FAQ: Datenschutz und Informationstechnologie in der Arztpraxis

Ursula Uttinger
Marcel Waldvogel

EQUAM STIFTUNG

vsfm Verband Schweizerischer Fachhäuser für Medizinal-Informatik

HIN

EQUAM STIFTUNG

Inhaltsverzeichnis

Vorwort

Für Ärztinnen, Ärzte, MPA, Praxismanager_innen ist der sorgfältige Umgang mit den ihnen anvertrauten Patientendaten ein wichtiges Anliegen. Doch wie kann man diese Daten schützen?

Die Lage ist oftmals nur schwer durchschaubar. Rechtsquellen behandeln das Thema auf einer übergeordneten Ebene und sind nicht einfach zu interpretieren. Zudem wirft die zunehmende Digitalisierung der Arztpraxen viele Fragen auf. Patientendaten müssen inmitten eines rasanten technologischen Wandels bestmöglich geschützt werden. Mit dem vorliegenden FAQ (Frequently Asked Questions) halten Sie dazu eine erste Hilfestellung in den Händen.

Ursula Uttinger, Präsidentin des Datenschutzforums Schweiz und Marcel Waldvogel, Professor für Informatik an der Universität Konstanz, haben es in enger Zusammenarbeit mit der EQUAM Stiftung, sowie Ärztinnen und Ärzten und MPA erarbeitet. Das FAQ beantwortet nicht alle Fragen zum Thema Datenschutz und IT. Es ist keine verbindliche Quelle für den Rechtsfall, sondern soll in erster Linie praxisbezogene Anregung zur Diskussion sein.

Wir danken unseren Sponsoren der Health Info Net AG (HIN) und dem Verband Schweizerischer Fachhäuser für Medizinalinformatik (VSFM) herzlich für die Unterstützung bei der Erstellung dieser FAQ.

Wenn Sie Ihr Team für die Fragen des FAQ gezielt sensibilisieren möchten, informieren Sie sich auf unserer Website www.equam.ch/datenschutz-it über das Sensibilisierungsprogramm «Datenschutz und Informationstechnologie». Die nachfolgenden Fragen werden darin bearbeitet.

Uttinger U. & Waldvogel M.: FAQ Datenschutz und Informationstechnologie in der Arztpraxis, EQUAM Stiftung, Bern, 2018, revidiert 2019

EQUAM STIFTUNG

1. Welche Daten sollen wir bei Patienteneintritt erheben?

Bezüglich der Datenerhebung ist Art. 4 Abs 2 DSG relevant:
- *Personendaten dürfen nur rechtmässig bearbeitet werden.*
- *Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.*

1.1 Welche Mindestdaten dürfen wir erfragen? Administrativ

Die Administration darf Name, Geburtsdatum, Kontaktdaten, den Versicherungsträger und Versichertennummer erfragen, sofern die Abrechnung über die Krankenkasse erfolgt. Minimal erforderlich sind Name und Adresse für eine Rechnungsstellung, wenn die Krankenkasse nicht involviert werden sollte. Bei Fragen, die über dieses Minimum hinausgehen, muss es dem Patienten / der Patientin überlassen werden, ob er / sie diese beantwortet. Idealerweise kennzeichnen Sie zwingende Fragen auf einem Anmeldeformular.

1.2 Welche Mindestdaten dürfen wir erfragen? Medizinisch

Im Rahmen der medizinischen Behandlung müssen noch weitere Informationen erfragt werden wie vorbelastende / vorbestehende Erkrankungen, bekannte Allergien, Medikamentenunverträglichkeit so weit bekannt, übertragbare Krankheiten, Symptome etc. Besteht jedoch z.B. der Verdacht einer sexuell übertragbaren Krankheit, sind auch noch weitere Informationen zwingend und dürfen erfragt werden wie z.B. Schwangerschaft, sexuelle Ausrichtung etc. Es ist also zu unterscheiden, in welcher Funktion und in welchem Problemkontext Daten erhoben werden.

1.3 Was sollten wir mindestens in die Akten aufnehmen?

Im Verlauf der Behandlung sollten mindestens die zwei folgenden Informationskategorien dokumentiert werden:
1. Sachverhaltsfeststellungen der Ärztin / des Arztes wie Anamnese, Krankheitsverlauf, Diagnose
2. Angeordnete Therapien, verschriebene Medikamente, Arztzeugnisse
Wichtig ist, dass die Informationen möglichst objektiv notiert und dokumentiert werden.

1.4 Welche Fragen sollten wir nicht stellen?

In den meisten Fällen spielen Informationen über Religion, Hobbies und sexuelle Ausrichtung keine Rolle. Gerade letztere Frage kann jedoch je nach Krankheitsbild relevant sein.

1.5 Dürfen wir fragen, warum der / die Patient_in zu uns kommt, bzw. die Arztpraxis wechselt?

Diese Frage dürfen Sie stellen. Ob der / die Patient_in diese Frage beantwortet, ist aber ihm / ihr überlassen. Es kann auch kaum überprüft werden, ob eine Antwort korrekt ist.

1.6 Dürfen wir Daten von Familienangehörigen verlangen?

Grundsätzlich ist es nicht notwendig, Daten von Familienangehörigen zu erheben. Es kann aber dann sinnvoll sein, wenn man bei einem Notfall jemanden informieren muss. In diesem Sinne empfehlen wir, anstelle von Familienangehörigen zu erfragen, wer in einem Notfall informiert werden soll. Allerdings veralten solche Angaben auch schnell. Idealerweise fragen Sie periodisch nach, ob die Angaben noch stimmen.

1.7 Dürfen wir Fragen zu Einkommen, Vermögen, Sozialhilfe stellen?

Auch wenn es im Interesse der Praxis ist, dass Rechnungen bezahlt werden können, ist diese Frage heikel und sollte nicht gestellt werden. Insbesondere sind Fragen nach Sozialhilfe besonders schützenswert. Fragen nach Einkommen und Vermögen sind zwar nicht besonders schützenswert, könnten aber das Vertrauensverhältnis mit dem Patienten / mit der Patientin beeinträchtigen.

Wichtiger ist es, die zuständige Krankenversicherung zu kennen. Weiter gibt es grundsätzlich die Möglichkeit, Informationen zur Bonität über entsprechende Auskunfteien einzuholen. Dies ist auch ohne Einwilligung oder gegen den Willen der betroffenen Person möglich, sofern ein Vertragsabschluss mit der betroffenen Person eingegangen werden soll.

Im Zusammenhang mit der Rechnungsstellung ist zu beachten, dass Sie für eine allfällige Betreibung die Entbindung vom Berufsgeheimnis vorgängig einholen müssen. Diese Entbindung kann entweder der / die Patient_in selbst geben oder sie kann via Aufsichtsbehörden einverlangt werden.

Die Entbindung von der beruflichen Schweigepflicht benötigt eine Einwilligung von der betroffenen Person – dies gilt auch wenn eine spezialisierte Firma das Inkasso vornimmt. Oft wird die Entbindung auf dem Anmeldeformular eingeholt. Streng genommen genügt dies nicht. Würde eine betroffene Person dagegen klagen, sind die Chancen gut, dass sie Recht erhielte.

Wenn, dann sollten Sie eine solche Entbindung von der beruflichen Schweigepflicht pro Behandlung einholen. Damit wäre klar, dass die Entbindung für die konkrete nächste Behandlung gilt. In der Praxis dürfte dies aber sehr aufwändig sein, so dass man meist auf eine Entbindung bei der Anmeldung abstellt.

1.8 Was, wenn der / die Patient_in falsche Angaben liefert?

Neben Art. 4 Abs. 2 DSG ist für die Datenrichtigkeit Art. 5 DSG relevant:

- *Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.*
- *Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden.*

Für die Richtigkeit der Daten ist der Dateninhaber verantwortlich. Datenschutzrechtlich ist der Dateninhaber die Person, die bestimmt, welche Daten zu welchem Zweck erhoben werden. Das heisst, die Arztpraxis ist dafür verantwortlich, dass die Daten korrekt sind. Falschangaben durch die betroffene Person selbst sind jedoch kaum als solche erkennbar.

Es empfiehlt sich deshalb, klar festzuhalten, von wem man Angaben erhalten hat. Die Datenrichtigkeit hat eine grosse Bedeutung. So sollte sichergestellt werden, dass Daten im elektronischen System nicht versehentlich verändert werden können, ohne dass nachvollziehbar ist, wer diese Änderung vollzogen hat und aus welcher Quelle diese Informationen stammen. → 6.

1.9 Was, wenn der / die Patient_in sich weigert, Fragen zu beantworten?

Es ist zu unterscheiden, ob es sich um eine Frage handelt, die relevant ist, um den Patienten / die Patientin zu behandeln oder ob es ergänzende Fragen sind. Handelt es sich um zwingende Fragen, muss abgewogen werden, ob der / die Patient_in behandelt werden kann.

Welche Fragen zwingend sind, kann nicht allgemein beantwortet werden. Je nach Krankheit / Unfallereignis sind andere Daten relevant. Man sollte dabei eine Risikoabwägung vornehmen: Was kann passieren und welche Risiken gibt es, wenn gewisse Informationen nicht vorhanden sind? Idealerweise werden, soweit bekannt, die Risiken fehlender Informationen mit dem Patienten / mit der Patientin besprochen.

1.10. Was sollen wir beim Empfang von Patientinnen / Patienten beachten?

Gerade beim Empfang ist der Datenschutz heikel: Einerseits sollte der / die Patient_in schnell bedient und richtig identifiziert werden, andererseits kann es vorkommen, dass mehrere Personen gleichzeitig die Praxis betreten.

Doch nicht nur wenn zwei Personen beim Empfang stehen, auch wenn das Telefon klingelt und man mit einem Patienten spricht, sollten Dritte keine medizinischen Informationen mithören können.

In beiden Fällen ist darauf zu achten, dass MPA und der / die Patient_in so miteinander sprechen, dass keine weiteren Patienten erfahren, welche Krankheiten diese_r Patient_in hat.

EQUAM STIFTUNG

2. Wie handhaben wir das Recht der Patientinnen und Patienten auf die Herausgabe Ihrer Daten?

Für die Datenherausgabe ist Art. 8 DSG relevant:

- *Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.*
- *Der Inhaber der Datensammlung muss der betroffenen Person mitteilen: alle über sie in der Datensammlung vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten; den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.*
- *Daten über die Gesundheit kann der Inhaber der Datensammlung der betroffenen Person durch einen von ihr bezeichneten Arzt mitteilen lassen.*
- *Lässt der Inhaber der Datensammlung Personendaten durch einen Dritten bearbeiten, so bleibt er auskunftspflichtig. Der Dritte ist auskunftspflichtig, wenn er den Inhaber nicht bekannt gibt oder dieser keinen Wohnsitz in der Schweiz hat.*
- *Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen. Der Bundesrat regelt die Ausnahmen.*
- *Niemand kann im Voraus auf das Auskunftsrecht verzichten.*

2.1 Was bedeutet das Recht auf Herausgabe der Daten?

Gemäss Datenschutzgesetz hat jede Person das Recht, eine Kopie ihrer Daten vom Inhaber der Datensammlung (hier der Arztpraxis) zu erhalten. Dies gilt auch für Krankenakten, bzw. das Patientendossier.

2.2 Müssen wir sämtliche Daten herausgeben?

Grundsätzlich müssen Sie sämtliche Daten herausgeben. Nebst dem Patientendossier also auch Untersuchungsergebnisse, Labor- und Röntgenbefunde, Diagnosen, Gutachten, Berichte, Zeugnisse.

Es gibt aber folgende Ausnahme: Sogenannte «persönliche Arbeitshilfsmittel» also etwa persönliche Notizen, die ausserhalb der KG geführt werden unterstehen nicht dem Datenschutzgesetz und damit entfällt eine Herausgabepflicht. Bei persönlichen Arbeitshilfsmitteln ist zu beachten, dass keine Drittpersonen, also auch nicht eine MPA, Zugriff auf diese Daten haben sollten. Im Normalfall dürften solche Arbeitshilfsmittel im Laufe der Behandlung in ein offizielles Dokument übertragen werden.

Der / die Patient_in ist der / die eigentliche Auftraggeber_in. Das heisst, er / sie bleibt Inhaber_in seiner / ihrer Daten. Es kann nicht sein, dass ihm / ihr Informationen / Daten vorenthalten werden.

Zu beachten ist, dass bei der Datenherausgabe nicht eine Persönlichkeitsverletzung einer Drittperson erfolgt, also Daten von Drittpersonen herausgegeben werden. In seltenen Fällen kann dies dazu führen, dass Sie Namen von Drittpersonen, die auf einem herauszugebenden Dokument aufgeführt sind, abdecken. Ob die Daten abzudecken sind, hängt mit deren Relevanz für die anfragende Person zusammen und ob allenfalls dieser Drittperson Vertraulichkeit zugesichert worden ist. In einem solchen Fall muss eine Interessenabwägung vorgenommen werden.

Bei der Herausgabe der Daten ist zu überprüfen, ob nicht Informationen in der Akte stehen, die eigentlich zu einem anderen Patienten / zu einer anderen Patientin gehören. Insbesondere bei der Ablage von eingehenden Berichten im Rahmen von Scanvorgängen sind solche Fehlzuordnungen bekannt.

2.3 Müssen wir die Daten immer dem Patienten / der Patientin direkt herausgeben?

Stellt der / die Patient_in ein Auskunftsbegehren gestützt auf Art. 8 DSG können die medizinischen Daten, und nur diese, über einen Arzt des Vertrauens der anfragenden Person herausgegeben werden. Dies ist dann der Fall, wenn dadurch eine allfällige Selbstgefährdung der anfragenden Person vermieden werden kann. Es ist allerdings die anfragende Person, die entscheidet, welcher Arzt die Daten erhält. Dieser gibt dann wiederum der anfragenden Person die Daten heraus und erklärt sie ihr allenfalls.

2.4 Dürfen wir zwischen elektronischen Daten und Daten in Papierform unterscheiden?

Grundsätzlich spielt es keine Rolle, ob es sich um elektronische Informationen oder Daten in Papierform handelt. Papierakten müssen kopiert werden, elektronische Daten sind auszudrucken oder auf einem elektronischen Datenträger zu übergeben.

2.5 In welcher Form müssen wir die Daten herausgeben?

Sie müssen Daten so herausgeben, dass die anfragende Person sie lesen kann. Gerade bei grossen Mengen kann sich ein USB-Stick oder auch eine CD als sinnvoll erweisen. Insbesondere können elektronische Daten einfacher geordnet und mittels Stichworten abgesucht werden.

2.6 Kann ein_e Patient_in eine Berichtigung von Daten verlangen?

Zuerst ist zu beachten, dass nur objektive Daten berichtigt werden können. Beispielsweise sollten Sie ein falsches Geburtsdatum berichtigen. Ebenfalls sollten Sie z.B. berichtigen lassen, wenn z.B. eine Operation am linken, und nicht am rechten Fuss durchgeführt wurde. Bei objektiven Tatsachen kann die betroffene Person jederzeit eine Berichtigung der Daten verlangen. Idealerweise wird die Korrektur mit Datum und Grund für die Korrektur festgehalten.

Anders sieht es aus, wenn es sich nicht um objektive Tatsachen, sondern um Meinungen des Arztes / der Ärztin oder der MPA handelt. Besteht beispielsweise beim Arzt / bei der Ärztin der Eindruck einer Überforderung oder einer psychischen Erkrankung wie einer Psychose, so kann dieser zwar anhand von Symptomen entstanden sein. Es bleibt aber eine Meinung. In diesen Fällen hat die betroffene Person das Recht, einen Vermerk anbringen zu lassen. Ein Vermerk ist ähnlich wie eine Gegendarstellung und zeigt die Sichtweise der betroffenen Person.

2.7 Wem gehören die Unterlagen? Dem Arzt / der Ärztin oder dem Patienten / der Patientin?

Gewisse Unterlagen gehören dem Arzt / der Ärztin. Für diese hat er / sie auch eine entsprechende Aufbewahrungspflicht. Andere Daten gehören jedoch dem Patienten / der Patientin – denn Unterlagen, die der / die Patient_in dem Arzt / der Ärztin übergeben hat, gehören grundsätzlich noch dem Patienten / der Patientin. Je nach kantonalem Recht haben Ärzte und Ärztinnen die Pflicht, Originalakten aufzubewahren.

Da die Krankenakten im Interesse der Patientinnen und Patienten geführt werden, kann der / die Patient_in die Originalakten verlangen. Der Arzt / die Ärztin sollte sich bei der Herausgabe der Originalakten schriftlich von der Aufbewahrungspflicht befreien lassen. → 6.8

3. Wie handhaben wir Weitergabe von Daten an Dritte?

3.1 Müssen wir unterscheiden, wem wir Daten weitergeben?

Sie können Daten nicht beliebig Dritten weitergeben – selbst wenn diese Drittpersonen ebenfalls einem Berufsgeheimnis unterstehen. Grundsätzlich können Sie davon ausgehen, dass Sie einer nachbehandelnden Ärztin sämtliche relevanten Unterlagen auch ohne ausdrückliche Einwilligung der betroffenen Person herausgeben dürfen. → 3.3

Familienangehörige haben demgegenüber kein Anrecht auf Daten oder Informationen, es sei denn, die betroffene Person habe eine ausdrückliche Einwilligung erstellt.

Gegenüber den Versicherern ist zu unterscheiden, um welche Art Versicherung es sich handelt:

- Unfallversicherer haben ein Anrecht auf Informationen im Zusammenhang mit dem Unfall. Denn hier gilt das sogenannte Naturalleistungsprinzip. Das bedeutet, dass im Zusammenhang mit einer Behandlung nach einem Unfall der Unfallversicherer und nicht die betroffene Person Auftraggeber ist. Folglich hat der Unfallversicherer als Auftraggeber ein Anrecht auf Daten und Informationen.
- Krankenversicherer in der Grundversicherung haben die Aufgabe, eine Leistung in Bezug auf Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit (WZW) zu prüfen. In diesem Sinne haben die Krankenversicherer ein Anrecht auf Daten, um diese gesetzliche Prüfung vornehmen zu können. Besonders sensible Daten kann man auch dem vertrauensärztlichen Dienst eines Krankenversicherers zustellen.
- Sämtliche übrigen Versicherer, wie Zusatzversicherer in der Krankenversicherung, Lebensversicherer etc. müssen eine Einwilligung der betroffenen Person vorweisen. Eine Weitergabe von Daten ohne Einwilligung mit Entbindung der ärztlichen Schweigepflicht würde gegen das Berufsgeheimnis verstossen.
- Formulare von Sozialversicherern müssen vollständig und wahrheitsgetreu ausgefüllt werden, wenn diese im Zusammenhang mit der Geltendmachung eines Leistungsanspruchs der betroffenen Person stehen (Art. 29 ATSG).
- Der Arbeitgeber darf nur die Informationen erhalten, die er braucht, um zu wissen, ab wann eine Person wieder arbeiten und welche Tätigkeiten sie ausführen kann. Eine Diagnose braucht der Arbeitgeber im Normalfall nicht zu kennen. Ausnahmen bestehen dann, wenn die Person in einem sehr heiklen Bereich arbeitet, wie in gewissen medizinischen Forschungsabteilungen oder Funktionen mit erhöhten Sorgfaltspflichten.

3.2 Was passiert, wenn wir Daten ohne Entbindung des Arztgeheimnisses weitergeben?

Die betroffene Person kann eine Anzeige wegen Verletzung der beruflichen Schweigepflicht einreichen. Die Verletzung der beruflichen Schweigepflicht ist mit einer Höchststrafe von drei Jahren Gefängnis bedroht.

Eine Verletzung der Schweigepflicht kann auch zwischen Ärztinnen und Ärzten gegeben sein. Hinterfragen Sie: Braucht ein anderer Arzt / eine andere Ärztin tatsächlich dieses Wissen, diese Daten?

3.3 Dürfen wir die Daten einem / einer vor- bzw. nachbehandelnden Arzt / Ärztin immer weitergeben?

Es stellt sich die Frage, welche Daten tatsächlich benötigt werden. Insbesondere der / die nachbehandelnde Arzt / Ärztin sollte die Vorgeschichte möglichst umfassend kennen. Darum dürfen Sie diesem / dieser umfassende Informationen mitgeben.

Beim vorbehandelnden Arzt / bei einer vorbehandelnden Ärztin müssen Sie klären, ob dieser mit dem Patienten / mit der Patientin weiterhin Kontakt hat. Wurde beispielsweise ein_e Patient_in im Notfall in der Ferienregion behandelt, muss dieser Arzt / diese Ärztin nicht über den weiteren Verlauf Bescheid wissen.
Anders sieht es aus, wenn der / die vorbehandelnde Arzt / Ärztin der Hausarzt / die Hausärztin ist, zu dem der / die Patient_in wieder gehen wird.

Heute werden vermehrt «walk-in»-Praxen besucht. Da ist es ebenfalls nur in den seltensten Fällen sinnvoll und damit legitim, diese über den weiteren Verlauf einer Behandlung zu informieren.

3.4 Ist ein Outsourcing eine Weitergabe an Dritte?

Für ein Outsourcing ist Art. 10a DSG relevant:

- *Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:*
  - *die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und*
  - *keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.*
- *Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.*
- *Dritte können dieselben Rechtfertigungsgründe geltend machen wie der Auftraggeber.*

Beim Outsourcing handelt es sich um eine Auslagerung einer Tätigkeit an einen Dritten. Eine solche Datenbearbeitung durch Dritte ist im Datenschutz ausdrücklich vorgesehen. Auftraggeber und Auftragnehmer gelten nun nicht mehr als Dritte zueinander.

3.5 Dürfen wir Daten durch einen Dritten bearbeiten lassen?

Eine Datenbearbeitung durch Dritte ist im Datenschutzgesetz vorgesehen. Heikler als die datenschutzrechtlichen Vorgaben sind die Vorgaben des Berufsgeheimnisses: Bei einer Da-

tenbearbeitung durch einen Dritten wird dieser zur Hilfsperson und untersteht dann ebenfalls der strengeren Regelung von Art. 321 StGB. Eine Verletzung des Berufsgeheimnisses kann mit einer Strafe von bis zu drei Jahren Gefängnis geahndet werden.

Bei einer Datenbearbeitung durch Dritte sollte noch unterschieden werden, ob es sich um eine medizinische Arbeit wie z.B. Laboratorien oder einen externen IT-Spezialisten handelt. Idealerweise wird der / die Patient_in vorgängig informiert, wenn man Daten durch Dritte bearbeiten lässt.

Bei medizinischen Arbeiten ist den betroffenen Personen bewusst, dass für sie das Berufsgeheimnis gemäss Art. 321 StGB gilt, bei anderen Tätigkeiten sollten die Auftragnehmer speziell darauf hingewiesen werden, dass sie durch die Übernahme der Tätigkeit zu einer Hilfsperson werden und denselben Schweigepflichten unterstehen wie eine Medizinalperson.

Wichtig ist, dass die Verantwortung auch für die Bearbeitung der Daten durch einen Dritten beim Auftraggeber bleibt. Im eigenen Interesse schaut der Auftraggeber, dass dieser Dritte sich an sämtliche Vorgaben hält und Daten nicht missbräuchlich bearbeitet.

3.6 Wie gehen wir mit Anfragen der Polizei und weiteren Behörden um?

Je nachdem gibt es eine spezielle Verfügung, die einen Arzt / eine Ärztin verpflichtet, den Behörden Informationen weiterzuleiten. Aber auch hier gilt: zuerst nachfragen und gegebenenfalls eine schriftliche Verfügung (= Anordnung einer Behörde) verlangen.

3.7 Gibt es Fälle von Anzeigepflicht?

Es gibt sogenannte «Meldepflichtige Krankheiten», die je nach Kriterium innert 2 Stunden, 24 Stunden oder 1 Woche dem BAG zu melden sind. Das BAG hat dazu einen Leitfaden verfasst: http://www.bag.admin.ch/k_m_meldesystem/00733/

Bei Fahruntüchtigkeit etwa haben Ärztinnen und Ärzte demgegenüber keine Meldepflicht, sondern nur ein Melderecht. Das bedeutet, dass der Arzt / die Ärztin eine Fahruntüchtigkeit den entsprechenden Behörden melden kann, eine Pflicht besteht jedoch nicht, denn eine solche könnte das Vertrauensverhältnis Arzt / Ärztin – Patient_in beeinträchtigen.

Ebenfalls besteht eine Meldepflicht bei schweren Delikten gegen Leib und Leben, die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind, wie beispielsweise schwere Körperverletzung, sexuelle Nötigung, Vergewaltigung. Bei der Meldepflicht sind die kantonalen Gesetze zu beachten.

Auch über die Gefährlichkeit von Strafgefangenen gibt es je nach Kanton eine Meldepflicht gegenüber den Strafverfolgungsbehörden. Besteht eine Anzeigepflicht, kann eine Unterlassung zu einer Begünstigung führen, die selbst mit einer Freiheitsstrafe bis zu drei Jahren bedroht ist.

3.8 Wie steht es bei der medizinischen Forschung?

Bei der medizinischen Forschung braucht es für die Datenweitergabe die Einwilligung der betroffenen Person, sofern die Daten nicht anonym bearbeitet werden. Die Einwilligung hat freiwillig zu erfolgen und der Betroffene muss ausreichend informiert sein, was das Ziel der Forschung ist, welche Daten dazu genutzt werden und wie umfassend die Daten genutzt werden.

Daten sind dann anonym, wenn sie nicht mehr einer Person zugeordnet werden können. Bei genetischen Daten dürfte dies üblicherweise nicht der Fall sein, bei anderen gesundheitsbezogenen Angaben ist eine Anonymisierung oft möglich, insbesondere bei statistischen Auswertungen.

Kann weder eine Einwilligung eingeholt werden noch mit anonymisierten Daten gearbeitet werden, kann allenfalls die kantonale Ethikkommission eine Bewilligung für die Datenbearbeitung erteilen.

3.9 Was ist mit Daten für die Qualitätskontrolle?

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 Patienten notwendig, etwa via eine Erklärung auf dem Anmeldeformular. Handelt es sich bei den Dritten um Hilfspersonen, die unter der Aufsicht und Weisung des Arztes /der Ärztin / der Praxis tätig sind, so unterstehen diese der beruflichen Schweigepflicht.

Unabhängig ob Hilfsperson oder Dritte ist darauf zu achten, dass diese sich der beruflichen Schweigepflicht bewusst sind. Eine solche Verpflichtung sollte schriftlich vereinbart werden.

4. Wie gestalten wir digitalen Datenaustausch möglichst sicher?

Für die Datensicherheit ist Art. 7 DSG zentral:
- *Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.*
- *Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit.*

4.1 Welche Optionen zur Mailverschlüsselung gibt es?

Grundsätzlich macht eine Verschlüsselung Sinn, weil dadurch besser sichergestellt werden kann, dass nur der Besitzer des Schlüssels die Daten verstehen kann. So wird die Vertraulichkeit gewahrt. Bei Verschlüsselung unterscheiden wir zwischen Inhaltsverschlüsselung (auch als Ende-zu-Ende oder E2E-Verschlüsselung bekannt) und Transportverschlüsselung. Transportverschlüsselung schützt vor Mithören auf Datenleitungen und Routern zwischen den Mailprovidern. Absender, Empfänger, Betreff und Inhalt der Mail sind damit vor Horchern an der Leitung sicher. Viele Mailprovider aktivieren heute automatisch Transportverschlüsselung, wenn sowohl der Provider des Absenders als auch der des Empfängers diese unterstützt.
Die Mailprovider selbst haben aber Zugang zu diesen Informationen. Falls der Provider nicht auf den Inhalt der Mail zugreifen können soll, kann zusätzlich noch der Inhalt der Mail zwischen den beiden Benutzern verschlüsselt werden. Absender, Empfänger und Betreff sind für die beteiligten Provider trotzdem einsehbar.

Während Transportverschlüsselung heute als Standard gilt, bleibt die Ende-zu-Ende-Verschlüsselung aufgrund von Aufwand und Kosten immer noch die Ausnahme. Eine praktikable Möglichkeit ist die Nutzung von ZIP- oder PDF-Verschlüsselung mit einem sicheren Passwort, welches nicht auch für einen anderen Kommunikationspartner verwendet wurde. Dieses Passwort kann man dem Gegenüber z.B. via SMS senden.

4.2 Ist eine Verschlüsselung von Mail immer zwingend?

Nein. Insbesondere, wenn der / die Patient_in erklärt hat, dass die Daten auch unverschlüsselt übermittelt werden dürfen. Allerdings stammen eingehende Mails nicht notwendigerweise von der Person die vorgibt, die Mail geschrieben zu haben. Zudem sollte die Praxis nie von sich aus eine unverschlüsselte E-Mail-Konversation mit einem Patienten / mit einer Patientin initiieren. → 6.6 / → 7.5

4.3 Was nützt ein Disclaimer am Ende der Mail?

Einige Absender hängen am Ende der Mail automatisch einen so genannten Disclaimer, d.h. einen (häufig langen) Text an, der sagt, wie der Empfänger mit der Mail umgehen soll. Ins

besondere wird dort aufgeführt, dass falsche Empfänger die Mail löschen und den Absender informieren sollen. Dies ist rechtlich für den Empfänger nicht bindend. Es kann sogar beim Empfänger Verwirrung auslösen oder ihn möglicherweise umso mehr zum Missbrauch dieser Daten verleiten oder rechtmässige Absender verunsichern. Wir empfehlen deshalb, keine Disclaimer zu nutzen.

4.4 Ist das Versenden von Daten per Fax sicher?

Ein nicht verschlüsseltes Fax ist genau wie ein nicht verschlüsseltes Mail oder ein nicht verschlüsselter Telefonanruf. Die wenigsten Faxgeräte sind verschlüsselt, da die entsprechenden Geräte sehr teuer und aufwändig in der Handhabung sind. Insofern ist ein Fax nur bedingt sicher. Ausserdem darf nicht vergessen werden, dass man sich bei der Faxnummer schnell vertippt und das Dokument damit an einen falschen Empfänger gerät.

4.5 Was ist die Cloud?

Ein geflügeltes Wort sagt, es gäbe keine Cloud, es gäbe nur die Rechner von jemand Anderem. Unter «Cloud» im weiteren Sinne verbirgt sich jeder standardisierte Dienst, der online angeboten wird und Ressourcen (Speicher, Verarbeitung etc.) via Internet nutzt. Im engeren Sinne wird darunter Cloudspeicher verstanden, also die Möglichkeit, Daten über eine Webseite oder App online zu speichern und so verschiedenen Geräten und Nutzern zugänglich zu machen. In den meisten Praxen ist die Erbringung aller Dienstleistungen im Hause nicht wirtschaftlich. Die Nutzung von externen Angeboten zur Datenverarbeitung wird deshalb immer wichtiger.

4.6 Ist das Nutzen einer Cloud auch ein digitaler Datenaustauch im weitesten Sinne?

Wenn die Gesamtgrösse der Anhänge 15 Megabyte überschreitet, werden viele Mailprovider diese Mail nicht annehmen. Insbesondere in diesem Fall bietet sich auch die Nutzung eines Online-Cloudspeichers an. Es gelten daher ähnliche Überlegungen wie beim Versand per Mail. Zusätzlich zu den Kriterien an die Auswahl eines Mailproviders ist hier zu berücksichtigen, dass die Daten meist nach der Übermittlung vom Absender manuell gelöscht werden müssen. Datenablagen in einer Cloud werden immer gebräuchlicher. Dabei ist es wichtig, den Cloud- Anbieter sorgfältig auszusuchen. Idealerweise sollten die Daten in der Schweiz bleiben.

4.7 Wie gehen wir mit Fernwartung um?

Fernwartungssoftware ist für einen effizienten IT-Support unumgänglich. Die typische eingesetzte Software gilt als sicher. Die Person am anderen Ende der Fernwartung hat jedoch vollständigen Zugriff auf Ihren Rechner und möglicherweise das Netz. Fernwartungssoftware hebelt auch den typischen Schutz einer Firewall aus. Geben Sie nie einem Unbekannten Zugriff zu Ihrem Fernwartungssystem. → 6.6 / → 7.5

EQUAM STIFTUNG

5. Wie organisieren wir den Zugang zu den Daten innerhalb der Praxis?

In Abwesenheit von autorisierten Personen soll kein Zugang zu fremden Daten möglich sein. Dazu sind die Praxisanwendungen und der Zugriff auf die Daten mit einem sicheren Passwort zu schützen. → 5.4

So sagt Art. 9 VDSG: Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:

- *Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;*
- *Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;*
- *Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;*
- *Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;*
- *Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;*
- *Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;*
- *Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;*
- *Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.*

5.1 Genügt es, wenn der Bildschirmschoner automatisch nach 10 Minuten einschaltet?

Der Bildschirmschoner alleine ist ungenügend, denn dadurch ist der Computer noch nicht passwortgeschützt. Erst, wenn der Bildschirmschoner auch eine Bildschirmsperre nach sich zieht, ist der Schutz da. Welche Zeitdauer sinnvoll ist, hängt von der Platzierung des Rechners ab.

Rechner, zu denen Fremde keinen Zugang haben bzw. die immer im Blickfeld einer Mitarbeitenden stehen, müssen nicht gesperrt werden. Wenn der Rechner im Behandlungszimmer steht, sollte er immer dann gesperrt sein, wenn ein_e Patient_in alleine dort wartet. Nur wenn der Rechner die Akte des im Raum wartenden Patienten anzeigt und ein Wechsel zu anderen Daten nicht möglich ist, muss er nicht gesperrt werden.

Die Sperrzeit sollte so gewählt werden, dass die Sperre während dem normalen Arbeiten möglichst nicht aktiv wird, ein Zugang für Unberechtigte jedoch zuverlässig vermieden wird. Insbesondere bei längeren Abwesenheiten sollte die Bildschirmsperre aktiviert werden. Im Alltag ist ein Fingerabdruckleser zum Entsperren sinnvoll. Für den professionellen Datendieb sind Fingerabdrücke zwar kein Hindernis, d.h. sie sollten nicht für das morgendliche Einloggen genutzt werden. Im Tagesbetrieb ist der Abdruck aber schnell und effektiv.

5.2 Ist es sinnvoll, Passworte pro User vorzugeben?

Passworte sollten immer persönlich sein und weder zwischen Mitarbeitenden geteilt, noch bei unterschiedlichen Systemen eingesetzt werden. Insbesondere sollte das Praxispasswort nicht auch für Web- oder Maildienste Dritter eingesetzt werden, auch nicht in leicht abgewandelter Form.

5.3 Genügt ein Passwort pro Arbeitsplatz?

Mit geteilten Passwörtern wird sorgloser umgegangen als mit persönlichen. Insbesondere bei Personalwechsel wird das gemeinsame Passwort meist nicht geändert. Weil mehrere Personen das Passwort kennen wird häufig auch ein einfacheres gewählt. Deshalb raten wir von «globalen» Passwörtern ab.

5.4 Was macht ein sicheres Passwort aus?

Ein Passwort sollte für einen Angreifer nur nach sehr langer Zeit erkennbar werden. Insbesondere sollte das Passwort sicher vor automatischen Angriffen sein, die z.T. Abermillionen Passwörter pro Sekunde überprüfen können. Lexikonworte, Vornamen von Partnern, Geburtsdaten oder eine Kombination davon sind nicht sicher. Auch das Ersetzen einzelner Buchstaben (O"0, I"0, I"1 etc.) erschwert einen Angriff kaum. In diesem Sinne sei ein Passwort empfohlen, das mindestens 10 Zeichen lang ist und aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen besteht. Zahlen und Sonderzeichen sollten nicht nur am Ende vorkommen.

5.5 Wie erzeuge ich ein sicheres Passwort?

Am einfachsten ist die Passworterzeugung mit einem Passwortmanager. Alternativ kann man die Anfangsbuchstaben eines Merksatzes nutzen, inklusive einiger absichtlich eingebauter Tippfehler. Oder man drückt zuerst wild auf der Tastatur herum und ändert dann ein paar Zeichen, bis man sich das Passwort gut merken kann.

5.6 Müssen wir das Passwort alle drei Monate wechseln?

Ein häufiger Passwortwechsel führt dazu, dass man das Passwort entweder aufschreibt, immer wieder ähnliche Passworte aussucht oder (zu) einfache Passworte verwendet. Entsprechend raten wir von einem automatischen regelmässigen Passwortwechsel ab.

Das Passwort sollte aber gewechselt werden, wenn davon auszugehen ist, dass ein unbefugter Dienst oder eine unbefugte Person davon Kenntnis erlangt hat, z.B. durch allzu neugieriges Über-die-Schulter- Gucken bei der Passworteingabe (Shoulder Surfing).

Wenn Sie das Passwort für den Onlinedienst A bei der Anmeldemaske für den Onlinedienst B eingeben, erfährt der Dienst B dieses Passwort. Normalerweise wird B das Passwort gleich wieder vergessen. Ein bösartiger oder gehackter Dienstanbieter B kann es aber missbrauchen. Ein Passwortmanager hilft, diesen Fehler und den daraus resultierenden Missbrauch zu vermeiden.

5.7 Wie merke ich mir die unzähligen kryptischen Passwörter?

Für die Verwaltung der Passwörter für Webdienste etc. empfehlen wir, einen Passwortmanager zu nutzen. Die Login-Passwörter für Arbeitsplatzrechner müssen im Kopf gespeichert werden. Idealerweise nutzen Sie ein Single-Sign-On; so müssen Sie sich nur ein Passwort merken.

5.8 Geht das nicht einfacher?

Alternativ zu Passwörtern können biometrische Merkmale genutzt werden. Dazu zählt beispielsweise der Fingerabdruckleser am Rechner oder am Smartphone. Fingerabdrücke sind insbesondere auf dem Smartphone sehr bequem geworden. Sie bieten einen sehr hohen Schutz gegen Angriffe aus der Ferne, sind aber für Personen mit Zugang zu den Räumen einfach auszuhebeln. Gefundene Fingerabdrücke auf Trinkgläsern oder dem Touchscreen können zum Austricksen des Fingerabdrucklesers vor Ort eingesetzt werden. Smartcards oder berührungslose Token sind sehr sicher, wenn die Trägerin sicherstellt, dass keine Unbefugten Zugang dazu erhalten (Diebstahl, Herumliegenlassen, …).

5.9 Wir verlangen, dass alle Mitarbeitenden ihr Passwort in einem verschlossenen Couvert hinterlegen. Ist das sinnvoll?

Daten, die auch bei Abwesenheit (Unfall, Krankheit, Teilzeit etc.) anderen zugänglich sein sollten, sollten auch bereits im Anwesenheitsfall zugänglich sein. Entsprechend sollten alle relevanten Dokumente auf gemeinsam zugreifbaren Verzeichnissen liegen bzw. mit einer Software mit der Möglichkeit zur Vergabe von Zugriffsrechten verwaltet werden.

Falls die verwendete Software die Vergabe von Zugriffsrechten nicht unterstützt, bleibt nur die Couvert-Methode. Dabei sollte ein Zugriff auf ein Passwort und die damit geschützten Daten erkennbar und nachvollziehbar sein.

5.10 Gibt es dazu weitere Informationen?

18-Sekunden-Video zu Passworthygiene: https://youtu.be/VWtVMaHTh0E
Passwortmanager (einer von Vielen): https://keepass.info

6. Wie stellen wir Rückverfolgbarkeit bei der Bearbeitung digitaler Daten sicher?

6.1 Was ist Rückverfolgbarkeit?

Rückverfolgbarkeit bedeutet, die Quelle von Daten und Änderungen rekonstruieren zu können: Von wem kam wann die Überweisung? Wer hat diese Daten eingetragen? Wer hat sie verändert? Welchen Datenstand repräsentieren sie?

6.2 Wann benötigen wir Rückverfolgbarkeit?

Rückverfolgbarkeit ermöglicht es, zu wissen, zu welchem Zeitpunkt welche Daten vorhanden gewesen sind. So können Sie nachweisen, wie sich eine Datenbearbeitung entwickelt hat. Im Rahmen von Qualitätskontrollen oder einem Rechtsfall ist Nachvollziehbarkeit sinnvoll oder gar notwendig. Idealerweise kann auch festgestellt werden, wer die Daten wann bearbeitet hat. Dem Patienten / der Patientin eine Antwort geben zu können auf die Frage, woher man denn das jetzt schon wieder wisse, kann sehr hilfreich sein. Rückverfolgbarkeit kann zudem helfen, den Entscheid für einen Behandlungsprozess besser nachvollziehen zu können und die Behandlung optimal zu gestalten, gerade wenn viele Mitarbeitende in Teilzeit beschäftigt sind.

6.3 Wie stellen wir sie bei Dokumenten sicher?

Wenn jeder Benutzer sein persönliches Login verwendet, speichert der Fileserver im Normalfall den Nutzer ab, der die letzte Änderung gemacht hat. Die meisten Textverarbeitungsprogramme unterstützen auch einen Überarbeitungsmodus, der alle Änderungen au zeichnet. Die Darstellung früherer Versionen kann zur besseren Übersicht ausgeblendet bleiben, ohne dass die Aufzeichnungen dabei verloren gehen. Frühere Änderungen in anderen Programmen lassen sich mittels Inspektion der Back-ups rekonstruieren. Falls dies häufig und feingranular erfolgen soll, ist Spezialsoftware vonnöten.

6.4 Wie stellen wir sie innerhalb der Praxisanwendungen sicher?

Die Praxissoftware muss entsprechende Funktionen bereitstellen und jede Person muss ihr persönliches Login nutzen.

6.5 Wie stellen wir sie bei Bestellungen via Webformular sicher?

Bei Onlinebestellungen (z.B. Medikamente) ist ein benutzerspezifisches Login nötig, wenn unterschieden werden soll, wer welche Bestellung getätigt hat. → 5.2

6.6 Wie stellen wir sie bei eingehenden Aufträgen via Mail sicher?

Es ist relativ einfach, den Absender einer Mail zu fälschen oder verwirrend ähnlich zu machen. Trauen Sie deshalb keiner Mail (und keiner Information darin, wie z.B. Link oder Telefonnummer), wenn die Mail unerwartet kommt oder Unerwartetes verlangt (Phishing oder Social Engineering), insbesondere, wenn darin gedroht oder zur Eile gedrängt wird.

Als Empfänger ist es schwer, diese Überprüfung einfach und zuverlässig zu machen, es sei denn, man setzt für die Mailkommunikation Zertifikate oder einen spezialisierten Provider ein. → 7.5

6.7 Wie stellen wir sie bei ausgehenden Mails sicher?

Um nachvollziehen zu können, wer innerhalb der Praxis eine bestimmte Mail versandt hat, empfehlen wir personalisierte Mailadressen. Um auch bei Abwesenheit einer Mitarbeiterin eine rasche Auskunft zu ermöglichen, können automatische Abwesenheitsnachrichten genutzt werden. Da diese meist nicht konsequent eingesetzt werden, kann ein gemeinsamer Zugang auf ein oder mehrere Eingangspostfächer sinnvoll sein. Dabei bieten sich insbesondere folge Optionen an:

— Alle sehen das gemeinsamen Eingangspostfach (z.B. info@meinepraxis.ch), schreiben aber ihre Mails aus dem persönlichen Konto. Mithilfe der «Antwort an»-Funktion des Mailprogrammes antwortet der / die Patient_in dann wieder in das gemeinsame Eingangspostfach.
— Alle nutzen nur das gemeinsame Postfach, «unterschreiben» aber mit ihrem Namen.

6.8 Welche Aufbewahrungsfristen müssen wir einhalten?

Die Aufbewahrungsfristen sind kantonal geregelt. Mit anderen Worten: Es gibt keine für die ganze Schweiz gültigen Aufbewahrungsfristen. In den meisten Kantonen besteht eine 10-jährige Aufbewahrungsfrist für medizinische Daten. Für bestimme Dokumentationen im Laborbereich, für Blut und Blutprodukte, im Bereich von Transplantationen und medizinischen Strahlenquellen besteht eine 20-jährige Aufbewahrungspflicht.

6.9 Welche Daten müssen wir aufbewahren?

Der Umfang der aufzubewahrenden Akten wird allgemein formuliert: Es geht um die Führung der Krankengeschichte. Enthalten sind Befunde, Diagnosen, der Nachvollzug der Behandlungsgeschichte, aber auch wie ein_e Patient_in über mögliche Risiken und Nebenwirkungen aufgeklärt wurde.

EQUAM STIFTUNG

7. Wie sorgen wir für Datensicherheit auf unseren Praxiscomputern?

7.1 Wie gehen wir mit Software und Up-dates um?

Heute ist jeder Rechner direkt oder indirekt mit dem Internet verbunden. Entsprechend ist auf einen optimalen Schutz vor allfälligen Angriffen zu achten. Das bedeutet insbesondere, dass nur Software eingesetzt werden darf, die vom Hersteller noch gepflegt und mit Updates versorgt wird. Sicherheitsupdates sollten unverzüglich eingespielt werden. Nicht mehr benötigte Software sollte nicht mehr verwendet und auch deinstalliert werden.

7.2 Welche Gefahren gehen von Websiten aus?

Mitarbeitende sollten von Praxisrechnern aus nur eine kleine, kontrollierte Zahl von Webseiten besuchen. Immer wieder werden Rechner von Werbebannern aus infiziert. Aus diesem Grund empfehlen wir einen Ad-Blocker im Browser.

Software sollte nur von zuverlässiger Quelle installiert werden. Eine Quelle ist nicht deshalb zuverlässig, weil sie an einen bekannten Namen erinnert oder grafisch sorgfältig aufgemacht ist. Am besten fragen Sie einen IT-Experten im Einzelfall um Rat. Software, die darum bittet, den Virenschutz während der Deinstallation auszuschalten, birgt ein besonderes Risiko.

Eine einfache Massnahme mit hohem Sicherheitsgewinn ist die Trennung von privaten und beruflichen Aktivitäten. Dies gilt ganz besonders in der Arztpraxis. Wir empfehlen deshalb, die private Nutzung von Praxisrechnern mit Zugang zu Patientendaten zu verbieten.

7.3 Wie schnell veraltet ein Virenschutzprogramm?

Ein Virenschutzprodukt besteht meist über viele Jahre. Eine installierte Version eines Antivirenprogramms hat eine Lebensdauer von mehreren Monaten → 7.1 und sollte regelmässig aktualisiert werden, am besten automatisch. Neue Viren werden mehrmals am Tag entdeckt. Die Virendatenbank sollte daher mehrmals pro Tag aktualisiert werden. Dies geschieht meist automatisch.

7.4 Ist ein Antivirusprogramm zwingend?

Antivirensoftware muss heute nicht mehr als das zwingende Allheilmittel angesehen werden, welches sie früher einmal war. Sie schützt nur gegen einen Teil der Bedrohungen. Sie kann als Ergänzung zu den obigen Massnahmen → 7.1 / → 7.2 eingesetzt werden, kann diese aber nicht ersetzen.

7.5 Wie können wir verhindern, dass eine Mitarbeiterin, ein Mitarbeiter einem «Phishing»-Versuch aufsitzt?

Grundsätzlich sollte man Mailanhänge nur öffnen, wenn man den Absender kennt und den Anhang erwartet. Folgen Sie auf keinen Fall einem Link, bei dem Sie Kontoangaben oder Passworte bekannt geben müssen. Es sollte allen Mitarbeitenden bewusst sein, dass Mailabsender (Person und Organisation) sehr einfach gefälscht werden können.
Folgende Checkliste kann helfen:

- Kommt die Mail unerwartet?
- Ist der Inhalt unerwartet oder unüblich?
- Versucht mir das Gegenüber ein Angebot zu machen, das zu gut ist, um wahr zu sein?
- Versucht mich das Gegenüber unter Druck zu setzen («ganz dringend» …)?
- Stimmt die Sprache und Rechtschreibung mit dem überein, was ich von der Person erwarte?
- Bei Zweifeln:
  - Holen Sie eine Zweitmeinung ein.
  - Versuchen Sie den Absender per Telefon oder persönlich zu kontaktieren. Verwenden Sie dazu keine Informationen aus der Mail, denn auch diese könnten gefälscht sein.

7.6 Reicht eine Firewall?

Eine Firewall schützt Rechner und andere Geräte mit Netzzugang, einzelne Anwendungen oder Systemdienste vor eingehenden Internetverbindungen. Falls das Gerät oder die Software aber Internetzugang nach Aussen hat (Mailprogramm, Browser etc.), schützt eine Firewall nicht vor einer schlechten Konfiguration (z.B. schlechter oder fehlender Passwortschutz) oder Fehlern, durch welche die Software von aussen steuerbar wird. Die Firewall am Internetzugang schützt auch nicht vor einem anderen Gerät im internen Netz, das mit fehlerhafter oder bösartiger Software ausgestattet ist.

Es gilt also immer, zuerst die Software und Hardware selbst zu schützen. Als zusätzliches Hindernis kann dann darüber hinaus noch eine Firewall eingesetzt werden. Eine Firewall kann eine Komponente eines Sicherheitskonzepts darstellen. Alle Schutzmassnahmen, auch die Firewall, sind ohne richtige Konfiguration und Handhabung grösstenteils wirkungslos.

EQUAM STIFTUNG

8. Wie sorgen wir für Datensicherheit auf portablen Datenträgern?

8.1 Wie gehen wir mit externen Festplatten und USB-Sticks um?

Diese sollten immer verschlüsselt sein. Falls die Praxiscomputer Festplattenverschlüsselung unterstützen, sollten Sie diese nutzen. Ansonsten gibt es Programme, die Dateien oder Archive verschlüsseln, bzw. auf dem Laufwerk einen verschlüsselten Laufwerkscontainer anlegen.

8.2 Wie gehen wir mit unbekannten USB-Geräten um?

Herrenlose USB-Geräte sollten nicht mit Praxisrechnern verbunden werden. Sie können bereits beim Einstecken bösartige Software ausführen oder Eingaben simulieren. Es gibt USB-Sticks auf dem Markt, die beim Einstecken einen Hochspannungsstoss in den Rechner jagen und ihn damit zerstören können. Den Gerätetyp und dessen Fähigkeiten können Sie nicht von aussen erkennen: Eine bösartige Maus kann sich auch als CD-Laufwerk mit eingelegter CD oder als Tastatur ausgeben.

8.3 Ist zu unterscheiden zwischen verschiedenen Smartphone-Marken? Gibt es «sicherere»?

Grundsätzlich kann alleine vom Hersteller nicht auf die Qualität eines Einzelprodukts geschlossen werden. Neuere Geräte, insbesondere ausserhalb des Billigsegments, bieten aber häufig bessere Sicherheitstechnologien an, wie Datenverschlüsselung, Fingerabdrucksensor oder Fernlöschung. Ein Gerät mit wenig vorinstallierter zusätzlicher Software ist zu empfehlen. Diese kann nämlich Sicherheitslücken aufweisen und kann häufig nicht richtig deinstalliert werden.

Bei der Wahl eines Herstellers sollte man auf eine gute Up-date-Politik bei Sicherheitsproblemen achten. Dies ist wahrscheinlicher, je beliebter und neuer das Smartphone ist und je weniger Änderungen die installierte Software gegenüber der Version des Betriebssystemherstellers aufweist. Das Smartphone sollte nach kurzer Zeit der Nichtbenutzung automatisch sperren. Biometrische Kontrollen vereinfachen den Zugang.

8.4 Wie ist es mit Laptops und Tablets? Gibt es da einen Unterschied bezüglich Datensicherheit?

Im Allgemeinen gilt Ähnliches wie bei den Smartphones → 8.3 Zu bevorzugen sind bekannte Hersteller, die ihre Geräte möglichst ohne unnötige Zusatzsoftware ausliefern und sicherheitsrelevante Softwarefehler rasch mit Updates korrigieren.

8.5 Was machen wir mit Voice-over-IP (VoIP)-Telefonen?

VoIP-Telefone bieten eine Vielzahl von Komfortfunktionen. Solange Sie keine interne VoIP-Zentrale betreiben, sind diese Telefone aber jederzeit aus dem Internet erreichbar, auch bei aktivierter Firewall. Die Telefone sind vollwertige Computer. Deshalb ist es auch besonders wichtig, sie regelmässig mit Sicherheitsupdates zu versorgen. Die Überlegungen aus **8.3** und **8.4** gelten analog.

8.6 Gibt es dazu Schulungsunterlagen?

8-Sekunden-Video zu USB-Hygiene: https://youtu.be/dJ0HTaXME_0

9. Wie handhaben wir Daten-Back-ups?

9.1 Wozu dienen Back-ups?

Back-ups bieten eine «Undo»-Funktion im grossen Massstab. Sie sollen den Betrieb der Praxis weiter ermöglichen, wenn ganze Speichermedien kaputtgehen oder durch Softwarefehler bzw. Fehlbedienung einzelne Dateien, ganze Verzeichnisse oder Datenbanken (unabsichtlich oder absichtlich, z.B. durch Erpressungssoftware, sogenannte Ransomware) gelöscht oder verfälscht werden. Solche Fehler können über Wochen oder Monate unentdeckt bleiben. Entsprechend müssen alte Dateien auch über längere Zeitspannen hinweg wiederhergestellt werden können.

Für Praxen, die keinen eigenen Server betreiben, liegt die Verantwortung für das Back-up beim Serviceanbieter. Sie sollten sich über die Sicherheits- und Back-up-Vorkehrungen des Anbieters informieren.

9.2 Wie häufig sollen Back-ups angelegt werden?

Es ist gängige Praxis, tägliche Back-ups über eine Woche bis zu einem Monat aufzubewahren und zusätzlich wöchentliche oder monatliche Back-ups über mehrere Monate hinweg. So können Sie auch Fehler beheben, die längere Zeit unerkannt blieben.

Insbesondere bei grösseren Praxen ist zusätzlich ein stündliches Back-up zu empfehlen. Dies hilft insbesondere, die Rekonstruktionszeit nach einem Angriff durch Ransomware → **9.1** und sonstiger Malware (bösartige Software) zu minimieren, welche viele Dateien absichtlich innert kurzer Zeit löschen oder zerstören.

9.3 Welche Back-up-Medien gibt es?

Klassisch wurden für Back-ups Bänder genutzt, da sie auf wenig Platz und günstig relativ grosse Datenmengen speichern konnten. Heute sind aber USB-Festplatten so klein und günstig, dass sich der höhere Aufwand für Bandlaufwerke bei KMUs nur selten lohnt.

Für Back-ups, die mehrere Jahre gelagert werden sollen, bieten sich optische Medien an. Je nach Grösse der zu sichernden Daten können das CDs, DVDs oder Blu-Ray-Disks sein. Damit sie 5 bis 10 oder mehr Jahre halten, sollten sie fachgerecht gelagert werden, d.h. bei gleichmässiger, eher kühler Temperatur, trocken, dunkel und staubfrei. Je nach Medium sind zusätzliche Lagerungsbedingungen zu beachten.

9.4 Band oder Disk?

Disk ist heute häufig komfortabler und flexibler. Insbesondere für kleinere und mittlere Praxen dürfte die Disk das Medium der Wahl sein. Im Gegensatz zu Bändern sind keine speziellen, teuren Laufwerke und spezifische Software notwendig. Die Lebensdauer von Disks ist heute sehr gut und ein Back-up auf Disk wird von allen gängigen Betriebssystemen direkt unterstützt. Die Möglichkeit, mehrere unabhängige, günstige USB-Festplatten in Intervallen als Back-up-Medium zu nutzen, erhöht die Datensicherheit zusätzlich.

9.5 Dürfen wir Back-up-Bänder oder -Disks in der Praxis in einem Safe legen?

Die sichere Aufbewahrung soll gegen Diebstahl und Zerstörung (Absicht oder Naturgewalten) schützen. Ein entsprechend ausgelegter und gesicherter Tresor ist eine Möglichkeit. Eine Andere ist das sogenannte Off-Site-Back-up: Sie bewahren das Medium wird an einem anderen Ort auf, an dem dasselbe Schadensereignis nicht zeitgleich auftritt.

9.6 Ist es OK, wenn jeweils eine MPA oder eine Ärztin / ein Arzt die Back-up-Bänder oder -Disks nach Hause nimmt?

Das ist häufig die praktischste Möglichkeit für ein Off-Site-Back-up. → 9.5 Es ist allerdings darauf zu achten, dass Back-ups in privaten Räumen nicht in die Hände Dritter gelangen können. Auch stellt sich die Frage, wie nah die privaten Räume zur Praxis sind. Back-ups im selben Haus zu lagern, empfiehlt sich definitiv nicht: Wenn das Haus brennt, brennen Praxis und Privaträume.

Am besten legen Sie die Back-ups daheim ebenfalls in einen Safe. Falls dies nicht möglich ist, schützt eine Verschlüsselung der Disk bzw. des Back-ups die Daten zumindest gegen unbefugten Zugriff, wenn auch nicht vor Diebstahl, Feuer, Wasser oder Zusammenbruch des Hauses. Das Passwort für die Verschlüsselung sollte sicher sein → 5.4 und geschützt vor Zerstörung, Diebstahl oder unbefugtem Zugriff an einem unabhängigen Ort aufbewahrt werden. Ohne dieses Passwort sind die Back-ups unbrauchbar.

9.7 Nützen Sicherungskopien auf dem Server etwas?

Sie sind eine günstige und komfortable zusätzliche Methode, um bei einem kleinen Fehler rasch wieder auf einzelne Dateien zugreifen zu können. Sie können jedoch ein Back-up auf einen anderen Datenträger an einem anderen Ort nie ersetzen, da sie nicht vor Betriebssystem- oder Hardwarefehlern bzw. Diebstahl oder Elementarschäden schützen können.

9.8 Welche Daten-Back-ups werden empfohlen?

Sorgen Sie dafür, dass zumindest folgende Daten gesichert werden:

— Dokumente (Textverarbeitung, Tabellenkalkulation etc.)
— Emails
— Kontaktinformationen
— Datenbanken von Praxisanwendungen
— Konfigurationen und Passwörter von Anwendungen und Systemkonfigurationen
— Anwendungen und Betriebssystem, sofern sie nicht einfach durch Neuinstallation (z.B. ab separat gelagerter CD) wiederhergestellt werden können. Lizenzschlüssel für die Neuinstallation sollten in Papierform gelagert werden, da sie häufig von elektronischen Back-ups nicht berücksichtigt werden.

In vielen Fällen ist eine regelmässige Komplettsicherung („Image Back-up“) des Servers die einfachste Lösung. Insbesondere bei der Sicherung von Datenbanken aber auch von Mailcontainern muss darauf geachtet werden, dass diese Daten auch korrekt gesichert werden, während die Anwendung läuft. Beachten Sie dazu das Handbuch der Software oder lassen Sie sich von einem Experten beraten.

Je nach eingesetzter Soft- und Hardware fallen noch zusätzliche Daten auf weiteren Rechnern an, die ebenfalls gesichert werden sollten, wenn auch möglicherweise weniger häufig.

9.9 Wie stellen wir sicher, dass die Daten tatsächlich vom Back-up wieder zurück geladen werden können?

Sie sollten regelmässig Tests durchführen, ob die Daten auf dem Back-up auch lesbar sind und wiederhergestellt werden können (Restore). Dies sollte nach der Systemerstinstallation und nach grösseren Konfigurationsänderungen häufiger geschehen. Danach reicht, je nach Schutzbedarf, 1–2 Mal pro Jahr.

Am einfachsten können Sie dies bei den Dokumenten überprüfen: Wählen Sie dazu aus verschiedenen Verzeichnissen auf dem Server einige alte und neue Dateien zufällig aus, suchen Sie sie im Back-up an verschiedenen Daten, kopieren Sie sie in ein neues Verzeichnis und prüfen Sie sie auf Vollständigkeit. Bei den restlichen Daten ist die Überprüfung aufwändiger. Am Einfachsten geht es, wenn die Software selbst Überprüfungsmöglichkeiten bietet, was aber leider nur selten der Fall ist. Ansonsten sind allgemeingültige Rezepte sehr schwierig und Sie sollten sich den Rat eines Experten einholen.

10. Wie handhaben wir das Löschen von Daten?

10.1 Genügt es, wenn wir die Daten auf unserem Computer löschen?

Um Daten wirklich zu löschen, genügt es nicht, eine Datei zu löschen und den Papierkorb zu entleeren. Sie müssen zusätzlich mit anderen Daten überschrieben werden, damit sie vollständig verschwinden. Dafür sollten spezielle Datenlöschfunktionen oder -programme eingesetzt werden.

10.2 Können wir Daten in der Cloud löschen?

Die Daten bleiben im Normalfall, wie auch auf einem Computer → 10.1, bis zum nächsten Überschreiben durch das System bestehen. Darauf haben Sie als Nutzer meist keinen Einfluss. In der Cloud sind auch häufig noch zusätzliche Sicherungskopien und Back-ups vorhanden, die Sie nicht direkt beeinflussen können. Die sicherste Lösung ist es deshalb, nur verschlüsselte Daten in der Cloud abzulegen.

10.3 Wie entsorgen wir einen alten Computer?

Gelöschte Daten lassen sich sehr einfach rekonstruieren. Es gibt Verbrecher, die sich darauf spezialisiert haben, Second-Hand-Festplatten zusammenzutragen und die darauf enthaltenen Informationen und Passwörter zu missbrauchen. Alle Datenträger sollten vollständig überschrieben werden. Dies geschieht bei Festplatten mit einem speziellen Festplattenlöschprogramm oder einer Funktion wie «Formatieren mit vollständigem Überschreiben» des jeweiligen Betriebssystems.

Bei SSDs (Solid State Disks) sollte diese Funktion zwei Mal angewandt werden, um wirklich alle Daten zu überschreiben. Falls alle Daten auf der Festplatte oder SSD verschlüsselt sind, ist dieser vollständige Löschvorgang nicht nötig, aber trotzdem sicherheitshalber zu empfehlen.

10.4 Wie entsorgen wir ein Mobilgerät?

Die meisten Mobilgeräte bieten eine Funktion «Zurücksetzen auf Werkseinstellungen», die alles Notwendige erledigt.

10.5 Unser Gerät ist kaputt, wir können die Daten nicht mehr löschen. Was nun?

Auf keinen Fall einfach wegwerfen oder in den Elektroschrott geben. Falls sensible Daten darauf gespeichert sind. Experten können diese nämlich häufig doch in kurzer Zeit extrahieren!

Es gibt aber spezialisierte Entsorgungsfirmen, die sicherstellen, dass die Daten nicht missbraucht werden können. Die Techniken reichen vom Einsatz extrem starker Magnetfelder (schnell und effektiv bei Harddisk oder Band) bis zum Schreddern des Geräts.

EQUAM STIFTUNG

Anwendbarkeit der europäischen Datenschutzverordnung

Wie sieht es mit der Anwendbarkeit der europäischen Datenschutzgrundverordnung (DSGVO bzw. GDPR) aus?

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 eines Verantwortlichen oder eines Auftragsverarbeiters 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 niedergelassenen Verantwortlichen oder Auftragsverarbeiter, 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 einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Wann ist die DSGVO anwendbar, wenn ich Mitarbeitende aus der EU habe?

Grundsätzlich gilt das Marktortprinzip. Arbeiten EU-Bürger in der Schweiz – egal ob in die Schweiz umgezogen oder als Grenzgänger – gilt die schweizerische Gesetzgebung auch bezüglich Datenschutz und nicht die DSGVO.

Wie ist es, wenn wir Patienten aus der EU behandeln?

Auch hier gilt grundsätzlich das Marktortprinzip. Verletzt sich ein europäischer Tourist in den Ferien und kommt in die örtliche Arztpraxis, ist die DSGVO nicht anwendbar. Anders sieht es aus, wenn aktiv in der EU Patientinnen und Patienten als Kunden angeworben würden. Dann ist die Datenschutzgrundverordnung (DSVGO) anwendbar. Entscheidend ist, dass aktiv eine Dienstleistung in der EU angeboten wird. Als Indizien hierfür gelten Währung, Wegbeschreibung vom Ausland oder Sonderangebote für bestimmte europäische Zielgruppen.
Ist die DSGVO anwendbar, hat man verschiedene weitere Vorschriften zu beachten. So muss eine Vertretung in der EU definiert sein, die dort als Anlaufstelle fungiert und bei sämtlichen Fragen in der EU angegangen werden kann. Weiter braucht es einen betrieblichen Datenschutzbeauftragten. Dieser muss über eine entsprechende berufliche Qualifikation und Fachwissen im Gebiet Datenschutzrecht und Datenschutzpraxis verfügen.

EQUAM STIFTUNG

Abkürzungen

Abkürzung	Begriff
ATSG	Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts
BAG	Bundesamt für Gesundheit
DSG	Bundesgesetz über den Datenschutz
MPA	medizinische Praxisassistentin
StGB	Strafgesetzbuch
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VoIP	Voice-over-IP

Ausgewählte Gesetzesgrundlagen

— Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Stand am 1. Januar 2014) SR 235.1
https://www.admin.ch/opc/de/classifiedcompilation/19920153/

— Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993
https://www.admin.ch/opc/de/classifiedcompilation/19930159/
(Stand am 1. Dezember 2010) SR 235.11

Artikel und weitere Publikationen

— EDÖB: Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich, Bern 2002, unter:
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/bearbeitung-von-personendaten-im-medizinischen-bereich.html (zuletzt eingesehen am 31.10.2018)

— EDÖB: Krankengeschichte und Auskunftsrecht, unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/krankengeschichte-und-auskunftsrecht.html (zuletzt eingesehen am 31.10.2018)

— Fellmann, Walter: «Arzt und das Rechtsverhältnis zum Patienten», in: Kuhn, Moritz W. & Poledna, Tomas, Arztrecht in der Praxis, Zürich, Basel, Genf: Schulthess Juristische Medien 2007, S. 103–232

— Ramer, Paul: «Datenschutz und Arztpraxis», in: Hürlimann, Barbara et al. (Hg.), Datenschutz im Gesundheitswesen, Zürich: Schulthess Juristische Medien 2001, S. 21–48

— Uttinger, Ursula: «§ 10 Datenschutz im Gesundheitswesen », in: Passadelis, Nicolas et al. (Hg.), Handbücher für die Anwaltspraxis. Datenschutzrecht, Basel: Helbing Lichtenhahn Verlag, 2014, S. 323–354

— SAMW & FMH: Rechtliche Grundlagen im medizinischen Alltag. Ein Leitfaden für die Praxis. Basel, 2013