Inhaltsverzeichnis Datenschutzrichtlinien

Zweck	2
Geltungsbereich	2
Grundsätze des Datenschutzes	2
Verantwortlichkeit	3
Prinzip der Verhältnismässigkeit	3
Prinzip der Zweckbindung	3
Rechte der Bewohner und Mitarbeiter	4
Pflichten der Verantwortlichen	4
Umgang mit den Bewohnerdaten	4
Technische und organisatorische Massnahmen	6
Internet (Homepage) und Bilder / Fotos	7

Zweck

Die Gewährleistung des Datenschutzes und die Datensicherheit ist wichtig für den Schutz Bewohner und Mitarbeiter, über welche sensible Daten beschafft, verarbeitet, aufbewahrt und weitergegeben werden. Das vorliegende Dokument enthält Leitlinien, welche den Heimverantwortlichen und Mitarbeitenden aufzeigen, mit welchen Verhaltensweisen und Vorkehrungen der Umgang mit sensiblen Daten datenschutzkonform sichergestellt werden kann.

Die Leitlinien berücksichtigen die wichtigsten datenschutzrechtlichen Anforderungen, welche für den Heimalltag relevant sind. Sie basieren auf dem Bundesgesetz über den Datenschutz (19.6.1992) und der Verordnung zum Bundesgesetz (14.Juni 1993). Als Referenzkanton werden zudem für bestimmte Aspekte das Gesetz über den Schutz von Bewohnerdaten (6.6.1993) und die Informatiksicherheitsverordnung (17.12.1997) des Kantons Zürich berücksichtigt. Zudem fliessen die Richtlinien des Bundesgerichtsentscheid KVG vom 21. März 2007 (K12/06) ‚Edition von sensiblen Daten' ein.

Wir verweisen da wo die Gültigkeit das EU- Recht betrifft auf die gültige Gesetzgebung der DSGVO Verordnung 2018

Geltungsbereich

Die Richtlinien/Leitlinien gelten grundsätzlich für alle öffentlich/rechtlichen und privaten Heime im stationären Pflegebereich. Für Heime mit Rechtsstatus öffentlich/rechtlich bestehen allenfalls auf kantonaler und kommunaler Ebene zusätzliche Bestimmungen, sei es z.B. die kantonale Patientenrechtsverordnung, oder Weisungen der Gesundheitsdirektion im Bezug auf Einsichtsnahme in Bewohnerdossiers durch Angehörige, etc. Diese Bestimmungen sind in den folgenden Ausführungen nicht im Einzelnen berücksichtigt, sind aber durch die öffentlich/rechtlichen Heime zusätzlich zu beachten.

Grundsätze des Datenschutzes

Das Bundesgesetz über den Datenschutz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Dabei sind die folgenden Grundsätze zu beachten:

- Bewohner- bzw. Mitarbeiterdaten dürfen nur rechtmässig beschafft werden.
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
- Die Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Die rechtlichen Grundsätze gelten unabhängig von den angewandten Mitteln und Verfahren, also unabhängig davon, ob die Bearbeitung der sensiblen Daten manuell oder mit einer Software oder in Folge von E-Health erfolgt. Unter dem Begriff Bearbeiten von sensiblen Daten werden die Tätigkeiten

Beschaffung, Verwendung, Umarbeitung, Veränderung, Aufbewahrung, Weitergabe und Vernichtung von persönlichen Daten der Bewohner und Mitarbeiter verstanden.

Das Gleiche gilt auch im Zusammenhang mit Dokumenten, Unterlagen und Auskünften von und zu Mitarbeitenden der Sunnmatte.

Verantwortlichkeit

Für die Gewährleistung des Datenschutzes ist die Institution verantwortlich, die die Daten zur Erfüllung der Aufgaben bearbeitet oder bearbeiten lässt.

Die Geschäftsleitung ist also verantwortlich dafür, dass die Bestimmungen des eidg. und des kantonalen Datenschutzgesetzes umgesetzt und im Alterszentrum entsprechend angewendet werden.

Prinzip der Verhältnismässigkeit

Das Prinzip der Verhältnismässigkeit bedeutet, dass nur jene Daten im Alterszentrum gesammelt und verarbeitet werden dürfen, die für die Betreuung der Bewohner und für die verwaltungsmässige Abwicklung des Betreuungsverhältnisses bzw. der Mitarbeitenden erforderlich sind.

Dieser Grundsatz will besagen, dass ein Mitarbeiter im Alterszentrum nur jene Daten bearbeiten darf, die sie für einen bestimmten Zweck objektiv benötigt und die zum Bearbeitungszweck und zur Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen. Dies führt dazu, dass für elektronisch gespeicherte Daten differenzierte Zugriffsrechte so zu vergeben sind, dass jeder nur auf Daten zugreifen kann, die er zur Erledigung seiner konkreten Arbeit benötigt. Dies gilt auch für die Weitergabe von Daten.

Zur Verhältnismässigkeit gehört auch, dass sensible Daten nicht unbegrenzt, sondern nur so lange gespeichert werden dürfen, wie dies zur Betreuung und für die verwaltungsmässige Abwicklung des Betreuungsverhältnisses oder für die Mitarbeiterführung erforderlich sind.

Prinzip der Zweckbindung

Daten dürfen nur zu dem Zwecke bearbeitet werden, der bei der Beschaffung angegeben wurde, oder aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Die Daten dürfen also nicht wider Treu und Glauben bearbeitet werden, in einer Art, mit der die betroffenen Bewohner und Mitarbeitenden nicht rechnen mussten und mit der sie nicht einverstanden gewesen wäre. Heimliche Datenbeschaffung ist nicht erlaubt. Das Prinzip von Treu und Glauben verlangt daher auch, dass die Bearbeitung der Daten für die betroffenen Personen transparent erfolgen muss. Sie muss für die betroffene Person jederzeit erkennbar sein.

Die modernen Informatiksysteme erlauben multifunktionale Nutzungen. Die von der Informatikbearbeitung betroffenen Personen haben Anspruch zu wissen, wozu ihre Daten benutzt

werden. Werden Daten entgegen dem kommunizierten Bearbeitungszweck für weitere Zwecke verwendet, ist die Einwilligung der betroffenen Person nötig.

Rechte der Bewohner und Mitarbeiter

- Die Personen resp. deren gesetzlicher Vertreter haben das Recht auf umfassende Information über ihre Rechte, welche sie im Zusammenhang mit ihren persönlichen Daten im Alterszentrum haben.

- **Informationsrecht**
  Die Person muss konkret darüber informiert werden, welche Daten wie und zu welchem Zwecke beschafft, verarbeitet, aufbewahrt und an Dritte weitergegeben werden und dass dies papiermässig oder grösstenteils auch elektronisch erfolgt.

- **Einsichtsrecht**
  Die Personen haben jederzeit Einsichtsrecht in ihre Daten/Dossier zwecks Überprüfung der Richtigkeit und sie haben das Recht auf Berichtigung. (Prinzip der Datenintegrität)

- **Vollmachten**
  Die Personen haben das Recht, Vollmachten an Dritte (z.B. Angehörige) zwecks Einsicht in ihre Daten zu vergeben. Sie haben das Recht, solche Vollmachten jederzeit zu widerrufen.

Pflichten der Verantwortlichen

- Die Verantwortlichen sind verpflichtet, die Personen beim Eintritt oder bei Einführungen von Informatik Anwendungen über ihre Rechte zu informieren.
- Die Bewohnerverfügung (Vergabe von Vollmachten) muss mit der Bewohnenden geregelt werden
- Der Zusatz zum Pensions- oder Arbeitsvertrag ist in den üblichen Vertrag zu integrieren oder separat als Anhang unterzeichnen zu lassen. Die Zustimmung zum ergänzten Vertragswerk muss in einem aufgeklärten Klima erfolgen. Eine allfällige Verweigerung der Unterschrift muss schriftlich festgehalten werden.

Umgang mit den Bewohnerdaten

Im Alterszentrum werden hauptsächlich persönliche Daten bearbeitet. Die sensiblen Daten sind in hohem Masse schützenswert. Sie sind vertraulich zu behandeln, müssen sorgfältig aufbewahrt und vor Dritten geschützt werden.

- **Schutz vor unberechtigtem Zugriff**
  a. Die auf Papier festgehaltenen Daten (Pflegedokumentation, Dossier, Verträge, Notizen usw.) müssen durch bauliche (geeignete) Massnahmen (z.B. Verschluss) vor unberechtigtem Zugriff durch Dritte geschützt werden.
  b. Der Zugriff auf elektronisch geführte sensible Daten, muss durch strikte Passwortregelung auf die berechtigten Personen im Alterszentrum eingeschränkt werden. Der Kreis der Berechtigten ist, basierend auf der betriebsinternen

Arbeitsorganisation, möglichst klein zu halten.

- **Aufbewahrung und Archivierung der Bewohner- und Mitarbeiterdaten**
  Die entsprechenden Daten werden nach Austritt der Bewohnenden oder Mitarbeitenden im Archiv papiermässig und/oder elektronisch maximal 10 Jahre aufbewahrt und anschliessend vernichtet. Für das Archiv gelten die gleichen Richtlinien.

- **Einsichtsnahme in die eigenen Daten durch Bewohnende oder Mitarbeitende**
  Die Verantwortlichen müssen den Bewohnenden bzw. Mitarbeitenden Einsichtsrecht in ihre persönlichen Daten gewährleisten. Für die Offenlegung und Besprechung von sensitiven Gesundheitsdaten ist situativ ein Arzt/Ärztin zuzuziehen.

- **Einsichtsnahme des Pflegeteams in medizinische Bewohnerdaten**
  Die Geschäftsleitung ist berechtigt, relevante medizinische Daten an das Pflegeteam weiterzuleiten. Der oder die behandelnde Ärztin richtet sich nach den Instruktionen der Bewohnenden (Pensionärs-Pflegevertrag).

- **Einsichtnahme in sensible Daten durch Dritte**
  Drittpersonen darf nur Einsicht in die Daten gegeben werden, sofern diese über eine Vollmacht, ausgestellt durch die den Daten zugehörigen Person, verfügen.

- **Einsichtnahme in Daten durch Angehörige**
  'Angehörige' ist kein Rechtsbegriff. Die Angehörigen oder Vertretungsberechtigte Personen sind somit ‚Drittpersonen' gleichgestellt. Eine schriftliche Vollmacht ist dann nicht notwendig, wenn die Angehörigen oder Vertretungsberechtigte Personen im Beisein der Person Einsicht in die Daten nehmen.

- **Übergabe der Pflegebedarfs- und Leistungsverrechnungsdokumente an den Versicherer**
  Dem Versicherer dürfen nur das Erfassungsformular Abrechnung und diejenigen Dokumente zugestellt werden, die im Zusammenhang mit den kantonalen Tarifverträgen durch die betreffende CURAVIVA-Sektion vereinbart sind. Die Bekanntgabe dieser Informationen ist zwingend für die Abgeltung der KVG relevanten Pflegeleistungen durch die Versicherer. Die Versicherer haben durch einen Bundesgerichtsbeschluss Einsichtsrecht in die Daten von Bewohnenden.

- **Prüfung der Leistungspflicht durch Versicherer**
  Zur Prüfung der Leistungspflicht kann der Versicherer Einsicht in die Ergebnisse des Bedarfsklärungsinstrumentes und in die ärztliche Krankheitsdiagnose verlangen, sofern diese Krankheitsdiagnose Teil der bearbeiteten Bewohnerdaten des Bewohnenden sind.

  Die Verantwortlichen sind verpflichtet dem Versicherer, im Falle einer Überprüfung der Rechnungsstellung an den Versicherer sowie bei Controlling oder Nichteinverständnis bezüglich der Einteilung der Pflegestufen, sämtliche auch sensible Personendaten des Bewohners, insbesondere Pflegebericht, standardisierte Pflegeplanung, individuelle Pflegeplanung, Vitalzeichenkontrolle und individuelle Therapiepläne Einsicht zu gewähren. Die Einsicht erfolgt mit der Verpflichtung und dem Hinweis an den Versicherer, die Daten vertraulich zu behandeln und dafür zu sorgen, dass die Daten auch versicherungsintern datensicher aufbewahrt werden und nur für die mit der Bearbeitung des Falles zuständigen

Personen zugänglich sind. Ferner soll der Versicherer bei Einsicht in die Akten verpflichtet werden, die vertraulichen Akten aus der Grundversicherung nicht für die Zusatzversicherung zu verwerten.

Allein und ausschliesslich aufgrund einer schriftlichen, anderslautenden Instruktion des Bewohnenden ist die Geschäftsleitung berechtigt, die Akten dem Vertrauensarzt des Versicherers auszuhändigen.

- **Aufsicht des Kantons**
  Der Kanton kann im Rahmen seiner Aufsichtspflicht über Pflege und Betreuung Einsicht in alle Bewohner Unterlagen nehmen.
  Dieses Recht kann nur durch das Departement Gesundheit und Soziales resp. durch vom Kantonsarzt autorisierte Person wahrgenommen werden.

- **Weitergabe von Bewohnerdaten zur Beanspruchung von Ergänzungsleistungen**
  Der Pflegebedarfsausweis (=Unterlagen zuhanden der Versicherer) darf im Fall einer Beanspruchung von Ergänzungsleistungen und Pflegehilfen an das betreffende Amt, resp. an die zuständigen Gemeindestellen weitergegeben werden.

- **Übertritt in ein anderes Alterszentrum**
  Beim Übertritt von einem Alterszentrum in ein anderes dürfen die Bewohnerdaten nur mit Einverständnis der Bewohnenden weitergegeben werde. Am besten gibt das Alterszentrum die Unterlagen zusammen mit dem Pflegebericht des Bewohnenden mit und überlässt es ihm, die Unterlagen zu übergeben. Für die Übergabe von elektronischen Daten ist ebenfalls das Einverständnis des Bewohnenden nötig. Zudem ist der Austausch von Personendaten zwischen Heimen innerhalb eines Heimverbundes gegenüber den Bewohnenden transparent aufzuzeigen und zu regeln.

- **Weitergabe von elektronischen Bewohnerdaten**
  Elektronische Daten dürfen das Alterszentrum nur verlassen, sofern diese vollständig anonymisiert und der Zweck klar deklariert ist. Dies gilt beispielsweise für heimübergreifende statistische Auswertungen für die Berechnung von Qualitätskennziffern.
  Das Versenden von sensiblen Daten muss mittels eines verschlüsselten Account getätigt werden (End to End Verschlüsselung z.B. HIN Account Curaviva Gateway)

- **Ab April 2019 HIN secured Datenübermittlung**
  Sensible Daten betreffs Bewohnende oder Mitarbeitende dürfen nur per Mail mittels der HIN Curaviva Gateway Lösung verteilt und erhalten werden.

Technische und organisatorische Massnahmen

Bei der Bearbeitung von sensiblen und persönlichen Daten haben die Verantwortlichen sicherzustellen, dass die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Bewohnerdatendaten durch organisatorische und technische Massnahmen gewährleistet wird. Dies gilt unabhängig davon, ob die Bearbeitung der Daten manuell oder elektronisch via Informatik erfolgt.

Die Personendaten, welche im Alterszentrum bearbeitet werden, sind in hohem Masse schützenswert und somit ist das Risiko für die betroffenen Bewohnende gross. Die technischen und organisatorischen Massnahmen müssen angemessen sein und sind abhängig von der Grösse der Risiken, die bei Missbrauch von Informationen für die Bewohnenden, Mitarbeitenden und das Alterszentrum entstehen können.

- **Instruktion der Mitarbeiter**
  Die Mitarbeitenden müssen über die Bedeutung des Datenschutzes, über die Datenschutz – Richtlinien und über die spezifischen Bestimmungen und Schutzvorkehrungen im Alterszentrum informiert und instruiert werden.

- **Geheimhaltung**
  Die Einhaltung der gesetzlichen und vertraglichen Geheimhaltungs- und Sicherheitsbestimmungen muss durch die Mitarbeitenden schriftlich bestätigt werden.

- **Geheimhaltung durch Dritte**
  Externe technische Systembetreuer sowie externe Personen und Organisationen, welche im Auftrage des Alterszentrums Bewohner- oder Mitarbeiterdaten bearbeiten, haben eine Geheimhaltungsvereinbarung zu unterzeichnen, deren Verletzung mit einer Konventionalstrafe verknüpft werden sollte.

- **Schutz vor unberechtigtem physischem Zugriff**
  Die auf Papier festgehaltenen Bewohner- oder Mitarbeiterdaten (Pflegedokumentation, Dossier, Verträge, Gesprächsnotizen usw.) müssen durch bauliche (geeignete) Massnahmen (z.B. Verschluss) vor unberechtigtem Zugriff durch Dritte geschützt werden.

- **Informatiksicherheitsvorkehrungen**
  Siehe beigelegtes Merkblatt (IT Security Sunnmatte / Mathys Informatik AG).

- **Überwachung und Überprüfung von Daten Datenverkehr der Mitarbeiter**
  Das Alterszentrum Sunnmatte kann bei Bedarf den Datenverkehr der Mitarbeitenden überwachen und überprüfen lassen. Z. B. bei Verdacht auf Missbrauch von Internet, Facebook und weiteren Programmen!

Internet (Homepage) und Bilder / Fotos

Es ist immer wieder sehr schwierig, wie man in diesem doch sehr heiklen Bereich mit Bildern und damit mit sehr sensiblem und persönlichem Datenmaterial umgeht.

Sollten wir einmal Bildmaterial hochladen, das für betroffenen Personen, Mitarbeitenden und Ihre Angehörigen oder Vertretungsberechtigte Personen problematisch sind, so bitten wir um eine kurze Mitteilung an die Verwaltung des Alterszentrums. Wir werden das entsprechende Datenmaterial dann umgehend entfernen. Dies kann vor allem dann geschehen, wenn es sich bei der betroffenen Person um einen schon verstorbenen Bewohner oder bereits ausgetretenen Mitarbeitenden handeln. Wir

bitten Sie dazu schon im Voraus um Entschuldigung.

Mit der Annahme einer Arbeitsstelle in der Sunnmatte verbunden, ist auch die Veröffentlichung eines Mitarbeiterbildes und des Namens auf der Betriebs eigenen Webseite.

Informatiksicherheitsvorkehrungen

Im Weiteren wird auf das Merkblatt IT Security Sunnmatte / Mathys Informatik AG verwiesen!

Mit den Sicherheitsvorkehrungen beim Informatiksystem und bei Anwendungssoftware werden die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Bewohnerdatendaten sichergestellt.

Vor dem Einsatz und beim Betrieb eines Informatiksystems und einer Anwendungssoftware haben die Heimverantwortlichen die Sicherheitsvorkehrungen zu prüfen. Dabei geht es darum, die folgenden Fragen im Sinne einer Checkliste zu beantworten, resp. vom Lieferanten beantworten zu lassen: Vollständigkeit der Fragen ist nicht garantiert.

Die Nachfolgenden Punkte gilt es immer wieder zu überprüfen und auf mögliche Gefahrenproblematiken zu kontrollieren:

- Wird unbefugten Personen der Zugang zu den Informatiksystemen (Räume), welche Bewohner- und Mitarbeiterdaten bearbeiten, verwehrt?
- Wird unbefugten Personen die Benutzung von Anlagen wie W-LAN, Netzwerk usw., mit denen Bewohner- und Mitarbeiterdaten bearbeitet werden, verwehrt?
- Wird unbefugten Personen das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern beispielsweise durch Datenverschlüsselung verunmöglicht?
- Wird beim Transport von Bewohnerdaten durch entsprechende Schutzvorkehrungen (z.B. Datenverschlüsselung, Empfängeridentifikation, etc.) verhindert, sodass sensible Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Dies gilt insbesondere auch bei vernetzten Systemen und Datentransport via Internet?
- Wird die unbefugte Eingabe von Daten sowie die Einsichtnahme, Veränderung oder Löschung gespeicherter Bewohnerdaten durch entsprechende Zugriffsrechte verhindert?
- Sind die Zugriffsrechte differenziert ausgestaltet? Sind die Zugriffsrechte auf die Funktion des Benutzers ausgerichtet und auf diejenigen Daten beschränkt, die der Benutzer für die Erfüllung seiner Aufgabe benötigt?
- Werden die Zugriffsrechte laufend der aktuellen Arbeitsorganisation (Funktionen) angepasst und wird die korrekte Verwendung der Passwörter instruiert, durchgesetzt und regelmässig überprüft?
- Werden die Passwörter regelmässig überprüft und zwingend geändert
- Gibt es eine angemessene Eingabekontrolle, mit der überprüft werden kann, welche Daten zu welcher Zeit und von welcher Person eingegeben wurden?
- Können die Bewohnenden Einsicht in ihre persönlichen Daten nehmen und damit ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen oder bei Bedarf verhindern?
- Ist die tägliche/periodische Datensicherung geregelt? Werden die betreffenden Datenträger aus Sicherheitsgründen separat und örtlich getrennt vom Informatiksystem unter Verschluss aufbewahrt werden?
- Stehen für Notfälle ein Backup- und ein Restoreverfahren zur Verfügung?

- Ist beim Datenexport (z.B. für Statistikzwecke) die Anonymisierung der Bewohnerdaten sichergestellt und wird der Zweck des Datenexports überprüft