Datenschutz und IT in der Arztpraxis: ein Fass mit Boden

Marianne Jossen[a], Ursula Uttinger[b], Marcel Waldvogel[c]

[a] M.A., MPh, Verantwortliche Forschung & Entwicklung, EQUAM Stiftung (bis März 2018); [b] lic. iur. / exec. MBA HSG, Präsidentin Datenschutzforum Schweiz; [c] Dr. sc. ETH Zürich, Informatikprofessor Universität Konstanz

Für Ärztinnen, Ärzte, MPA, Praxismanagerinnen und Praxismanager ist der sorgfältige Umgang mit den ihnen anvertrauten Patientendaten ein wichtiges Element ihres Alltags. Doch was genau muss eine Praxis dabei berücksichtigen?

Der eHealth-Barometer 2016 [1] zeigt: Immer mehr Praxisärztinnen und -ärzte interessieren sich für eHealth, allerdings sehen nur 40% von ihnen darin ein Verbesserungspotential für ihr Arbeitsumfeld. Dieses Resultat könnte unter anderem im Zusammenhang mit einer skeptischen Haltung zum Datenschutz stehen.

So gehen Ärztinnen und Ärzte davon aus, dass der Datenschutz bei elektronischer Datenablage weniger gut gewährleistet ist als bei der traditionellen Krankengeschichtenführung auf Papier. Auch die EQUAM Stiftung stellt im Kontakt mit Ärztinnen, Ärzten und MPA fest: Die Digitalisierung verunsichert. Manch einen und eine beschleicht das Gefühl, der Datenschutz sei ein Fass ohne Boden. Eine Frage zieht die nächste nach sich, Rechtsquellen sind nicht einfach zu interpretieren, und bei der IT bleibt der Blick zwangsweise auf der Oberfläche haften. Zwischen 2015 und 2017 hat die EQUAM Stiftung Ärztinnen, Ärzte, MPA, Expertinnen und Experten eingeladen, diesem Fass einen Boden zu geben. Entstanden sind daraus zehn Fragen, mit denen sich jede Arztpraxis auseinandersetzen sollte:

1. Welche Daten erheben wir beim Patienteneintritt?
2. Wie handhaben wir das Recht der Patientinnen und Patienten auf die Herausgabe ihrer Daten?
3. Wie handhaben wir die Weitergabe von Daten an Dritte?
4. Wie gestalten wir digitalen Datenaustausch möglichst sicher?
5. Wie organisieren wir den Zugang zu Daten innerhalb der Praxis?
6. Wie stellen wir Rückverfolgbarkeit bei der Bearbeitung von Daten sicher?
7. Wie sorgen wir für Datensicherheit auf unseren Praxiscomputern?
8. Wie sorgen wir für Datensicherheit auf portablen Datenträgern?
9. Wie handhaben wir Daten-Backups?
10. Wie handhaben wir das Löschen von Daten?

Résumé

Pour les médecins, MPA, directrices et directeurs de cabinet, la gestion minutieuse des données des patients qui leur sont confiées est un élément important du quotidien professionnel. Mais comment gérer ces données conformément aux dispositions légales? La Fondation EQUAM a élaboré, ensemble avec des médecins, assistant_es médicales et médicaux et des expert_es dix questions qui permettent de discuter de manière structurée cette thématique complexe, tenant compte des aspects juridiques aussi bien que techniques.

Drei Grundsätze

Aus datenschutzrechtlicher Sicht sind drei wichtige Grundsätze im Zusammenhang mit den oben aufgeführten Fragen die «Verhältnismässigkeit», «Transparenz» und «Datensicherheit».

Verhältnismässigkeit

Der Grundsatz der «Verhältnismässigkeit» findet sich in Art. 4 Abs. 2 DSG [2]: «Ihre Bearbeitung [der Personendaten] hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.» Gerade im Zusammenhang mit der Frage «Welche Daten sollen wir bei Patienteneintritt erheben?» muss die Verhältnismässigkeit immer wieder geprüft werden. In der Praxis bedeutet dies, dass nicht einfach möglichst viele Daten erhoben werden dürfen. Vielmehr muss bei jeder Information, die man erfragen möchte, geprüft werden, ob man diese wirklich braucht. Gibt es auf die Frage «Warum?» eine schlüssige Antwort, die auch für eine unbeteiligte Person nachvollziehbar ist, dürfte die Erhebung dieser Information berechtigt sein. Beispielsweise ist die Frage, warum ein Patient die Arztpraxis wechselt, interessant, aber es muss dem Patienten überlassen blei-

EQUAM Stiftung

Aus dem Projekt zur Qualitätsarbeit in Hausarztpraxen mit Fokus auf Managed Care entstand im April 1999 die unabhängige EQUAM Stiftung zur Förderung der Qualität und Patientensicherheit in der ambulanten Medizin.
Mit den Qualitätsprogrammen begleitet die EQUAM Stiftung Gesundheitsprofis, misst und zertifiziert die Qualität, sensibilisiert zu aktuellen Themen und informiert sachgerecht. Die Qualitätsprogramme beschäftigen sich sowohl mit Struktur- als auch mit Prozess- und Ergebnisqualität. Die EQUAM-unabhängige Ombudsstelle schlichtet Konflikte zwischen den Patientinnen und Patienten und den Leistungserbringern der zertifizierten Praxen.

ben, ob er dazu eine Angabe machen will oder nicht. Fragen nach Religion, sexueller Ausrichtung oder Hobby sind meist nicht verhältnismässig – es sei denn, sie könnten mit einem konkreten Krankheitsbild im Zusammenhang stehen.

Transparenz

Ein weiterer Grundsatz des Datenschutzes ist die «Transparenz»: Grundsätzlich darf es keine «geheime» Datenbearbeitung geben. Werden Daten direkt bei der betroffenen Person erhoben, ist dies offensichtlich. Werden Daten bei Dritten erhoben, braucht es entweder eine gesetzliche Grundlage, die beispielsweise in Sozialversicherungsgesetzen zu finden ist, oder eine Einwilligung. Auch wenn Daten weitergegeben werden, muss die betroffene Person grundsätzlich informiert sein. Einzig, wenn Datenbearbeitung einem Dritten übergeben wird, wie beispielsweise die Betreuung der IT, kann von einer Information abgesehen werden. Wichtig ist, dass der Dritte die Schweigepflichten einhält und vom Auftraggeber entsprechend instruiert und kontrolliert wird.
Im Zusammenhang mit der Transparenz ist es auch ein zentrales Recht des Patienten, gestützt auf Art. 8 DSG, eine Kopie seiner Daten erhalten zu können. Grundsätzlich müssen sämtliche Daten, etwa Diagnosen, Gutachten, Berichte, der Verlauf der Krankengeschichte und Zeugnisse, dem Patienten als Kopie oder als Ausdruck herausgegeben werden. Einzig persönliche Arbeitsmittel, also etwas persönlichere Notizen, die ausserhalb der Krankengeschichte geführt werden, können zurückbehalten werden.

Datensicherheit

Bei der «Datensicherheit» geht es darum, wie Daten eines Patienten zwischen seinen Leistungserbringern so ausgetauscht werden können, dass sie an den richtigen Empfänger geraten und zwischendurch nicht eingesehen werden können. Die Überprüfung der Kontaktdaten und die Verschlüsselung sind dazu die wichtigsten Hilfsmittel. Zudem sollte sich jedes Team überlegen, wie verhindert werden kann, dass auf diesem oder anderem Wege Malware wie Viren oder Erpressungstrojaner in die Praxis geraten.
Auch innerhalb der Praxis sollten Daten vor neugierigen Blicken anderer Patienten oder Angreifern geschützt sein. Die Frage «Wie organisieren wir den Zugang zu Daten innerhalb der Praxis?» nimmt sich dem Thema an und berät zu sicherer Wahl von und Umgang mit Passwörtern. Die Nutzung persönlicher Passwörter und Konten ist auch eine der Voraussetzungen für die Nachverfolgbarkeit von Bearbeitungsvorgängen. Kommt es zu Bedienerfehlern, technischen Defekten oder Wasserschäden, ist ein Backup oft die letzte Rettung. Um zu verhindern, dass Originaldaten und Backup gleichzeitig Schaden nehmen, sollten Backups regelmässig auch ausser Haus gelagert werden. Dabei unterstützen Sie USB-Festplatten oder Onlinedienste. Die Daten sollten verschlüsselt abgelegt werden und der Schlüssel sicher aufbewahrt werden, damit die Daten im Bedarfsfall auch wieder rekonstruiert werden können.
Das Entsorgen der Datenträger: Auch nach dem Leeren des Papierkorbs oder Formatieren des Laufwerks sind viele Daten noch auf dem Datenträger und einfach zu rekonstruieren und können in falsche Hände geraten. Das ein- oder zweimalige Überschreiben des gesamten Datenträgers oder die Nutzung eines spezialisierten Entsorgungsunternehmens sind zuverlässige Methoden.

Fazit

Die zehn Fragen zum Thema Datenschutz und IT zeigen: Es ist möglich, sich mit diesem Thema fundiert auseinanderzusetzen, ohne die konkrete Welt der Arztpraxis und die Bedürfnisse von Patientinnen und Patienten, Ärztinnen, Ärzten und MPA aus den Augen zu verlieren.

Literatur

1 Golder L, et al. Schlussbericht Swiss eHealth Barometer 2016: Akteure im Gesundheitswesen. Bern: gfs, 2016.
2 Bundesgesetz über den Datenschutz SR 235.1.

Angebot

Weitere Antworten auf die Fragen des Datenschutzes und der IT für Arztpraxen finden Sie in unseren FAQs oder werden im Sensibilisierungsprogramm der EQUAM Stiftung erarbeitet. Dieses setzt sich zusammen aus einer Diskussion im Team und einem Workshop mit Ursula Uttinger und Marcel Waldvogel.
www.equam.ch/datenschutz-it

Korrespondenz:
EQUAM Stiftung
Effingerstrasse 25
CH-3008 Bern
Tel. 031 302 86 87
paula.bezzola[at]equam.ch
www.equam.ch