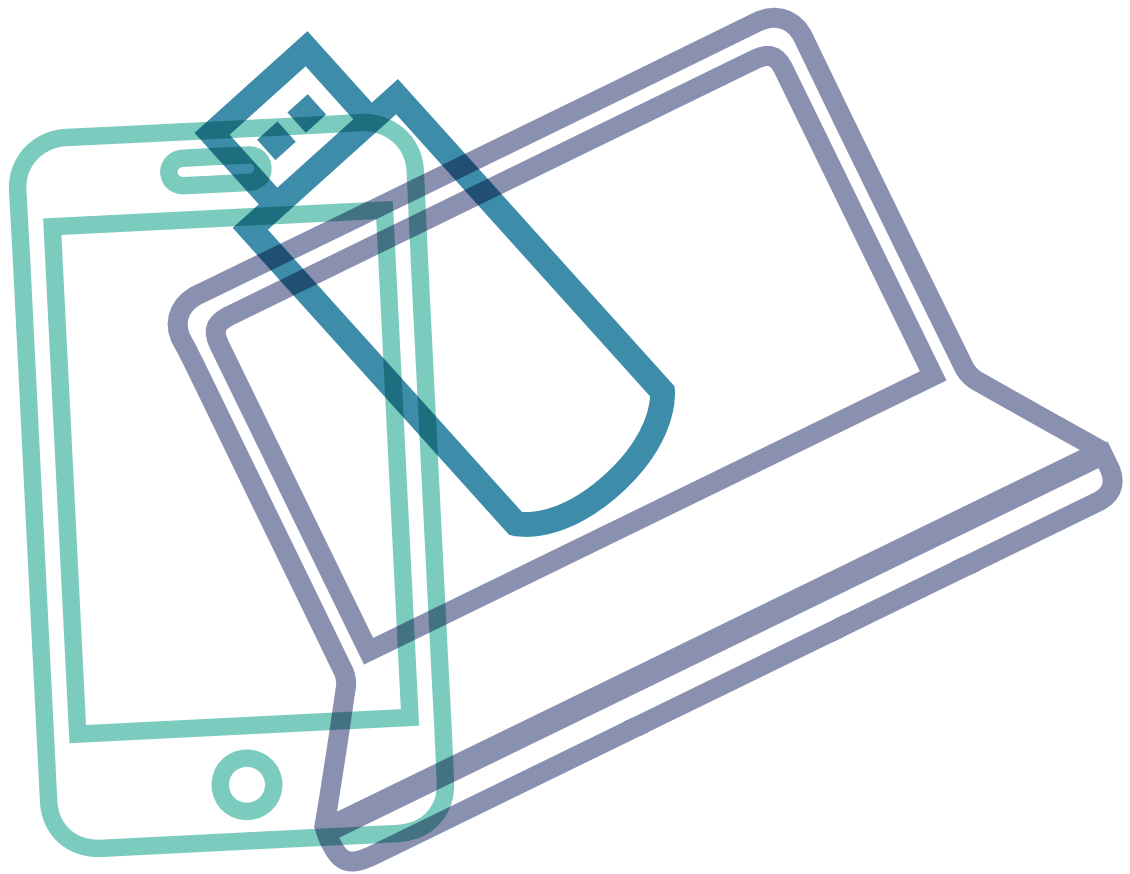


FAQ

DATENSCHUTZ UND INFORMATIONSTECHNOLOGIE IN DER ARZTPRAXIS

Ursula Uttinger
Marcel Waldvogel



1 WELCHE DATEN SOLLEN WIR BEI PATIENTENEINTRITT ERHEBEN?

1.1.	Welche Mindestdaten dürfen wir erfragen? Administrativ	6
1.2.	Welche Mindestdaten dürfen wir erfragen? Medizinisch	6
1.3.	Was sollten wir mindestens in die Akten aufnehmen?	6
1.4.	Welche Fragen sollten wir nicht stellen?	6
1.5.	Dürfen wir fragen, warum der Patient zu uns kommt bzw. die Arztpraxis wechselt?	6
1.6.	Dürfen wir Daten von Familienangehörigen verlangen?	6
1.7.	Dürfen wir Fragen zu Einkommen, Vermögen, Sozialhilfe stellen?	6–7
1.8.	Was, wenn der Patient falsche Angaben liefert?	7
1.9.	Was, wenn der Patient sich weigert, alle Fragen zu beantworten?	7
1.10.	Was sollen wir beim Empfang von Patienten beachten?	7

2 WIE HANDHABEN WIR DAS RECHT DER PATIENTEN AUF DIE HERAUSGABE IHRER DATEN?

2.1.	Was bedeutet das Recht auf Herausgabe der Daten?	8
2.2.	Müssen wir sämtliche Daten herausgeben?	8
2.3.	Müssen wir die Daten immer dem Patienten direkt herausgeben?	9
2.4.	Dürfen wir unterscheiden zwischen elektronischen Daten und Daten in Papierform?	9
2.5.	In welcher Form müssen wir die Daten herausgeben?	9
2.6.	Kann ein Patient eine Berichtigung von Daten verlangen?	9
2.7.	Wem gehören die Unterlagen? Der Ärztin oder dem Patienten?	9

3 WIE HANDHABEN WIR DIE WEITERGABE VON DATEN AN DRITTE?

3.1.	Müssen wir unterscheiden, wem wir Daten weitergeben?	9–10
3.2.	Was passiert, wenn wir Daten ohne Entbindung des Arztgeheimnisses weitergeben?	10
3.3.	Dürfen wir die Daten einem vor- beziehungsweise nachbehandelnden Arzt immer weitergeben?	10
3.4.	Ist ein Outsourcing eine Weitergabe an Dritte?	10
3.5.	Dürfen wir Daten durch einen Dritten bearbeiten lassen?	10–11
3.6.	Wie gehen wir mit Anfragen der Polizei und weiteren Behörden um?	11
3.7.	Gibt es Fälle von Anzeigepflicht?	11
3.8.	Wie steht es bei der medizinischen Forschung?	11
3.9.	Was ist mit Daten für die Qualitätskontrolle?	11

4 WIE GESTALTEN WIR DIGITALEN DATENAUSTAUSCH MÖGLICHTST SICHER?

4.1.	Welche Optionen zur Mailverschlüsselung gibt es?	12
4.2.	Ist eine Verschlüsselung von Mails immer zwingend?	12
4.3.	Was nützt ein Disclaimer am Ende der Mail?	12
4.4.	Ist das Versenden von Daten per Fax sicher?	12
4.5.	Was ist die Cloud?	12–13
4.6.	Ist das Nutzen einer Cloud auch ein digitaler Datenaustausch im weitesten Sinne?	13
4.7.	Wie gehen wir mit Fernwartung um?	13

5 WIE ORGANISIEREN WIR DEN ZUGANG ZU DATEN INNERHALB DER PRAXIS?

5.1.	Genügt es, wenn der Bildschirmschoner automatisch nach 10 Minuten einschaltet?	13–14
5.2.	Ist es sinnvoll, Passworte pro User vorzugeben?	14
5.3.	Genügt ein Passwort pro Arbeitsplatz?	14
5.4.	Was macht ein sicheres Passwort aus?	14
5.5.	Wie erzeuge ich ein sicheres Passwort?	14
5.6.	Müssen wir das Passwort alle drei Monate wechseln?	14–15
5.7.	Wie merke ich mir die unzähligen kryptischen Passwörter?	15
5.8.	Geht das nicht einfacher?	15
5.9.	Wir verlangen, dass jeder MA sein Passwort in einem verschlossenen Couvert hinterlegt. Ist das sinnvoll?	15
5.10.	Gibt es dazu weitere Informationen?	15

6 WIE STELLEN WIR RÜCKVERFOLGBARKEIT BEI DER BEARBEITUNG DIGITALER DATEN SICHER?

6.1.	Was ist Rückverfolgbarkeit?	15
6.2.	Wann benötigen wir Rückverfolgbarkeit?	15
6.3.	Wie stellen wir sie bei Dokumenten sicher?	16
6.4.	Wie stellen wir sie innerhalb der Praxisanwendungen sicher?	16
6.5.	Wie stellen wir sie bei Bestellungen via Webformular sicher?	16
6.6.	Wie stellen wir sie bei eingehenden Aufträgen via Email sicher?	16
6.7.	Wie stellen wir sie bei ausgehenden Emails sicher?	16
6.8.	Welche Aufbewahrungsfristen müssen wir einhalten?	16
6.9.	Welche Daten müssen wir aufbewahren?	16

7 WIE SORGEN WIR FÜR DATENSICHERHEIT AUF UNSEREN PRAXISCOMPUTERN?

7.1.	Wie gehen wir mit Software und Updates um?	17
7.2.	Welche Gefahren gehen von Webseiten aus?	17
7.3.	Wie schnell veraltet ein Virenschutz-Programm?	17
7.4.	Ist ein Antivirusprogramm zwingend?	17
7.5.	Wie können wir verhindern, dass ein MA einem «Phishing-Versuch» aufsitzt?	17
7.6.	Reicht eine Firewall?	18

8 WIE SORGEN WIR FÜR DATENSICHERHEIT AUF PORTABLEN DATENTRÄGERN?

8.1.	Wie gehen wir mit externen Festplatten und USB-Sticks um?	18
8.2.	Wie gehen wir mit unbekanntem USB-Geräten um?	18
8.3.	Ist zu unterscheiden zwischen verschiedenen Smartphone-Marken? Gibt es «sicherere»?	18
8.4.	Wie ist es mit Laptops und Tablets? Gibt es da einen Unterschied bezüglich Datensicherheit?	18
8.5.	Was machen wir mit VoIP-Telefonen?	18
8.6.	Gibt es dazu Schulungsunterlagen?	19

9 WIE HANDHABEN WIR DATENBACKUPS?

9.1.	Wozu dienen Backups?	19
9.2.	Wie häufig sollen Backups angelegt werden?	19
9.3.	Welche Backupmedium gibt es?	19
9.4.	Band oder Disk?	19
9.5.	Dürfen wir Backupbänder oder -disks in der Praxis in einen Safe legen?	19
9.6.	Ist es OK, wenn jeweils eine MPA oder Ärztin die Backupbänder oder -disks nach Hause nimmt?	19–20
9.7.	Nützen Sicherungskopien auf dem Server etwas?	20
9.8.	Welche Datenbackups werden empfohlen?	20
9.9.	Wie stellen wir sicher, dass die Daten tatsächlich vom Backup wieder zurück geladen werden können?	20

10 WIE HANDHABEN WIR DAS LÖSCHEN VON DATEN?

10.1.	Genügt es, wenn wir die Daten auf unserem Computer löschen?	20
10.2.	Können wir Daten in der Cloud löschen?	21
10.3.	Wie entsorgen wir einen alten Computer?	21
10.4.	Wie entsorgen wir ein Mobilgerät?	21
10.5.	Unser Gerät ist kaputt, wir können die Daten nicht mehr löschen. Was nun?	21

ABKÜRZUNGEN UND LITERATUR

22

Der Nachdruck und die Vervielfältigung des vorliegenden Textes sowie die ganze oder teilweise Verwertung von Grafiken oder Textauschnitten sind für interne Zwecke erlaubt. Es besteht jedoch die Verpflichtung, auf die Urheberschaft durch die EQUAM Stiftung hinzuweisen. Die externe Veröffentlichung bzw. Weitergabe an Dritte ist nicht gestattet bzw. bedarf einer ausdrücklichen schriftlichen Genehmigung durch die EQUAM Stiftung. Die ganze oder teilweise Verwertung von Grafiken oder Textauschnitten durch unberechtigte Dritte ist untersagt.

Uttinger U. & Waldvogel M.: FAQ Datenschutz und Informationstechnologie in der Arztpraxis, EQUAM Stiftung, Bern, 2017

VORWORT

SEHR GEEHRTE LESERIN, SEHR GEEHRTER LESER

Für Ärztinnen, Ärzte, MPA, Praxismanager und -managerinnen 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 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 Marianne Jossen, verantwortlich für Forschung und Entwicklung bei der EQUAM Stiftung, sowie 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 – ohne Sie hätten wir dieses FAQ so nicht realisieren können.

Wenn Sie Ihr Team für die Fragen des FAQ gezielt sensibilisieren möchten, dann informieren Sie sich auf der Homepage der EQUAM Stiftung (www.equam.ch) über das Qualitätsprogramm Datenschutz und Informationstechnologie. Die 10 Fragen des FAQ werden darin im Team zunächst in einem Online-Impulsfragebogen bearbeitet. Dabei visualisieren Sie Ihre Datenströme und tauschen sich über Datenbearbeitung in der Praxis aus. Der daran anschliessende Schulungsworkshop bringt mehrere Praxen zusammen. In einem ersten Teil werden die Teams zu den wichtigsten Begriffen und Fragen des Datenschutzes in der Arztpraxis geschult. Ein zweiter Teil ist dem Austausch unter den Teams gewidmet mit dem Ziel, Beispiele lokaler Umsetzung zu diskutieren und von den Anderen zu lernen.

Wir wünschen gute Lektüre!

PS: Im gesamten FAQ verwenden wir – wie schon bei diesem Vorwort – manchmal die weibliche, manchmal die männliche Form. Selbstverständlich sind alle Geschlechter jeweils mitgemeint.

Für alle weiteren Informationen zum Sensibilisierungsprogramm Datenschutz und IT nehmen Sie mit uns Kontakt auf:

EQUAM Stiftung
+41 61 271 01 11
office@equam.ch
www.equam.ch