Fact Sheet & FAQ:

Datenschutz in der Arztpraxis

Aktualisiert im Februar 2024

gemäss neuem Schweizerischen Datenschutzgesetz

Ursula Uttinger

Marcel Waldvogel

Andri Christen

EQUAM STIFTUNG

EQUAM STIFTUNG

Inhaltsverzeichnis

I) Das Wichtigste in Kürze

Seit der Inkraftsetzung des revidierten Datenschutzgesetzes (DSG) und den dazugehörigen Verordnungen, am 1. September 2023, gelten neue Bestimmungen im Umgang mit Personendaten. Mit der Revision wird der Schutz der Persönlichkeit und der Grundrechte von Personen, über die Personendaten bearbeitet werden, gestärkt.

In Arztpraxen werden zahlreiche besonders schützenswerte Personendaten erhoben, verarbeitet, aufbewahrt und weitergeleitet. Infolgedessen müssen die in Arztpraxen tätigen Personen, wie auch schon vor Inkraftsetzung des revidierten Gesetzes, die rechtlichen Datenschutzvorgaben umsetzen und einhalten.

Inhaltlich hat sich an den bereits im bisherigen (alten) Datenschutzgesetz (aDSG) verankerten Grundsätzen, für eine rechtmässige Datenverarbeitung, nichts geändert. Dennoch muss die Arztpraxis verschiedene neue Bestimmungen beachten, die eine Anpassung der bisherigen Datenverarbeitungsprozesse bedeuten können.

Im vorliegenden Fact Sheet und diesem FAQ werden anhand der für eine Arztpraxis wichtigsten Punkte erläutert, was Datenschutz ist und was es dabei zu beachten gilt. Leitfäden, Checklisten und Vorlagen zum Thema Datenschutz finden sich unter Punkt III).

Datenschutzgrundsätze

Das DSG und die dazugehörige Verordnung (DSV) umfassen verbindliche Vorschriften, die bei der Erhebung und Verarbeitung von Daten beachtet werden müssen. Die Einhaltung dieser Regelungen gewährleistet grundsätzlich eine rechtmässige Datenerhebung und -verarbeitung. Im Folgenden werden die wesentlichen Datenschutzgrundsätze kurz dargestellt.

Zweck des Datenschutzes

Das Datenschutzgesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Personendaten verarbeitet werden. Insbesondere wird damit die Transparenz der Datenverarbeitung und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten gewährleistet. Durch die Neuerungen im Datenschutzrecht soll zudem das Verantwortungsbewusstsein, der datenverarbeitenden Verantwortlichen, gesteigert werden. Dies geschieht etwa durch die Verpflichtung, bereits bei der Planung neuer Datenverarbeitungen, die Einhaltung der Datenschutzvorgaben zu berücksichtigen.

Schutzwürdige Daten in der Arztpraxis

Im Zusammenhang mit dem Datenschutz ist immer von Personendaten die Rede. Dabei handelt es sich um Daten, Informationen oder Angaben, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person gilt als identifizierbar, wenn sie direkt oder indirekt, zum Beispiel durch eine Telefonnummer, eine Anschrift oder eine AHV-

Nummer, oder durch die Kombination verschiedener Daten – wie Angaben zu einer Krankheit in einer Krankengeschichte – bestimmt werden kann. Des Weiteren erfolgt eine Kategorisierung der Daten nach ihrem Schutzbedarf. In Arztpraxen wird häufig mit besonders schützenswerten Personendaten umgegangen. Dazu zählen zum Beispiel Informationen über religiöse oder politische Überzeugungen, den Gesundheitszustand, die ethnische Herkunft sowie neu auch explizit genetische und biometrische Daten, die eine Person eindeutig identifizieren.

Massnahmen zum Datenschutz in meiner Arztpraxis

Grundsätzlich sind alle Personen, die in einer Arztpraxis arbeiten, dem Berufsgeheimnis – geregelt in den kantonalen (Gesundheits-)Gesetzen – verpflichtet, ein Verstoss ist in Artikel 321 des Strafgesetzbuches (StGB) geregelt. Dies schliesst das ärztliche Personal sowie deren Hilfspersonen ein. Unter Hilfspersonen versteht man jene Personen, die die Ärzteschaft direkt oder indirekt in ihrer professionellen Arbeit unterstützen und dabei Zugang zu vertraulichen Informationen (wie Patientendaten) erhalten. Dazu gehören beispielsweise Laborpersonal, medizinische Praxisassistent:innen, Buchhaltungspersonal, Reinigungskräfte usw.

Das Berufsgeheimnis verlangt, dass sämtliche Personen, die mit der Datenverarbeitung betraut sind, die Personendaten risikobasiert schützen. Im DSG werden diese Personen als „Verantwortliche“ bezeichnet. Dies bedeutet, dass die Arztpraxen den Datenschutzrisiken angemessene Datensicherheit gewährleisten müssen.

Im neuen Datenschutzgesetz versteht man unter dem rechtmässigen Umgang mit Daten die Beschaffung, das Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Weitergeben, Löschen oder Vernichten von Daten. Im nachfolgenden Abschnitt werden die wichtigsten Sachverhalte im Umgang mit Daten kurz zusammengefasst.

Datenbeschaffung

Als wichtigster Grundsatz gilt, dass die betroffene Person freiwillig in die Beschaffung von Personendaten einwilligen muss. Sie muss verständlich und nachvollziehbar über die Datenverarbeitungen und ihre Rechte informiert werden, insbesondere über den Verarbeitungszweck, an wen die Daten gegebenenfalls weitergegeben werden, sowie über ihr Recht auf Auskunft und Löschung ihrer Daten. Die Einholung einer Einwilligung ist für die Beschaffung und Verarbeitung von besonders schützenswerten Daten zwingend erforderlich und nur dann gültig, wenn sie auf Basis einer verständlichen Information freiwillig erteilt wird. Die Einwilligung muss schriftlich erfolgen, wobei rechtskonforme Datenschutz- und Einwilligungserklärungen zu verwenden sind. Geeignete und erläuterte Beispiele sowie Vorlagen lassen sich zum Beispiel auf den Internetseiten der FMH oder der Ärztekasse finden. Bereits bestehende Datenschutz- und Einwilligungserklärungen und der Anwendungsprozesse müssen gegebenenfalls angepasst werden.

Technik zur Datenaufbewahrung

Das DSG legt besonderen Wert auf eine datenschutzfreundliche Technikgestaltung und hohe Datensicherheit. Dies bedeutet, dass die Aufbewahrung von Personendaten, insbesondere von besonders schützenswerten Daten, technisch so gestaltet sein muss, dass die Datenschutzvorgaben eingehalten werden. Dabei sind spezifische technische Datensicherheitsaspekte vorgeschrieben, wie zum Beispiel die Festlegung von Verantwortlichkeiten, Regulierung der Zugriffs- und Benutzerrechte oder der Einsatz von Datenverschlüsselungstechniken. Es wird empfohlen, die Informatik- und Kommunikationsinfrastruktur (ICT) der Arztpraxis professionell konfigurieren und warten zu lassen. Die FMH hat Empfehlungen zum ICT-Grundschutz auf ihrer Internetseite veröffentlicht.

Aufbewahrung

Für die Aufbewahrung der verschiedenen Arten von Daten gelten verschiedene Vorgaben und Fristen. Diese sind bundesgesetzlich und teils kantonalgesetzlich festgelegt. Auf den Internetseiten der FMH und auch der Ärztekasse finden sich tabellarische Übersichten zu den gesetzlichen und standesrechtlichen Aufbewahrungsfristen.

Bearbeitung

Das ärztliche Personal sowie ihre Hilfspersonen bearbeiten, die im Rahmen ihrer Tätigkeit zahlreich beschafften Personendaten. Dies hat immer verhältnismässig zu erfolgen. Die Verhältnismässigkeit ist gegeben, wenn die Bearbeitung auf diejenigen Daten beschränkt wird, die für die Erfüllung der Aufgabe oder die Erreichung des angegebenen Zwecks geeignet und notwendig ist. Darunter fallen sämtliche Tätigkeiten der Verwendung, Veränderung, Bekanntgabe, Archivierung, Löschung oder Vernichtung von Personendaten. Da die Gesundheitsfachpersonen in Arztpraxen mit der Führung von Patientendossiers fast immer auch besonders schützenswerte Personendaten im grossen Umfang bearbeiten, müssen sie ein Verzeichnis der Bearbeitungstätigkeiten führen. Mit Hilfe eines solchen Verzeichnisses werden Prozesse und Verantwortlichkeiten der Datenbearbeitungstätigkeiten nachvollziehbar festgehalten und werden im Sinne einer besseren Datensicherheit transparent und überprüfbar. Konkret sollte aus dem Bearbeitungsverzeichnis unter anderem hervorgehen, welche Daten erhoben werden, wie sie bearbeitet werden, welche Datenschutzmassnahmen getroffen werden, wie lange die Daten gespeichert bleiben und an wen sie gegebenenfalls weitergeleitet werden. Zudem muss die zuständige Ansprechperson aufgeführt werden. Die FMH stellt einen Leitfaden und eine Vorlage für ein solches Verzeichnis auf ihrer Internetseite zur Verfügung.

Weitergabe von Daten

Das ärztliche Personal darf Personendaten weitergeben oder Dritten Auskunft geben, wenn dazu die Einwilligung der Patientinnen oder Patienten vorliegt, ein Gesetz dies vorsieht oder sie von der kantonalen Behörde vom Berufsgeheimnis entbunden wurde.

Auskunftsrecht

Patientinnen oder Patienten haben das Recht, Auskunft zu erhalten, welche Personendaten über sie bearbeitet werden. Mit dem Auskunftsrecht ist ein Anspruch auf die Herausgabe ihrer Daten verbunden. Sie kann somit eine Kopie ihrer Krankengeschichte verlangen. Grundsätzlich haben die Auskunft und Herausgabe innerhalb einer rechtlich vorgeschriebenen Frist und kostenlos zu erfolgen. Entsteht im Zusammenhang mit der Gesuchstellung und dem Bereitstellen der Informationen ein unverhältnismässig grosser Aufwand, darf in Ausnahmefällen der gesuchstellenden Person die entstandenen Kosten verrechnet werden.

Fazit

Die Änderungen im DSG lösen keinen unmittelbaren Handlungsbedarf bei bestehenden Arztpraxen aus. Auch bisher hatte die Arztpraxis angemessene und organisatorische Massnahmen für den Datenschutz umzusetzen. Bestehende Massnahmen zum Datenschutz sollten jedoch unbedingt hinsichtlich der Änderungen überprüft und gegebenenfalls angepasst werden.

II) FAQ aus dem Praxisalltag

Welche Grundvoraussetzung muss eine Arztpraxis erfüllen, damit der Datenschutz gewährleistet werden kann?

Arztpraxen müssen bestimmte physische Anforderungen erfüllen, um den Datenschutz sicherzustellen. Dies umfasst den beschränkten Zugang zu Praxisräumen ausschliesslich für autorisiertes Personal sowie die Möglichkeit, diese Räumlichkeiten einbruchsicher zu verschliessen.

Personenbezogene Daten, die in Papierform vorliegen, sollten in einem abschliessbaren Behältnis aufbewahrt werden. Es ist darauf zu achten, dass diese Unterlagen so gehandhabt werden, dass unbefugten Personen die Einsichtnahme verwehrt bleibt.

Des Weiteren sollten PC-Bildschirme so positioniert werden, dass sie für Unbefugte nicht einsehbar sind. ICT-Mittel, besonders jene Geräte, auf denen personenbezogene Daten gespeichert sind, müssen in Räumen aufbewahrt werden, die für Unbefugte nicht zugänglich sind.

Fragen zu Auskunft- und Herausgabegesuche über Personendaten

Welche Daten können für eine Auskunft oder Herausgabe verlangt werden?

Eine Arztpraxis ist grundsätzlich verpflichtet, alle Daten, insbesondere die Gesundheitsdaten der anfragenden Person, herauszugeben. Dies umfasst vor allem eine Kopie der Krankengeschichte.

Eine Ausnahme bilden sogenannte „persönliche Arbeitshilfsmittel“, wie etwa private Notizen der behandelnden Ärztinnen oder Ärzte, die nicht Bestandteil der Krankengeschichte sind. Diese fallen nicht unter das Datenschutzgesetz. Bei solchen persönlichen Arbeitshilfsmitteln ist zu gewährleisten, dass keine Drittperson, einschliesslich weitere Gesundheitsfachpersonen der Arztpraxis, Zugang zu diesen Informationen erhält.

Wie kann ich mich auf ein Auskunftsgesuch und Gesuch auf Datenherausgabe vorbereiten?

Arztpraxen können sich auf die Erteilung von Auskünften und die Herausgabe von Daten vorbereiten, indem entsprechende Prozessabläufe und die Verantwortlichkeiten definiert und schriftlich festgehalten werden. Es ist empfehlenswert, dass die Praxis auf ihrer Website entsprechende Informationen, insbesondere ein Kontaktadresse bereitstellt.

An wen dürfen die verlangten Daten ausgehändigt werden?

Die Daten sind grundsätzlich der gesuchstellenden Person mit Anrecht auf die Daten herauszugeben. Die anfragende Person muss unter Vorlage eines Identitätsnachweises (Personalausweis oder Reisepass) zur eindeutigen Identifizierung ihr Anliegen schriftlich (via E-

Mail oder Post) einreichen. Bei Anfragen durch Dritte ist das Vorliegen einer gültigen Vollmacht erforderlich.

Gelten unterschiedliche Regeln für digitale und Daten in Papierform?

Es ist unerheblich, ob die Informationen elektronisch gespeichert oder in Papierform vorliegen. Beide Datentypen unterstehen gleichermassen dem DSG.

In welcher Form müssen die Daten herausgegeben werden?

Die Daten sind so bereitzustellen, dass die anfragende Person sie problemlos lesen kann, wobei gleichzeitig die Vertraulichkeit der Informationen sicherzustellen ist. So muss sichergestellt werden, dass bei der Herausgabe der Daten die Persönlichkeitsrechte Dritter nicht verletzt werden. Sollten in der Krankengeschichte Informationen enthalten sein, die die Rechte und Interessen Dritter beeinträchtigen könnten, müssen diese Informationen vor der Weitergabe unkenntlich gemacht werden, beispielsweise durch Schwärzung.

Der gewählte Übertragungsweg muss sicher sein. Die Übermittlung kann via verschlüsseltes E-Mail, einem verschlüsselten Cloud-Speicherdienst, persönlich oder per Briefpost erfolgen. Eine Notiz über die Datenherausgabe sollte in der Krankengeschichte vermerkt werden. Bei umfangreichen Datensätzen empfiehlt es sich, einen mobilen Datenträger (z.B. USB-Stick) zu nutzen und diesen der anfragenden Person persönlich zu übergeben. Beim Einsatz von mobilen Datenträgern ist sicherzustellen, dass diese neu und nach allfälliger Zurückgabe nicht wiederverwendet werden, um das Risiko einer Einschleusung von Schadsoftware (Malware) in die ICT-Infrastruktur der Praxis zu verhindern.

Die betroffene Person kann die vertraulichen Unterlagen auch ohne verschlüsselte E-Mail erhalten, wenn sie über die damit verbundenen Risiken informiert wurde und diese bewusst in Kauf nimmt.

Dürfen Daten auch an Dritte weitergegeben werden?

Generell ist die Zustimmung der Patientin oder des Patienten für die Weitergabe ihrer Daten erforderlich. Eine rechtmässige Einwilligungserklärung berücksichtigt übliche Datenweitergaben, beispielsweise an andere Gesundheitsfachpersonen innerhalb der direkten Behandlungskette, die ebenfalls der ärztlichen Schweigepflicht unterliegen. Nachbehandelnde Institutionen brauchen oft keine Einwilligung, da dies bereits gesetzlich vorgesehen ist – sehr schön formuliert beispielsweise in § 19 Abs. 1 Patientenverordnung Kt. Aargau («Unmittelbar nachbehandelnde Personen sind über Diagnose und Zustand der Patientinnen und Patienten sowie über die erforderlichen weiteren Massnahmen rechtzeitig zu informieren, soweit dies für die fachgerechte Nachbehandlung erforderlich ist.»)

Die Weitergabe von Daten an Versicherungen hängt vom Zweck der Verwendung ab:

- Unfallversichernde haben Anspruch auf Informationen, die in direktem Zusammenhang mit dem Unfall stehen. Dies folgt dem Prinzip der Naturalleistung, welches besagt, dass die Unfallversicherung in Bezug auf die Behandlung nach einem Unfall

und nicht die betroffene Person die Auftraggebende ist. Daher hat die Unfallversicherung als Auftraggebende Anspruch auf Daten, die ausschliesslich den Unfall betreffen.

- Kostentragende der obligatorischen Krankenversicherung sind dazu verpflichtet, die Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit der erbrachten Leistungen zu überprüfen. In diesem Kontext haben Krankenversicherungen Anspruch auf Daten, die es ihnen ermöglichen, diese gesetzliche Überprüfung durchzuführen. Besonders sensible Daten können dem vertrauensärztlichen Dienst des Krankenversichernden übermittelt werden.
- Alle anderen Versicherungen, wie Zusatzkrankenversicherungen, Lebensversicherungen usw., benötigen die Einwilligung der betroffenen Person für den Datenzugriff. Eine Datenweitergabe ohne Einwilligung und ohne Aufhebung der ärztlichen Schweigepflicht stellt einen Verstoss gegen das Berufsgeheimnis dar und ist strafbar.
- Formulare von Sozialversicherungen müssen korrekt und wahrheitsgemäss ausgefüllt werden, sofern sie im Zusammenhang mit dem Anspruch der betroffenen Person auf Leistungen stehen.
- Arbeitgebende dürfen nur jene Informationen erhalten, die erforderlich sind, um festzustellen, ab wann eine Person ihre Arbeit wieder aufnehmen kann und welche Aufgaben sie dabei übernehmen darf. Diagnoseinformationen dürfen den Arbeitgebenden nicht mitgeteilt werden.
- Unter Vorlage einer schriftlichen behördlichen Verfügung können Polizei oder andere Behörden Auskunft oder die Herausgabe von Informationen fordern. Solche Anordnungen müssen vor der Auskunftserteilung auf ihre formale Gültigkeit hin überprüft werden.

Wann ist eine Vereinbarung für eine Auftragsbearbeitung oder eine Geheimhaltungsvereinbarung abzuschliessen?

Die Beauftragung Dritter zur Datenverarbeitung ist aus datenschutzrechtlicher Sicht zulässig. Wird eine Auftragnehmende mit der Datenverarbeitung betraut, wird diese zur Hilfsperson und unterliegt somit ebenfalls der ärztlichen Schweigepflicht gemäss Artikel 321 StGB. Eine Missachtung des Berufsgeheimnisses kann mit einer Freiheitsstrafe von bis zu drei Jahren geahndet werden.

Alle Personen, die in einer Arztpraxis tätig sind und potenziell mit sensiblen Informationen und Daten in Kontakt kommen, müssen die Geheimhaltungspflicht wahren. Dies betrifft beispielsweise das Reinigungspersonal, Wartungsdienste und Sicherheitsmitarbeitende. Durch den Abschluss einer Geheimhaltungsvereinbarung können Hilfspersonen rechtlich dazu verpflichtet werden, die Vertraulichkeit von Berufsgeheimnissen und persönlichen Daten zu gewährleisten.

Bei der Vergabe von Datenverarbeitungsaufgaben an Dritte, wie etwa Cloud-Dienstleistende oder Anbietende von Telefonantwortdiensten, ist es erforderlich, eine Auftragsverarbeitungs- sowie eine Geheimhaltungsvereinbarung zu unterzeichnen. Diese werden übli-

cherweise in die Verträge inkludiert. Für Auftragnehmende gelten dieselben Datenschutzbestimmungen und die Verpflichtung zur Wahrung des Berufsgeheimnisses nach Artikel 321 StGB wie für das Gesundheitsfachpersonal in Arztpraxen.

Werden Daten zur Bearbeitung Dritten übergeben (z.B. Ärztekasse, Treuhanddienste) ist eine schriftliche Vereinbarung für eine Auftragsbearbeitung notwendig (vgl. Vorlage FMH).

Wann dürfen Daten für die Forschung weitergegeben werden?

Anonymisierte gesundheitsbezogene Daten dürfen für die Forschung verwendet werden, wenn die betroffene Person von ihrem Widerspruchsrecht zur Anonymisierung ihrer Daten nicht Gebrauch gemacht hat. Daten sind dann anonym, wenn sie nicht mehr einer Person zugeordnet werden können.

Ist bei der Erhebung der gesundheitsbezogenen Personendaten die Weiterverwendung für die Forschung bereits beabsichtigt, so ist bereits zum Zeitpunkt der Erhebung die Einwilligung der betroffenen Person einzuholen, beziehungsweise die Person über ihr Widerspruchsrecht zu informieren.

Werden bereits bestehende Daten für die Forschung weiterverwendet bzw. weitergegeben, so sind diese, wenn immer möglich, zu verschlüsseln. Verschlüsselte Daten dürfen zu Forschungszwecken weiterverwendet werden, wenn die betroffene Person vorgängig informiert worden ist und nicht widersprochen hat. Daten in unverschlüsselter Form dürfen zu Forschungszwecken weiterverwendet werden, wenn die betroffene Person hinreichend aufgeklärt wurde und schriftlich eingewilligt hat.

Weiterführende Informationen zur Humanforschungsregelung finden sich auf den Internetseiten des Portals zur Humanforschung in der Schweiz (kofam), des Bundesamts für Gesundheit oder von swissethics, der Dachorganisation der Kantonalen Ethikkommissionen.

Wie garantiert man den Datenschutz bei einer Qualitätskontrolle durch Dritte?

Im Rahmen von Qualitätskontrollen werden Daten durch Dritte kontrolliert. Je nach Konstellation handelt es sich dabei um Hilfspersonen oder externe Dritte. Sehen externe Dritte Daten ein, so ist ein Einverständnis der Patientinnen oder Patienten via Datenschutz- und Einwilligungserklärung notwendig und mit den Auftragnehmenden ist eine Geheimhaltungs- und Auftragsvereinbarung abzuschliessen. Handelt es sich bei den Dritten um Hilfspersonen, die unter der Aufsicht und Weisung des ärztlichen Personals sind, so unterstehen diese der beruflichen Schweigepflicht.

Fragen zur Informatik- und Kommunikationsinfrastruktur (ICT)

Wie muss die ICT-Infrastruktur aufgebaut, unterhalten und gewartet sein, um den Datenschutz zu gewährleisten?

Eine sichere ICT-Umgebung erfordert umfangreiche Massnahmen in Bezug auf den Aufbau, den Unterhalt und die Wartung sowie die Entwicklung von Sicherheitsanforderungen und

die Sensibilisierung der Mitarbeitenden für eine angemessene Datenschutz- und Sicherheitskultur. Die ICT-Infrastruktur und die organisatorischen Massnahmen müssen den Anforderungen des Datenschutzes gerecht werden. Dies impliziert konkret, dass die Daten:

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden können (Integrität);
- nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

Wie garantiere ich die rechtlich geforderte Datenvertraulichkeit?

Die Verantwortliche und die Auftragsbearbeitende ergreifen Massnahmen, um sicherzustellen, dass ausschliesslich befugte Personen Zugang zu den Daten erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle).

Zutritt zu Räumlichkeiten und Anlagen, in denen personenbezogene Daten verarbeitet werden, darf nur befugten Personen gewährt werden (Zugangskontrolle).

Es muss sichergestellt sein, dass keine unbefugten Personen in der Lage sind, Daten zu verarbeiten (Benutzerkontrolle).

Wie garantiere ich die Datenverfügbarkeit und -integrität?

Die Verantwortliche und die Auftragsbearbeitende ergreifen Massnahmen, damit nur befugte Personen Zugang zu Datenträgern haben und transportieren dürfen (Datenträger- und Transportkontrolle).

Durch geeignete Massnahmen muss sichergestellt werden, dass bei Verlust oder Beschädigung der Datenträger, die Verfügbarkeit der Personendaten und der Zugang rasch wiederhergestellt werden können (Wiederherstellung).

Die ICT-Infrastruktur muss stets auf dem neusten Sicherheitsstand gehalten werden, so dass ein unbefugter Zugriff möglichst ausgeschlossen werden kann (Systemsicherheit).

Wie garantiere ich die Nachvollziehbarkeit?

Die Verantwortliche und die Auftragsbearbeitende ergreifen Massnahmen, damit überprüft werden kann, welche Daten wann und durch wen eingegeben, verändert oder gelöscht werden (Eingabekontrolle).

Die Datenbekanntgabe oder -übertragung muss nachträglich überprüft werden können (Bekanntgabekontrolle).

Muss ich die Datenbearbeitung protokollieren?

ICT-Systeme und Anwendungen sollten so eingerichtet werden, dass Veränderungen an aufbewahrten Daten ersichtlich und nachvollziehbar sind. Auch sollten sicherheitsrelevante Aktivitäten, wie Login-Versuche, An- und Abmeldungen sowie Änderungen an den Daten und System- oder Anwendungsabstürze protokolliert werden (sogenanntes Logging). Die

Protokolle sollten zentral gesammelt und aufbewahrt werden und nur mit eingeschränkten Benutzerrechten einsehbar sein.

Welches sind wichtigsten konkreten Massnahmen zum Schutz meiner digitalen Daten

Die FMH hat für einen minimalen ICT-Grundschutz elf Anforderungen bzw. Empfehlungen formuliert:

- Verantwortlichkeiten bestimmen und Vorgaben erlassen
- ICT-Mittel in einem Inventar aufnehmen
- Zugriffsschutz regulieren und Benutzerrechte verwalten
- Praxismitarbeitende für Datensicherheit sensibilisieren
- Endgeräte vor Schadsoftware schützen
- Netzwerk schützen
- ICT-Umgebung konfigurieren und warten
- Digitale Daten sicher ablegen
- Digitale Daten sicher austauschen
- Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen
- Externe Dienstleistende beauftragen und überwachen

Brauche ich für meine Arztpraxis eine datenschutz- und datensicherheitsverantwortliche Person?

In einer Arztpraxis obliegt die Verantwortung für den Schutz der Patientendaten dem ärztlichen Personal. Die Leitung der Praxis trägt die Gesamtverantwortung, insbesondere für den datenschutzkonformen Betrieb der ICT-Umgebung und für das Personal. Idealerweise sollte die Rolle des Datenschutz- und Datensicherheitsverantwortlichen (DSDS-V) sowie der ICT-Betriebsverantwortlichen in Bezug auf Datenschutz und Datensicherheit jeweils einer Person zugewiesen werden. Die DSDS-V ist üblicherweise für den Erlass und die Einhaltung der Datenschutz- und sicherheitsvorgaben verantwortlich, während die Verantwortung für den Aufbau und den Betrieb der ICT-Infrastruktur bei der ICT-betriebsverantwortlichen Person liegt. Diese Rollen können von der Geschäftsleitung, dem ärztlichen Personal, internen oder externen Praxismitarbeitenden oder auch durch einen ICT-Dienstleister wahrgenommen werden.

Muss ich ein ICT-Inventar führen?

Um die Datenvertraulichkeit zu gewährleisten, sollte in einer Arztpraxis ein Inventar sämtlicher ICT-Mittel geführt werden. Der Schutz von Daten und Informationen bedingt den Einsatz von bekannter und sicherer Hard- und Software. Mit Hilfe einer Inventarliste lässt sich überprüfen, ob die eingesetzten ICT-Mittel auf dem neuesten technischen Stand und damit sicher sind und wer mit welchem ICT-Mittel auf welche Daten Zugriff hat. Die Liste sollte von der ICT-Betriebsverantwortlichen regelmässig überprüft und aktualisiert werden, so dass die Zweckerfüllung garantiert ist.

Wie verwalte ich Zugriffs- und Benutzerrechte?

Die Bewilligung und der Entzug von Zugriffs- und Benutzerrechten obliegt der Datenverantwortlichen, welche gegenüber der betroffenen Person (Der Patientin oder des Patienten) die Verantwortung für die Sicherstellung ihrer Rechte übernimmt. In aller Regel ist das das ärztliche Personal. Die Vergabe und die Löschung von den Benutzerrechten können durch die DSDS-V erfolgen.

Wie ist mit Fernzugriffen auf meine ICT-Infrastruktur für Wartungszwecke umzugehen?

Fernzugriffe für Wartungszwecke durch externe ICT-Dienstleistende sind mit einem gewissen Risiko verbunden, da sich die Identität der externen Person und ihre Umgebung nicht überprüfen lassen. Um die Risiken für einen Missbrauch zu verringern, haben die Fernzugriffe über separate, persönliche Benutzerkonten zu erfolgen. Die Aktivitäten auf diesen Benutzerkonten sind zur Erkennung von auffälligem Verhalten und zur Sicherstellung der Nachvollziehbarkeit aufzuzeichnen und zu überwachen. Der Fernzugriff durch externe ICT-Dienstleistende sollte nie ohne vorgängige Anmeldung und ausdrücklicher Genehmigung der Datenverantwortlichen erfolgen. Unbekannte sollten nie Zugriff zu dem Fernwartungssystem erhalten.

Genügt ein Passwort pro Arbeitsplatz oder Computer?

Passwörter sollten nicht für einzelne Arbeitsplätze oder Computer, sondern individuell für jede Person angelegt werden. Dadurch sind Passwörter persönlich und direkt mit den entsprechenden individuellen Benutzerkonten verknüpft. Die Verwendung von unpersönlichen Benutzerkonten ist zu vermeiden.

Was macht ein sicheres Passwort aus?

Generell gilt: Je komplexer das Passwort, desto sicherer ist es. Die Mindestanforderungen an Passwörter entwickeln sich stetig weiter, parallel zu den technischen Möglichkeiten, Passwörter zu entschlüsseln. Aus diesem Grund empfehlen wir, sich z.B. auf der Website von HIN zu informieren, wo Sie eine Anleitung für die Erstellung sicherer Passwörter finden.

Soll ein Passwort regelmässig erneuert werden?

Ein regelmässiger Passwortwechsel kann dazu führen, dass die Nutzerinnen oder Nutzer dazu neigen, das Passwort aufzuschreiben, ähnliche Passwörter wiederholt zu verwenden oder sich für allzu einfache Passwörter zu entscheiden. Daher wird von einer automatisierten, regelmässigen Änderung der Passwörter abgeraten. Ein Passwort sollte nur dann erneuert werden, wenn die Vermutung besteht, dass es einem unbefugten Dienst oder einer unbefugten Person bekannt geworden ist.

Wie sind die Passwörter zu verwalten?

Zur Verwaltung mehrerer Passwörter wird die Nutzung eines Passwortmanagers empfohlen. Dieser generiert starke und einzigartige Passwörter und speichert sie verschlüsselt ab. Der Zugriff auf den Passwortmanager erfolgt über ein Masterpasswort.

Als Alternative zu Passwörtern können auch biometrische Merkmale eingesetzt werden. Beim Einsatz von biometrischen Verfahren, wie zum Beispiel Fingerabdruck- oder Gesichtserkennung für Endgeräte, welche von der Praxis zur Verfügung gestellt werden, ist zu beachten, dass das biometrische Verfahren jeweils immer auch an eine PIN oder ein Passwort gekoppelt ist. Dadurch verfügt jedes Endgerät über zwei Optionen zur Ent- und Verriegelung. Biometrische Verfahren ersetzen die Notwendigkeit von Passwörtern jedoch nicht vollständig.

Sollten Multi-Faktor-Authentifizierungen verwendet werden?

Multi-Faktor-Authentifizierung (MFA oder Zweifaktor-Authentifizierung, 2FA) kombiniert zwei oder mehr unabhängige Nachweise zur Berechtigungsprüfung: Etwas, das die Benutzenden kennen, wie zum Beispiel ein Passwort; etwas, das die Benutzenden besitzen, wie beispielsweise ein Mobiltelefon, das mittels SMS-Versand oder über eine Authentifizierungs-App verifiziert wird; und / oder etwas, das die Benutzenden sind, wie zum Beispiel biometrische Merkmale (z.B. Gesicht oder Fingerabdruck), die sich technisch verifizieren lassen.

Daher ist die Zwei-Faktor-Authentifizierung sicherer als die alleinige Nutzung eines Passwortes und sollte, wann immer möglich, angewendet werden. Falls das 2FA-Verfahren zusätzliche Notfallcodes bereitstellt, sollten diese ausgedruckt und an einem für Unbefugte unzugänglichen Ort aufbewahrt werden.

Dürfen besonders schützenswerte Daten auch in der Cloud aufbewahrt werden?

Vereinfacht lässt sich sagen: «Die Cloud ist der Computer von jemand anderem». Technisch gesehen, versteht man unter «Cloud» im weitesten Sinne jeden standardisierten Dienst, der online angeboten wird und Ressourcen wie Speicherplatz und Rechenleistung über das Internet zur Verfügung stellt. Im Sinne der Datenspeicherung bezieht sich der Begriff auf Cloudspeicher, also die Möglichkeit, Daten online über eine Webseite oder App zu speichern und sie verschiedenen Geräten und Nutzenden zugänglich zu machen.

Für die meisten Praxen ist es wirtschaftlich und technisch nicht sinnvoll, alle digitalen Dienstleistungen intern zu erbringen. Daher gewinnt die Nutzung externer Datenverarbeitungsangebote zunehmend an Bedeutung. Die Inanspruchnahme von Cloud-Diensten birgt jedoch im Vergleich zu einer internen Lösung Risiken, die insbesondere bei der Auswahl des Anbietenden beachtet werden müssen. So sind z.B. die Möglichkeiten zur Kontrolle der vertraglichen Vereinbarung bezüglich des Datenschutzes und der Datensicherheit sowie der Datenbearbeitung durch die Anbietenden oftmals eingeschränkt, weshalb der Leistungsbezug auf Vertrauen basiert.

Wie garantieren wir die Datensicherheit bei der Verwendung von E-Mails?

Der unverschlüsselte Datenaustausch per E-Mail zwischen Arztpraxis, Patientinnen oder Patienten und den Akteuren der Gesundheitsbranche ermöglicht es einem Angreifenden, die Kommunikation mitzulesen und sensible Informationen abzufangen. Daher sind E-Mails mit personenbezogen Daten zu betroffenen Personen (Patientinnen oder Patienten) zu verschlüsseln. Es empfiehlt sich eine Verschlüsselungslösung zu wählen, welche für die Kommunikation zwischen den Akteuren der Gesundheitsbranche eingesetzt wird. Weit verbreitet sind mittlerweile die Produkte der Health Info Net AG (HIN).

Ist eine Verschlüsselung von E-Mails immer zwingend?

Von einer Verschlüsselung kann abgesehen werden, wenn die Patientin oder der Patient erklärt hat, dass die Daten auch unverschlüsselt übermittelt werden dürfen. Dazu ist eine informierte Einwilligung der betroffenen Person, in sie über die damit verbundenen Risiken informiert wurde, erforderlich.

Braucht es einen Datenschutz-Disclaimer am Ende der E-Mail?

Einige Absenderinnen oder Absender hängen am Ende der E-Mail automatisch einen so genannten Disclaimer, d.h. einen (häufig langen) Text an, der sagt, wie die Empfängerinnen oder Empfänger mit der E-Mail umgehen sollen. Insbesondere wird dort aufgeführt, dass falsche Empfängerinnen oder Empfänger die E-Mail löschen und die Absenderin oder den Absender informieren sollen. Dies ist rechtlich für die E-Mail Empfangenden nicht bindend. Es kann sogar bei den Empfangenden Verwirrung auslösen oder sie möglicherweise umso mehr zum Missbrauch dieser Daten verleiten. Wir empfehlen deshalb, keine Disclaimer zu nutzen.

Ist das Versenden von Daten per Fax sicher?

Nachrichten, die personenbezogene Daten enthalten und per Fax gesendet werden, müssen ebenfalls verschlüsselt werden. Faxgeräte, die eine Verschlüsselung ermöglichen, sind in der Regel kostspieliger und komplizierter in der Handhabung. Daher ist die Übermittlung mittels verschlüsselter E-Mails vorzuziehen.

Fragen zur Absicherung vor Datenverlust

Ist eine Absicherung der Daten zum Schutz vor Datenverlust vorgeschrieben?

Um die Datenschutzvorgaben zu erfüllen, ist ein Schutz vor Datenverlust unerlässlich. Datenkopien, die getrennt und sicher vom sogenannten Produktivsystem aufbewahrt werden, werden als Daten-Backups oder als redundante Datensicherung bezeichnet. Sie ermöglichen die Wiederherstellung verlorener oder beschädigter Daten.

Was versteht man unter redundanter Datensicherung (Daten-Backups)?

Datenredundanz bedeutet, dass zwei oder mehr Kopien einer Datei an unterschiedlichen Orten oder in verschiedenen Systemen gespeichert werden. Diese Speicherstrategie ermöglicht den schnellen Zugriff auf die Daten, selbst wenn eines der Systeme ausfällt. Dank redundanter Daten können Organisationen im Falle eines Hardwareausfalls den Betrieb mit minimaler Unterbrechung fortsetzen. Sollten Daten versehentlich oder durch Malware gelöscht, beschädigt oder überschrieben werden, können diese Fehler jedoch auch auf die redundanten Kopien übertragen werden. Zur Wiederherstellung der Daten sind daher zeitlich verzögerte Kopien notwendig, die als Daten-Backups oder redundante Datensicherungen bezeichnet werden.

In der Praxis der redundanten Datensicherung werden häufig mehrere Datenkopien aufbewahrt, um bei einem Ausfall eines Computersystems die Verfügbarkeit und Konsistenz der Daten zu gewährleisten. Eine effektive redundante Datensicherung sichert die Daten nicht nur, sondern erhält auch ihre Konsistenz. Für Arztpraxen ist es daher unerlässlich, eine redundante Datensicherung zu implementieren, bei der die Daten nicht nur auf verschiedenen Servern – einschließlich verschlüsselter Cloud-Speicher – gesichert werden, sondern auch in räumlich getrennten Umgebungen, um höchste Sicherheit und Verfügbarkeit zu gewährleisten.

Welche Daten müssen aufbewahrt werden und für wie lange?

Personendaten dürfen und müssen, entsprechend dem im DSG verankerten Grundsatz der Verhältnismässigkeit, so lange aufbewahrt werden, wie sie für die Erfüllung der Aufgaben einer Arztpraxis geeignet und notwendig sind. Bundes- und kantonale Gesetze definieren spezifische Aufbewahrungsfristen für verschiedene Unterlagen, die personenbezogene Daten enthalten. Daten und Unterlagen können ausschliesslich elektronisch aufbewahrt werden. Die FMH bietet in ihrem Leitfaden zur Aufbewahrung und Archivierung von Personendaten eine detaillierte Übersicht über die Aufbewahrungsfristen für die unterschiedlichen Arten von Unterlagen.

Wieso müssen Daten gelöscht werden?

Personendaten dürfen ausschliesslich für den Zweck des zwischen der Praxis und der Patientin oder des Patienten geschlossenen Behandlungsvertrags aufbewahrt und verarbeitet werden. Sobald die Daten für diesen Zweck (inkl. der Verjährungs- und Aufbewahrungsfristen) nicht mehr benötigt werden, müssen sie unwiderruflich gelöscht, vernichtet oder anonymisiert werden. Zudem haben die betroffenen Personen das Recht, eine Löschung ihrer Daten zu fordern, sofern keine Rechtfertigungsgründe für deren weitere Aufbewahrung vorliegen oder gesetzliche Aufbewahrungsfristen dem Entgegenstehen. Gesetzliche Aufbewahrungsfristen gehen dem Wunsch nach Löschung vor.

Welches sind die Sicherheitsanforderungen an die Löschung von Daten?

Methoden zur Datenlöschung und Datenvernichtung entsprechen den Datenschutzvorgaben, wenn die Daten mit der Löschung oder Vernichtung unwiderruflich gelöscht sind. Die

FMH stellt in ihrem Leitfaden zur Aufbewahrung und Archivierung von Personendaten eine tabellarische Übersicht möglicher Methoden zur sicheren Löschung von Daten zur Verfügung.

Fragen zu Datenschutzverletzungen

Die Datenschutzverantwortlichen einer Arztpraxis sind verpflichtet, angemessene Massnahmen zu ergreifen, um die Personendaten vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen. Im Falle einer Datenschutz- oder Datensicherheitsverletzung sind gesetzlich vorgeschriebene Massnahmen zu ergreifen, die dem Risiko für die Persönlichkeitsrechte der betroffenen Personen angemessen sind. Für Arztpraxen ist es ratsam, Prozesse zu definieren, die festlegen, welche Massnahmen in solchen Fällen zu ergreifen sind.

Was muss bei einer Datenschutzverletzung unternommen werden?

Das DSG sieht eine Meldepflicht für Datensicherheitsverletzungen vor. Demzufolge müssen Datensicherheitsverletzungen, die wahrscheinlich ein hohes Risiko für die Persönlichkeits- und Grundrechte der betroffenen Personen darstellen, unverzüglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden. Es ist im Einzelfall zu prüfen, inwieweit eine Datensicherheitsverletzung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen darstellt. Der EDÖB hat für die Meldung ein spezielles Meldeportal eingerichtet: https://databreach.edoeb.admin.ch/report

Wie ist vorzugehen, wenn Patientendaten betroffen sind?

Unabhängig von der Meldepflicht, informiert die Verantwortliche die betroffene Person von der Verletzung der Datensicherheit, wenn es zu ihrem Schutz erforderlich ist. Der EDÖB kann zudem aufgrund der Meldung eine Information an die betroffene Person verlangen. Grundsätzlich empfiehlt sich eine Meldung niederschwellig vorzunehmen und nicht zu hoffen, dass es nicht auffällt.

Was ist eine DSFA (= Datenschutz-Folgenabschätzung)?

Eine DSFA stellt ein Instrument dar, um die Risiken einer Datenbearbeitung für betroffene Personen besser abschätzen zu können. Als Datenschutzrisiken gelten:

- Unberechtigter Zugriff zu Personendaten (von einer internen oder externen Person oder einem System)
- Unerwünscht Modifikation der Personendaten (absichtlich oder unbeabsichtigt; z.B. von einer internen oder externen Person oder wegen einer Fehlkonfiguration)
- Verlust der Personendaten (absichtlich oder unbeabsichtigt; z.B. von einer internen oder externen Person)
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten
- Unbefugte Aufhebung der Pseudonymisierung (Verschlüsselung)

Muss eine DSFA erstellt werden?

Die Bearbeitung von Personendaten erfordert eine Risikoabschätzung. Gemäß Datenschutzgesetz (DSG) muss diese in Form einer Datenschutz-Folgenabschätzung (DSFA) erfolgen. Ein besonders hohes Risiko besteht, wenn umfangreich mit besonders schützenswerten Personendaten gearbeitet wird. Dies ist beispielsweise bei Patientendaten der Fall.

Für die Bearbeitung von Patientendaten besteht eine Pflicht zur Führung einer Dokumentation. Von der Erstellung einer DSFA sind private Verantwortliche ausgenommen, wenn sie zur Bearbeitung der Daten gesetzlich verpflichtet sind. Dies trifft beispielsweise auf Arztpraxen zu.

Für Bearbeitungen, für die es keine gesetzliche Verpflichtung gibt, bedarf es jedoch in der Regel einer DSFA, sofern ein hohes Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen besteht.

Wann haften wir wegen einer Datenschutzverletzung?

Eine Haftung aus Verletzung des Datenschutzes besteht immer dann, wenn deswegen ein finanzieller Schaden für eine betroffene Person entsteht. Es braucht einen adäquaten Kausalzusammenhang zwischen der Verletzung und dem finanziellen Schaden.

Fragen zur Anwendbarkeit der europäischen Datenschutz-Grundverordnung (DSGVO)

Für die Anwendbarkeit der DSGVO ist primär Art. 3 DSGVO relevant:

1. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung einer Verantwortlichen oder einer Auftragsverarbeitenden in der europäischen Union (EU) erfolgt, unabhängig davon, ob die Verarbeitung in der EU stattfindet.
2. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeitende, wenn die Datenverarbeitung im Zusammenhang damit steht
    a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
    b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.
3. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch eine nicht in der Union niedergelassene Verantwortliche an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Ist die DSGVO anwendbar im Falle von Mitarbeitenden aus der EU?

Das Marktortprinzip ist grundsätzlich anwendbar. Wenn EU-Bürgerinnen und Bürger der Schweiz tätig sind – unabhängig davon, ob sie in die Schweiz umgezogen sind oder als Grenzgängerinnen und Grenzgänger arbeiten – findet das schweizerische Datenschutzgesetz (DSG) Anwendung und nicht die Datenschutz-Grundverordnung (DSGVO).

Wie ist es, wenn Patienten aus der EU behandelt werden?

Das Marktortprinzip findet grundsätzlich Anwendung. Verletzt sich eine europäische Touristin oder ein Tourist während ihrem Urlaub in der Schweiz, so ist die Datenschutz-Grundverordnung (DSGVO) nicht anzuwenden. Die Situation ändert sich jedoch, wenn gezielt in der EU-Patientinnen oder Patienten als Kunden geworben werden. In solchen Fällen gilt für den Schutz der Daten dieser Personen die Datenschutzgrundverordnung (DSGVO). Entscheidend ist hierbei, dass aktiv Dienstleistungen zur Gewinnung von Patientinnen oder Patienten in der EU angeboten werden.

Bei Anwendbarkeit der DSGVO sind verschiedene zusätzliche Bestimmungen zu beachten. So ist beispielsweise eine rechtliche Vertretung in der EU zu benennen. Zudem ist die Ernennung einer betrieblichen Datenschutzbeauftragten erforderlich. Diese muss über die entsprechende berufliche Qualifikation, sowie Fachwissen im Bereich des Datenschutzrechts und der Datenschutzpraxis verfügen.

III) Leitfäden, Checklisten und Vorlagen

- EDÖB (Datenschutz- und Öffentlichkeitsbeauftragten): Datenschutz im Zusammenhang mit Gesundheitsdaten, unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit.html
- FMH (Foederatio Medicorum Helveticorum): Leitfäden, Checklisten und Vorlagen der FMH zum Thema Datenschutz unter https://www.fmh.ch/themen/ehealth/datenschutz.cfm
- Ärztekasse: Muster und Checklisten unter https://www.aerztekasse.ch/datenschutzgesetz/neues-datenschutzgesetz/
- Kofam (Koordinationsstelle für die Forschung am Menschen): Leitfäden, Checklisten und Vorlagen zum Thema Forschung am Menschen: https://kofam.ch/de
- Swissethics (Schweizerische Vereinigung der Forschungsethikkommissionen): Leitfäden, Checklisten und Vorlagen zum Thema Forschung am Menschen: https://swissethics.ch/

IV) Relevante Gesetzesgrundlagen

- Bundesgesetz über den Datenschutz vom 25. September 2020 SR 235.1: https://www.fedlex.admin.ch/eli/oc/2022/491/de
- Verordnung über den Datenschutz (DSV) vom 31. August 2022 SR 235.11: https://www.fedlex.admin.ch/eli/oc/2022/568/de
- Bundesgesetz über die Forschung am Menschen vom 30. September 2011 SR 810.30: https://www.fedlex.admin.ch/eli/cc/2013/617/de

Autor:innen:

Ursula Uttinger, Präsidentin des Vereins SHPP für Datenschutz im Gesundheitswesen und Dozentin an der HSLU, Marcel Waldvogel, IT-Sicherheitsexperte und ehemaliger Informatikprofessor, haben es in Zusammenarbeit mit der EQUAM Stiftung (u.a. Andri Christen), sowie Ärzt:innen und MPA erarbeitet. Das Fact Sheet und die FAQ beantwortet nicht alle Fragen zum Thema Datenschutz und IT.

Informationen zum Dokument:

Die erste Version dieses FAQ wurde mit der finanziellen Unterstützung von Health Info Net AG (HIN) und dem Verband Schweizerischer Fachhäuser für Medizinalinformatik (VSFM) erstellt.

Zitiervorschlag:

Uttinger Ursula, Waldvogel Marcel, Christen Andri: Fact Sheet & FAQ: Datenschutz in der Arztpraxis, EQUAM Stiftung, Bern, 2018, revidiert 2019, überarbeitet gemäss neuem Datenschutzgesetz DSG, 2024.