Datenschutz- und Datensicherheits-Policy der XAD-Stammgemeinschaft

Version / Datum	Freigegeben durch
V1.30 / 14.02.2020	GV XAD

XAD-Stammgemeinschaft

Metainformationen	
Version / Datum	Version 1.30 / 14.02.2020
Verteiler	XAD-Stammgemeinschaft

Versionshistorie	Datum	Bemerkung
V0.50	08.05.2019	Entwurf 1 zum Review
V0.60	17.06.2019	Einarbeitung Feedback aus dem Review
V0.70	18.09.2019	Abgabe des Dokuments zum Review
V0.80	25.09.2019	Einarbeitung des Feedbacks aus Review
V0.90	26.09.2019	Bereinigungsarbeiten Begriffe
V1.00	26.09.2019	Finale Fassung
V1.10	21.01.2020	Anpassung Gültigkeit
V1.20	06.02.2020	Anpassungen Review GL axsana
V1.23	31.01.2020	Review XAD und Überführung in xsana-Layout
V1.30	14.02.2020	Freigabe

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Ziel und Zweck

Die Datenschutz- und Datensicherheits-Policy (DSDS-Policy) der XAD-SG (XAD-SG) definiert die Grundsätze und den Aufbau des Datenschutz- und Datensicherheitsmanagementsystems (DSDS-MS) der XAD-SG sowie die geltenden Standards und Prozeduren für den Datenschutz und die Datensicherheit (DSDS) im Zusammenhang mit dem elektronischen Patientendossier (EPD). Dadurch wird mit der DSDS-Policy die Basis für ein gemeinsames Verständnis und die fortlaufende Verbesserung des zugehörigen Regelwerks gemäss der geltenden Gesetzgebung gelegt.

1.2 Geltungsbereich

Der Geltungsbereich der DSDS-Policy basierend auf den gesetzlichen Bestimmungen der Verordnung über das elektronischen Patientendossier des Bundes (EPDV) und der EPDV des Eidgenössischen Departement des Innern (EPDV-EDI) einschliesslich dessen Anhang 2 betreffend die technischen- und organisatorischen Zertifizierungsvoraussetzungen (TOZ) wird aus organisatorischer und technischer Perspektive festgelegt. Das Kriterium, ob ein System, eine Organisation oder deren Prozesse zum Geltungsbereich zählen, ist die Bearbeitung gemäss Art. 3 des Bundesgesetzes über den Datenschutz (DSG) von EPD-Daten durch die Organisation, durch ein System oder in einem Prozess.

Der Geltungsbereich der DSDS-Policy umfasst organisatorisch

- die XAD-Stammgemeinschaft, das heisst, die Zentralen Dienste und die ihr angeschlossenen Gesundheitseinrichtungen, deren Tochter- und Beteiligungsgesellschaften,
- Lieferanten, Dienstleister oder Partner (Dritte), die EPD-Daten im Sinne von Art. 3 DSG bearbeiten
- werden sowie Prozesse, bei denen EPD-Daten im Sinne von Art. 3 DSG bearbeitet werden.

Der Geltungsbereich der DSDS-Policy umfasst technisch

- die gesamten nach EPDV definierten Informatikmittel, 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 Gesundheitsfachpersonen (GFP) und Hilfspersonen (HIP) verändert werden können.

1.3 Abgrenzung

- Personen und Prozesse, die keine Verbindung zum EPD und den EPD-Daten haben, sind nicht Teil des Geltungsbereichs dieser DSDS-Policy.
- Primärsystem der Gesundheitseinrichtungen fallen nicht unter den Geltungsbereich der DSDS-Policy.

1.4 Änderungen

- Änderungen an der DSDS-Policy der XAD-SG können durch die Gesamtverantwortung XAD-SG und der Datenschutz- und Datensicherheitsverantwortung der XAD-SG (DSDS-V XAD-SG) beantragt werden.
- Änderungsanträge werden durch die DSDS-V XAD-SG beurteilt, mit der DSDS-Expertengruppe diskutiert und durch die Gesamtverantwortung der XAD-SG abgenommen. Bei positivem Entscheid wird die Änderung in die bestehende Dokumentation eingearbeitet.
- Die DSDS-Policy 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.

1.5 Kontrolle

Die DSDS-Policy wird einmal jährlich, durch die DSDS-V XAD-SG auf ihre Zweckmässigkeit und Aktualität überprüft. Verbesserungsvorschläge werden der Gesamtverantwortung der XAD-SG präsentiert und bei positivem Befinden gemäss dem in Kapitel 1.4 beschriebenen Prozess beantragt.

DSDS-Policy der XAD-SG stets dem aktuellen Stand der Technik und den geltenden Best Practice-Ansätzen, um dadurch einen vollumfänglichen und bestmöglichen Schutz zu gewährleisten. Dabei wird auf etablierte Ansätze gesetzt, sodass die DSDS-Policy, wenn möglich, nur alle zwei bis drei Jahre angepasst werden muss. Grundlegend richten sich die Anforderungen immer nach den gesetzlichen Grundlagen zum elektronischen Patientendossier (siehe Kapitel 1.7).

1.6 Inkrafttreten

Das vorliegende Dokument Datenschutz- und Datensicherheits-Policy der XAD-SG tritt per 26.09.2019 in Kraft.

1.7 Mitgeltende Dokumente

Typ	Name	Beschreibung
Gesetz	Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG)	Das EPDG ist seit dem 15. April 2017 in Kraft und regelt die Voraussetzungen für die Bearbeitung der Daten des EPD und legt die Massnahmen fest, die die Einführung, Verbreitung und Weiterentwicklung des EPD unterstützen.
	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 des EPD Anwendung findenden Vertraulichkeitsstufen und Zugriffsrechte, die Patientenidentifikationsnummer, die Aufgaben von Gemeinschaften und Stammgemeinschaften, die einzusetzenden Identifikationsmittel, die Akkreditierung, die Zertifizierung sowie die Abfrage-dienste.
	Verordnung vom 22. März 2017 des Eidgenössischen Departements des Innern über das elektronische Patientendossier (EPDV-EDI)	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), Evaluation und Forschung (Anhang 6), Mindestanforderungen an das Personal, technische und organisatorische Zertifizierungsvoraussetzungen für Herausgeber von Identifikationsmitteln (Anhang 7 und Anhang 8) sowie Anforderungen an die Metadaten für den Dienst zur Abfrage von Gesundheitseinrichtungen und Gesundheitsfachpersonen (Anhang 9).
	Anhang 2 der Verordnung des EDI vom 24. Juni 2019 über das elektronische Patientendossier	Der Anhang 2 der Verordnung des EDI vom 24. Juni 2019 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 DSDS-MS bietet die «Umsetzungshilfe Datenschutz und Datensicherheit im EPD» von eHealth-Suisse.

Tabelle 1: Mitgeltende Dokumente

2 Rollen und Verantwortlichkeiten

Innerhalb der XAD-SG müssen bestimmte Aufgaben, Rollen und Verantwortlichkeiten gemäss den gesetzlichen Vorgaben wahrgenommen werden. Die Rollen innerhalb (blau und hellblau schattiert) sowie ausserhalb (grau schattiert) der XAD-SG sind der Abbildung 1: Rollen im Kontext des EPD zu entnehmen. Die XAD-SG besteht demzufolge aus der Gesamtheit der Rollen und der dazugehörigen Organisationen (Zentrale Dienste und Gesundheitseinrichtungen).

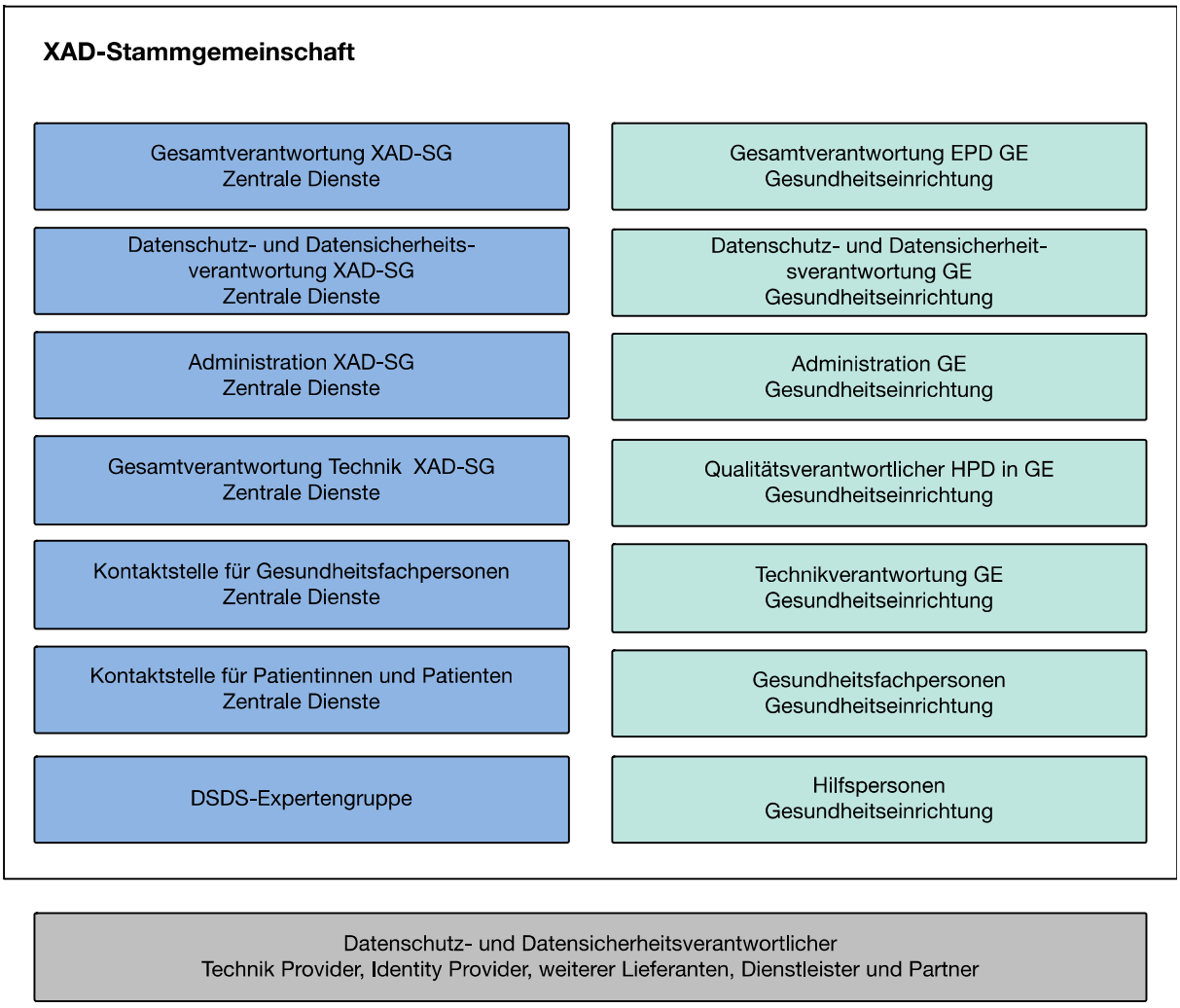

Abbildung 1: Rollen im Kontext des EPD

In den folgenden Unterkapiteln werden die Aufgaben und Verantwortlichkeiten betreffend den Datenschutz und die Datensicherheit der Rollen im Kontext des EPD erläutert.

2.1 Zentrale Dienste

Gesamtverantwortung XAD-SG

Die Gesamtverantwortung XAD-SG ist für den Betrieb der XAD-SG verantwortlich und schafft die Rahmenbedingungen innerhalb der XAD-SG für die Umsetzung und Nachhaltung der Datenschutz- und Datensicherheitsthematik über die ganze Organisation der XAD-SG hinweg. Die Gesamtverantwortung XAD-SG ist Entscheidungsträger und trägt die damit einhergehende Hauptverantwortung für Datenschutz- und Datensicherheit in der XAD-SG.

Datenschutz- und Datensicherheitsverantwortung XAD-SG

Die Gesamtverantwortung XAD-SG wird durch einen Mitarbeitenden der Zentralen Dienste der XAD-SG oder durch einen beauftragten Dritten besetzt, wer in seiner Funktion unabhängig gegenüber Personen und Rollenträgern, die von der Sicherheit ihrer Schutzobjekte abhängig sind, auftritt.

Die Aufgaben und Verantwortlichkeiten der Rolle der Datenschutz- und Datensicherheitsverantwortung XAD-SG umfassen das Führen des DSDS-MS der XAD-SG, die Überwachung der Einhaltung der Datenschutz- und Datensicherheitsvorschriften sowie den Erlass von Vorgaben und Umsetzungsempfehlungen für die EPD-Beteiligten gemäss dem Geltungsbereich (s. Kapitel 1.2 Geltungsbereich).

Gesamtverantwortung Technik XAD-SG

Mitarbeitende der Zentralen Dienste oder beauftragte Dritte, welche für die Verwaltung, den Auf- und Ausbau sowie den Betrieb der EPD-Systeme der XAD-SG zuständig sind, tragen die Verantwortung für sämtliche EPD-Systeme (logisch und/oder physisch) und haben die nachfolgenden Aufgaben:

- Umsetzung der Vorgaben des DSDS-MS bei den unterstellten EPD-Systeme.
- Entwicklung und Implementierung von Instandhaltungsplänen für die unterstellten EPD-Systeme.
- Aktualisierung des Dokuments «Inventar der Informatikinfrastruktur».

Administration XAD-SG

Mitarbeitende der Zentralen Dienste oder beauftragte Dritte, welche für die Verwaltung von Gesundheitseinrichtungen und der Administratorenrollen zuständig sind. Zur Administration XAD-SG zählt auch die Gesamtverantwortung Administration XAD-SG als Vorsteherin. Die Rollen tragen die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten.

Kontaktstelle für Gesundheitsfachpersonen

Diese Kontaktstelle unterstützt die Gesundheitsfachpersonen angeschlossener Gesundheitseinrichtungen beim Umgang mit dem EPD und Einhaltung von Vorgaben des DSDS-MS. Sie trägt die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten.

Kontaktstelle für Patientinnen und Patienten

Diese Kontaktstelle unterstützt die Patientinnen und Patienten beim Umgang mit dem elektronischen Patientendossier. Sie trägt die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten.

DSDS-Expertengruppe

Die DSDS-Expertengruppe setzt sich aus maximal fünf Vertretern der Gesundheitseinrichtungen zusammen. Die DSDS-Expertengruppe ist beratend tätig und reflektiert die organisatorische Sicht einer Gesundheitseinrichtung und wirkt bei der Beurteilung und Einschätzung betreffend die Umsetzbarkeit der Vorgaben des DSDS-MS der XAD-SG sowie beim Review und der Diskussion der Vorgabendokumente des DSDS-MS mit.

2.2 Technik und Identity Provider, weitere Dritte

Die Rolle des Datenschutz- und Datensicherheitsverantwortlichen beim Technik Provider, Identity Provider oder bei weiteren Lieferanten, Dienstleister oder Partner (beispielsweise für Dossiereröffnungsstellen) umfasst

- die Einhaltung der Vorgaben des DSDS-MS der XAD-SG und
- die Aktualisierung des Dokuments «Inventar der Informatikinfrastruktur».

2.3 Gesundheitseinrichtung

Gesamtverantwortung EPD GE

Die Gesamtverantwortung EPD GE schafft die Rahmenbedingungen innerhalb der GE für die Umsetzung und Nachhaltung der Datenschutz- und Datensicherheitsthematik betreffend das EPD über die ganze Organisation der GE hinweg. Die Gesamtverantwortung EPD GE ist Entscheidungsträger und trägt die damit einhergehende Hauptverantwortung für den Datenschutz- und Datensicherheit betreffend das EPD in der GE. Die Gesamtverantwortung GE ernennt die Rolle der Datenschutz- und Datensicherheitsverantwortung GE und besetzt sie durch einen Mitarbeitenden der GE oder durch einen beauftragten Dritten, der in seiner Funktion unabhängig gegenüber Personen und Rollenträgern, die von der Sicherheit ihrer Schutzobjekte abhängig sind, auftritt.

Datenschutz- und Datensicherheitsverantwortung GE

Die Aufgaben und Verantwortlichkeiten der Rolle der Datenschutz- und Datensicherheitsverantwortung GE umfassen die Überwachung der Einhaltung der Datenschutz- und Datensicherheitsvorschriften in der GE, den Erlass von Umsetzungsempfehlungen für die eigene GE und die Begleitung der Umsetzung. Die DSDS-V GE muss ihre Funktion fachlich unabhängig ausüben können. Zu ihren Aufgaben zählen

- die Sicherstellung der Umsetzung der Vorgaben des DSDS-MS bei allen EPD-Systeme der GE
- die Entwicklung und Implementierung von Instandhaltungsplänen für die EPD-Systeme der GE und
- die Aktualisierung des Dokuments «Inventar der Informatikinfrastruktur» betreffend der GE.

Administration GFP und HIP in GE

Mitarbeitende der angeschlossenen Gesundheitseinrichtung, welche für die Administration und Verwaltung der GFP, HIPs und Gruppen zuständig sind. Sie übernehmen die Verwaltung der Eintritte und Austritte, die Stammdatenpflege sowie die Verwaltung von Gruppen sowie die Zuweisung von HIPs zu GFPs. Zur Administration GFP und HIP in GE zählt auch die Rolle Verantwortung Administration GFP und HIP in GE als Trägerin der Verantwortung für die oben aufgeführten Aufgaben. Die Rollen tragen die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten

Qualitätsverantwortlicher Health Provider Directory (HPD) in GE

Die Stammgemeinschaft ist verpflichtet, für die von ihr registrierten Daten im Dienst zur Abfrage der Gesundheitseinrichtungen und Gesundheitsfachpersonen (HPD national) die Personen zu nennen, die für die Aktualität und Korrektheit der Angaben verantwortlich sind. Die Rolle trägt die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten.

Technikverantwortung GE

Die Technikverantwortung GE oder beauftragte Dritte, welche für die Verwaltung und die Administration der EPD-Systeme der GE zuständig sind, tragen die Verantwortung für sämtliche EPD-Systeme der GE (logisch und/oder physisch) und haben innerhalb der GE die nachfolgenden Aufgaben:

- Umsetzung der Vorgaben des DSDS-MS bei den unterstellten EPD-Systeme.
- Entwicklung und Implementierung von Instandhaltungsplänen für die unterstellten EPD-Systeme.
- Aktualisierung des Dokuments «Inventar der Informatikinfrastruktur».

Gesundheitsfachpersonen der Gesundheitseinrichtung (GFP)

Mitarbeitende der Gesundheitseinrichtung, welche der ärztlichen Schweigepflicht unterstehen und Einsicht in die EPD-Daten ihrer Patienten haben und Daten darin bearbeiten. Sie tragen die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten.

Hilfspersonen der Gesundheitseinrichtung (HIP)

Mitarbeitende der Gesundheitseinrichtungen, welche der ärztlichen Schweigepflicht unterstehen, und im Namen von GFPs Einsicht in die EPD-Daten von Patienten haben und Daten darin bearbeiten können. Sie tragen die Verantwortung, sich an die Vorgaben des DSDS-MS bei der Bearbeitung von EPD-Daten zu halten.

3 Aufbau des Datenschutz- und Datensicherheitsmanagementsystems

Das DSDS-MS ist Bestandteil des SGMS. Die Basis für den Aufbau des DSDS-MS der XAD-SG bilden die gesetzlichen Vorgaben. Die relevanten Vorgaben des DSDS-MS leiten sich von den gesetzlichen Vorgaben ab und sind für die EPD-Beteiligten gemäss dem Geltungsbereich (s. Kapitel 1.2 Geltungsbereich) verbindlich. Ausnahmen sind schriftlich dokumentiert.

Das Reglement DSDS gemäss Anschlussvertrag umfasst sämtliche Vorgabendokumente (Policy, Richtlinie, Weisungen, Konzepte und Checklisten) des DSDS-MS. Die Vorgabendokumente sind im DSDS-MS hierarchisch auf drei Ebenen organisiert. Die Ebenen unterscheiden sich durch die Merkmale Zuständigkeit und Entscheidungskompetenzen, typische Geltungsdauer, Geltungsbereich, Detaillierungsgrad und Inhalt.

Die übergeordnete DSDS-Policy (Ebene 1) bildet das Fundament des DSDS-MS und enthält die grundsätzliche Zielsetzung, Grundsätze sowie die Rahmenbedingungen des Datenschutzes und der Datensicherheit.

Die daraus abgeleitete DSDS-Richtlinie (Ebene 2) enthält die Mindestanforderungen an den Datenschutz und die Datensicherheit zur Implementierung der DSDS-Policy. Die Einhaltung dieser Anforderungen kann durch die XAD-SG überprüft werden.

Ergänzend zur DSDS-Policy und Richtlinie kann die XAD-SG Ausführungsbestimmungen wie zum Beispiel Weisungen, Konzepte und Checklisten (Ebene 3) herausgeben. Die Ausführungsbestimmungen dienen als Orientierungshilfe zur Umsetzung der Anforderungen aus der DSDS-Policy und der DSDS-Richtlinie und bezwecken unter anderem die Reduzierung von Fehlern auf proaktive Art und Weise.

In den entsprechenden Dokumenten leiten sich die Anforderungen und Massnahmen, die in Bezug auf die Risiken zu ergreifen sind, von der EPDV-EDI sowie deren Anhang 2 und der internationalen Informationssicherheitsnorm ISO/IEC 27000x ab.

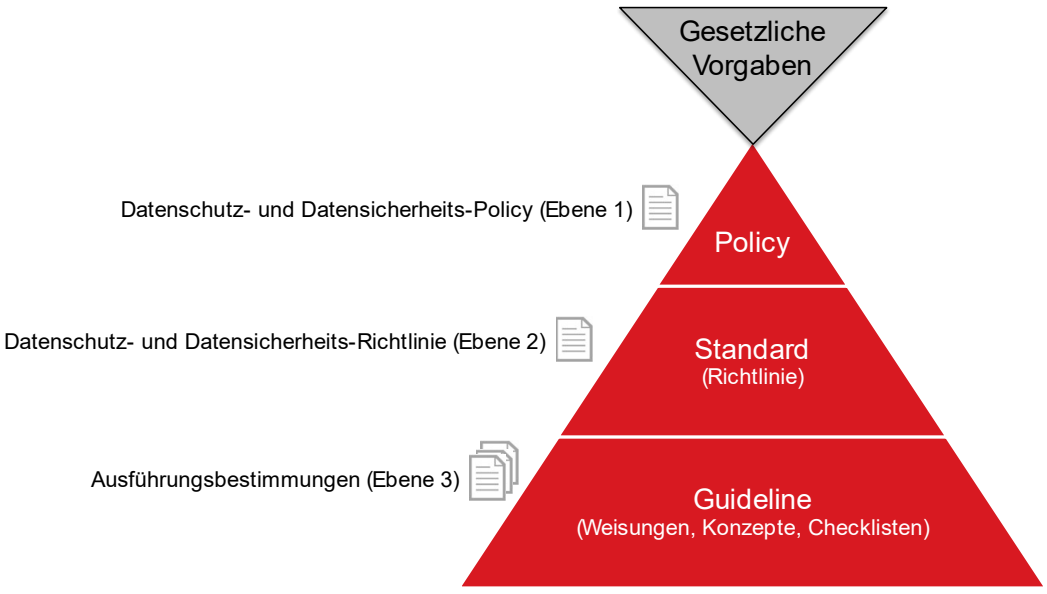

Abbildung 2: Aufbau des Datenschutz- und Datensicherheitsmanagementsystem

4 Grundsätze Datenschutz und Datensicherheit

Die DSDS-Policy hält nachfolgend fest, welche Anforderungen die EPD-Beteiligten gemäss dem Kapitel 1.2 Geltungsbereich zwingend erfüllen müssen und welche Vorgaben für die gesamte Lieferkette der XAD-SG gelten respektive geltend gemacht werden.

4.1 Vertragsgestaltung

Verträge der gesamten Lieferkette, welche neu erstellt, verlängert oder verändert werden, müssen die Anforderungen dieser DSDS-Policy, der DSDS-Richtlinie und der Ausführungsbestimmungen zwingend erfüllen.

Insbesondere sind bei Verträgen mit Dritten gemäss dem Geltungsbereich (s. Kapitel 1.2 Geltungsbereich) die folgenden Punkte einzuhalten:

- Die Pflicht des Technik Providers, Identity Providers oder der weiteren Lieferanten, Dienstleister oder Partner die Daten nur zu den Zwecken zu bearbeiten, die mit der XAD-SG vertraglich vereinbart wurden.
- Die Pflicht des Technik Providers, Identity Providers oder der weiteren Lieferanten, Dienstleister oder Partner zur Einhaltung der Datensicherheit gemäss den gesetzlichen Bedingungen des EPDG und dessen Ausführungsvorschriften (s. Kapitel 1.7 Mitgeltende Dokumente).
- Die Pflicht des Technik Providers, Identity Providers oder der weiteren Lieferanten, Dienstleister oder Partner zur Beachtung der ärztlichen Schweigepflicht bei der Einsicht oder der Bearbeitung von medizinischen Daten (Geheimhaltungsvereinbarung).
- Die Informationspflicht bei allfälligen Verstössen gegen die geltende Gesetzgebung und/oder vertraglich festgelegten Standards und Richtlinien im Rahmen des EPDG oder des DSG.
- Gewährung des Kontrollrechts der XAD-SG.
- Gewährung der Ausübung des Kontrollrechts durch einen von der XAD-SG beauftragten Dritten.

Die erwähnten Punkte sind auch bei Verträgen mit weiteren Dritten wie zum Beispiel Subunternehmer oder Subdienstleister von Dritten gemäss dem Geltungsbereich (s. Kapitel 1.2 Geltungsbereich) einzuhalten.

Das Kontrollrecht der XAD-SG bezieht sich sowohl auf Gesundheitseinrichtungen als auch auf Dritte gemäss dem Geltungsbereich (s. Kapitel 1.2 Geltungsbereich). Es ermöglicht dedizierte Überprüfungen der Einhaltung der Vorgaben des DSDS-MS durch die Zentralen Dienste der XAD-SG oder einen selektierten Partner durchführen zu lassen. Die Ergebnisse dieser Überprüfung werden dokumentiert und rapportiert. Auf der Basis dieses Berichts kann einer Gesundheitseinrichtung der Zugang zur EPD-Plattform der XAD-SG entzogen werden.

4.2 Fristen zur Umsetzung

Sollten zwischen dem geforderten und dem effektiven Sicherheitsniveau Diskrepanzen identifiziert werden, sind Übergangsprozesse zu definieren, damit die festgestellten Sicherheitslücken innert nützlicher Frist beseitigt werden. Die entsprechende Frist für die Behebung der Diskrepanz wird schriftlich festgehalten und der Gesamtverantwortung XAD-SG zur Beurteilung des weiteren Vorgehens vorgelegt.

4.3 EPD-Schutzziele

Alle Daten innerhalb der EPD-Systeme (logisch und/oder physisch) müssen gemäss den gesetzlichen Vorgaben der Anforderungen an Gemeinschaften nach Anhang 2 der EPDV-EDI geschützt werden (s. dazu auch Kapitel 1.7 Mitgeltende Dokumente). Dadurch wird beabsichtigt, die Zertifizierung zur Stammgemeinschaft gemäss den TOZ-Vorgaben unter Berücksichtigung eines verhältnismässigen Einsatzes von Informatikmitteln, Personal und anderer Ressourcen zu jedem Zeitpunkt aufrecht erhalten zu können.

4.4 Ressourcen

Für die zeitgerechte Umsetzung der Massnahmen, die sich aus der DSDS-Policy und den zugehörigen Standards (vgl. Kapitel 3 Aufbau des Datenschutz- und Datensicherheitsmanagementsystems) ergeben, sind ausreichend personelle und materielle Mittel zur Verfügung zu stellen. Alle Massnahmen, die sich aus der DSDS-Policy, der DSDS-Richtlinie und den Ausführungsbestimmungen ableiten lassen, werden priorisiert, terminiert und fristgerecht umgesetzt.

5 Berichtwesen

Die XAD-SG ist gesetzlich dazu verpflichtet ein Berichtswesen zum Bereich Datenschutz- und Datensicherheit zu etablieren, um im stetigen Informationsaustausch zur Sicherheit der vorhandenen EPD-Daten von Patientinnen und Patienten zu sein.

5.1 Datenschutz- und Datensicherheits-Jahresbericht

Einmal pro Jahr muss ein detaillierter Datenschutz- und Datensicherheitsjahresbericht durch die Zentralen Dienste XAD-SG erstellt und den angeschlossenen Gesundheitseinrichtungen zugestellt werden. Dieser beinhaltet die folgenden Themen:

- Rückblick auf Berichtsperiode
  - zu relevanten Entwicklungen in der Gesetzgebung
  - zu organisatorischen und technologischen Entwicklungen und Veränderungen innerhalb und ausserhalb der XAD-SG sowie
  - zu Risiken, Sicherheitsvorfällen, Kontrollen und daraus entstandenen Massnahmen.
  - Überprüfung des Inventars der Informatikinfrastruktur
- Ausblick auf bevorstehende Berichtsperiode
  - über die anstehenden Herausforderungen gemäss der Risikoanalyse und
  - über die geplanten und/oder werden bereits umgesetzten Massnahmen und Aktionen.

5.2 Organisatorisch und technologische Anpassungen (EPDV Art. 36)

Grössere organisatorische und/oder technologische Änderungen müssen jeweils proaktiv kommuniziert werden. Dazu gehören personelle Änderungen wie die Ernennung eines Datenschutz- und Datensicherheitsbeauftragten oder auch die Zusammenarbeit mit Dritten.

Diese Anforderung betrifft sowohl die Kommunikation der einzelnen Gesundheitseinrichtungen an die Zentralen Dienste der XAD-SG als auch die Kommunikation der Zentralen Diensten der XAD-SG gegenüber den Gesundheitseinrichtungen und dem Bundesamt für Gesundheit (BAG) als übergeordnete Bundesstelle.

5.3 Sicherheitsvorfälle (EPDV Art. 12)

Sollte es zu Sicherheitsvorfällen innerhalb der XAD-SG oder in der gesamten Lieferkette kommen, die einen Zusammenhang mit dem elektronischen Patientendossier haben, so müssen diese kommuniziert werden. Die Art des Vorfalls und dessen Tragweite werden als Kriterien zur Bestimmung, welche Stakeholder in diese Kommunikation eingebunden werden müssen, herangezogen. Generell gilt es, solche Ereignisse immer möglichst zeitnahe entsprechend dem aktuellen Wissens- und Kenntnisstand zu adressieren.

Diese Anforderung betrifft die Kommunikation der einzelnen Gesundheitseinrichtungen an die Zentralen Dienste der XAD-SG als auch die Kommunikation der Zentralen Dienste der XAD-SG gegenüber den Gesundheitseinrichtungen, dem BAG oder gar der Öffentlichkeit, sollte es sich um eine grobe Verletzung des Bundesgesetzes über den Datenschutz handeln.

6 Anhang

6.1 Abkürzungsverzeichnis

Abkürzung	Bedeutung
Abs.	Absatz
Art.	Artikel
BAG	Bundesamt für Gesundheit
Bst.	Buchstabe
DSDS	Datenschutz- und Datensicherheit
DSDS-Expertengruppe	Datenschutz- und Datensicherheit-Expertengruppe
DSDS-MS	Datenschutz- und Datensicherheitsmanagementsystem
DSDS-Policy	Datenschutz- und Datensicherheits-Policy
DSDS-V GE	Datenschutz- und Datensicherheitsverantwortung Gesundheitseinrichtung
DSDS-V XAD-SG	Datenschutz- und Datensicherheitsverantwortung Zentrale Dienste der SG XAD
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
EDI	Eidgenössisches Departement des Innern
EPD	Elektronisches Patientendossier
EPDG	Bundesgesetz über das elektronische Patientendossier (SR 816.1)
EPDV	Verordnung über das elektronischen Patientendossier (SR 816.11)
GE	Gesundheitseinrichtung
GFP	Gesundheitsfachpersonen
HIP	Hilfspersonen
HPD	Health Provider Directory
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
s.	siehe
TOZ	Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften (SR 816.111 Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier)
vgl.	vergleiche
XAD-SG	XAD-Stammgemeinschaft

6.2 Glossar

Begriff	Bedeutung
EPD-Beteiligte	EPD-Beteiligte in diesem Dokument umfasst sämtliche vom organisatorischen Geltungsbereich tangierten Personen und Organisationen.
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.
Dritte	Dritte wird in diesem Dokument stellvertretend für Lieferanten, Dienstleister oder Partner verwendete.
EPD-Daten	Als EPD-Daten verstehen sich alle behandlungsrelevanten Daten (medizinische 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.
Lieferkette	Die gesamte Lieferkette der XAD-SG im Kontext des EPD umfasst die XAD-SG (Zentrale Dienste und angeschlossene Gesundheitseinrichtungen) sowie Dritte (Technik Provider, Identity Provider und weitere Lieferanten, Dienstleister und Partner) einschliesslich Unterlieferanten respektive -dienstleister von Dritten oder angeschlossenen Gesundheitseinrichtungen.
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.

Änderungsnachverfolgung

Datum	Wer	Beschluss / Änderung
22.05.2019	D. Böhringer und A. Hermann	Aufnahme DSDS-Board (Name geändert auf DSDS-Expertengruppe) die als beratendes Gremium bestehend aus Vertretern der GE bei Änderungen und/oder beim Aufbau am DSDS-Framework miteinbezogen werden.
22.05.2019	D. Böhringer und A. Hermann	Kein Beschlussrecht / Genehmigungsrecht betreffend die Änderungen und/oder den Aufbau des DSDS-Framework durch GE.
20.09.2019	D. Böhringer, A. Lengen, C. Morales und M. Schoch	Inhaltliche Abnahme des Dokuments DSDS-Policy der XAD-SG. Anpassung der Rolle Dossiereröffnungsstellen. Sie gehören nicht zu den Rollen der XAD-SG und GE, sondern fallen unter Dritte (Outsourcing). Das Kontrollrecht der XAD-SG kann auch durch einen durch die XAD-SG beauftragten Dritten ausgeübt werden. Anpassung der Rollenbeschreibung Administration XAD-SG.
24.09.2019	M. Winkler, C. Morales und M. Schoch	Übernahme der nachfolgenden Begriffe mit den folgenden Abkürzungen: XAD-Stammgemeinschaft (XAD-SG), Gesamtverantwortung XAD-SG, Datenschutz- und Datensicherheitsverantwortung XAD-SG (DSDS-V XAD-SG), Gesamtverantwortung Technik XAD-SG und Administration XAD-SG. Beschluss, dass DSDS-Expertengruppe zur XAD-Stammgemeinschaft gehört. Übernahme der folgenden Begrifflichkeiten: **EPD-Daten** steht für sämtliche behandlungsrelevanten respektive medizinische Daten. **EPD-Informatikmittel** (Name auf EPD-Systeme geändert) umfasst den gesamten technischen Scope. **EPD-Akteure** wird durch EPD-Beteiligte ersetzt, da der Begriff EPD-Akteur bereits besetzt ist.
31.01.2020	D. Misteli, A. Lengen, M. Winkler und C. Morales	Anpassung diverse Begriffe und Formulierungen. Anpassung Datum Inkrafttreten. Übernahme neues xsana Layout.