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet werden.	
5.1.2 a	Gemeinschaften müssen mindestens sicherstellen, dass: a) die Mitarbeitenden der Kontaktstelle ihre Rechte und Pflichten sowie die Massnahmen bezüglich Datenschutz und Datensicherheit kennen; b) die Mitarbeitenden mit Zugriff auf Daten des elektronischen Patientendossiers sorgfältig ausgewählt werden und entweder der ärztlichen Schweigepflicht nach Artikel 321 StGB unterstehen oder vertraglich zur Schweigepflicht verpflichtet werden; c) Zugriffe der Mitarbeitenden der Kontaktstelle auf die Endgeräte der Gesundheitsfachpersonen ausschliesslich mit Einwilligung der jeweiligen Gesundheitsfachperson erfolgen und dokumentiert werden.	
11.1.2 a	Stammgemeinschaften müssen mindestens sicherstellen, dass: a) die Mitarbeitenden ihre Rechte und Pflichten sowie die Risiken und Massnahmen bezüglich Datenschutz und Datensicherheit kennen.	

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

6.1.1	Sämtliche Personen, die Zugriff auf das EPD haben, sind zur Geheimhaltung und Einhaltung der Vorgaben des DSDS-MS zu verpflichten.	**Vorgaben XAD**
6.1.2	▪ Sämtliche Mitarbeitende der Gesundheitseinrichtungen, die Zugriff auf das EPD erhalten, müssen im Rahmen des Eintrittsprozesses der XAD-SG eine initiale Schulung in Form eines E-Learning zum Thema Datenschutz und Datensicherheit absolvieren **bevor** sie den Zugriff erhalten. ▪ Sämtliche Mitarbeitende der Zentralen Diensten und Dritten, die Zugriff auf das EPD erhalten, müssen eine initiale Schulung in Form eines E-Learning zum Thema Datenschutz und Datensicherheit absolvieren **bevor** sie den Zugriff erhalten. ▪ Die Ergebnisse sowie die Bestätigung der Durchführung des E-Learning sind bei Bedarf der DSDS-V XAD-SG zu übergeben.	
6.1.3	Die DSDS-V GE stellt sicher, dass sämtliche Mitarbeitenden, die Zugriff auf das EPD haben, mindestens jährlich zu ausgewählten Themen sensibilisiert werden. Die Durchführung der Sensibilisierungsmassnahmen sowie die Teilnehmerliste sind	

nachvollziehbar zu dokumentieren und bei Bedarf als Nachweis der DSDS-V XAD-SG zu übergeben.

6.1.4 Sämtliche Mitarbeitende der Zentralen Dienste und Dritten, die Zugriff auf das EPD haben, sollen mindestens jährlich zu ausgewählten Themen sensibilisiert werden. Die Durchführung der Sensibilisierungsmassnahmen sowie die Teilnehmerliste sind nachvollziehbar zu dokumentieren und bei Bedarf als Nachweis der DSDS-V XAD-SG zu übergeben.

7 Berichtwesen und Dokumentation

Relevante TOZ

4.10 Die von Dritten und allfälligen Unterlieferanten gelieferten Dienstleistungen, Berichte und Aufzeichnungen müssen von den Gemeinschaften regelmässig überwacht und überprüft werden, so dass sichergestellt ist, dass:

a) die vertraglich festgelegten Bedingungen für den Datenschutz- und die Datensicherheit eingehalten werden (vgl. Ziff. 4.9.2);

b) Datenschutz- und Datensicherheitsvorfälle und -probleme angemessen bearbeitet werden;

c) Änderungen der Dienstleistungen einem gelenkten Änderungsmanagement unterliegen.

4.11.2 Der oder die Datenschutz- und Datensicherheitsverantwortliche muss:

a) die Einhaltung der Datenschutz- und Datensicherheitsvorschriften durch die Gemeinschaft, durch die angeschlossenen Gesundheitseinrichtungen sowie durch Dritte (vgl. Ziff. 4.1) überwachen;

b) seine oder ihre Funktion fachlich unabhängig ausüben können;

c) über die zur Erfüllung seiner oder ihrer Aufgaben erforderlichen fachlichen Kompetenzen und Ressourcen verfügen;

d) die Kommunikation an die verantwortlichen Entscheidungsträger und weitere zu informierende Stellen sicherstellen.

Die Umsetzungsverantwortung für die nachstehenden Vorgaben ist unter Kapitel 8.4 festgehalten.

7.1 Nachweispflicht Gesundheitseinrichtungen

Vorgaben XAD

7.1.1 Die GE haben im Rahmen des Onboarding-Prozesses der XAD-SG eine Selbsteinschätzung bezüglich Maturität des Datenschutzes und der Datensicherheit zu machen.

7.1.2 Die DSDS-V XAD-SG definiert die Art und den Umfang der Nachweise zur Kontrolle der Einhaltung und der Umsetzung der Datenschutz- und Datensicherheitsanforderungen durch die Gesundheitseinrichtungen.

7.1.3 Die DSDS-V XAD-SG kann basierend auf dem Ergebnis der Selbsteinschätzung einer Gesundheitseinrichtung zusätzlich weitere Nachweise von den Gesundheitseinrichtungen einfordern.

7.1.4 Die DSDS-V GE ist verpflichtet, die Nachweise zur Kontrolle der Einhaltung der Datenschutz- und Datensicherheitsanforderungen der Gesundheitseinrichtung jährlich oder auf Anfrage an die DSDS-V XAD-SG zu übergeben.

7.1.5 Die Gesundheitseinrichtungen haben bei Bedarf an die DSDS-V XAD-SG folgende Nachweise zu liefern:

- Nachweis N00: Vertragseinhaltung (TOZ)
- Nachweis N01: Definition behandlungsrelevante Daten
- Nachweis N02: Dokumentation Prozess/Protokolle Notfallzugriff
- Nachweis N03: Dokumentation Konfiguration Endgeräte
- Nachweis N04: Dokumentation Patchmanagement
- Nachweis N05: Dokumentation Netzwerksicherheit
- Nachweis N06: Dokumentation Sicherheitsvorfälle
- Nachweis N07: Dokumentation Risikomanagement
- Nachweis N08: Reporting Sensibilisierung

7.2 Nachweispflicht Dritte

7.2.1 Die DSDS-V XAD-SG definiert die Art und den Umfang der Nachweise zur Kontrolle der Einhaltung und der Umsetzung der Datenschutz- und Datensicherheitsanforderungen durch Dritte. **Vorgaben XAD**

7.2.2 Dritte sind verpflichtet, die Nachweise zur Kontrolle der Einhaltung und der Umsetzung der Datenschutz- und Datensicherheitsanforderungen an die DSDS-V der XAD-SG zu übergeben.

7.2.3 Dritte haben an die DSDS-V XAD-SG folgende Nachweise zu liefern:

- Nachweis N00: Vertragseinhaltung (TOZ)
- Nachweis N02: Dokumentation Prozess/Protokolle Notfallzugriff
- Nachweis N04: Dokumentation Patchmanagement
- Nachweis N05: Dokumentation Netzwerksicherheit
- Nachweis N06: Dokumentation Sicherheitsvorfälle
- Nachweis N07: Dokumentation Risikomanagement
- Nachweis N08: Reporting Sensibilisierung
- Nachweis N09: Dokumentation Prozess Aufhebung EPD

7.3 Nachweispflicht Datenschutz- und Datensicherheitsverantwortung XAD

7.3.1 Die DSDS-V XAD-SG hat Nachweise zu liefern, damit die Gesamtverantwortung XAD-SG die Einhaltung und Umsetzung der gesetzlichen Anforderungen bei der Führung des DSDS-MS und der Überwachung der Einhaltung der Datenschutz- und Datensicherheitsanforderungen prüfen kann. **Vorgaben XAD**

7.3.2 Die DSDS-V XAD-SG hat an die Gesamtverantwortung XAD-SG folgende Nachweise zu liefern:

- Lieferobjekte DSDS-MS
- Katalog der Schutzobjekte
- Reporting Sensibilisierung
- Berichte über durchgeführte Penetration Tests
- Vorgaben an die Konfiguration von Endgeräten
- Liste Administratoren sicherheitsrelevanter Infrastrukturelemente
- Liste Lieferanten und Dienstleistungserbringer

7.4 Nachweispflicht Zentrale Dienste

7.4.1 Die Gesamtverantwortung XAD-SG hat an die DSDS-V XAD-SG folgende Nachweise zu liefern: **Vorgaben XAD**

- Nachweis N03: Dokumentation Konfiguration Endgeräte
- Nachweis N04: Dokumentation Patchmanagement
- Nachweis N05: Dokumentation Netzwerksicherheit
- Nachweis N06: Dokumentation Sicherheitsvorfälle
- Nachweis N08: Reporting Sensibilisierung
- Nachweis N09: Dokumentation Prozess Aufhebung EPD

8 Anhang

8.1 Referenzierte technische und organisatorische Zertifizierungsvoraussetzungen

Kapitel	TOZ
2.1 Datenschutz- und Datensicherheitsverantwortung	4.2.1, 4.11.1, 4.11.2
2.2 Datenschutz- und Datensicherheitsverantwortung GE	4.2.1
2.3 Datenschutz- und Datensicherheitsverantwortung von Lieferanten und Dienstleistungserbringern	4.9.1, 4.9.2, 4.9.3, 4.9,4, 2.4 b
2.4 Sicherheitsprozesse	4.2.1, 4.3.3
2.5 Vorgehen bei Verstössen	-
3.1 Definition behandlungsrelevante Daten	2.4 a
3.2 Verschlüsselung	2.5, 4.12, 4.13.1 d, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8, 3.2.9, 3.2.10
3.3 Demografische Patientensuche	2.9.19, 3.3.1
3.4 Erkennung von Anomalien	3.3, 4.3.2
3.5 Protokolldaten und Protokollierung	2.10, 4.2.1 c, 4.13.3
3.6 Umgang mit Testdaten	4.12.2 e
3.7 Gruppen GFP/HIP	1.5, 8.6.1
3.8 Katalog der Schutzobjekte	4.6.1
4.1 Sichere Konfiguration Endgeräte	2.2, 4.4.3, 4.5, 4.7.1 c, 4.7.2, 4.7.3
4.2 Schutz vor Schadsoftware	4.5.1
4.3 Authentisierung und Autorisierung	2.2, 4.8.1, 4.8.2 b, 4.8.2 c, 5.1.2 c, 11.1.2 c
4.4 Zertifikate	2.9.26
4.5 Lebenszyklus von Systemen	4.14.1
5 Netzwerk	4.15.2, 4.15.3, 4.15.4, 4.15.5, 4.16.1, 4.16.2
6 Sensibilisierung	4.2.2, 4.8.2, 5.1.2 a, 11.1.2 a
7 Berichtswesen und DokumentationNachweispflicht Gesundheitseinrichtungen	4.10, 4.11.2

8.2 Referenzierte Dokumente

Dokument Nr.	Titel	Version
[01]	DSDS-Policy	1.30

8.3 Abkürzungsverzeichnis

Abkürzung	Bedeutung
2FA	Zwei-Faktoren-Authentifizierung
Abs.	Absatz
Art.	Artikel
BAG	Bundesamt für Gesundheit
Bst.	Buchstabe
CA	Certification Authority
DSDS-MS	Datenschutz- und Datensicherheitsmanagementsystem
DSDS-Policy	Datenschutz- und Datensicherheitspolicy
DSDS-Richtlinie	Datenschutz- und Datensicherheitsrichtlinie
DSDS-V GE	Datenschutz- und Datensicherheitsverantwortung Gesundheitseinrichtung
DSDS-V XAD-SG	Datenschutz- und Datensicherheitsverantwortung der Zentralen Dienste der XAD-Stammgemeinschaft
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
EDI	Eidgenössisches Departement des Innern
EPD	Elektronisches Patientendossier
EPDG	Gesetzgebung Elektronisches Patientendossier (SR 816.1)
EPDV	Verordnung zum Elektronischen Patientendossier (SR 816.11)
GE	Gesundheitseinrichtung
GFP	Gesundheitsfachpersonen der Gesundheitseinrichtung
HIP	Gesundheits-Hilfspersonen der Gesundheitseinrichtung
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KIS	Klinikinformationssystem
PACS	Picture Archiving Communication System
XAD-SG	XAD-Stammgemeinschaft

TOZ	Technische- und Organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften

8.4 Geltungsbereich

Die nachfolgende Tabelle zeigt den Geltungsbereich pro Anforderungen und legt somit die Verantwortung fest.

Nr.	GE mit Portal-lösung	GE mit Integrations-paket S	GE mit Integrations-paket M	GE mit Integrations-paket L	Zentrale Dienste	DSDS-V XAD-SG	Kontakt-stellen	Identity Provider	Technik Provider	Weitere Dritte
2.1.1						x				
2.1.2						x				
2.1.3						x				
2.2.1	x	x	x	x						
2.2.2	x	x	x	x						
2.2.3	x	x	x	x						
2.2.4										
2.3.1								x	x	x
2.3.2								x	x	x
2.3.3								x	x	x
2.4 a						x				
2.4.1.1						x				
2.4.1.2	x	x	x	x		x	x	x	x	x
2.4.1.3						x				
2.4.1.4	x	x	x	x						
2.4.1.5	x	x	x	x						
2.4.1.6						x				
2.4.1.7						x				
2.4.1.8						x				
2.4.1.9									x	
2.4.1.10									x	
2.4.2.1					x					
2.4.2.2					x					
2.4.2.3					x					
3.1.1	x	x	x	x						
3.1.2		x	x	x					x	

Nr.	GE mit Portal-lösung	GE mit Integrations-paket S	GE mit Integrations-paket M	GE mit Integrations-paket L	Zentrale Dienste	DSDS-V XAD-SG	Kontakt-stellen	Identity Provider	Technik Provider	Weitere Dritte
3.2.2		x	x	x				x	x	x
3.2.3		x	x	x				x	x	x
3.2.4		x	x	x				x	x	x
3.2.5		x	x	x				x	x	x
3.2.6		x	x	x				x	x	x
3.2.7		x	x	x				x	x	x
3.2.8		x	x	x				x	x	x
3.2.9		x	x	x				x	x	x
3.2.10		x	x	x					x	
3.3.1									x	
3.4.1									x	
3.4.2									x	
3.4.3									x	
3.5.1		x	x	x						
3.5.2		x	x	x						
3.5.3		x	x	x						
3.5.4		x	x	x					x	
3.5.5		x	x	x					x	
3.6.1		x	x	x					x	
3.6.2		x	x	x					x	
3.7.1	x	x	x	x						
3.7.2	x	x	x	x						
3.7.3	x	x	x	x						
3.7.4	x	x	x	x						
3.8.1						x				
3.8.2						x				
3.8.3						x				
4.1.1	x	x	X	x	x		x		x	
4.1.2	x	x	X	x	x		x		x	
4.1.3	x	x	x	x	x		x		x	

Nr.	GE mit Portal-lösung	GE mit Integrations-paket S	GE mit Integrations-paket M	GE mit Integrations-paket L	Zentrale Dienste	DSDS-V XAD-SG	Kontakt-stellen	Identity Provider	Technik Provider	Weitere Dritte
4.1.4	x	x	x	x	x		x		x	
4.1.5	x	x	x	x	x		x		x	
4.1.6	x	x	x	x	x		x		x	
4.1.7	x	x	x	x	x		x		x	
4.2.1	x	x	x	x	x		x	x	x	x
4.2.2	x	x	x	x	x		x	x	x	x
4.2.3	x	x	x	x	x		x	x	x	x
4.2.4	x	x	x	x	x		x	x	x	x
4.3.1.1	x	x	x	x	x		x		x	
4.3.1.2		x	x	x					x	
4.3.2.1	x	x	x	x						
4.3.2.2	x	x	x	x						
4.3.2.3							x			
4.3.3.1	x	x	x	x	x		x		x	
4.3.3.2	x	x	x	x	x		x		x	
4.3.3.3	x	x	x	x	x		x	x	x	
4.4.1		x	x	x					x	
4.4.2		x	x	x					x	
4.4.3		x	x	x					x	
4.4.4		x	x	x					x	
4.4.5		x	x	x					x	
4.4.6		x	x	x					x	
4.4.7		x	x	x					x	
4.4.8		x	x	x					x	
4.5.1		x	x	x	x	x		x	x	x
4.5.2		x	x	x	x	x		x	x	
4.5.3		x	x	x	x	x		x	x	
4.5.4		x	x	x	x	x		x	x	
4.5.5						x				
4.6.1					x					x

Nr.	GE mit Portal-lösung	GE mit Integrations-paket S	GE mit Integrations-paket M	GE mit Integrations-paket L	Zentrale Dienste	DSDS-V XAD-SG	Kontakt-stellen	Identity Provider	Technik Provider	Weitere Dritte
5.1.1									x	
5.1.2		x	x	x						
5.1.3		x	x	x					x	
5.1.4								x	x	
5.1.5		x	x	x				x	x	
5.1.6		x	x	x				x	x	
6.1.1	x	x	x	x	x		x	x	x	
6.1.2	x	x	x	x	x		x	x	x	x
6.1.3	x	x	x	x			x			
6.1.4					x				x	x
7.1.1	x	x	x	x						
7.1.2						x				
7.1.3						x				
7.1.4	x	x	x	x						
7.1.5	x	x	x	x						
7.2.1						x				
7.2.2								x	x	x
7.2.3								x	x	x
7.3.1						x				
7.3.2						x				
7.4.1					x					

8.5 Glossar

Begriff	Bedeutung
Bearbeiten im Zusammenhang mit Daten	«Bearbeiten» bezieht sich gemäss DSG Art. 3 auf jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere auf das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.
EPD-Beteiligte	EPD-Beteiligte in diesem Dokument umfassen sämtliche vom organisatorischen Geltungsbereich tangierten Personen und Organisationen.
EPD-Daten	Als EPD-Daten verstehen sich alle behandlungsrelevanten Daten oder Dokumente, welche im EPD-Kontext durch Patienten gemeinsam mit seinem Behandelnden in das

	EPD publiziert werden sollen. Im EPD sollen alle wichtigen Dokumente, die für einen weiteren Behandlungsverlauf relevant sind, zur Verfügung stehen.
EPD-Systeme	Die EPD-Systeme umfassen sämtliche Systeme der Gemeinschaften und Stammgemeinschaften und/oder Gesundheitseinrichtungen gemäss EPDV-EDI, welche im Rahmen des elektronischen Patientendossiers sowie für den Zugriff auf das elektronische Patientendossier insbesondere Endgeräte eingesetzt werden. Der Begriff umfasst auch unterstützende Systeme, über die EPD-Daten bearbeitet (im Sinne des Art. 3 DSG) werden oder mit denen die Berechtigungsregeln der Gesundheitsfachpersonen und Hilfspersonen verändert werden können.
Portal	Der Begriff Portal umfasst in diesem Dokument ▪ das Zugangsportal für Patientinnen und Patienten, ▪ das Zugangsportal für Gesundheitsfachpersonen und Hilfspersonen und ▪ das Administrationsportal.
Risiko	Risiken ergeben sich aus der Eintrittswahrscheinlichkeit und einer Schadensauswirkung bei Eintritt eines Risikos, die für Bedrohungen geschätzt werden.
Sicherheitsvorfall	Sicherheitsvorfälle sind Ereignisse, welche die Vertraulichkeit, die Integrität oder die Verfügbarkeit der Daten beeinträchtigen.
Schwachstelle	Schwachstellen beziehen sich auf Mängel und Sicherheitslücken in Systemen, dessen Ausnutzung durch einen Angreifer den Schutzobjekten (Informationen, Daten, Anwendungen, Systeme und Prozesse) Schaden hinzufügt.