Datenschutzweisung

Kantonsspital Baden AG, Baden

01.08.2021

Inhaltsverzeichnis

Änderungsprotokoll

Version, Datum	Status	Autor	Freigabe	Beschreibung
0.1, 18.12.2013	Entwurf	Swiss Infosec AG	-	Finale Version
1.0, 2.6.2014	Entscheid	Arbeitsgruppe	2.6.2014	Beschlossen durch Geschäftsleitung
2.0, 1.1.2020	Version 2	Leitung L&C	27.1.2020	Aktualisierung
3.0, 1.8.2021	Version 3	Leitung L&C	21.8.2021	Aktualisierung

Datenschutzweisung

1 Einführung

1.1 Zweck und Umfang

Die vorliegende Weisung definiert Vorgaben für das Bearbeiten von Personendaten über Patientinnen und Patienten, Mitarbeitende, Stellenbewerber/innen, Partner und Lieferanten innerhalb der Kantonsspital Baden AG (nachfolgend KSB genannt). Dabei sollen missbräuchliche Datenbearbeitungen und Verletzungen von Persönlichkeitsrechten verhindert werden.

Die Datenschutzweisung stellt das Hauptdokument zum Datenschutz dar. Sie enthält Vorgaben für alle Mitarbeitenden des KSB, die personenbezogene Daten gemäss Kap. 1.2 bearbeiten.

1.2 Geltungsbereich

Die Datenschutzweisung gilt für alle Mitarbeitenden des KSB. Sie ist für jede Bearbeitung von Personendaten verbindlich.

Das Bearbeiten von Personendaten umfasst jeden Umgang mit personenbezogenen Daten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten. Dabei handelt es sich insbesondere um das Bearbeiten von

- Patientendaten
- Personaldaten von internen und externen Mitarbeitenden, inklusive Daten über Stellenbewerber und ehemalige Mitarbeitende
- Administrative Daten über Partner und Lieferanten, soweit Personendaten betroffen sind.

Der Schutz umfasst alle personenbezogenen Daten, die auf Papier oder in digitaler Form festgehalten sind oder mündlich geäussert werden.

Für diese Weisung trägt die von der Geschäftsleitung ernannte Datenschutzbeauftragte die Dokumentenverantwortung.

1.3 Definitionen und Abkürzungen

Die folgenden Definitionen und Abkürzungen werden in der Datenschutzweisung verwendet.

Definition / Abkürzung	**Beschreibung**
Bearbeiten von Personendaten	Das Bearbeiten von Personendaten umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten.
Bearbeitungsreglement	Bearbeitungsreglemente müssen für automatisierte Datensammlungen, die besonders schützenswerte Daten und Persönlichkeitsprofile enthalten oder Dritten zugänglich gemacht werden, erstellt werden.
Bekanntgabe von Personendaten	Bekanntgeben ist jedes Zugänglichmachen von Personendaten, wie das Einsichtgewähren, Auskunftgeben, Weitergeben oder Veröffentlichen.

Definition / Abkürzung	Beschreibung
Besonders schützenswerte Personendaten	Besonders schützenswerte Personendaten sind Angaben, bei denen aufgrund ihrer Bedeutung, des Zusammenhangs, Zwecks oder der Art der Bearbeitung, der Datenkategorie oder anderer Umstände eine besondere Gefahr einer Persönlichkeitsverletzung besteht (§ 3 Abs. 1 lit. k IDAG[1]), wie a) die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit; b) den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand; c) Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung; d) polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen.
Besondere Patientengruppen	Darunter fallen Personalarztpatienten (Patienten der Personalärzte und Personalärztinnen), Mitarbeitende als KSB-Patienten (Mitarbeitende, die das KSB als behandelndes Spital wählen) und VIPs (Patienten, die anonym bleiben möchten). Diese Daten sind besonders zu schützen, der Zugriff gegenüber Mitarbeitenden des KSB ist auf das absolut Notwendige einzuschränken.
Dateneigner	Für Informationen, insbes. eine Datensammlung, verantwortliche Funktion innerhalb des KSB. Der Dateneigner klassifiziert und inventarisiert diese, erstellt nach Bedarf ein Bearbeitungsreglement, definiert datenschutzrechtliche Anforderungen zu ihrem Schutz, bestimmt die zum Bearbeiten der Daten befugten Personen und deren Zugriffrechte.
Datensammlung	Unter Datensammlung ist jeder Bestand von Personendaten über mehr als eine Person zu verstehen, der so aufgebaut ist, dass die Daten nach betroffenen (natürlichen und juristischen) Personen erschliessbar sind, z.B. über Namen, Mitarbeiter- oder andere Ordnungsnummern. Beispiele von Datensammlungen sind: Karteien, Archive, Listen, Adressbestände usw. Es spielt keine Rolle, ob Datensammlungen in Form von Papier-Datensammlungen existieren oder elektronisch gespeichert sind. Werden Daten aus solchen Datensammlungen herausgezogen und einem eigenständigen Zweck zugeführt, liegt eine neue Datensammlung vor.
Patientendaten	Unter Patientendaten werden alle über den Patienten vorhandenen Informationen im Spital verstanden, dies umfasst neben administrativen Daten auch medizinische Informationen (Falldaten).

[1] Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau, siehe Kap. 8 der Weisung.

Definition / Abkürzung	Beschreibung
Personendaten	Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen, bzw. dieser zugeordnet werden können. Beispiele: Name, Adresse, Nationalität, AHV-Nr., Geburtsdatum, Arbeitsort, Ausbildung, Betreibungen, Beruf, finanzielle Situation, Konfession, Sprache, usw. Personendaten sind auch Bilder, Grafiken, Fotografien etc. Es genügt, dass Personendaten, ohne einen Namen zu nennen, einer bestimmten Person zugeordnet werden können.
Persönlichkeitsprofil	Ein Persönlichkeitsprofil ist eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch ausserberufliche Beziehungen und Tätigkeiten, die ein Gesamtbild oder ein wesentliches Teilbild der betreffenden Person ergeben. Menge und Inhalt der Daten ist also entscheidend. Beispiele von Persönlichkeitsprofilen sind: Graphologisches Gutachten, Assessment Berichte, Bewerbungsdossiers, Personaldossiers.
Stammdaten	Daten, die selten oder nie ändern, z.B. Adressen von Ärzten, Krankenkassen und Lieferanten, PLZ, Kostenstellen, Kontenrahmen.

1.4 Fragen und Meldungen zum Datenschutz

Bestehen Unklarheiten zur Bearbeitung oder der Weitergabe von Personendaten kann der Mitarbeitende die Datenschutzbeauftragte kontaktieren. Die Datenschutzbeauftragte ist die zentrale Anlaufstelle für Fragen des Datenschutzes und wird aktiv unterstützt durch die Geschäftsleitung des KSB.

1.5 Überwachung und Auditing

Die Erfüllung der intern festgelegten Datenschutzbestimmungen wird durch Sicherheitskontrollen, Systemüberwachungen sowie durch regelmässige interne und externe Audits überprüft.

2 Genereller Umgang mit Personendaten

2.1 Grundsätze

Die Mitarbeitenden des KSB beachten bei der Bearbeitung von Personendaten folgende Grundsätze:

Zweck	Personendaten dürfen grundsätzlich nur zum Zweck, zu welchem sie beschafft werden, bearbeitet werden, siehe § 11 IDAG (Zweckbindung).
Legitimation	Personendaten werden im KSB zur Erfüllung von gesetzlichen Aufgaben bearbeitet. Die Ermächtigung zur Bearbeitung von Personendaten ist durch verschiedene Rechtsgrundlagen gegeben, siehe § 8 IDAG (Grundsatz).
Beschaffung	Die Beschaffung der Daten erfolgt auf folgende Arten: • Rechtmässig, nach Treu und Glauben und verhältnismässig. Ist die gesetzliche Grundlage der Beschaffung nicht ersichtlich, ist der Zweck der Datenbearbeitung anzugeben, siehe § 13 IDAG (Informationspflicht).
Verhältnismässigkeit	Personendaten werden nur gemäss dem oben genannten Zweck bearbeitet. • Für den Zugriff auf Personendaten gilt das Prinzip „Need to Know“, das auch die Grundlage für das Benutzer- und Rollenkonzept bildet. • Personendaten werden nur solange bearbeitet, wie es die gesetzlichen Grundlagen erlauben. Das Prinzip der Datenvermeidung und Datensparsamkeit ist zu beachten, insbesondere beim Einsatz von Informatiksystemen, siehe § 9 IDAG (Verhältnismässigkeit).
Transparenz	Datensammlungen werden inventarisiert. Das Inventar dient der Ordnungsmässigkeit und der Gewährleistung der Auskunftsbereitschaft, siehe § 23 IDAG (Grundsatz).
Datenrichtigkeit	Der Dateneigner kontrolliert regelmässig, ob Personendaten richtig, vollständig und aktuell sind. Die Korrektheit der Daten besteht aus Datenrichtigkeit und Berichtigung von Daten, siehe § 10 IDAG (Korrektheit der Daten) und § 27 IDAG (Berichtigung).
Datensicherheit	Personendaten müssen während des gesamten Bearbeitungs- und Aufbewahrungsprozesses geschützt und durch angemessene Massnahmen gesichert werden. Mittels Verordnung wird der Datenschutz bei elektronischer Bearbeitung von Personendaten geregelt, siehe § 12 IDAG (Datensicherheit).
Ausbildung/Sensibilisierung	Mitarbeitende erhalten hinsichtlich ihrer Verantwortung für den Datenschutz und ihrer Tätigkeit die entsprechende Sensibilisierung und Ausbildung. Sie erhalten Zugriff auf Dokumente, Formulare, Meldungen und Informationen zum Thema Datenschutz über die entsprechende Intranet-Seite.

2.2 Verpflichtung auf Datenschutz

Mitarbeitende werden im Rahmen des Arbeitsvertrags auf den Datenschutz verpflichtet. Vorgaben betreffend Datenschutz werden in angemessener Weise in Anstellungsverträge aufgenommen. Die Verpflichtung wird nachweisbar dokumentiert und im Personaldossier abgelegt.

2.3 Klassifizierung von Personendaten

Personendaten werden entsprechend den gesetzlichen Vorgaben und den Bedürfnissen des KSB klassifiziert. Die Klassifizierung erfolgt aufgrund des Schutzbedarfs der Daten durch den Dateneigner.

Zur Klassifizierung werden Personendaten in folgende Kategorien D1 und D2 unterteilt:

Klassifizierungsstufe:		**Definition nach Datenschutzgesetz:**		
D2: Erhöhte Datenschutzrelevanz		Besonders schützenswerte Personendaten		
D1: Geringe Datenschutzrelevanz		Personendaten		
Patienten-daten	**Stammdaten**	Name, Vorname, Adressen, Geschlecht etc.	X	
	Administrative Daten	Abrechnungs- und Kostenstellen, Finanzdaten	X	
	Medizinische Daten	Falldaten		X
	Daten besonderer Patientengruppen	Alle Personendaten von Personalarztpatienten, Mitarbeitenden als KSB-Patienten und VIPs	X	X
Personaldaten	**Personaldaten**	Name, Vorname, Personalnummer etc.	X	
	Besonders schützenswerte Daten	Daten bzgl. Gewerkschaft, Gesundheit, soziale Hilfe etc.		X
	Persönlichkeitsprofile	Verknüpfung Stammdaten und Bewegungsdaten: pers.bez. Merkmale & Eigenschaften/Vorlieben		X

Mitarbeitende haben sich bezüglich Klassifizierung und Schutz der Personendaten an die Vorgaben des Dateneigners zu halten. Bei Unklarheiten kontaktieren sie den Dateneigner oder die Datenschutzbeauftragte.

Die Klassifizierung wird auf den gesamten Prozess der Bearbeitung angewendet, also auch auf IT-Mittel / IT-Systeme, Applikationen, Räume und Gebäude.

2.4 Inventarisierung

Datensammlungen, die Personendaten enthalten, werden durch den zuständigen Dateneigner inventarisiert. Zusätzlich identifiziert er die zur Bearbeitung der Daten benötigten Prozesse und Systeme. Alle diese datenschutzrelevanten Objekte werden im Inventar dokumentiert.

Anhand des Inventars erstellt die Datenschutzbeauftragte ein Register der Datensammlungen und Datenbearbeitungen. Eine Kopie davon stellt sie der beauftragten Person für Öffentlichkeit und Datenschutz jährlich per 1. Januar zu. Die im Vorjahr eingetretenen Änderungen sind hervorzuheben.

2.5 Bearbeitung von Datensammlungen

Eine Datensammlung ist jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.

2.5.1 Verantwortung

Für die einzelnen Datensammlungen sind Dateneigner benannt. Dateneigner stellen die Einhaltung der datenschutzrechtlichen Anforderungen in technischer und organisatorischer Hinsicht sicher. Sie bestimmen die zum Bearbeiten der Daten befugten Personen und deren Zugriffrechte nach dem Need-to-Know-Prinzip.

Grundsätzlich müssen Mitarbeitende vom Dateneigner zur Bearbeitung einer Datensammlung autorisiert werden. Die Zuordnung der Dateneigner und der aktuelle Stand des Inventars der Datensammlungen kann im Intranet eingesehen werden.

2.5.2 Interne Meldepflicht

Jeder Mitarbeitende hat neue Datensammlungen vor deren Eröffnung an die Datenschutzbeauftragte zu melden. Von dieser internen Meldepflicht ausgenommen sind Datensammlungen, die auf eine Zeit von weniger als 6 Monaten und allein zum Zwecke angelegt werden, später in eine bereits gemeldete Datensammlung integriert zu werden. Selbstverständlich unterliegen Personendaten aus solchen nicht meldepflichtigen Datensammlungen ebenfalls dem Datenschutz.

Wesentliche Änderungen an der Datensammlung oder der Datenbearbeitung (insbesondere das Löschen von Datensammlungen oder wenn bspw. neue Felder mit besonders schützenswerten Personendaten hinzukommen etc.) hat der Mitarbeitende der Datenschutzbeauftragten zu melden.

Meldepflichtige Bearbeitung von Datensammlungen

Bearbeitet ein Mitarbeitender Datensammlungen, so muss er bei folgenden Tätigkeiten Rücksprache mit dem Dateneigner nehmen. Kennt er diesen nicht, hat er die Datenschutzbeauftragte zu kontaktieren.

- Erstellung einer neuen Datensammlung, die aufgrund neuer Daten angelegt wird.
- Erstellung einer neuen Datensammlung, die aus der Kombination von anderen Datensammlungen entsteht.
- Erstellung einer neuen Datensammlung dadurch, dass Daten aus bestehenden Datensammlungen abgerufen und einem eigenständigen neuen Zweck zugeführt werden.
- Übertragung einer bestehenden Datensammlung auf ein neues Medium (Übertragung einer sog. „Papierdatensammlung" auf ein Informatiksystem).
- Vollständige und nicht rückgängig machbare physische Zerstörung der Datensammlung.

Eine vollständige und unveränderte Kopie einer bestehenden Datensammlung darf der Mitarbeitende anlegen, falls dies für seine Arbeitstätigkeit nötig ist und dem Zweck der kopierten Datensammlung entspricht.

Zur Erhebung von Datensammlungen zwecks Inventarisierung ist ein geeignetes Hilfsmittel (bspw. ein Formular) zu verwenden.

Verhalten bei Unklarheiten

Bestehen Unklarheiten über das Vorliegen einer neuen meldepflichtigen Datensammlung, ist die Datenschutzbeauftragte zu konsultieren.

2.6 Bearbeitungsreglemente

Für automatisierte Datensammlungen, die besonders schützenswerte Personendaten und Persönlichkeitsprofile enthalten oder Dritten zugänglich gemacht werden, ist durch den Dateneigner, in Zusammenarbeit mit der Datenschutzbeauftragten, ein Bearbeitungsreglement zu erstellen.

Das Bearbeitungsreglement dient als eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung. Das Reglement beinhaltet Angaben über die interne Organisation des KSB sowie über die Struktur, in der die Datensammlung oder das automatisierte Bearbeitungssystem eingebettet ist. Es beschreibt die Datenbearbeitungs- und Kontrollprozeduren und enthält alle Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung und der eingesetzten IT-Systeme. Es regelt namentlich Art und Umfang der Zugriffsberechtigung auf Personendaten.

Das Reglement muss bei Bedarf durch den Dateneigner angepasst und nachgeführt werden. Es wird durch die Datenschutzbeauftragte kontrolliert und abgenommen und den interessierten Personen mittels Publikation auf dem Internet oder in anderer Form zugänglich gemacht.

Ein Bearbeitungsreglement kann für mehrere Datensammlungen gültig sein, wenn es tatsächlich für die bezeichneten Datensammlungen zur Anwendung gelangt und für jede betreffende Datensammlung die notwendigen Anforderungen erfüllt.

2.7 Einsichts- und Auskunftsgesuche sowie Weitergabe an Dritte

Generell gibt es drei Arten von Auskunftsbegehren entsprechend des Gesuchstellers zu unterscheiden:

1. **Mitarbeitende**
   Anfragen von Mitarbeitenden zu ihren Personal- und Mitarbeiterdaten sind an die Abteilung Human Resources des Departements Direktion zu richten, siehe dazu Kap. 3.3.
2. **Patienten**
   Bei Anfragen von Patienten erteilt die behandelnde Ärztin resp. der behandelnde Arzt Auskunft und gewährt Einsicht in die medizinischen Daten des Patienten gemäss Kap. 4.5.1. Auskunftsbegehren bezüglich administrativer Daten zum Abrechnungsverfahren werden durch die Abteilung Rechnungswesen des Departements Finanzen bearbeitet.
3. **Dritte: Andere externe natürliche oder juristische Personen**
   Diese Anfragen sind an die Datenschutzbeauftragte zu richten, welche das Auskunftsbegehren entweder selbst bearbeitet oder nach eigenem Ermessen dem entsprechenden Departement überträgt.

2.7.1 Weitergabe von Personendaten innerhalb des KSB

Grundsätzlich darf der Mitarbeitende Personendaten von einer Abteilung zur anderen übermitteln, falls diese zur Erfüllung des Auftrags notwendig sind. Sollen diese Daten neu für einen anderen Zweck bearbeitet werden, so muss vorgängig der verantwortliche Dateneigner informiert werden.

2.7.2 Weitergabe von Personendaten an Dritte

Die Weiterleitung und Weitergabe von Personendaten an Dritte erfolgt in der Regel durch automatisierte und genehmigte Prozesse. Im Einzelfall prüft die Datenschutzbeauftragte, ob die Zulässigkeit gegeben ist und die Schutzmassnahmen bei der Übermittlung der Daten ausreichend sind.

2.8 Anonymisierung / Pseudonymisierung

Personenbezogene Daten, die so verändert werden, dass sie nicht mehr oder nur mit einem unverhältnismässig grossen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, unterliegen den Anforderungen des Datenschutzes nicht mehr.

Personendaten gelten als anonymisiert, wenn diejenigen Daten entfernt werden, welche die Identifizierung der betroffenen Person ermöglichen. Auch aufgrund der Verknüpfung von einzelnen Attributen darf kein Rückschluss auf eine Person möglich sein.

Bei der Pseudonymisierung handelt es sich um das Verändern von personenbezogenen Daten durch eine Zuordnungsvorschrift (z.B. die Verwendung von Pseudonymen). Dadurch können die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Kenntnis oder Nutzen der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden. Es wird auch von verschlüsselten Daten gesprochen.

Dürfen Personendaten einer bestimmten oder bestimmbaren natürlichen Person nicht mehr zugeordnet werden können, so hat der Mitarbeitende diese zu anonymisieren. Nur wenn die Identifizierung beibehalten werden muss, hat er diese zu pseudonymisieren. Welche Identifikationsmerkmale der Mitarbeitende zu entfernen bzw. zu verändern hat, um die Bestimmbarkeit des Betroffenen auszuschliessen, hängt vom Einzelfall ab und hat in Zusammenarbeit mit dem Dateneigener oder der Datenschutzbeauftragten zu erfolgen.

2.9 Archivierung / Vernichtung von Personendaten

Die Mitarbeitenden haben Personendaten so aufzubewahren, dass Unbefugten keine Einsicht möglich ist. So hat das Aufbewahren von Personendaten in Papierform in abschliessbaren Räumen oder Behältnissen zu erfolgen.

Der Dateneigner legt die Dauer der Aufbewahrung nach der Art der Personendaten fest. Bei der

Festlegung der Aufbewahrungsdauer richtet er sich nach den gesetzlichen Vorgaben.

Die Vernichtung von Papierunterlagen erfolgt mittels der spitaleigenen Sammelbehälter (Container).

2.10 Datenbearbeitung durch Dritte / Outsourcing

Gemäss § 18 IDAG (Datenbearbeitung im Auftrag) hat sich das KSB zu vergewissern, dass Dritte bzw. Outsourcing-Partner die Datensicherheit bei der externen Bearbeitung von Patientendaten gewährleisten. Verträge mit Outsourcing-Partnern sind präzise zu formulieren, Sicherheitsmassnahmen explizit zu vereinbaren. Ebenso ist der Outsourcing Partner zur Geheimhaltung zu verpflichten[2].

Die Umsetzung der Verträge und die Einhaltung der vereinbarten Sicherheitsmassnahmen sind mindestens jährlich zu kontrollieren bzw. durch den Partner zu bestätigen und nachzuweisen. Er hat aufzuzeigen, dass Datenschutzvorgaben und Sicherheitsmassnahmen angemessen und effektiv berücksichtigt werden.

Daraus ergeben sich folgende verbindlichen Vorgaben für eine Beauftragung eines Dritten seitens des KSB:

- Generell darf der Dritte Daten nur so bearbeiten, wie es das KSB selber dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Eine Datenbearbeitung, die unrechtmässig ist, bleibt auch dann unrechtmässig, wenn sie durch Dritte vorgenommen wird.
- Das KSB bleibt Inhaberin der Datensammlung und trägt weiterhin die volle datenschutzrechtliche Verantwortung für die ausgelagerte Datenbearbeitung.
- Auch bei Outsourcing von Datenbearbeitungen bleibt die gesetzliche Auskunftspflicht des KSB als Inhaberin der Datensammlung gegenüber betroffenen Personen bestehen. Es ist sicherzustellen, dass das KSB trotz Auslagerung ihrer Auskunftspflicht jederzeit nachkommen kann.
- Das KSB ist dafür verantwortlich, dass der Outsourcingnehmer die Datensicherheit gewährleistet.
- Das KSB lässt grosse Sorgfalt walten bei der Auswahl, der Instruktion und der Überwachung eines Outsourcingnehmers. Die ausgelagerte Funktion ist zudem in das Interne Kontrollsystem des KSB zu integrieren.
- Die Datenbearbeitung durch Dritte muss stets in einem schriftlichen Vertrag (Outsourcing-Vertrag) geregelt sein. Schnittstellen, Verantwortlichkeiten, Zuständigkeiten und Haftungsfragen sind vertraglich zu regeln.
- Im Outsourcing-Vertrag und mit internen Massnahmen ist sicherzustellen, dass bei einem unerwarteten Ausfall des Outsourcingnehmers (z.B. aufgrund ausserordentlicher Kündigung oder Einstellung der Geschäftstätigkeit) einerseits die Datensicherheit gewährleistet bleibt und andererseits dem KSB und seinen Patienten keine übermässigen Schäden entstehen.

Outsourcing-Vertrag

Das Vertragsverhältnis mit dem Dritten (Outsourcing-Vertrag) ist so zu gestalten, dass die Einhaltung der oben dargestellten Grundsätze sichergestellt ist. Im Einzelnen soll ein Outsourcing-Vertrag folgende Punkte eindeutig, vollständig und unmissverständlich regeln:

- Bezeichnung der Vertragspartner (Name, Rechtsform, Anschrift, Vertreter)
- Gegenstand des Datenbearbeitungsauftrages
- Genaue Umschreibung des Zwecks und der Aufgaben (Datenbearbeitungen), die der Outsourcingnehmer zu erfüllen hat. Der Outsourcingnehmer muss verpflichtet werden, die Daten ausschliesslich zweck- und weisungsgebunden zu verwenden, womit die Verwendung der Daten für eigene Zwecke des Outsourcingnehmers oder fremde Zwecke ausgeschlossen wird
- Statuierung, dass das KSB alleiniger „Eigentümer“/Berechtigter an den zur Verfügung gestellten und bearbeiteten Daten bleibt und Klärung der Eigentums- und Nutzungsverhältnisse bezüglich der eingesetzten Hard- und Software

[2] Hierfür stellt die Abteilung Legal & Compliance eine Vorlage zur Verfügung.

- Ort der zu erbringenden Leistung (insbes. zur eindeutigen Identifikation einer Datenbearbeitung im Ausland, die erhöhten Anforderungen unterliegen kann)
- Fixierung der Sicherheitsstandards für den Datenaustausch und die Sicherheitsanforderungen, die der Outsourcingnehmer bei der Datenbearbeitung zu erfüllen hat
- Genaue Beschreibung der Datenschutzmassnahmen, die der Outsourcingnehmer umzusetzen hat, und wie er dies sicherstellen und nachweisen wird. Der Outsourcingnehmer muss jederzeit gewährleisten und nachweisen können, dass er die im Auftrag des KSB bearbeiteten Daten und die dafür eingesetzten Systeme mittels technischer, personeller und organisatorischer Massnahmen angemessen gegen unbefugten Zugriff, unbefugtes Bearbeiten und Verlust schützt
- Statuierung, dass der Outsourcingnehmer sich strikt an die Weisungen des KSB zur Datenbearbeitung zu halten hat. Dies beinhaltet insbesondere auch das Recht des KSB zur Weisung, die Daten an das KSB herauszugeben oder die Daten unwiederbringlich zu vernichten.
- Die weisungsberechtigten Personen des KSB und die Kontaktpersonen seitens des Outsourcingnehmers sind zu bestimmen
- Berichterstattungspflicht des Outsourcingnehmers: einerseits periodisch, anderseits unverzüglich bei Unregelmässigkeiten, Störungen, besonderen Vorfällen und Verdacht auf Datenschutzverletzungen
- Pflicht des KSB, sich zu vergewissern, dass der Outsourcingnehmer die notwendigen Sicherheitsstandards einhält und tatsächlich anwendet, und daraus abgeleitet das Recht der KSB, beim Outsourcingnehmer jederzeit Überprüfungen durchzuführen und Einsicht zu nehmen, um die Einhaltung der gesetzlichen Datenschutzvorschriften und der vertraglichen Regelungen zu überprüfen („Right-to-Audit Clause“). Beschreibung der Tiefe und Breite solcher Überprüfungen, ihrer Kostenfolgen und der Modalitäten ihrer Durchführung
- Verbot des Anfertigens von Kopien durch den Outsourcingnehmer, ausser zum Zweck der Datensicherung im vertraglich vereinbarten Umfang
- Schriftliche Verpflichtung der Mitarbeitenden des Outsourcingnehmers zur Geheimhaltung sowie zur Einhaltung der gesetzlichen Datenschutzvorschriften
- Modalitäten der Änderung von wesentlichen Vertragsbestandteilen, z.B. Vorgehen bei Tests und Freigabe von Änderungen der Datenbearbeitungsverfahren, technischer und organisatorischer Datenschutzmassnahmen
- Gegebenenfalls Laufzeiten und Kündigungsfristen der Datenbearbeitung, Voraussetzungen und Vorgehensweise zu ordentlicher und fristloser Kündigung. Es ist vertraglich festzuhalten, dass die Verletzung datenschutzrechtlicher Pflichten durch den Outsourcingnehmer das KSB zu einer ausserordentlichen Vertragskündigung berechtigt
- Verpflichtung des KSB und Outsourcingnehmer zu einer kontrollierten Rückabwicklung und Beendigung der Datenbearbeitungen durch den Outsourcingnehmer (vor und nach Vertragsende), auch im Falle einer ausserordentlichen Kündigung
- Ausschluss des Einsatzes von Unterauftragnehmern des Outsourcingnehmers. Soll der Einsatz von Unterauftragnehmern zugelassen werden, so sind die obigen Punkte auch für jeden einzelnen Unterauftragnehmer eindeutig, vollständig und unmissverständlich zu regeln.
- Das KSB ist verpflichtet, die betroffenen Patienten über das Outsourcing bzw. den Beizug Dritter bei der Datenbearbeitung hinreichend zu informieren.

Datenbearbeitung für Dritte (Insourcing)

Sowohl bei der Beauftragung durch eine Tochtergesellschaft des KSB als auch bei einer Beauftragung durch ein aussenstehendes Unternehmen sind die für die Datenbearbeitung durch Dritte geltenden Anforderungen zu erfüllen. Die im vorhergehenden Abschnitt „Datenbearbeitung durch Dritte / Outsourcing“ statuierten Pflichten des Outsourcingnehmers finden sinngemäss Anwendung.

Alle Verträge, in welchen das KSB als Outsourcingnehmer auftritt, sind aus Beweis- und Dokumentationsgründen schriftlich abzuschliessen. Dabei kann auf die vorliegende Weisung verwiesen werden.

3 Umgang mit Personaldaten

Mitarbeitende der Abteilung Human Resources sind insbesondere für die sorgfältige und korrekte Bearbeitung der Personaldaten in den Personaldossiers verantwortlich. Sie haben nur auf diejenigen Daten Zugriff, welche sie für die eigentliche Erfüllung ihrer Aufgaben benötigen.

Personaldaten dürfen nur soweit bearbeitet werden, als dies aus betrieblichen Gründen, namentlich im Hinblick auf die ordnungsgemässe Durchführung des Arbeitsvertrags, notwendig ist (Art. 328b OR).

Das Bearbeiten von Personaldaten erfolgt unter Einhaltung der gesetzlichen Datenschutzbestimmungen und gemäss Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB (siehe Kap. 8). Personaldaten sind durch angemessene technische und organisatorische Vorkehrungen vor dem Zugriff Unbefugter zu schützen. Bei der Bearbeitung von klassifizierten Personaldaten, elektronisch wie von Hand, sind zusätzlich entsprechende Behandlungsregeln einzuhalten.

3.1 Personal- und Führungsdossier

Das KSB führt für jeden aktiven Mitarbeitenden ein individuelles Dossier. Besonders vertrauliche Unterlagen müssen in einem verschlossenen Kuvert zum Schutz vor direkter Einsichtnahme durch nicht berechtigte Mitarbeitende aufbewahrt werden.

Das parallele Führen inoffizieller "grauer" Schattendossiers ist untersagt. Einzelne Daten zu Mitarbeitenden, die zu dienstlichen Zwecken in Systemen gespeichert werden, fallen nicht darunter. Diese Daten sind ebenfalls angemessen zu schützen.

Das Führungsdossier ist die Grundlage für die/den Vorgesetzte/n zum Führen und Betreuen ihrer/seiner Mitarbeitenden. Es wird durch sie/ihn verwaltet und entweder beiihr/ihm oder bei der Abteilung Human Resources aufbewahrt.

Weitere Regelungen zum Umgang mit Personaldaten sind der Weisung Personaldaten zu entnehmen.

3.2 Aufbewahrung und Archivierung

Während der Anstellungsdauer des Mitarbeitenden werden die Personaldossiers in den Räumen der Abteilung Human Resources aufbewahrt.

Nach Beendigung des Arbeitsverhältnisses wird das Personaldossier archiviert und gemäss den gesetzlichen Bestimmungen während maximal 10 Jahren im Archiv aufbewahrt.

Bewerbungsunterlagen werden vernichtet, falls keine Anstellung erfolgt. Das Bewerbungsschreiben bleibt beim KSB, ebenso bleibt der Bewerbungseingang registriert.

Papierunterlagen und elektronische Datenträger sind via Aktenvernichter oder firmeneigenen Sammelbehälter (Container) zu entsorgen.

3.3 Auskunftsrecht

Mitarbeitende haben grundsätzlich ein umfassendes Recht auf Auskunft über den Inhalt ihres Personaldossiers. Das KSB ist verpflichtet, die Auskunft schriftlich und kostenlos, in Form eines Ausdruckes oder einer Fotokopie, zu erteilen. Dieses Auskunftsrecht kann im gegenseitigen Einverständnis auch durch eine Einsichtnahme in das Personaldossier an Ort und Stelle ersetzt werden.

Das KSB kann die Auskunft verweigern, einschränken oder aufschieben, soweit eigene überwiegende Interessen oder solche Dritter es erfordern und es die Personendaten nicht an Dritte bekannt gibt.

Bei Fragen oder Unklarheiten ist die Datenschutzbeauftragte beizuziehen.

3.4 Auskunftspflicht gegenüber Dritten

Auskunftsgesuche von Dritten (Polizei, Behörden, Versicherungen, Presse, Geschäftspartner, Stellenvermittlungsbüros, Lieferanten etc.) sind der Datenschutzbeauftragten zu melden, die diese prüft, bevor die Bekanntgabe durch die Abteilung Human Resources erfolgt.

Grundsätzlich darf Dritten bekannt gegeben werden, dass sich eine Person in einem Anstellungsverhältnis zum KSB befindet, falls diese nicht ausdrücklich etwas anderes bestimmt hat. Eine Mitteilung von Daten über Mitarbeitende an staatliche Behörden, namentlich das Amt für Migration und Integration (MIKA) und Versicherern, darf erfolgen, sofern dies für die Erfüllung von deren Aufgaben unabdingbar ist und im Interesse der Mitarbeitenden erfolgt.

Auskünfte über die Modalitäten der Anstellung, über das Einkommen sowie berufliche Referenzen sowie andere weiterführende Auskünfte bedürfen der ausdrücklichen Zustimmung der betroffenen Person.

3.5 Beantwortung von Auskunftsbegehren

Auskunftsbegehren müssen innert 30 Tagen beantwortet werden.

Die/der Mitarbeitende der Abteilung Human Resources prüft die Identität des gesuchstellenden Mitarbeitenden und eruiert bei Bedarf unter Mithilfe des Dateneigners, welche Datensammlung von der Auskunft betroffen ist.

Die Abteilung Human Resources ist für die Beschaffung der notwendigen Unterlagen verantwortlich. Der Mitarbeitende erhält auf Verlangen Fotokopien bzw. „Hardcopies" von elektronischen Daten. Wo es angezeigt erscheint, kann die schriftliche Auskunft durch Einsichtnahme vor Ort ersetzt werden.

Telefonische Auskünfte werden nicht erteilt.

Über Auskunft und Einsichtnahme ist ein Kurzprotokoll zu erstellen, in dem die allfällige Aushändigung von Kopien bzw. Ort und Zeitpunkt der Einsichtnahme vermerkt wird. Das Kurzprotokoll ist bei Einsichtnahme vom Gesuchsteller zu unterzeichnen.

Das Protokoll wird im Personaldossier abgelegt.

4 Umgang mit Patientendaten

Mitarbeitende sind beim Umgang mit Patientendaten an das kantonale Datenschutzgesetz sowie an das Berufsgeheimnis und Amtsgeheimnis (Art. 320 und 321 StGB) gebunden. Die Schweigepflicht (§ 19 GesG[3], Berufsgeheimnis) schützt die Vertrauensbeziehung der behandelten Person zum medizinischen Personal.

Im Zusammenhang mit der Schweigepflicht und der Bekanntgabe von Patientendaten ist der Anhang zum Reglement Datenschutz (Patienten) - Ärztliche bzw. berufliche Schweigepflicht in Kap. 9 zu beachten.

4.1 Grundsätze der Datenbearbeitung

Mitarbeitende dürfen Daten von Patientinnen und Patienten nur in dem Umfang bearbeiten, als ein Behandlungsauftrag gegeben ist. Diese Daten müssen also für die fachgerechte medizinische Betreuung, für weitere Dienstleistungen des Spitals in diesem Zusammenhang oder für die administrative Betreuung der Patientinnen und Patienten unabdingbar sein.

Der Mitarbeitende muss die Behandlungsdokumentation unter Wahrung der Schweigepflicht so verwalten, dass Unbefugten die Einsicht verwehrt bleibt und das Berufsgeheimnis gewährleistet ist. Den berechtigten Patientinnen und Patienten ist der Zugang dazu zu ermöglichen.

4.2 Daten besonderer Patientengruppen

Folgenden Patientengruppen gewährleistet das KSB einen besonderen Schutz ihrer Daten:

- Personalarztpatienten (Patienten der Personalärztinnen),
- Mitarbeitende als KSB-Patienten (Mitarbeitende, die das KSB als behandelndes Spital wählen) und
- VIPs (Patienten, die anonym bleiben möchten).

[3] Gesundheitsgesetz des Kantons Aargau, siehe Kap. 8 der Weisung.

Bereits bei ihrer Erfassung werden sowohl administrative wie medizinische Daten dieser Patientengruppen speziell gekennzeichnet, damit sie nur sehr eingeschränkt einsehbar sind und der Zugriff durch Mitarbeitende des KSB auf das absolut Notwendige beschränkt ist. Damit sollen die Anonymität der behandelten Person und die Geheimhaltung ihrer Daten so weit wie möglich sichergestellt werden.

4.3 Recht auf Berichtigung

Jede behandelte Person hat Anspruch darauf, dass unrichtige oder nicht notwendige Personendaten über sie/ihn berichtigt oder vernichtet werden.

- Die/der behandelnde Ärztin/Arzt nimmt die Berichtigung von Personendaten des Patienten vor, indem sie/er einen entsprechenden Vermerk anbringt.
- Bestreitet die/der behandelnde Ärztin/Arzt die Unrichtigkeit, so hat sie/er bzw. das KSB die Richtigkeit zu beweisen. Die betroffene Person hat im Rahmen des Zumutbaren bei der Abklärung mitzuwirken. Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten, insbesondere von solchen, die eine Wertung menschlichen Verhaltens enthalten, bewiesen werden, so kann die betroffene Person verlangen, dass eine angemessene Gegendarstellung vorgenommen wird. Ist eine Patientin oder ein Patient bspw. mit dem Inhalt eines Berichts an den Hausarzt nicht einverstanden, kann sie resp. er einen Berichtigungsvermerk verlangen, der dem Hausarzt zugestellt wird, ohne dass die/der behandelnde Ärztin/Arzt des KSB den Bericht ändert.

Die/der Ärztin/Arzt protokolliert allfällige Änderungen an den Patientendaten bzw. legt den Berichtigungsvermerk im Dossier ab.

4.4 Recht auf Sperrung

Jede betroffene Person kann nach § 16 IDAG die Bearbeitung ihrer Daten sperren lassen, wenn sie ein schützenswertes Interesse nachweist. Folgende Regeln sind zu beachten:

- Der Mitarbeitende hat Anträge auf Sperrung von Daten der Datenschutzbeauftragten weiterzuleiten, die die rechtliche Zulässigkeit prüft.
- Wenn die Sperrung rechtlich zulässig ist, beauftragt die Datenschutzbeauftragte den Applikationsverantwortlichen zur Sperrung der Daten.
- Die betroffene Person wird durch die Datenschutzbeauftragte über die Sperrung, ggf. über die Nichtzulässigkeit der Sperrung oder entsprechende Auflagen, schriftlich informiert.

Der Dateneigner protokolliert die Sperrung.

4.5 Recht auf Einsicht und Herausgabe

Die nachfolgenden Regelungen ergänzen die Richtlinie für die Herausgabe von Patientenakten_Patienten-daten.

4.5.1 Einsichtsrecht des Patienten

Grundsätzlich besteht gemäss § 22 PatV[4] ein Recht auf Auskunft und Einsicht in sämtliche administrativen und medizinischen Daten durch die/den Patientin/Patienten.

- Die/der behandelnde Ärztin/Arzt gewährt auf Verlangen der behandelten Person Einsicht in die bearbeiteten Daten bzw. in die Patienten- und Falldaten und erläutert diese bei Bedarf.
- Die Identifikation der behandelten Person wird von der/dem behandelnden Ärztin/Arzt vorgenommen.

Der betreffenden Person ist Einsicht in die Patientendaten zu gewähren oder eine Kopie oder ein Ausdruck der Patientendaten zu erstellen, siehe Kap. 4.5.2. Im Dossier muss festgehalten werden, wer, was, wem, wann (Datum) Einsicht gewährt bzw. herausgegeben hat.

[4] Verordnung über die Rechte und Pflichten der Patientinnen und Patienten, siehe Kap. 8

4.5.2 Herausgabe an Patienten

Falls ein Patient die Herausgabe der Behandlungsdokumentation (Krankengeschichte) verlangt, verschickt das Chefarztsekretariat oder eine vom Chefarztsekretariat designierte Person eine Kopie einzelner Akten an ihn. Die Herausgabe der gesamten Dokumentation erfolgt, sofern nicht anders vereinbart, durch die Abteilung Legal & Compliance.

Alternativ zum Versand übergibt die/der behandelnde Ärztin/Arzt die Kopie der gesamten Behandlungsdokumentation oder Teile davon direkt der behandelten Person.

Eine Ausnahme von der Herausgabepflicht bilden Notizen des medizinischen Personals, die ausschliesslich zum persönlichen Gebrauch bestimmt sind.

4.5.3 Herausgabe an Patientenangehörige

Falls eine behandelte Person die Herausgabe der Behandlungsdokumentation (Krankengeschichte) an Angehörige verlangt, hat der zuständige Mitarbeitende eine schriftliche Zustimmung der behandelten Person einzuholen bzw. zu prüfen, ob bereits eine solche schriftliche Vereinbarung vorliegt. Sofern eine Ermächtigung des Patienten vorliegt, haben Angehörige Anrecht auf Aktenkopien.

Die Übergabe bzw. der Versand erfolgt gemäss Kap. 4.5.2 an den bezeichneten Angehörigen der behandelten Person. Bei der persönlichen Übergabe kann die/der behandelnde Ärztin/Arzt einen Identitätsnachweis (bspw. Identitätskarte) der betroffenen Person verlangen.

4.5.3.1 Auskunft gegenüber Angehörigen

Der behandelnde Arzt darf an nächste Angehörige grundsätzlich nur Auskunft erteilen, sofern ein Einverständnis des Patienten vorliegt (entsprechende Angaben sind der Eintrittserklärung zu entnehmen) oder soweit aus den Umständen nicht auf einen Geheimhaltungswillen des Patienten geschlossen werden muss (§ 21 Abs. 2 PatV). Als nächste Angehörige gelten dann insbesondere der Lebenspartner, danach die Blutsverwandten (in der Reihenfolge Kinder, Eltern, Geschwister).

Kann ein solches Einverständnis durch den Patienten aus gesundheitlichen Gründen nicht mehr erteilt werden, darf der behandelnde Arzt den nächsten Angehörigen wie urteilsfähigen Kindern, Eltern, dem Ehepartner oder Lebenspartner der behandelten Person Auskünfte über den Gesundheitszustand, die Behandlung, die Heilungsaussichten geben, sofern aus den Umständen nicht auf einen Geheimhaltungswillen geschlossen werden muss.

Die/der behandelnde Ärztin/Arzt erteilt die oben genannten Auskünfte in mündlicher Form.

Bei verstorbenen Patienten sind die nächsten Angehörigen berechtigt, in den Obduktions- und Schlussbericht über verstorbene Personen Einsicht zu nehmen (§ 24 Abs. 1 PatV). Nächste Angehörige und andere Dritte sind berechtigt, in die Patientendokumentation Einsicht zu nehmen, soweit sie über ein berechtigtes Interesse verfügen und keine überwiegenden öffentlichen oder privaten Interessen, namentlich der weiterbestehende Geheimhaltungswille der verstorbenen Person, entgegenstehen (§ 24 Abs. 2 PatV).

Zu beachten ist auch, dass die/der Ärztin/Arzt mit dem Tod einer behandelten Person die nächsten Angehörigen in den Entscheidungsprozess, ob Privaten Auskunft oder Einsicht in medizinische Daten des Verstorbenen gewährt werden soll, einzubeziehen hat.

4.5.4 Herausgabe an vor- und nachbehandelnde Ärzte und Institutionen

Mitarbeitende dürfen Informationen über den gesundheitlichen Zustand des Patienten, bspw. Behandlungsdokumentationen oder Austrittsberichte, an Personen und Stellen weitergeben, die einen Behandlungsauftrag zu erfüllen haben, sofern die behandelte Person nicht ausdrücklich etwas anderes bestimmt hat. Hierzu gehören vor- und nachversorgende Ärzte.

Gemäss § 19 PatV sind unmittelbar nachbehandelnde Personen über Diagnose und Zustand des Patienten sowie über die erforderlichen weiteren Massnahmen zu informieren, soweit dies für die fachgerechte Nachbehandlung erforderlich ist. Die Einwilligung in die Weitergabe an Nachversorger erteilt die behandelte Person nebst der vorgenannten gesetzlichen Ermächtigungsnorm mit der Anmeldung am KSB (siehe Anmeldeformular rechte Spalte). Die Einwilligung erstreckt sich hierbei nebst Ärzten auch auf Pflegefachkräfte nachbehandelnder Institutionen. Es gilt die Vermutung, dass

Ärzte und Institutionen, die während sechs Monaten nach Behandlungsabschluss Informationen zum Gesundheitszustand erbitten als Nachverfolger zu qualifizieren sind. Danach ist von nachversorgenden eine Patienteneinwilligung einzuverlangen.

Gemäss § 20 PatV sind zuweisende Ärzte lediglich über die Diagnose zu informieren, wenn aus den Umständen nicht auf einen Geheimhaltungswillen des Patienten geschlossen werden muss.

Vor- und Nachversorgern soll, sofern nicht auf einen Geheimhaltungswillen der behandelten Person geschlossen werden muss, jene Information weitergegeben werden, die sie zur Erfüllung ihrer Aufgabe brauchen. Innerhalb des KSB, unter KSB-Mitarbeitenden, kann der Begriff „vor- und nachbehandelnd“ grosszügig ausgelegt werden. Alle, die mit der Betreuung einer behandelten Person im KSB zu tun haben, können über KISIM auf die behandlungsrelevanten Informationen zugreifen.

Bei einer Weitergabe an eine externe Stelle muss der der Ärztin resp. dem Arzt die Behandlungskette klar bekannt sein. An zuweisende Ärzte, bzw. an Ärzte, an die das KSB direkt weitergewiesen hat, können Patientendaten weitergegeben werden (als Teil einer standard procedure).

Die angefragte KSB-Stelle bzw. der behandelnde Arzt übergibt die Kopie der gesamten Behandlungsdokumentation oder versendet die Daten über eine gesicherte Email-Adresse oder postalisch an die/den vor- oder nachbehandelnden Ärztin/Arzt. Das Original verbleibt beim KSB und unterliegt der Aufbewahrungspflicht.

4.5.5 Herausgabe an Krankenkassen

Mitarbeitende dürfen an obligatorische Krankenkassen nur die Daten weitergeben, die ihnen eine Beurteilung der Leistungspflicht und Wirtschaftlichkeit ermöglicht. Spezifiziert die Krankenkasse, welche Akten sie benötigt (z.B. Austrittsbericht, Operationsbericht), sind diese auszuhändigen. Ist die Anfrage allgemein oder sind den gewünschten Akten weitere Dokumente angehängt, entscheidet die/der Ärztin/Arzt, welche Dokumente relevant sind. Nicht relevante Informationen in einem auszuhändigenden Dokument sind, soweit möglich, durch unkenntlich zu machen.

Die Akten sind ausschliesslich dem Vertrauensarzt zuzustellen. Bei Verdacht, dass es sich nicht um Einzelfallprüfungen sondern systematische Prüfungen durch die Krankenkasse handelt, informiert die Versandstelle den Chefarzt.

Kopien der erforderlichen Akten verschickt das Chefarztsekretariat oder eine vom Chefarztsekretariat designierte Person.

4.6 Bekanntgabe an Dritte ausserhalb des Behandlungsprozesses

Mitarbeitende dürfen Patientendaten nur an Dritte bekanntgeben, sofern die allgemeinen datenschutzrechtlichen Grundsätze, das Gesundheitsgesetz und die Patientenverordnung (insbesondere §§ 19, 20 und 21 PatV[5]) nicht verletzt werden. So dürfen Dritten Auskünfte über behandelte Personen (§ 21 PatV) und Einsicht in die Krankenakte (§ 23 PatV) nur mit deren Einverständnis gewährt werden. Bei der Bekanntgabe von Patientendaten ist zudem der Anhang zum Reglement Datenschutz (Patienten) - Ärztliche bzw. berufliche Schweigepflicht in Kap. 9 zu beachten.

Dritte müssen vor Erhalt der Daten – auf Verlangen schriftlich – nachweisen, dass sie die gewünschten Patientendaten bearbeiten dürfen. Der Bedarf kann bspw. durch einen gesetzlichen Auftrag oder durch eine ausdrückliche Einwilligung der behandelten Person gegeben sein. Zudem muss begründet werden, dass die Patientendaten auch tatsächlich benötigt werden (Verhältnismässigkeit).

Je nach Art der Anfrage (bspw. per Telefon) ist die Identität der anfragenden Person angemessen zu prüfen und zu verifizieren (bspw. durch Rückruf).

4.6.1 Allgemeine Meldepflichten

Folgende Meldepflichten bestehen gemäss Kap. 9 dieser Weisung für Ärzte, Spitäler bzw. Laboratorien und entbinden sie von der Schweigepflicht:

- Meldung von Schwangerschaftsabbrüchen an die zuständige Gesundheitsbehörde unter Wahrung

[5] Verordnung über die Rechte und Pflichten der Patientinnen und Patienten, siehe Kap. 8 der Weisung.

der Anonymität der betroffenen Frau (Art. 119 Abs. 5 StGB).

- Meldung aussergewöhnlicher Todesfälle an die Staatsanwaltschaft (§ 20 GesG i.V.m. § 59 VBOB).
- Meldung übertragbarer Krankheiten, die grosse Ausbrüche verursachen können und gegen deren Auswirkung anerkannte vorbeugende Massnahmen existieren, an die zuständige kantonale Behörde, gemäss Verordnung des EDI über Arzt- und Labormeldungen, http://www.bag-anw.admin.ch/infreporting/pdf/d/mvo2008_d.pdf.
- Meldung einer vorsätzlichen Verbreitung gefährlicher übertragbarer menschlicher Krankheiten an die Staatsanwaltschaft Baden (§ 20 GesG).

4.6.2 Allgemeine Melderechte

Folgende Melderechte bestehen gemäss Kap. 9:

- Meldung fahruntauglicher Lenker an die für den Fahrausweisentzug zuständige Behörde (Art. 14 Abs. 4 SVG).
- Meldung von Verbrechen oder schweren Vergehen, die ihnen in Ausübung ihres Berufs bekannt werden an die Strafverfolgungsbehörden (§ 21 Abs. 2 lit. d GesG).
- Meldung von Betäubungsmittelmissbrauch an eine Behandlungs- oder Fürsorgestelle (Art. 15 Abs. 1 BtmG).
- Meldung strafbarer Handlungen an Minderjährigen oder zum Schutz des Kindeswohls an die Kindes- und Erwachsenenschutzbehörde (Art. 314c ZGB) oder an die Anlaufstelle häusliche Gewalt oder die Kinderschutzgruppe des KSB (§ 21 Abs. 2 lit. a GesG i.V.m. § 61 lit. a VBOB).
- Meldung, dass der Patient hilfs- und schutzbedürftig ist, an die Kindes- und Erwachsenenschutzbehörde oder die Anlaufstelle häusliche Gewalt des KSB, § 21 Abs. 2 lit. b GesG i.V.m § 61lit. b VBOB.
- Information des Partners (Partnernotifikation) oder anderer Personen bei schwerer Gefährdung durch den Patienten; unmittelbar bei Notstand (Art. 17 StGB), ansonsten muss die/der Ärztin/Arzt beim Rechtsdienst des Departements für Gesundheit und Soziales um Entbindung vom Berufsgeheimnis ersuchen.

4.6.3 Bekanntgabe an Nicht-KVG-Versicherer

Mitarbeitende haben an Lebensversicherungen, Unfallversicherungen und weitere Nicht-KVG-Versicherer nur medizinische Daten weiter zu geben, die ausschliesslich für die Schadenabwicklung notwendig sind. Eine schriftliche Ermächtigung der behandelten Person muss vorliegen bzw. eingeholt werden.

4.6.4 Bekanntgabe an Behörden

Als Behörden gelten bspw. kantonale und staatliche Behörden, Versicherungen. Folgende Regeln sind zu beachten:

- Mitarbeitende dürfen Personendaten einer anderen Behörde bekanntgeben, wenn die verantwortliche Behörde zur Erfüllung ihrer Aufgabe gesetzlich dazu verpflichtet oder ermächtigt ist, oder die Behörde, die die Personendaten verlangt, nachweist, dass sie zu deren Bearbeitung gesetzlich befugt ist und keine Geheimhaltungspflicht entgegensteht, oder trotz Unvereinbarkeit der Zwecke die betroffene Person ausdrücklich zugestimmt hat oder es in ihrem Interesse liegt.
- Die Datenschutzbeauftragte bestimmt über die Art und Weise (schriftlich, mündlich, elektronisch, automatisiert) und Umfang der Weitergabe/Bekanntgabe von Personendaten sowie die zu treffenden Schutzmechanismen. Die Bestimmungen werden den Mitarbeitenden des KSB im Anhang zum Reglement Datenschutz (Patienten) - Ärztliche bzw. berufliche Schweigepflicht in Kap. 9 kommuniziert.

Strafverfolgungsbehörde

Mitarbeitende haben im Rahmen einer Strafverfolgung durch die Staatsanwaltschaft, nach Rücksprache mit der Datenschutzbeauftragten, Daten, die für die Abklärung eines Vergehens oder Verbrechens erforderlich sind, bekannt zu geben. Dazu muss ein schriftlich begründetes Gesuch der Staatsanwaltschaft vorliegen (Editionsverfügung). Je nach Einzelfall muss ein ärztlicher Bericht oder die ganze Krankengeschichte ausgehändigt werden. Zudem können Ärzte und Pflegepersonal, welche sachdienliche Hinweise geben können, auch als Zeugen einvernommen werden. Sie müssen allerdings vom Rechtsdienst des Departements Gesundheit und Soziales vom Berufs- und Amtsgeheimnis entbunden sein.

5 Systemtechnische Datenschutzmassnahmen

Folgende Datenschutzanforderungen sind auf Systemebene zu berücksichtigen.

Datensicherheit bei der Kommunikation und bei Serversystemen:

Wenn folgende Fragen mit "Ja" beantwortet werden können, ist die Datensicherheit gegeben:

- Werden bei der Kommunikation und bei Transaktionen die Vertraulichkeit, Integrität (Richtigkeit), Aktualität und Authentizität der Daten durch den Einsatz modernster Technologien gewährleistet (z.B. durch Verschlüsselung, Firewall, Antivirenschutzprogramme, Anti-Spamfilter, Zugang nur über Passwort bei beschränktem Berechtigungskreis)?
- Ist die Datensicherheit bei Servern durch angemessene organisatorische und technische Massnahmen garantiert?
- Wird die Korrektheit, nämlich, dass Personendaten richtig und, soweit es der Zweck des Bearbeitens verlangt, vollständig sind, verifiziert?
- Können falsche Daten mit Begründung korrigiert werden?
- Sind die Daten vor unberechtigter Kenntnisnahme oder Verfälschung geschützt?
- Sind die mit der Verarbeitung von Personendaten und der Nutzung entsprechender Applikationen und Systeme eingesetzten Mitarbeitenden über den korrekten Umgang informiert?
- Haben Mitarbeitende nur auf jene Patientenakten Zugriff, die einen direkten Behandlungsbezug aufweisen?

5.1 Zugriffsberechtigungen

Zugriffsberechtigungen sind nach dem Need-to-Know-Prinzip umzusetzen, das heisst, dass Mitarbeitende nur auf Patienten- und Falldaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigten. Der Zugriff darf nur bei existierendem Behandlungsauftrag oder bei Vorliegen eines Auftrages bzw. einer Anordnung durch eine/n Ärztin/Arzt erfolgen.

Administrative und medizinische Daten besonderer Patientengruppen (Personalarztpatienten, Mitarbeitende als KSB-Patienten und VIPs) sind speziell zu kennzeichnen, damit der Zugriff darauf entsprechend eingeschränkt werden kann.

Für jede Applikation, die besonders schützenswerte Personendaten bearbeitet und Persönlichkeitsprofile enthält oder die Daten Dritten zugänglich macht, ist im Rahmen des Bearbeitungsreglements ein Rollen- und Berechtigungskonzept erforderlich. Dabei ist die Umsetzung der Regelungen dieses Kapitels aufzuzeigen.

Zwei Zugriffsarten sind zu unterscheiden:

Fallbasierter Zugriff: Wenn Mitarbeitende Patienten betreuen resp. einen Behandlungsauftrag haben

Wenn folgende Fragen mit "Ja" beantwortet werden können, ist ein fallbasierter Zugriff gegeben:

- Ist eine aktive Mitarbeit am Behandlungsprozess des Patienten erforderlich, d.h. durch den Patienten gewünscht oder durch die/den behandelnde/n Ärztin/Arzt explizit angefordert resp. beauftragt?

- Ist ein Zugriff auf den aktiven Fall zur Ausführung des Auftrages oder zur Dokumentation und Speicherung von Ereignissen notwendig?
- Können nur Daten eingesehen werden, die zur Erfüllung des Auftrages absolut notwendig sind (Verhältnismässigkeit)?

5.1.1 Such- und Exportfunktionen

Folgende Regelungen sind im Zusammenhang mit Such- und Exportfunktionen zu beachten:

- Zugriffsberechtigungen gelten auch für Suchfunktionen
- Such- und Exportfunktionen sind zu protokollieren
- Zugriffe auf Exportfunktionen sind einzuschränken
- Browsen in Patientendaten ist durch das Setzen von restriktiven Zugriffsberechtigungen zu unterbinden
- Zugriffe auf VIPs und eigene Mitarbeitende sind einzuschränken (bspw. mittels Flag in der entsprechenden Anwendung)

5.1.2 Administrative Zugriffe

Administrative Zugriffe sind nur sehr restriktiv zu vergeben und auf IT- und Fachapplikationsverantwortliche zu beschränken. Sie unterliegen einer besonderen Bewilligungspflicht.

Alle Aktivitäten, für die privilegierte Berechtigungen notwendig sind (gilt für Anwendungen mit Personendaten aber auch für Systeme); sind ausführlich zu protokollieren und regelmässig zu kontrollieren.

Benutzer mit privilegierten Berechtigungen müssen über eine eindeutige Userkennung (User Account) verfügen, damit sie anhand des Benutzernamens eindeutig identifiziert werden können. Ggf. haben sie eine Geheimhaltungserklärung zu unterzeichnen.

5.2 Protokollierung

Es sind zwei Typen von Protokollen zu unterscheiden:

Das Ereignisprotokoll

Das Ereignisprotokoll (als minimale Protokollierung) ist für die Meldung von Ereignissen bspw. bei Fehlern, unberechtigten Zugriffen, Systemzuständen usw. zu nutzen. Der Protokollinhalt besteht im Minimum aus: Datum; Uhrzeit; Benutzer-Account; Ereignis (ggf. Errorcode).

Das Verlaufsprotokoll

Das Verlaufsprotokoll (als ausführliche Protokollierung) ist zur Sicherstellung der Nachvollziehbarkeit zu nutzen und kann auch Elemente eines Ereignisprotokolls beinhalten (auch bekannt unter dem Namen Audit-Trail). Der Protokollinhalt besteht im Minimum aus: Datum; Uhrzeit; Benutzer-Account; vorgenommene Änderung, Eingabe / ausgeführte Aktion / betroffene Daten, resp. Datensätze; Begründung / Zweck der Bearbeitung oder des Zugriffes.

Schutz der Protokolle

Durch das Anlegen von Protokollen, die Personendaten beinhalten bzw. eine personenbezogene Aufzeichnung vornehmen, wird wiederum eine Datensammlung geschaffen, die dem Datenschutzgesetz unterliegt und die entsprechend zu schützen ist.

Folgende Regelungen sind zu befolgen:

- Die Protokolle sind alle zwei Wochen auszuwerten.
- Die Protokollierung unterliegt der Zweckbindung.
- Eine nachträgliche Änderung der Protokolldaten darf nicht möglich sein.
- Die Protokolle sind während eines Jahres revisionssicher aufzubewahren.
- Der Zugriff auf die Protokolle ist auf diejenigen Personen einzuschränken, die die Einhaltung der

Datenschutzvorschriften kontrollieren resp. die Protokolle auswerten.

Präventive Massnahmen zur Sicherstellung des Datenschutzes sind einer Protokollierung vorzuziehen.

6 Auswertung der Protokolle

6.1 Grundsätzliches

Die Auswertung der Protokolle ist, wenn immer möglich, automatisiert mit entsprechenden Analysewerkzeugen vorzunehmen. Die mit der Systemüberwachung beauftragten Stellen (in der Regel die Administratoren) sind berechtigt, die Protokolldaten anonym auszuwerten und einzusehen.

Sobald die anonyme Überprüfung Hinweise oder einen Verdacht auf Verletzung der Datenschutzbestimmungen des KSB liefern, informiert der zuständige Administrator den Leiter Informatik. Dieser nimmt bei Bedarf Rücksprache mit der Datenschutzbeauftragten. Danach beantragt der Leiter Informatik bei der Geschäftsleitung eine personenbezogene Auswertung. Falls dem Antrag stattgegeben wird, erteilt der Leiter Informatik den Auftrag für eine personenbezogene Auswertung. Nach der Auswertung beurteilen die Datenschutzbeauftragte und der Leiter Informatik, ob es sich um einen Verstoss handelt und die Leitung Human Resources involviert werden muss. Die Geschäftsleitung wird über das Ergebnis informiert.

6.2 Missbräuchliche KISIM-Zugriffe

KISIM-Zugriffe auf Patientenakten von behandelten Personen, die ausserhalb der eigenen Organisationseinheit erfasst wurden, werden protokolliert und mit dem Zweck, unberechtigte Zugriffe zu identifizieren und durch konsequente Ahndung zukünftig zu verhindern, ausgewertet. Die Auswertung erfolgt für Pflege und übriges medizinisches Personal (Ärzteschaft, MPAs, Physiotherapeutinnen und –therapeuten etc.) gesondert, durch zwei einzelne berechtigte Personen des jeweiligen Departements.

6.3 Sanktionierung

Aufgrund der Schwere des Verstosses entscheidet die Leitung Human Resources in Absprache mit der Datenschutzbeauftragten und ggf. der Geschäftsleitung, über angemessene Disziplinarmassnahmen und Sanktionen. Diese reichen von einfachen Verweisen, sofortiger Freistellung bis zur Anzeige bei Vorliegen einer Straftat. Bei materiellen oder immateriellen Schäden behält sich das KSB vor, zusätzlich Haftpflichtforderungen zu stellen. Bei unberechtigten KISIM-Zugriffen findet zuerst ein Gespräch statt und es sich eine schriftliche Begründung an die Departementsleitung abzugeben, im Wiederholungsfall kommt es zum schriftlichen Verweis, der schriftlichen Verwarnung und beim 4. Unberechtigten Zugriff schliesslich zur Kündigung.

7 Organisation des Datenschutzes

7.1 Geschäftsleitung

Die Geschäftsleitung definiert mit der Datenschutzweisung die übergeordneten Grundsätze für die Gewährleistung des Datenschutzes beim KSB. Sie ernennt eine datenschutzverantwortliche Person, die Datenschutzbeauftragte, die mit der Durchsetzung der datenschutzrechtlichen Vorgaben.

7.2 Vorgesetzte

Die Vorgesetzten aller Stufen sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung des Datenschutzes verantwortlich, insbesondere im Rahmen der Geschäftsprozesse. Sie sorgen in Zusammenarbeit mit der Datenschutzbeauftragten für Schulung und Sensibilisierung der Mitarbeitenden. Sie nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, Massnahmen zum Datenschutz einzuhalten.

7.3 Medizinisches Personal

Für die Einhaltung des Datenschutzes sind diejenigen Stellen, bei denen der Patient behandelt wird,

verantwortlich. Für medizinische Daten trägt der Chefarzt die Gesamtverantwortung. Die/der jeweilige behandelnde Ärztin/Arzt sowie sämtliche Mitarbeitenden des KSB sind ihrerseits verantwortlich, dass sie den Datenschutz der Patientinnen und Patienten, welche sie behandeln bzw. von denen sie Daten bearbeiten, einhalten.

7.4 Datenschutzbeauftragte

Die Datenschutzbeauftragte ist die Ansprechperson für den Datenschutz. Sie nimmt insbesondere folgende Aufgaben wahr:

- Die Überwachung der Anwendung der Vorschriften zum Datenschutz
- Behandlung von Meldungen betreffend der Missachtung von Vorschriften
- Beratung bei der Anwendung von Massnahmen
- Prüfung und Umsetzung neuer datenschutzrechtlicher Bestimmungen
- Kontrolle und Abnahme der Bearbeitungsreglemente
- Bewilligung von Auskunftsgesuchen und Datensperrungen sowie Anfragen zur Weitergabe von Personendaten an Dritte
- Führen des Registers der Datensammlungen mit Personendaten innerhalb des KSB und jährliche Abgabe einer Kopie an die beauftragte Person für Öffentlichkeit und Datenschutz
- Überwachung der Datensammlungen bezüglich Erstellen / Anlegen, Mutation und Löschung
- Durchführung unabhängiger Kontrollen
- Abgabe von Empfehlungen zur Verbesserung des Datenschutzes
- Jährliche Information der Geschäftsleitung über ihre Tätigkeit und den Stand des Datenschutzes beim KSB

7.5 Dateneigner

Im Aussenverhältnis ist das KSB formell Inhaberin sämtlicher Datensammlungen, die es unterhält. Im Innenverhältnis sind die Dateneigner für die Datensammlungen verantwortlich.

Die Dateneigner haben folgende Aufgaben und Verantwortlichkeiten:

- Gewährleistung des Datenschutzes bei den ihnen zugewiesenen Datensammlungen sowie deren Überwachung
- Sicherstellung der Qualität, Datenintegrität und Richtigkeit der Daten
- Klassifizierung und Inventarisierung der Datensammlungen und der zu ihrer Bearbeitung benötigten Prozesse und Systeme sowie deren Beschreibung
- Festlegung der Aufbewahrungsdauer
- Erarbeitung von Bearbeitungsreglementen, sofern solche nötig sind, sowie deren Überwachung und Einhaltung
- Meldung neuer Datensammlungen vor deren Eröffnung an die Datenschutzbeauftragte
- Meldung von Löschungen und Änderungen von Datensammlungen an die Datenschutzbeauftragte
- Meldung der Bekanntgabe von Personendaten sowie der Übermittlung von Datensammlungen ins Ausland an die Datenschutzbeauftragte
- Unterstützung bei Auskunftsbegehren
- Bestimmung der zum Bearbeiten der Daten befugten Personen und deren Zugriffrechte

7.6 Leitung Human Resources (Abteilung Human Resources)

Die Leitung Human Resources und die im Personalbereich tätigen Mitarbeitenden sind für die

sorgfältige und datenschutzkonforme Bearbeitung der Personaldaten verantwortlich.

7.7 Leiter Informatik (Abteilung Informatik)

Der Leiter Informatik trägt die Verantwortung, dass die Datensicherheit und datenschutzrechtliche Massnahmen technisch umgesetzt werden. Dabei unterstützen ihn insbesondere die Applikations- und Systemverantwortlichen. Er arbeitet eng mit der Datenschutzbeauftragten zusammen, um die Konformität der Massnahmen zu prüfen. So beurteilt er Risiken, Vorfälle und Beinahe-Vorfälle, welche den Datenschutz gefährden können.

7.8 Mitarbeitende

Alle Mitarbeitenden sind für den Datenschutz in ihrem Aufgabenbereich verantwortlich und verpflichtet, Personendaten nach den gesetzlichen und internen Bestimmungen zu bearbeiten. Kritische Aufmerksamkeit und eigenverantwortliches Verhalten werden vorausgesetzt. Mitarbeitende können sich bei Unklarheiten oder für Auskünfte jederzeit an ihren Vorgesetzten oder an die Datenschutzbeauftragte wenden. Mögliche oder tatsächliche Datenschutzverletzungen haben sie auf direktem Weg der Datenschutzbeauftragten mitzuteilen.

8 Anhang I: Gesetzliche Grundlagen

Folgende gesetzlichen Grundlagen (Aufzählung ohne Anspruch auf Vollständigkeit) sind beim Umgang mit **Personendaten**, und damit auch im Umgang mit Patienten- und Personaldaten, generell zu beachten:

- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1)
- Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11)

Zusätzlich sind folgende gesetzliche Grundlagen beim Umgang mit **Patientendaten** zu beachten:

- Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB, SR 311.0); insbes.:
    - Art. 320: Amtsgeheimnis
    - Art. 321: Berufliche Schweigepflicht
- Gesundheitsgesetz des Kantons Aargau vom 20. Januar 2009 (GesG, AGS 301.100); insbes.:
    - § 15: Einzelne Berufspflichten für Personen, die in Berufen des Gesundheitswesens tätig sind
    - § 19: Schweigepflicht, Berufsgeheimnis
    - § 20: Meldepflichten
    - § 21: Melderechte, Aufhebung Schweigepflicht
    - § 28: Grundsätze Rechte und Pflichten der Patientinnen und Patienten
- Verordnung über die Rechte und Pflichten der Patientinnen und Patienten vom 11. November 2009 (PatV, AGS 333.111); insbes.:
    - § 5: Grundsatz Einwilligung in Untersuchungen und Behandlungen
- Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau vom 24. Oktober 2006 (IDAG, AGS 150.700) sowie die dazu gehörende Verordnung (VIDAG SAR 150.711)
- Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB für die Bearbeitung von Personendaten im medizinischen Bereich, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/bearbeitung-von-personendaten-im-medizinischen-bereich.html?

Mitarbeitende haben im Umgang mit **Personaldaten** folgende gesetzliche Grundlagen zu beachten:

- Pflichten des Arbeitgebers / Schutz der Persönlichkeit des Arbeitnehmers (Art. 328b OR, SR 220)
- Leitfaden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB für die Bearbeitung von Personendaten im Arbeitsbereich - Bearbeitung durch private Personen, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/leitfaeden/bearbeitung-von-personendaten-im-arbeitsbereich.html?

Zudem gelten die Allgemeinen Anstellungsbedingungen des KSB (AAB).

9 Anhang II: Ärztliche bzw. berufliche Schweigepflicht

Anhang zum Reglement Datenschutz (Patienten) - Ärztliche bzw. berufliche Schweigepflicht

1. Rechtsgrundlagen

a) Die berufliche Schweigepflicht gemäss Strafgesetzbuch Art. 321[6] StGB
Die berufliche Schweigepflicht bezeichnet die Pflicht der Ärzteschaft, Apotheker/innen, Hebammen, Psychologen/innen, Pflegefachpersonen, Physiotherapeuten/innen, Ergotherapeuten/innen, Ernährungsberater/innen, Informationen, die ihnen im Rahmen der beruflichen Tätigkeit anvertraut worden sind, oder die sie bei deren Ausübung wahrgenommen haben, geheim zu halten.

b) Die berufliche Schweigepflicht gemäss Datenschutzgesetz Art. 35[7] DSG
Die berufliche Schweigepflicht nach Art. 35 DSG betrifft sämtliche Personen, deren Beruf (beispielsweise als Psychologen, Therapeuten, Patientenaufnahme) die Kenntnis besonders schützenswerter Personendaten erfordert.

c) Im gleichen Sinn äussert sich auch die Verordnung über die Rechte und Pflichten der Patientinnen und Patienten des Kantons Aargau (PatV, SAR 333.111).

Die genannten Personen haben die Pflicht, Personendaten, von denen sie bei der Ausübung ihres Berufes erfahren, geheim zu halten. Dies beginnt bereits beim Namen einer Person im Hinblick auf eine den Gesundheitszustand betreffende Frage.

Die Geheimhaltungspflicht bleibt auch nach Beendigung der entsprechenden Berufsausübung oder Ausbildung bestehen.

2. Schweigepflichtiger Personenkreis

Ärzteschaft, Pflegepersonal und sämtliche in der Behandlungskette tätigen Personen, inklusive administrativem Hilfspersonal sind im Sinne von Art. 321 StGB zum Schweigen verpflichtet.

Das übrige Spitalpersonal unterliegt der Schweigepflicht gemäss Art. 35[8] DSG

3. Was fällt unter die Schweigepflicht?

Die berufliche Schweigepflicht und das DSG/IDAG schützen Gesundheitsdaten in jeder Form: Papierakten, Karteikarten, Video-Aufzeichnungen, elektronische Patientenakten, sämtliche elektronischen Patientendaten, aber auch mündliche Informationen. Dies betrifft alle

---

6 Art. 321 StGB
Verletzung des Berufsgeheimnisses
1. […] Ärzte, Zahnärzte, Chiropraktoren, Apotheker, Hebammen, Psychologen, Pflegefachpersonen, Physiotherapeuten, Ergotherapeuten, Ernährungsberater, Optometristen, Osteopathen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Die Verletzung des Berufsgeheimnisses ist auch nach Beendigung der Berufsausübung oder der Studien strafbar. Ebenso werden Studierende bestraft, die ein Geheimnis offenbaren, das sie bei ihrem Studium wahrnehmen.
2. Der Täter ist nicht strafbar, wenn er das Geheimnis auf Grund einer Einwilligung des Berechtigten oder einer auf Gesuch des Täters erteilten schriftlichen Bewilligung der vorgesetzten Behörde oder Aufsichtsbehörde offenbart hat.
3. Vorbehalten bleiben die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.

7 Art. 35 DSG
1. Wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat, wird auf Antrag mit Haft oder mit Busse bestraft.
2. Gleich wird bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Tätigkeit für den Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.
3. Das unbefugte Bekanntgeben geheimer, besonders schützenswerter Personendaten oder Persönlichkeitsprofile ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

8 vgl. dazu § 8 ff. IDAG und § 19 GesG
Personen, die in Berufen des Gesundheitswesens tätig sind, sowie ihre Hilfspersonen haben über Geheimnisse, die ihnen infolge ihres Berufs anvertraut worden sind, oder über Wahrnehmungen, die sie in Ausübung des Berufs gemacht haben, zu schweigen.

personenbezogenen Daten und Tatsachen wie zum Beispiel

a) die Tatsache, dass überhaupt ein Behandlungsverhältnis besteht
b) die Art der Verletzung oder Erkrankung, der Unfallhergang, der Krankheitsverlauf
c) Untersuchungsergebnisse, Diagnosen und Verdachtsdiagnosen
d) durchgeführte Massnahmen
e) Tod des Patienten

4. Wem gegenüber gilt die Schweigepflicht?

Die Schweigepflicht gilt grundsätzlich gegenüber allen, ausser der behandelten Person. Die/der Patient/in ist Geheimnisherr, das heisst Patientendaten dürfen gegenüber Dritten nur offenbart werden, wenn der Geheimnisherr den Geheimnisträger (beispielsweise die/den Ärztin/Arzt) von ihrer/seiner Schweigepflicht befreit oder ein Gesetz dies ausdrücklich erlaubt oder ein positiver Entbindungsentscheid des Departements Gesundheit und Soziales (DGS) vorliegt. Als Dritte gelten alle Personen, die nicht in der Behandlungskette tätig sind.

Beispiel 2:
Obwohl alle Ärzte der Schweigepflicht unterstehen, gilt jeder Arzt, der nicht mit der Behandlung des betreffenden Patienten X betraut ist, als Dritter. Ohne dass eine der unten genannten Ausnahmen gegeben ist, darf deshalb Arzt A seinem Kollegen B keine Angaben über Patient X machen.

5. Wann kann die ärztliche Schweigepflicht aufgehoben werden?

Das ärztliche Berufsgeheimnis gilt nicht absolut und kann in folgenden Fällen aufgehoben werden (Art. 321 Ziff. 3 StGB, § 21 Abs. 2 GesG und § 15 Abs. 1 IDAG):

- eine Einwilligung des Berechtigten oder
- eine schriftliche Bewilligung/Anweisung der Aufsichtsbehörde[9] liegt vor.
- Zudem ist eine Aufhebung auch möglich, wenn in einer eidgenössischen oder kantonalen Bestimmung gegenüber einer Behörde die Zeugnispflicht oder die Auskunftspflicht vorgesehen ist (Art. 321 Ziff. 3 StGB).

Für die medizinische Forschung gelten Sonderregelungen, die in dieser Schrift nicht behandelt werden.

a) Einwilligung des Berechtigten

Die behandelte Person kann je nach Situation ausdrücklich - das heisst mündlich oder schriftlich - oder stillschweigend in die Weitergabe ihrer persönlichen Gesundheitsdaten einwilligen. Sie muss freiwillig und ohne Druck entscheiden können, ob sie ihre Einwilligung geben will. Die Einwilligung ist ferner nur gültig, wenn sich die behandelte Person über das Ausmass der ganzen Datenbearbeitung, den Zweck und den/die Empfänger der Daten im Klaren ist. Daher sind die pauschalen Einwilligungserklärungen nichtig, welche auf manchen Formularen für Versicherungsanträge oder in den Allgemeinen Geschäftsbedingungen zu finden sind.

b) Auskünfte an vor-/nachbehandelnde Ärzte und weitere zusammenarbeitende Stellen

Stillschweigende Einwilligung wird vermutet in Bezug auf vor- und nachbehandelnde Ärzte. Diesen darf, sofern nicht auf einen Geheimhaltungswillen des/der Patienten/in geschlossen werden muss, jene Information weitergegeben werden, die sie zur Erfüllung ihrer Aufgabe brauchen (§ 19f. PatV).

Beispiel 3:
Arztrapporte dienen der interdisziplinären Zusammenarbeit von Ärzten und der Qualitätssicherung. Es ist davon auszugehen, dass sich die stillschweigende – unter dem Vorbehalt, dass nur die nötigen Informationen weitergegeben werden – Einwilligung auch auf diese Arztrapporte bezieht. Dagegen sind in Schulungsveranstaltungen die Unterlagen zu anonymisieren, sofern nicht eine ausdrückliche Einwilligung der Patientin resp. des Patienten vorliegt.

Bei der unmittelbaren Zusammenarbeit zwischen verschiedenem medizinischen Personal darf von der stillschweigenden Zustimmung der behandelten Person ausgegangen werden,

[9] § 25 Abs. 3 PatV: Bewilligungen oder Anweisungen zur Aktenherausgabe werden durch das Generalsekretariat des DGS erteilt.

soweit diese um die Zusammenarbeit weiss und soweit nur jene Angaben ausgetauscht werden, die im konkreten Fall für die Zusammenarbeit wirklich notwendig sind. Gleiches gilt für den Datenaustausch mit allen Personen im gleichen Spital, sofern es der Erledigung einer objektiv notwendigen Aufgabe dient.

Beispiel 4:
Für die Weitergabe der Patientennamen an Gemeindeseelsorger, Laienhelfer, kommunale freiwillige Betreuungsdienste und andere Organisationen kann nicht von vornherein von der stillschweigenden Zustimmung des/der Patient/in ausgegangen werden. Die Information solcher Dienste kann unentbehrlich sein, um soziale Netze während einem längeren Spitalaufenthalt von chronisch Kranken aufrechtzuerhalten und der Vereinsamung der Menschen entgegenzuwirken. Der Entscheid darüber, ob sie solche Dienste beanspruchen will, obliegt einzig der zu behandelnden Person und für deren Benachrichtigung ist in jedem Fall ihre Einwilligung erforderlich

c) Informationen an den nächsten Angehörigen oder den gesetzlichen Vertreter

Nächste Angehörige im Sinn des Gesundheitsgesetzes sind die von der urteilsfähigen Patinentin bezeichneten Personen. Trotz Nachfragens wird die behandelte Person in vielen Fällen die zu informierenden Angehörigen nicht ausdrücklich bezeichnen. Hier gilt eine Vermutungsumkehr: Sofern nicht auf einen Geheimhaltungswillen der behandelten Person geschlossen werden muss, wird eine stillschweigende Einwilligung für die Weitergabe behandlungsrelevanter Informationen vermutet.[10] Als nächste Angehörige gelten dann insbesondere der Lebenspartner, danach die Blutsverwandten (in der Reihenfolge Kinder, Eltern, Geschwister).[11]

Beispiel 5:
Telefonisch wird angefragt: „Wurde mein Kind/Mann/Frau ins Spital gebracht?“
Kann der Anrufer glaubhaft machen, dass er nächster Angehöriger ist, ist die gewünschte Auskunft zu erteilen, sofern der/die Patient/in nicht ausdrücklich gewünscht hat, seine/ihre Angehörigen seien nicht zu informieren.

Der Geheimhaltungswille des/der Patienten/Patientin ist jedoch zu vermuten bei bestimmten Krankheiten/Behandlungen.

Beispiel 6:
Patient/in möchte sterilisiert werden und lässt erkennen, dass sie das nicht mit ihrem Mann besprochen hat.

Beispiel 7:
Patientin möchte abtreiben und lässt erkennen, dass sie dies nicht mit ihrem Mann besprochen hat.

Beispiel 8:
Patientin möchte abtreiben, Kind ist nicht mit ihrem Gatten gezeugt worden.

In diesen Fällen hat die/der Ärztin/Arzt den ausdrücklichen oder vermuteten Geheimhaltungswillen zu respektieren. Informationen darf sie/er nur weitergeben, wenn sie/er ausdrücklich dazu ermächtigt ist.

Beispiel 9:
Patient wird erstmals HIV-positiv getestet und zeigt sich in Bezug auf das Schutzverhalten gegenüber seiner Partnerin, die keine Kenntnis hat über die Infektion, uneinsichtig. Der Arzt hält die sofortige Information der Partnerin für erforderlich, um sie zu schützen.

Ein Recht des Arztes zur Information (Partnernotifikation) ist dort gegeben, wo der Arzt sieht, dass die behandelte Person ihren Partner oder andere Personen an Leib und Leben schwer gefährdet. In diesen Fällen überwiegt das Schutzinteresse der Gefährdeten. Hält der Arzt die Bedrohung für so imminent, dass Sofortmassnahmen nötig sind, kann er die

---

10 § 20 PatV: Sofern aus den Umständen nicht auf einen Geheimhaltungswillen des Patienten geschlossen werden muss, wird die Zustimmung für Auskünfte an vor- und nachbehandelnde Ärzte, den gesetzlichen Vertreter und den nächsten Angehörigen vermutet.

11 § 2 Abs. 2 PatV

gefährdeten Personen informieren. Das unrechtmässige Verhalten wird durch Notstand im Sinne von Art. 17 StGB gerechtfertigt. Ist nicht unmittelbares Handeln nötig, muss der Arzt beim Rechtsdienst des Departements für Gesundheit und Soziales um Entbindung vom Berufsgeheimnis ersuchen.

Beispiel 10:
Anlässlich einer anderen Behandlung wird erkannt, dass eine Patientin HIV-positiv ist. Die Patientin zeigt sich in Bezug auf das Schutzverhalten gegenüber ihrem Partner, der keine Kenntnis hat über die Infektion, uneinsichtig. Die Patientin bleibt noch einige Tage stationär im Spital. Das Schutzinteresse besteht, aber bis zum Austritt ist genügend Zeit, um die Entbindung vom Arztgeheimnis einzuholen.[12]

d) Informationspflichten bei urteilsunfähigen Patienten

- **Urteilsunfähige Person hat eine gesetzliche Vertretung**
  Die gesetzliche Vertretung ist gleich zu informieren wie die zu behandelnde Person, wenn sie urteilsfähig wäre. Die gesetzliche Vertretung erteilt die Einwilligungen zu Untersuchungen, Behandlungen und Eingriffen. In Notfällen (wenn der gesetzliche Vertreter nicht erreicht werden kann) darf die Zustimmung vermutet werden. Verweigert die gesetzliche Vertretung die Zustimmung ist die Einwilligung der Kindes- und Erwachsenenschutzbehörde erforderlich[13].

  Aber: Während die/der urteilsfähige Patient/in lebensrettende Massnahmen ablehnen kann, gilt die Verweigerung der Zustimmung zu einer lebensrettenden Massnahme immer als missbräuchlich[14].

  Aber auch: Die gesetzliche Vertretung hat Anspruch auf Anhörung bei der Auslegung von Patientenverfügungen[15].

  In dringenden Fällen entscheidet die/der Ärztin/Arzt, ob die Verweigerung der Zustimmung missbräuchlich ist und deshalb missachtet werden kann[16].

- **Urteilsunfähige Person hat keine gesetzliche Vertretung**
  In diesen Fällen haben die nächsten Angehörigen ein Recht auf Information und Anhörung, die/der Ärztin/Arzt entscheidet jedoch im vermuteten Interesse des Patienten[17].

e) Urteilsfähige, aber nicht handlungsfähige Person

Die gesetzliche Vertretung ist vor grösseren oder mit erheblichen Risiken verbundenen Eingriffen zu informieren. Diese Information hat zu unterbleiben, wenn die/der urteilsfähige Patient/in dies so wünscht.[18]

Beispiel 11:
Die urteilsfähige 16-jährige Patientin möchte nicht, dass ihre Familie über die Abtreibung informiert wird. Die Mutter der Patientin fragt nach, ob ihre Tochter im Spital sei oder sie fragt nach, weshalb ihre Tochter im Spital sei. Der Arzt darf keine Auskunft erteilen.

f) Ermächtigung durch die vorgesetzte Behörde

Willigt die behandelte Person nicht ein und ermächtigt kein Gesetz ausdrücklich die Herausgabe von Gesundheitsdaten, kann nur der Rechtsdienst des Departements für Gesundheit und Soziales beziehungsweise das Verwaltungsgericht von der Schweigepflicht

---

12 Hier ist darauf hinzuweisen, dass das Entbindungsgesuch dem Patienten zur schriftlichen Stellungnahme innert (i.d.R.) 10 Tagen zugestellt wird. Nach Eingang der Stellungnahme (und allfällig weiteren einzuholenden Informationen) ergeht ein schriftlicher Entscheid des DGS, Generalsekretariat). Aufgrund der genannten Frist und der Bearbeitung sowie der Zeit für die postalischen Zustellungen und dem Abwarten der Rechtskraft des Entscheides, reichen "einige Tage" nicht aus, um eine rechtskräftige Ermächtigung der Behörde zur Offenbarung des Geheimnisses zu erhalten.

13 § 6 Abs. 2 PatV

14 § 6 Abs. 2 PatV

15 Dies gilt nur, wenn die Patientenverfügung auslegungsbedürftig ist.

16 § 6 Abs. 2 PatV

17 § 6 Abs. 3 PatV

18 § 21 PatV

entbinden.[19]

g) Gesetzliche Entbindungen von der Schweigepflicht (Meldepflichten und Melderechte)
Ärzte/innen können nur zu Meldungen an Ämter verpflichtet werden, wenn das Gesetz es so vorsieht. Daneben gibt es auch Gesetze, die ein Recht (aber keine Pflicht) für Meldungen enthalten. In diesen Fällen entbindet das Gesetz im beschriebenen Umfang von der ärztlichen Schweigepflicht. Hierzu ist das Informationsblatt Melderechte und Meldepflichten auf den Intranet zu beachten.

6. Verhältnis zum Vertrauensarzt von Krankenkassen

Ärzte/Spitäler sind verpflichtet, den Krankenkassen alle Angaben zu machen, die zur Feststellung des Anspruchs auf Leistungen notwendig sind. Oder anders: Der Krankenkasse sind nur jene Informationen zuzustellen, die zur Beurteilung des Leistungsanspruchs notwendig sind. Ob die Diagnose dazu gehört, ist umstritten. In der Regel reicht eine Rahmendiagnose (letzte 2 Ziffern des ICD-Codes) aus. Ist eine differenziertere Diagnose zur Abklärung des Leistungsanspruchs nötig, muss die Kasse dies begründen. Die Zustellung erfolgt dann an den Vertrauensarzt. Dieser sollte sich darauf beschränken, gegenüber der Kasse über das Ausmass ihrer Leistungspflicht Stellung zu nehmen. Entsteht ein Streit über die Leistungspflicht, braucht es zur Deblockierung der medizinischen Akten das Einverständnis des Geheimnisherrn.[20]

7. Zeugnisverweigerungsrecht

Ärzte im Kanton Aargau haben das Recht, im Prozess das Zeugnis zu verweigern. Damit sie aussagen dürften, bedarf es der Entbindung vom Arztgeheimnis durch den Geheimnisherrn oder durch den Rechtsdienst des Departements Gesundheit und Soziales. Doch auch bei vorliegender Entbindung kann die/der Ärztin/Arzt das Zeugnis verweigern. In der Regel wird sie/er versuchen abzuschätzen, ob der Geheimnisherr völlig ohne Druck und in voller Kenntnis der Konsequenzen die Entbindung erteilt hat und/oder ob die Aussage im Interesse des Patienten ist.

8. Sanktionen

Zuwiderhandlung gegen Art. 321 StGB wird auf Antrag mit einer Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft**.**

Verletzung der beruflichen Schweigepflicht gemäss Art. 35 DSG wird mit Busse bestraft.

01.08.2021, Claudia Wyss, Datenschutzbeauftragte der Kantonsspital Baden AG

Genehmigt durch die Geschäftsleitung

Adrian Schmitter, CEO

19 § 25 PatV und IDAG § 36 - 39
20 Brühwiler, S. 244ff