Datenschutz sicher implementieren

Offene Pflegedokumentationen oder nicht entzogene Systemzugänge ehemaliger Mitarbeitender zeigen, wie schnell Datenschutzverletzungen im Alltag entstehen können. Erfahren Sie, wie moderner Datenschutz in der Pflege systematisch aufgebaut und dauerhaft sichergestellt wird.

Text: Frank Boje

Foto: Adobe Stock/naka

Daten zur Gesundheit der Bewohner, persönliche Informationen wie Name, Adresse und Kontaktdaten, soziale und familiäre Hintergründe, finanzielle Informationen, Betreuungs- und Behandlungsdaten, Informationen über den Entwicklungsstand und viele mehr, werden in Pflege und Gesundheit verarbeitet und gespeichert. Und es werden mit zunehmender Digitalisierung mehr werden – man denke nur an die elektronische Patientenakte oder digitale Behandlungspläne. Diese große Fülle an sensiblen Informationen macht die Gesundheits- und Pflegebranche so attraktiv für Hackerangriffe. Laut dem Horizon Report 2025 wurden im Jahr 2024 weltweit 183 Millionen Patientendaten kompromittiert. Das ist ein Anstieg von neun Prozent im Vergleich zum Vorjahr. Aber Datenschutzverstöße drohen nicht nur von außen, sondern finden nahezu täglich auch intern statt. Dabei haben sensible Daten einen besonders hohen Schutzbedarf:

1. Gesetzliche Einstufung: Gesundheitsdaten fallen unter die besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO und unterliegen strengeren Schutzbestimmungen.

2. Rechtliche Verpflichtungen: Neben der DSGVO müssen Gesundheitseinrichtungen auch spezifische Branchenvorschriften und die ärztliche Schweigepflicht beachten. Für die Kirchen gelten das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) und das Kirchliche Datenschutzgesetz (KDG).
3. Vertrauensschutz: Das Vertrauen zwischen Bewohner und dem Versorgenden ist essenziell und muss durch angemessenen Datenschutz gewahrt werden.
4. Begehrlichkeit für Dritte: Gesundheitsdaten sind für verschiedene Akteure wie Pharmafirmen, Versicherungen, aber auch Cyberkriminelle von großem Interesse, was den Schutzbedarf erhöht.

Um den hohen Schutzbedarf umzusetzen, müssen viele Maßnahmen und Vorgaben berücksichtigt werden. Hier einige Beispiele:

- Einwilligungserfordernis: Die Verarbeitung von Gesundheitsdaten ist grundsätzlich nur mit ausdrücklicher Einwilligung oder aufgrund gesetzlicher Erlaubnis zulässig.
- Technische und organisatorische Maßnahmen: Einrichtungen und Organisationen müssen besondere Vorkehrungen treffen, um die Daten angemessen zu schützen.
- Meldepflichten: Bei Datenschutzverstößen bestehen Meldepflichten, z. B. an die Aufsichtsbehörden.
- Dokumentationspflichten: Sie bestehen grundsätzlich in vielen Bereichen des Datenschutzes. Bei Datenschutzverstößen müssen unabhängig von der Meldepflicht intern der genaue Hergang, die Gegenmaßnahmen und die künftige Prävention dokumentiert werden.

Sensibilisierung und Schulung von Mitarbeitenden sind essenziell

Es gibt also viel zu tun. Datenschutz funktioniert aber nur, wenn alle an einem Strang ziehen. Ohne die aktive Beteiligung der Mitarbeitenden können sensible Daten und Informationen nicht wirkungsvoll geschützt werden. Ihnen kommt deshalb eine wichtige Wächterfunktion zu.

Geschäftsführung, IT-Sicherheits- und Datenschutzverantwortliche sind verantwortlich für eine klare Definition von Datenschutz im Haus und die Kommunikation der dafür nötigen Prozesse:

- Ist die Nutzung mobiler Endgeräte im Dienst über Richtlinien geregelt?
- Dürfen private E-Mail und Internet im Dienst genutzt werden?
- Sind die Mitarbeitenden der Vertraulichkeit, auf die Verschwiegenheit und die Grundsätze des Datenschutzes verpflichtet?

Die Beschäftigung mit Datenschutz und IT-Sicherheit endet niemals. Grund dafür ist die rasante technologische Entwicklung und der Anpassungsbedarf des Datenschutzes. Man denke nur an die neuen Möglichkeiten der Datenverarbeitung und -analyse durch Künstliche Intelligenz. Deshalb ist es wichtig, Mitarbeiterinnen und Mitarbeiter regelmäßig zu sensibilisieren, zu schulen und gegebenenfalls Angriffe zu simulieren.

Dafür eignen sich eine Vielzahl an Angeboten, wie Online-Kurse, Präsenzschulungen oder Inhouse-Simulationen. Außerdem sind Handlungsempfehlungen ein wichtiges Tool – zum Beispiel für das Erkennen und den Umgang mit Phishing-Mails. Dabei wird der Empfänger solcher Mails, SMS oder Anrufe verleitet, vertrauliche Informationen preiszugeben. Es gibt inzwischen Kampagnen (sogenanntes Spear-Phishing), die hochgradig auf eine einzelne Person zugeschnitten sind. Notfallpläne geben Mitarbeitenden Sicherheit, im Ernstfall das Richtige zu tun und keine Zeit zu verschwenden. Wenn im Haus von Anfang an eine datenschutzfreundliche Arbeitsweise gelebt wird, hemmen sie auch das Alltagsgeschäft nicht. Im Gegenteil.

CHECKLISTE

- Datenschutzbeauftragten benennen (intern oder extern)
- Mitarbeiter schulen (Sensibilisierung, klare Richtlinien)
- Datenschutzkonzept erstellen (Verarbeitungsverzeichnis, Risikoanalyse, Schutzmaßnahmen)
- Technische & organisatorische Maßnahmen dokumentieren und umsetzen (Zugriffsbeschränkungen, Passwortrichtlinien, Verschlüsselung, sichere Entsorgung)
- Einwilligungen einholen (für Datennutzung von Bewohnern, Angehörigen, Mitarbeitern)
- Betroffenenrechte sicherstellen (Informationspflichten, Auskunftsrecht und Recht auf Löschung)
- Aufbewahrungs- & Löschfristen beachten (gesetzliche Vorgaben einhalten)
- Datenweitergabe prüfen (Verträge mit Auftragsverarbeitern, sichere Übermittlung)
- Datenschutzvorfälle dokumentieren & melden (Meldepflichten nach DSGVO)
- Regelmäßige Audits & Kontrollen durchführen

183

Millionen Patientendaten wurden im Jahr 2024 kompromittiert, so der Horizon Report 2025.

Das 1x1 des Datenschutzes: Datenminimierung, Zweckbindung, Transparenz

Es dürfen nur personenbezogene Daten gesammelt und verarbeitet werden, die für die Betreuung und Pflege relevant sind. Die Datenerhebung muss auf das Notwendige beschränkt bleiben, beispielsweise Name, Kontaktdaten, Gesundheitsinformationen und Pflegestufe. Eine Überprüfung der Alltagsroutinen offenbart viele Baustellen für den Datenschutz:

- Wo hängt der Dienstplan mit welchen sensiblen Informationen?
- Wie werden Abwesenheitslisten dargestellt und wo werden sie veröffentlicht?
- Gibt es Geburtstagslisten von Mitarbeitenden und oder Bewohnern?
- Liegen Einwilligungen für Zimmerbeschriftungen oder Informationssysteme im Foyer vor?
- Werden Aufbewahrungsfristen beachtet und wird Datenmüll fachgerecht entsorgt?
- Sind Rollen und Rechtekonzepte für Software-Anwendungen konsequent umgesetzt?
- Gilt das Need-to-know-Prinzip? (Es besagt, dass nur Personen Zugang zu bestimmten Informationen erhalten sollten, die diese für die Ausführung ihrer Arbeit tatsächlich benötigen.)
- Ist der Einsatz von KI – z.B. durch sprachgestützte Pflegedokumentation oder Sprachassistenten in Zimmern von Bewohnern – geregelt?
- Wie wird die Datenweitergabe an Angehörige oder Dritte gelebt?

Besondere Aufmerksamkeit kommt immer mehr Messengerdiensten wie WhatsApp, Facebook-Messenger oder Signal zu. Mit über zwei Milliarden Nutzenden ist WhatsApp der beliebteste unter ihnen, aber auch einer derjenigen, der für umfangreiche Datennutzung bekannt ist, Daten in die USA überträgt und mit dem Mutterkonzern META teilt. Wenn Mitarbeitende Messengerdienste einsetzen, häufig ohne Rücksprache, dann liegt es daran, dass ein Bedarf vorhanden ist. Die Einrichtungsleitung sollte daher nicht mit Verboten reagieren, sondern Alternativen aufzeigen, die besser passen, und dann einheitlich in der Organisation eingesetzt werden. Teamwire ist beispielsweise ein DSGVO-konformer Messenger speziell für Unternehmen, der verschiedene Datenschutzgesetze und -standards erfüllt. Datenschutzbeauftragte können über die am Markt erhältlichen datenschutzkonformen Anwendungen Auskunft geben und helfen, den passenden Messenger zu identifizieren.

Praxistipp: Was ist, wenn die Polizei Auskunft verlangt?

Wenn Ermittlungsbehörden Daten anfordern, muss eine rechtliche Grundlage bestehen. Zum Beispiel die Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten (Art. 6 Abs. 1 c), DSGVO). Um eine nachweisbare Entscheidung zum Sachverhalt treffen zu können, müssen Einrichtungen folgendes prüfen:

- Identitätsprüfung der ermittelnden Behörde und des Polizeibeamten sowie Vorlage des Aktenzeichens
- Zweck der Anfrage
- Welcher Tatvorwurf liegt vor?
- Liegt ein staatsanwaltschaftlicher Ermittlungsauftrag vor?
- Auf welcher Rechtsgrundlage erfolgt die Anfrage?

Ohne die aktive Beteiligung der Mitarbeitenden können sensible Daten und Informationen nicht wirkungsvoll geschützt werden.

Die Antworten auf diese Fragen sind schriftlich vorzulegen. Erst dann kann die Datenherausgabe geprüft werden. Wenn Daten an Ermittlungsbehörden herausgegeben werden, muss die Person, deren Daten betroffen sind, davon in Kenntnis gesetzt werden. Diese Pflicht entfällt nur, wenn die Ermittlungsbehörden dies aus ermittlungstaktischen Gründen untersagen.

Notfallmanagement – was passiert bei Datenschutzverstößen?

Datenpannen sind schnell passiert. Ein offener E-Mail-Verteiler oder der Fehlversand von Bewohnerunterlagen an eine falsche Adresse. Was ist nun zu tun? Müssen Behörden oder Betroffene informiert werden?

Eine Meldepflicht an die Aufsichtsbehörde besteht gemäß Art. 33 DSGVO, wenn durch den Verstoß der Schutz personenbezogener Daten verletzt wird. Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit grenzte dies einmal folgendermaßen ein: Bei der Datenpanne muss es sich um einen [...]

Sicherheitsbruch handeln, bei dem Daten unrechtmäßig Dritten offenbart werden oder infolge eines Sicherheitsbruchs gelöscht oder zeitweise unzugänglich gemacht werden. Mögliche Beispiele sind Hacking und Datendiebstahl sowie SQL-Lücken, Bugs im Webserver, verlorengegangene USB-Sticks oder Laptops sowie der Einbruch in Serverräume, die mit dem Verlust von Hardware einhergehen.[2] [...]

Datenschutzverstöße müssen innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Datenschutzaufsichtsbehörde gemeldet und dokumentiert werden.

Sobald ein Datenschutzvorfall eintritt, wenn unbefugte Dritte beispielsweise durch eine erfolgreiche Phishing-Kampagne an Daten gelangen, dann sind die Aufsichtsbehörden zu informieren. Besteht ein hohes Risiko für die betroffene(n) Person(en) müssen auch diese benachrichtigt werden (gemäß Art. 34 DSGVO).

Dabei sind Fristen zu beachten: Datenschutzverstöße müssen innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Datenschutzaufsichtsbehörde gemeldet und dokumentiert werden.

Die Praxis zeigt, dass der Umgang mit Datenpannen nicht trivial ist. Deshalb ist gute Vorbereitung das A und O. Ein Feueralarm muss regelmäßig geprobt werden, um Handlungsabläufe zu festigen. Das gilt auch für den Datenschutz. Handlungsleitende Richtlinie geben Sicherheit und das Proben des Ernstfalls offenbart Schulungsbedarf. Deshalb haben sich Notfallpläne, Schulungen und Handbücher für Mitarbeitende so bewährt! Gerade auch vor dem Hintergrund der zunehmenden Digitalisierung und damit einhergehenden Cyberkriminalität.

Ein umfassender IT-Notfallplan sollte folgende Elemente enthalten:

- Ziele und Umfang des Plans
- Verantwortlichkeiten
- Kommunikationsplan
- Priorisierung kritischer Systeme und Prozesse
- Notfallreaktionsverfahren
- Datenwiederherstellung und Backup-Strategie
- Externe Kontakte und Ressourcen zur Unterstützung
- Test- und Überprüfungsverfahren
- Schulungen und Bewusstseinsbildung Mitarbeitender
- Laufende Aktualisierung und Pflege des Plans

Datenschutz systematisch und ganzheitlich denken

Der Datenschutz ist in der Pflege nicht das beliebteste aller Themen, er hat aber mit zunehmender Digitalisierung auch die Branchen erreicht, die naturgemäß wenig technikgetrieben sind. Deshalb ist die Geschäftsführung von stationären und ambulanten Pflegediensten verpflichtet, technische und organisatorische Maßnahmen umzusetzen, die sensible Daten wirkungsvoll schützen. Es empfiehlt sich, Datenschutz über die gesamte Organisation hinweg holistisch zu denken und Maßnahmen entlang einer umfassenden Strategie umzusetzen und zu überprüfen. Externe Datenschutzbeauftragte und Experten können personell schwach besetzte Einrichtungen unterstützen, die gesetzlichen Anforderungen einzuhalten. ■

DAS WICHTIGSTE IN KÜRZE

Eine einsehbare Dokumentation auf dem Pflegewagen, Fotos von Wunddokumentation, die in eine Cloud hochgeladen werden, oder der Zugriff von Ex-Mitarbeitenden auf Systeme, der nicht rechtzeitig entzogen wird – dies sind Beispiele aus der Praxis, die schnell passieren und eine Verletzung des Datenschutzes darstellen. Die Geschäftsführung von Einrichtungen und Organisationen ist dafür verantwortlich, dass der Schutz sensibler Daten jederzeit gewährleistet ist. Dafür haftet sie auch. Deshalb ist es essenziell, umfassende Datenschutzstrategien zu erarbeiten, umzusetzen und permanent zu überprüfen.

Foto: Althammer & Kill

Frank Boje, Berater für Datenschutz und Informationssicherheit, Althammer & Kill

Info: www.althammer-kill.de