Also sprach Hippokrates

Christoph Schäfer

Es gibt Berufsgruppen, denen eine gewisse Technikferne unterstellt wird. Ärzte und Juristen dürften dabei die Umfragen anführen. Dieser Eindruck täuscht: Gerade im Gesundheitswesen kommt modernste Technik zum Einsatz. Neben der elektronischen Patientenakte eröffnet die Telemedizin in Diagnostik und Therapie stetig neue Möglichkeiten. Und diese Gesundheitsdaten müssen verarbeitet werden – die schützenswertesten Informationen, die das Datenschutzrecht kennt. Wie hätte Hippokrates sich verhalten?

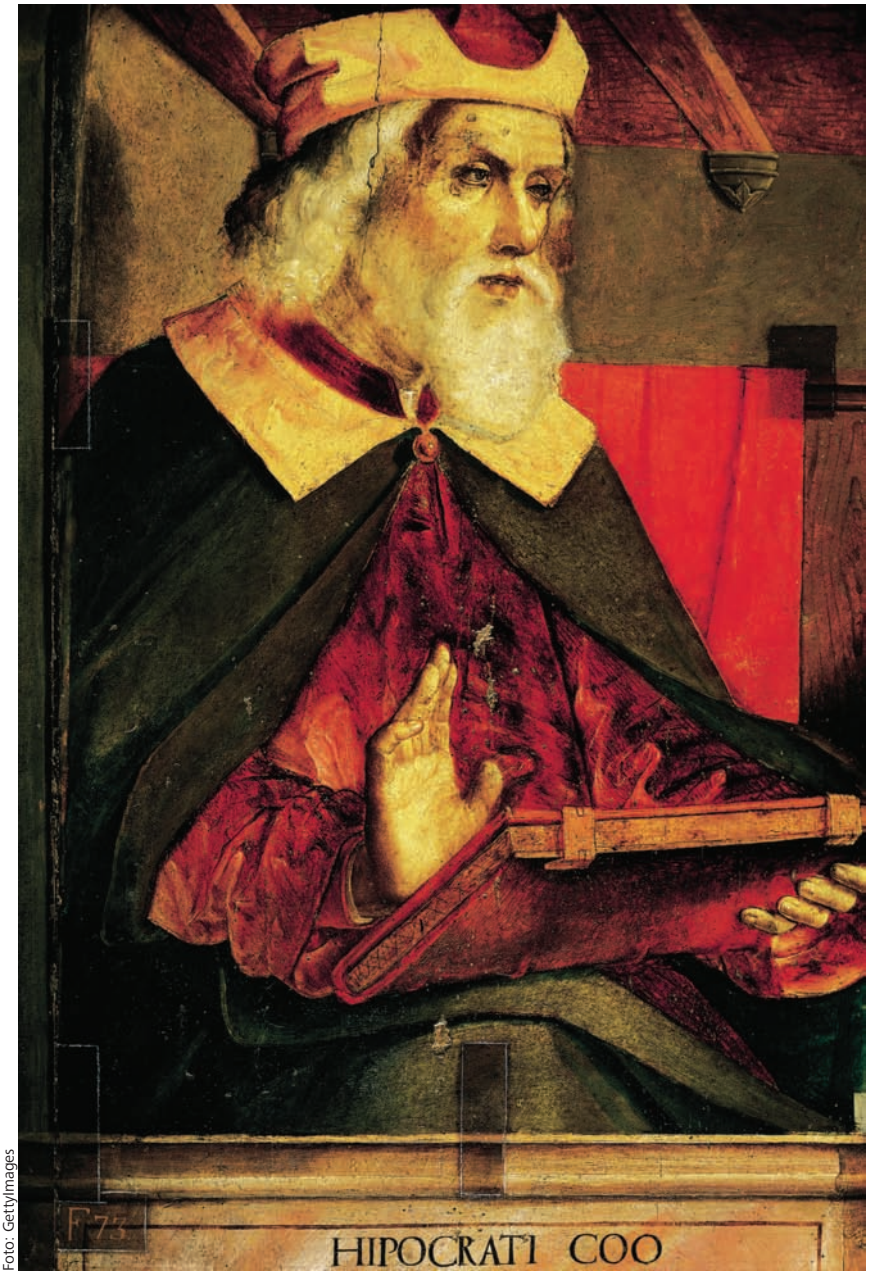

Foto: GettyImages

Vor rund 2.500 Jahren wurde die erste Datenschutznorm verschriftlicht. Im hippokratischen Eid heißt es „Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und das man nicht nach draußen tragen darf, werde ich schweigen und es geheim halten." Die Ärzte waren damit die ersten Datenschützer, denn der Eid bringt die Anforderungen des Datenschutzes an den Mediziner genau auf den Punkt – auch heute noch. Die fortschreitende Technik macht es allerdings nicht leichter, dem gerecht zu werden.

Anders als der Name vermuten lässt, geht es beim Datenschutz nur indirekt um Daten an sich. Vielmehr entschied das Bundesverfassungsgericht bereits 1983, dass jeder grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen kann. Mit dem sogenannten Recht auf informationelle Selbstbestimmung wurde unser Datenschutz-Grundrecht geschaffen. Die zentrale Aussage des Urteils ist: „Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung voraus, den Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu schützen." Damit wird klar, dass es eben nicht nur um die Datenverarbeitung, sondern vielmehr um die Selbstbestimmung und die Privatsphäre geht. Geregelt ist der Datenschutz in einer Vielzahl von Gesetzen – allen voran im Bundesdatenschutzgesetz (BDSG).

Die „Orientierungshilfe Krankenhausinformationssysteme“ der Datenschutzbeauftragten des Bundes und der Länder liegt in der Version 2 (März 2014) vor: https://www.datenschutz-bayern.de/technik/orient/oh-kis.pdf

Die Vorschriften des BDSG greifen nach dem Subsidiaritätsprinzip allerdings nur dann, wenn es keine spezielleren Vorschriften gibt. Kaum eine andere Branche hat so explizite und zahlreiche Datenschutzregelungen wie das Gesundheitswesen. Und das zu Recht, denn Gesundheitsdaten sind nach der Definition des BDSG besonders schützenswerte Daten.

Für Krankenhäuser gelten zunächst die Krankenhausgesetze der Länder mit sehr unterschiedlich ausgeprägten Regelungen zum Datenschutz. Werden Sozialdaten verarbeitet, greift das Sozialgeheimnis, das in den Sozialgesetzbüchern (§§ 35 SGB I und 67 a ff. SGB X) geregelt ist. Daneben existieren sehr spezifische Regelungen wie etwa die des Gendiagnostikgesetzes (GenDG), die bei speziellen Therapieansätzen zu beachten sind. Die Liste lässt sich fast beliebig fortsetzen. Letztlich gilt sogar für den Internetauftritt des Krankenhauses ein eigenes Gesetz – das Telemediengesetz (TMG). Findet sich zu einem Sachverhalt keine spezielle Reglung, so greifen die Vorgaben des BDSG.

Die Vorschriften stehen aber nicht isoliert, sondern bedingen sich gegenseitig. Beispielsweise verlangt das BDSG die Löschung von Daten, wenn sie für die Erfüllung des Zwecks (also die Behandlung eines Patienten) nicht mehr erforderlich sind (§ 35 Absatz 2 Nr. 3 BDSG). Wann dieser Zeitpunkt eintritt, schreibt zum Beispiel die (Muster-)Berufsordnung der Ärzte vor: Ärztliche Aufzeichnungen müssen generell für die Dauer von zehn Jahren nach Abschluss der Behandlung aufbewahrt werden (§ 10 Absatz 3 MBO-Ä).

Eine spezielle Regelung stellt auch die ärztliche Verschwiegenheitspflicht – das sogenannte Patientengeheimnis – dar, die in der (Muster-)Berufsordnung geregelt (§ 9 MBO-Ä) und deren Missachtung nach dem Strafgesetzbuch (§ 203 StGB) unter Strafe gestellt ist.

Hippokrates 2.0 und seine Helfer

Hippokrates’ Eid ist umso schwieriger umzusetzen, werden Patientendaten nicht mehr nur im Kopf oder in der (schriftlichen) Patientenakte vorgehalten. Heute fließen diese Daten in die unterschiedlichsten Informationssysteme ein und werden teilweise sogar an Dienstleister weitergegeben. Die Verantwortung für die Erfüllung der Verschwiegenheitspflicht ist damit aber nicht abgegeben. Der moderne Hippokrates muss seine informationstechnischen Systeme verstehen und beherrschen. Dazu muss er ein Sammelsurium rechtlicher und technischer Vorschriften kennen, um den Anforderungen des Datenschutzes gerecht zu werden. Ohne Hilfe geht das nicht.

Aus dem Sammelsurium ein ordentliches Datenschutzkonzept zu erstellen, ist eine Herausforderung, die professionelle Unterstützung erfordert. Einerseits bedarf es IT-Experten, die die Informationssysteme installieren und warten – was gleich die nächsten Probleme eröffnet, denn eine Offenbarung des Patientengeheimnisses muss dabei vermieden werden. Andererseits kommt dem Datenschutzbeauftragten im Gesundheitswesen eine besondere Rolle zu: Immerhin wird die Verschwiegenheitspflicht auf ihn erweitert, wenn er für einen Arzt tätig wird (§ 203 Absatz 2 a StGB).

Neben dem medizinischen Personal werden weitere Helfer benötigt. Über den Dienstleister zur Aktenvernichtung, den Anbieter des Krankenhausinformationssystems (KIS), den Leasinggeber des Multifunktionsdruckers bis hin zum externen Schreibbüro – das moderne Gesundheitswesen kommt ohne Dienstleister nicht mehr aus.

Trau, schau, wem – das Patientengeheimnis

Für den Mediziner sind zwei Dinge wichtig: Erstens muss er aus Datenschutzsicht immer „Herr der Daten“ bleiben, es müssen also entsprechende Verträge geschlossen und durchgesetzt werden. Zweitens ist stets darauf zu achten, dass das Patientengeheimnis gewahrt bleibt, andernfalls muss eine Schweigepflichtsentbindung eingeholt werden – in beiden Fällen sind viele organisatorische, rechtliche und/oder technische Aspekte zu beachten.

Um im Gesundheitswesen Dienstleister einzusetzen, müssen immer beide Aspekte – Datenschutz und Verschwiegenheitspflicht – beachtet werden. Die Unterstützung durch ein externes Schreibbüro ist im Sinne des Patientengeheimnisses entweder nur mit einer Schweigepflichtsentbindung oder mit dem Verhindern der Offenbarung des Patientengeheimnisses möglich. Favorisiert wird meist der letzte Fall, und Ärzte sprechen ihre Diktate „anonym“. Ganz so einfach ist dies aber nicht, denn letztlich muss das extern geschriebene Diktat einem Patienten wieder zugeordnet werden. Von Anonymität kann also keine Rede sein.

Vielmehr wird der Versuch unternommen, pseudonym zu diktieren. Das meint, dass Daten nur mit einem gewissen Aufwand und Zusatzwissen wieder zugeordnet werden können. Klassischerweise geschieht das über die Patienten- oder Fallnummer.

Doch ist es so einfach? Eine Verwechslung muss ausgeschlossen werden, weshalb der Fallnummer oft noch das Geburtsdatum und Teile des Vor- und Nachnamens beigefügt werden. In Kombination mit gewissen Inhalten des Diktats, beispielsweise dem Namen des Hausarztes, ist es mit der Pseudonymisierung nicht mehr weit her. Um ein externes Schreibbüro einzusetzen, müssen Ärzte sich klare Vorgaben machen, wie ein Diktat zu besprechen ist. Letztlich ist die (echte) Pseudonymisierung ein durchaus praktikables Mittel, um eine Offenbarung des Patientengeheimnisses auszuschließen.

Wäre da nicht das Datenschutzrecht, denn auch pseudonymisierte Daten sind personenbezogene Daten und damit ist das Datenschutzrecht auch auf diese voll anwendbar. Zunächst muss eine sorgfältige Auswahl des Dienstleisters erfolgen, wobei weniger wirtschaftliche als Sicherheits- und Datenschutzaspekte eine Rolle spielen. Das Datenschutzrecht unterscheidet zudem zwei Arten der Datenweitergabe: Eine Übermittlung personenbezogener Daten an ein externes Schreibbüro würde der Einwilligung des Patienten bedürfen – das ist ebenso unpraktisch, wie es die Schweigepflichtsentbindung ist. Alternativ kommt die sogenannte Auftragsdatenverarbeitung (§ 11 BDSG) in Betracht. Schließt der Auftraggeber eine entsprechende Vereinbarung mit dem Dienstleister ab, stellt die Datenweitergabe keine einwilligungsbedürftige Übermittlung dar, denn der Dienstleister wird so behandelt, als wäre er eine interne Stelle.

Doch trivial ist ein solches Auftragsverhältnis nicht. Das Datenschutzrecht stellt umfassende Anforderungen an die Inhalte des Vertrags. Zudem treffen den Auftraggeber Kontroll- und Prüfpflichten, denn er hat sich „vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“ (§ 11 Absatz 2 Satz 4 und 5 BDSG).

Datenschutz heißt auch Daten schützen

Neben diesen rechtlichen und organisatorischen Fragen spielt auch die technische Sicherheit eine Rolle. Bei der Weitergabe der Audio-Dateien an das externe Schreibbüro wie auch bei der Rückübermittlung der geschriebenen Dokumente muss sichergestellt werden, dass diese keinem Dritten zur Kenntnis gelangen. Eine Übermittlung per E-Mail scheidet grundsätzlich aus, sofern die Inhalte nicht verschlüsselt werden. Eine postalische Übersendung per Einschreiben auf CD wäre zwar vorbildlich, kann aber aus offensichtlichen Gründen nicht die Lösung sein. Vielmehr sollte dem Dienstleister ein geschützter Zugriff im eigenen System eingerichtet werden, in dem er die Daten abholen und zurückstellen kann. Schränkt der Auftraggeber Zugriffberechtigungen entsprechend ein, behält er selbst die Hoheit über die technische Sicherheit und kann unberechtigte Zugriffe auf die Daten ausschließen.

Letztlich muss jeder, der geschäftsmäßig personenbezogene Daten verarbeitet, die erwähnten technischen und organisatorischen Maßnahmen (Anlage zu § 9 Satz 1 BDSG) umsetzen. Dies trifft nicht nur das externe Schreibbüro, sondern auch den Auftraggeber selbst. Viele dieser Regelungen, beispielsweise die zur Zutrittskontrolle, bestehen schon aus anderen Gründen, jedoch ist eine systematische Betrachtung nach den Vorgaben des Datenschutzrechts geboten.

Unter anderem besteht die implizite Vorgabe, dass nur die Personen auf Daten Zugriff haben dürfen, die diesen auch wirklich benötigen. Wie im analogen Leben, wo zum Beispiel nicht jeder Mitarbeiter im Krankenhaus den Schlüssel zu allen Räumen und Schränken hat, muss dies auch in der digitalen Welt umgesetzt werden. Was selbstverständlich klingt, ist es tatsächlich nicht immer. Anfang Januar berichtete die Boulevard-Presse, dass 1.600 Mitarbeiter der Klinik in Grenoble, in der Michael Schumacher nach seinem Ski-Unfall behandelt wurde, auf dessen Krankenakte zugreifen können. Möglich macht das der Betrieb eines KIS ohne das erforderliche Rollen- und Berechtigungskonzept, das die Zugriffe auf die Akte steuert. Nachdem zwei Ermahnungen per E-Mail mit einer Erinnerung an das Patientengeheimnis vermutlich eher zu mehr als zu weniger Zugriffen geführt hatten, wurde die Akte letztlich mit einem Passwort versehen. Nach dem Datenschutzrecht muss es die Regel und nicht die Ausnahme sein, dass nur die notwendigen Personen Zugriff auf eine Akte haben.

Was Hippokrates machen würde

Mit zunehmender IT-Durchdringung des Gesundheitswesens steigen auch die Datenschutz- und Sicherheitsanforderungen. Im Kern geht es nach wie vor um Hippokrates' Eid: Patientendaten müssen geheim bleiben. Der vorbildliche Hippokrates hat in jedem Fall ein Datenschutz- und Sicherheitskonzept, das ihm in der Einhaltung seines Eids hilft. In der Einbindung von Dienstleistern ist er sehr vorsichtig. Natürlich benötigt er Unterstützung, damit er sich nicht selbst mit technischen und rechtlichen Fragen beschäftigen muss, und wird daher das Gelesene zum Anlass nehmen, sich mit dem Datenschutzexperten seines Vertrauens auf einen Kaffee zu treffen. Er will und soll Menschen helfen, gesund zu bleiben oder es wieder zu werden, und dient damit einem Grundrecht, nämlich dem Recht auf körperliche Unversehrtheit. Gleichrangig ist aber auch das Grundrecht auf Datenschutz. Hippokrates Selbstverständnis ist es, beidem gerecht zu werden.

Anschrift des Verfassers:

Christoph Schäfer
Secorvo Security Consulting GmbH
Ettlinger Straße 12–14
76137 Karlsruhe
E-Mail: christoph.schaefer@secorvo.de