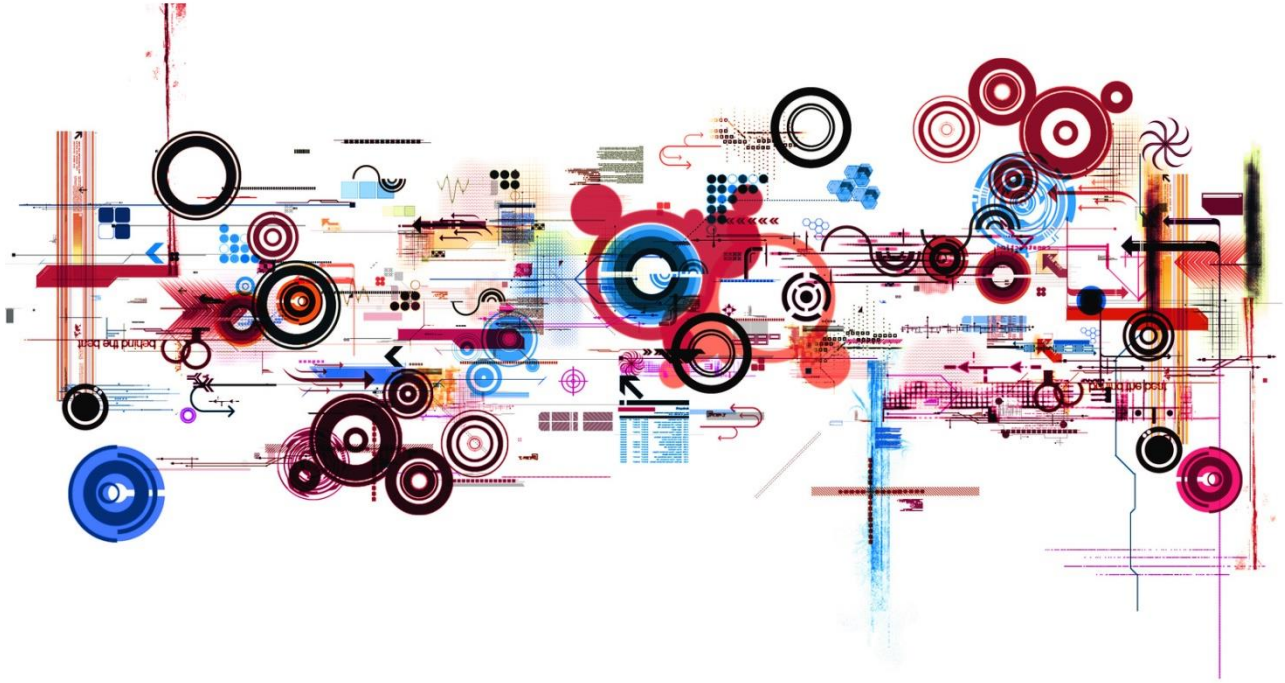
Datenschutz in Arztpraxen und Kliniken – ausgewählte Aspekte

Oliver Ebert, RA und FA für IT-Recht
Hochschullehrbeauftragter für e-commerce und Internetrecht
REK Rechtsanwälte, Stuttgart, Balingen




AT&T
4:38 PM
89 %
„Nächster Termin ?“
„Roland Müller zurückrufen, will schon wieder Viagra“
17
Monday, October 2011
Roland Müller,
Musterstr. 10, 12345
Musterstadt
Tel: 089 12345

Ärztliche Schweigepflicht:

„Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.“

Hippokratischer Eid (Auszug)

Ärztliche Schweigepflicht:

Ärzte dürfen keine Informationen, die ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt worden sind, gegenüber Dritten offenbaren.

Die Schweigepflicht umfasst alle Tatsachen, die nur einem bestimmten, abgrenzbaren Personenkreis bekannt sind und an deren Geheimhaltung der Patient ein schutzwürdiges Interesse hat.

Als solche Tatsache gilt bereits der bloße Umstand, dass ein Patient überhaupt bei einem Arzt in Behandlung ist !

Rechtsgrundlagen

§ 203 Strafgesetzbuch (StGB) (Auszug)

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1.
Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
[..]

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Rechtsgrundlagen

§ 9 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO) (Auszug)

(1) Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist - auch über den Tod der Patientin oder des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen der Patientin oder des Patienten, Aufzeichnungen über Patientinnen und Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

[…]

(3) Ärztinnen und Ärzte haben ihre Mitarbeiterinnen und Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

[…]

Rechtsgrundlagen

§ 4 BDSG (Auszug)

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

[..]

Ärztliche Schweigepflicht:

Konflikt in der Praxis:

Zur Durchführung einer Behandlung ist es in den allermeisten Fällen unabdingbar, dass (besondere) personenbezogene Daten (§ 3 Abs.1, Abs. 9 BDSG) vom Arzt erhoben, gespeichert und verarbeitet werden.

Eine Weitergabe dieser Daten ist nur im Ausnahmefall zulässig.

Der Arzt muss sicherstellen, dass die Daten zuverlässig geschützt bleiben.

Bruch der Schweigepflicht nur in Ausnahmefällen zulässig

Einwilligung des Patienten

Die Übermittlung/Preisgabe personenbezogener Patientendaten ist zulässig, wenn eine ausdrückliche oder stillschweigende Einwilligung des Patienten vorliegt.

Einwilligung muss sich auf konkreten Übermittlungsvorgang beziehen.

Cave:

- Pauschale Einwilligungserklärung nicht ausreichend
- Wirksame Einwilligung nur, wenn Patient den Inhalt, Umfang und Reichweite der Schweigepflichtentbindung überhaupt begreift
- Einwilligung muss regelmäßig erneuert werden (ggf. jedes Quartal!)

Bruch der Schweigepflicht nur in Ausnahmefällen zulässig

Gesetzlich normierte Ausnahme von der Schweigepflicht

Gesetzliche Übermittlungsbefugnisse und -pflichten finden sich insbesondere im Sozialgesetzbuch V (SGB V) für den Bereich der vertragsärztlichen Versorgung, zur Übermittlung an die Kassenärztlichen Vereinigungen, z. B. zu Zwecken der Abrechnung, Wirtschaftlichkeitsprüfung und Qualitätssicherung oder zur Übermittlung an Krankenkasse (§ 284 i. V. m. § 295 SGB V) bzw. an den medizinischen Dienst (§§ 276, 277 SGB V).

Auch im Infektionsschutzgesetz (§§ 6 ff. IfSG), dem Betäubungsmittelgesetz oder im Bereich der gesetzlichen Unfallversicherung (§§ 201 ff. SGB VII) sind entsprechende Übermittlungsbefugnisse bzw. -pflichten gesetzlich statuiert

Bruch der Schweigepflicht nur in Ausnahmefällen zulässig

Wahrnehmung berechtigter Interessen des Arztes

Soweit im Einzelfall zwingend zur Wahrnehmung berechtigter Interessen des Arztes erforderlich, kann Offenlegung auch ohne Einwilligung zulässig sein.

Beispiele:

- Strafrechtliches (Ermittlungs-)Verfahren gegen den Arzt (ggf. auch Praxismitarbeiter)
- Abwehr zivilrechtlicher Ansprüche des Patienten
- Durchsetzung zivilrechtlicher Ansprüche gegen den Patienten

Bruch der Schweigepflicht nur in Ausnahmefällen zulässig

Bei nicht anders abwendbarer Gefahr für höherwertiges Rechtsgut

Ohne gesetzliche Übermittlungsbefugnis und ohne Einwilligung des Patienten kann eine Durchbrechung der ärztlichen Schweigepflicht allenfalls gem. § 34 StGB gerechtfertigt sein, um eine Gefahr für ein höherwertiges Rechtsgut (Leben, Gesundheit und Freiheit) abzuwenden.

Voraussetzung

- Die Gefahr darf nicht anders abwendbar sein
- Gefahr muß konkret sein (bloße Risikoerhöhung reicht nicht)
- Gefahr muß unmittelbar bevorstehen

Grundsätzlich gilt: vorherige Androhung erforderlich !

Probleme

- Verpflichtung zur Dokumentation/Datenspeicherung
  Lokal ? Zentral im Netzwerk ? Webbasiert/Extern ?

- (Fern-)Wartung von Praxissoftware

- Schutz vor Angriffen/Komprimittierung

- Schutz der Datenintegrität

- Einlesen des Speichers von Selbstmessgeräten (zB Blutzucker, Blutdruck)

- Nutzung von Smartphones in der Arztpraxis

Verpflichtung zur Dokumentation

Ärzte müssen die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen dokumentieren.

Hierzu ist - in unmittelbarem zeitlichen Zusammenhang mit der Behandlung - eine Patientenakte zu führen (in Papierform oder elektronisch).

Aufzeichnungen sind nicht lediglich Gedächtnisstützen für Behandler, sondern dienen auch dem Interesse an ordnungsgemäßer Dokumentation.

Aufbewahrungsdauer: mindestens 10 Jahre

Erstellung einer Patientenakte

Normative Verpflichtungen zur Dokumentation / Patientenakte

Verpflichtung aus § 10 Abs. 1 MBO, 630f BGB, § 57 Abs. 3 BMV-Ä bzw. § 13 Abs. 10 EKV sowie vertraglich aus dem Behandlungsvertrag

Zur Erfüllung dieser Verpflichtungen wie auch im Rahmen der Zweckbestimmung des Behandlungsvertrags ist der Arzt gem. § 28 BDSG berechtigt, die von ihm als notwendig erachteten Daten zu erheben und speichern.

Gesonderte Einwilligung bzw. Information des Patienten **nicht** erforderlich !

Erstellung einer Patientenakte

Normative Verpflichtungen zur Dokumentation / Patientenakte

§ 630 f BGB (eingefügt durch Patientenrechtegesetz)

(1) Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn der ursprüngliche Inhalt erkennbar bleibt.

(2) Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen.

Erstellung einer Patientenakte

Normative Verpflichtungen zur Dokumentation / Patientenakte

§ 10 MBO (Musterberufsordnung der Ärzte)

(1) Ärztinnen und Ärzte haben über die in Ausübung ihres Berufes gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen zu machen. Diese sind nicht nur Gedächtnisstützen für die Ärztin oder den Arzt, sie dienen auch dem Interesse der Patientin oder des Patienten an einer ordnungsgemäßen Dokumentation.

[…]

(3) Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht.

[…]

Verpflichtung zum Datenschutz

§ 10 Abs. 5 MBO:

Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern

Ärztinnen und Ärzte haben hierbei die Empfehlungen der Ärztekammer zu beachten.

-> „**Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“** nebst **„Technischer Anlage“**

§ 9 BDSG:

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Verstösse implizieren grds. (mindestens) Fahrlässigkeit im Sinne des § 203 StGB !

Praktische Anforderungen

Unbefugte dürfen keinen Zugriff /Einblick in Patientendaten erhalten:

- Passwortschutz, Berechtigungssystem
- Monitor des Arztes im Besprechungszimmers nicht generell einsehbar
- Server/Datenbank muss zugriffssicher verwahrt sein (Schrank/Raum)
- Einsatz von Firewall und tagesaktuellem Virenscanner
- Fernwartung/Wartung: nur zulässig, wenn die einzelnen Maßnahmen durch den Arzt autorisiert und überwacht werden können.
- WLAN/Bluetooth im Praxisnetzwerk müssen abgesichert sein

Praktische Anforderungen

Unbefugte dürfen keinen Zugriff /Einblick in Patientendaten erhalten:

- Auszumusternde Datenträger vollständig unlesbar machen.
- Patientendaten sollten nur verschlüsselt gespeichert werden
- Bei Faxübertragung: Empfängernummer prüfen, ggf. Fax ankündigen
- Bei eMail: Empfängeradresse prüfen (cave: Autovervollständigung!)
- BÄK: Telefonie per Voice-over-IP „nicht abhörsicher“
  ->besondere Schutzvorkehrungen erforderlich gem. „Technische Anlage“)

Praktische Anforderungen

Unbefugte dürfen keinen Zugriff /Einblick in Patientendaten erhalten:

Bundesärztekammer:

„Es wird empfohlen, den in der Anlage (vgl. Kapitel 3 der Technischen Anlage) dargestellten technischen Vorgaben zu folgen.

Kann dies nicht sichergestellt werden, so sind Patientendaten auf einem Praxiscomputer zu speichern, der **über keinen Internetanschluss** verfügt.“

Weitere Anforderungen

§ 630f Abs1. S 2 BGB:

„Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn der ursprüngliche Inhalt erkennbar bleibt.“

-> Änderungen in Patientenakte müssen nachvollziehbar sein

Lokale Datenspeicherung

Bei einer ausschließlich lokalen Datenspeicherung werden alle Daten ausschließlich im Praxis-/Kliniknetzwerk gespeichert.

Hierfür keine Einwilligung erforderlich.

Es muss hinreichend sichergestellt sein, dass dort keine unberechtigten Personen Zugriff auf Patientendaten erhalten können, beispielsweise bei (Fern-)Wartungsmaßnahmen.

Externe Datenspeicherung/“Online-Akten“

Problematisch: Nutzung von internetbasierten Plattformen

Vom Arztgeheimnis geschützte Daten werden an Dritte übermittelt und dort gespeichert bzw. weiterverarbeitet.

Zur Meidung einer Strafbarkeit muss daher sichergestellt sein, dass eine wirksame, laufend erneuerte Einwilligung der Patienten vorliegt.

Weitere Probleme:

- Sicherstellung der Aufbewahrungsfrist (§ 10 MBO)
- Warum externe Speicherung, wenn Speicherung ohne Datenweitergabe auch inhouse möglich (Gebot der „Datensparsamkeit“, § 3a BSDG)
- Datenschutz bei/durch ausländischen Unternehmen

Datenaustausch mit Patienten

Einseitiger Datenversand vom Patienten zum Arzt

Ein Arzt, der zur Kommunikation mit Patienten eine eMail-Adresse angibt oder Datenempfangsmöglichkeiten bereitstellt, muss jedoch darüber aufklären bzw. darauf hinweisen, dass unverschlüsselte Kommunikation per eMail generell unsicher und risikobehaftet ist.

Bidirektionale Kommunikation bzw. Datenversand an Patienten:

nur zulässig, wenn Patient zuvor in die Datenübermittlung per eMail eingewilligt hat.

Verwendung von Terminkalendern/Smartphones

Moderne Smartphones bieten komfortable Möglichkeiten zur Terminplanung, Adressverwaltung und Unterstützung der Praxisorganisation.

Risiko:

Daten werden oft nicht ausschließlich im Telefonspeicher, sondern auch in einer „Datencloud“ bzw. auf Servern des Anbieters abgespeichert.

Ohne Einwilligung nur bei Anonymisierung/Pseudnomyisierung (vor der Datenübermittlung!) oder ausreichender Verschlüsselung zulässig

Verwendung kostenloser eMail-Accounts

Nicht wenige Ärzte nutzen zur Patientenkommunikation kostenfreie eMail-Zugänge, beispielsweise von gmail, hotmail, gmx, web.de oder yahoo.

Risiko:

Oft sehen die dortigen Nutzungsbestimmungen vor, dass der Betreiber die emails sichten und analysieren darf („email-scanning“).

Ohne Einwilligung nur bei Anonymisierung/Pseudnomyisierung (vor der Datenübermittlung!) oder ausreichender Verschlüsselung zulässig