Ausgabe 5 · Januar 2024

Innovations

(un)Recht

Datenschutz – Wann kann es teuer werden?

Sie und ich, wir möchten in der Regel nur das preisgeben, was wir selbst bestimmen.
Fakt ist, dass wir seit Jahren keine vollständige Kontrolle mehr über unsere eigenen Daten haben.
Bereits wer im Internet surft, oder einen PC benutzt, hinterlässt Spuren, die für Laien nicht sichtbar sind, aber für Hacker und Kriminelle, die mit sensiblen Datensätzen und auf gebrauchten Datenträgern viel Geld verdienen können. Dies ist nur eine Konsequenz ungenügend geschützter Daten.
Umso sensibler ist Datenschutz in Unternehmen, insbesondere im Gesundheitswesen, wo Dokumente und Daten von Patienten involviert sind.
Zusammen mit Rechtsanwalt und Titularprofessor Michael Hochstrasser gehen wir zentralen Fragen rund um den Datenschutz in Arztpraxen auf den Grund.
Der erfahrene Mann kennt sich mit der Thematik bestens aus und hat gemeinsam mit Partnern die mediX-Ärztenetze und mediX-Praxen bei der Umsetzung des revidierten Datenschutzgesetzes unterstützt.

Michael Hochstrasse
im Interview

Warum ist die Einhaltung des Datenschutzes für eine Arztpraxis heute wichtiger denn je?

In einer Arztpraxis werden Daten über die Gesundheit der Patienten bearbeitet, zum Teil sind dies auch Daten, welche die Intimsphäre betreffen. Auch genetische Daten können in einer Arztpraxis vorkommen. Diese Daten sind sensibel. Rechtlich spricht man dort von besonders schützenswerten Daten. Heutzutage werden immer mehr Daten elektronisch gespeichert und ausgetauscht. Wo viele Daten sind, besteht dementsprechend das Risiko, dass diese in falsche Hände geraten. Der Schutz der Daten ist deshalb zentral.

Was hat sich in den letzten Jahren konkret verändert?

Immer mehr Arztpraxen führen das Patientendossier elektronisch. Die Anforderungen an den Datenschutz ändern sich laufend. Ging es früher, plakativ gesagt, darum, den Aktenschrank abzuschliessen, müssen heute Computer und Server so gesichert werden, dass keine Unbefugten zugreifen können. Mit dieser Entwicklung geht einher, dass die medizinische Versorgung stark vernetzt ist. Eine Hausärztin arbeitet zusammen mit spezialisierten Ärzten, mit dem Spital, der Apotheke oder Spitex-Diensten. Dabei werden zwangsläufig Daten ausgetauscht. Es ist wichtig, dass der Patient weiss, was mit seinen Daten geschieht und er darauf vertrauen kann, dass seine Daten sicher sind.

Was ist die Herausforderung dabei?

Ganz sicher den Überblick zu behalten. Bei der Umsetzung des neuen Datenschutzgesetzes mit den mediX-Praxen haben wir viel Zeit darauf verwendet, uns einen Überblick zu verschaffen, wer von den Beteiligten (Hausärztin, Labor, Spitex, Krankenversicherung usw.) welche Daten von wem erhält, wer für die Daten verantwortlich ist, und wer sie in wessen Auftrag bearbeitet. Was auf dem Papier einfach erscheint, ist in der Praxis oftmals komplex.

Wo stolpern viele Einrichtungen?

Seriös betriebener Datenschutz ist aufwändig. Ärztinnen und Ärzte müssen zunehmend administrative Aufgaben erledigen und für den Patienten bleibt immer weniger Zeit. Der Datenschutz frisst zusätzlich Zeit – Zeit, die sowieso schon fehlt. Um die Datenflüsse und die Risiken zu verstehen und mögliche Sicherheitsmassnahmen evaluieren zu können, muss sich die Ärztin zusätzliches IT-Wissen aneignen. Im Ergebnis wird der Datenschutz als aufwändig und kompliziert empfunden und so zu einer lästigen Zusatzaufgabe.

Wann kann es teuer kommen?

Teuer kann es bei einer Verletzung der Datensicherheit werden, wenn unbefugte Dritte in den Besitz der Daten gelangen und sich zeigt, dass die betroffene Praxis die datenschutzrechtlichen Vorschriften nicht umgesetzt hat. Die Cyberkriminalität ist ein grosses Problem. Spitäler sind besonders exponiert. Es kann aber auch eine kleine Praxis treffen. Werden Daten verschlüsselt, wird es teuer, die Daten wiederherzustellen und zusätzlich die Lücken im Sicherheitssystem zu schliessen.
Die Erfahrung in der EU, wo die Datenschutzgrundverordnung (DSGVO) schon ein paar Jahre länger in Kraft ist, zeigt aber, dass es nicht nur bei einer Verletzung der Datensicherheit teuer werden kann, sondern auch dann, wenn sich bei einer Kontrolle oder bei Abklärungen infolge einer Anzeige ergibt, dass die Vorschriften nicht oder ungenügend umgesetzt wurden.
In der Schweiz sind vor allem die Verletzung der Informationspflicht, die Verletzung der Vorschriften über die Auftragsbearbeitung und die Weitergabe von Daten ins Ausland ohne Einhaltung der entsprechenden Voraussetzungen mit Strafe bewehrt. Der Bussenrahmen geht bis CHF 250'000. Er ist damit viel tiefer als in der EU. Weil die Bussen in der Schweiz aber nicht gegen das Unternehmen, sondern gegen die verantwortliche Person verhängt werden, sind sie nicht weniger abschreckend.

Gibt es Schlüsselpunkte für eine gute Handhabung?

Viele Vorschriften sind sinnvoll. Es gibt aber auch Vorschriften, die man umsetzen muss, bei denen der Erkenntnisgewinn – ehrlich gesagt – gering ist. Auf der anderen Seite kann man mit einfachen, unscheinbaren Mitteln etwas bewirken. Ein Beispiel aus der Umsetzung mit den mediX-Praxen: Je nach Praxisräumen kann es sein, dass ein Patient im Wartezimmer mithört, was am Empfang oder am Telefon gesprochen wird. Es gibt verschiedene Lösungen, um das zu verhindern. Ein einfaches und doch effektives Mittel ist, Musik im Wartezimmer laufen zu lassen.
Über die gesetzlich vorgesehenen Instrumente, wie das Verzeichnis der Bearbeitungstätigkeiten, die Datenschutzerklärung oder die Datenschutz-Folgenabschätzung, hinaus haben wir bei der Umsetzung in Zusammenarbeit mit einzelnen Praxen ein Datenschutzkonzept entwickelt, das zum Beispiel Vorschläge für die Gestaltung des Empfangs und des Wartezimmers enthält. Es ist zentral, die Mitarbeitenden für den Datenschutz zu sensibilisieren und sie zu schulen. Die Mitarbeitenden sollten ermuntert werden, die Augen offenzuhalten und ihre Inputs aufzunehmen. Schlussendlich sollte sich jeder Arzt bewusst sein, dass er eine Vorbildfunktion hat. Wenn der Arzt zu locker mit dem Datenschutz umgeht, kann er nicht erwarten, dass sein MPA die Thematik ernst nimmt.

Welche Probleme haben sich bei der Umsetzung gezeigt?

Schwierig ist es, wenn nicht alle Beteiligten am gleichen Strick ziehen. Wir haben das bei den mediX-Praxen mit den ADV erlebt. ADV sind Vereinbarungen zur Auftragsdatenbearbeitung. Wenn eine Praxis Daten, für die sie verantwortlich ist, von Dritten bearbeiten lässt, muss sie sich vergewissern, dass dieser Dritte die Daten nur so bearbeitet, wie sie selbst es tun dürfte. Ausserdem muss sie sich überzeugen, dass die Datensicherheit gewährleistet ist. Das geschieht meist in Form der ADV. Deshalb sollten Praxen, z. B. mit externen Buchhaltern, Cloudbetreibern und Anbietern von Praxisinformationssystemen, ADV abschliessen.
Viele dieser Dienstleister setzen das neue Datenschutzgesetz vorbildlich um. Wir haben aber die Erfahrung gemacht, dass es vereinzelte Dienstleister gibt, die es ablehnen, eine ADV abzuschliessen, oder die ein Muster vorlegen, das den gesetzlichen Vorgaben nicht genügt. Das ist egoistisch, weil die Praxen als Verantwortliche der Daten dafür einstehen müssen, dass die Vorschriften über die Auftragsbearbeitung eingehalten sind. Im Grunde müsste man solche Dienstleister bestrafen, indem man nicht mehr mit ihnen zusammenarbeitet. Allerdings ist der Wechsel des Praxisinformationssystems mit grossem Aufwand verbunden, sodass der Arztpraxis – rein praktisch – oft keine andere Wahl bleibt, als die Faust im Sack zu machen.
Ich hoffe, dass die Behörden dies berücksichtigen werden, wenn sich die Frage stellt, ob eine Praxis die Vorgaben des Datenschutzgesetzes richtig umgesetzt hat. Wir überlegen auch, die schwarzen Schafe beim EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsberater) zu melden. Unabhängig davon hoffe ich auf die Vernunft der Anbieter: Sie sind Dienstleister. Es müsste in ihrem Interesse sein, zufriedene Kunden zu haben. Dazu gehört, die Kunden bei ihren Problemen zu unterstützen – und nicht ihnen Probleme zu bereiten.

Was wird in den nächsten Jahren noch auf uns zukommen?

Das Schwierige an der Zukunft ist, dass sie ungewiss ist. Lassen wir uns überraschen. Sicher wird es nicht weniger Daten und nicht weniger Probleme geben. Künstliche Intelligenz ist ein allgegenwärtiges Thema. Sie wird auch im Gesundheitswesen einen immer grösseren Platz einnehmen. Sie wird Chancen bieten und Risiken bringen. Eine zentrale Herausforderung wird sein, zu verstehen, wie die KI arbeitet, woher sie ihre Daten bezieht und wie sie zu ihrer Empfehlung kommt.

Wie kann man sich hierfür rüsten?

Die Augen offenhalten und die Entwicklungen kritisch verfolgen.

Wie soll ich mich als Unternehmen/Praxis bei einem Datenklau verhalten?

In einem solchen Fall ist es wichtig, nicht kopflos zu handeln. Zuerst gilt es, abzuklären, was genau passiert ist. In einigen Fällen ist das rasch klar, in anderen Fällen braucht es IT-Spezialisten, um dies herauszufinden. Anschliessend ist zu prüfen, ob unmittelbarer Handlungsbedarf besteht, ob das IT-System vom Netz getrennt werden muss. Besteht ein hohes Risiko für die Persönlichkeit der betroffenen Personen, verlangt das Gesetz eine Meldung an den EDÖB. Wenn es zum Schutz der betroffenen Personen nötig ist, sind auch diese zu informieren. Das ist zum Beispiel der Fall, wenn Passwörter entwendet wurden; dann müssen die Betroffenen dies wissen, um ihr Passwort ändern zu können. Besteht eine Versicherung, sollte diese frühzeitig ins Boot geholt werden.

Was muss ich als Patient beachten?

Als Patient kann ich darauf achten, ob der Arzt den Schutz "meiner" Daten ernst nimmt. Wenn ich an den Empfang komme und dort die Krankengeschichte der letzten Patientin offen herumliegt, muss ich davon ausgehen, dass es die Praxis mit dem Schutz meiner Daten auch nicht so genau nimmt.
Weiter ist es sinnvoll, sich als Patient kritisch mit dem Thema auseinanderzusetzen und sich zu überlegen, für welche Zwecke die persönlichen Daten verwendet werden sollen und für welche nicht. Das setzt voraus, dass man versteht, was mit den Daten geschieht. Zum Beispiel eine Gesundheits-App, die Daten aufzeichnet und übermittelt: Will ich das als Patient? Wer erhält meine Daten und zu welchem Zweck? Was sind meine Vorteile, was die Risiken?
Skeptisch sollte man immer dann sein, wenn es etwas "gratis" gibt. Wenige Sachen sind wirklich gratis. "Gratis"-E-Mails oder "Gratis"-Nachrichten sind bei näherem Hinsehen in der Regel nicht gratis. Man zahlt bloss nicht in Geld, sondern in anderer Form, etwa mit Daten. Ich behaupte: Im Gesundheitswesen ist es nicht anders.

Wie oft muss ich als Arzt/Spital eine Datenschutzvereinbarung mit meinen Patienten anpassen bzw. erneuern?

Ich empfehle den Arztpraxen und Spitälern, keine Datenschutzvereinbarung mit den Patienten zu schliessen. Das Gesetz verlangt, dass die Betroffenen bei der Beschaffung von Daten angemessen informiert werden, unter anderem über den Bearbeitungszweck und gegebenenfalls die Empfänger der Daten. Jedoch braucht es in der Schweiz – und im Gegensatz zur EU – grundsätzlich keine Einwilligung der Betroffenen.
Eine Vereinbarung setzt voraus, dass beide Seiten zustimmen. Auch eine Änderung ist deshalb nur möglich, wenn beide

zustimmen. Schliesst ein Arzt oder ein Spital mit den Patienten eine Datenschutzvereinbarung, so können sie diese nur mit Zustimmung der Patienten später wieder ändern. Die Zustimmung jedes einzelnen Patienten einzuholen, ist meist nicht möglich oder zumindest sehr aufwändig.
Die Information kann demgegenüber einseitig erfolgen, zum Beispiel in Form einer Datenschutzerklärung auf der Website oder eines Schreibens, das im Wartezimmer ausliegt oder am Empfang abgegeben wird. Das ist viel flexibler und die Daten können aktualisiert werden. Die Datenschutzerklärung kann und muss immer dann angepasst werden, wenn sich etwas ändert. Es empfiehlt sich, die datenschutzrechtlichen Vorgänge in einer Praxis oder im Spital in regelmässigen Abständen zu überprüfen.

Wer überwacht die Einhaltung?

Das Gesetz sieht keine generelle Kontrolle vor. Zum Teil erfolgt eine Kontrolle im Rahmen von Zertifizierungen oder aufgrund von Vorgaben von Gemeinwesen oder Verbänden. Die Ahndung von Verstössen erfolgt grundsätzlich durch die Strafverfolgungsbehörden. Weder die Staatsanwaltschaft noch die Polizei haben aber die Ressourcen oder Lust, flächendeckende Kontrollen durchzuführen. Auch der EDÖB tut dies nicht. Meist werden diese Behörden auf Anzeige hin tätig oder wenn sich anlässlich einer Verletzung der Datensicherheit Anhaltspunkte für eine ungenügende Umsetzung des Datenschutzes ergeben.
Im Grund gilt: Jede Praxis und jedes Spital muss für sich schauen und ist selbst dafür verantwortlich, dass die Vorschriften eingehalten werden.

Was raten Sie abschliessend jedem Mediziner?

Datenschutz ist wichtig, gerade im Gesundheitswesen. Datenschutz darf aber nicht zum Selbstzweck verkommen. Man sollte nicht blindlings handeln, sondern sich überlegen, wozu man etwas tut.
Der Datenschutz darf auch nicht dazu führen, dass andere Themen vernachlässigt werden. Ein Beispiel: Die Ärztin untersteht dem Arztgeheimnis. Was sie im Rahmen ihrer Tätigkeit erfährt, darf sie nicht weitererzählen, sonst macht sie sich strafbar. Nur weil der Datenschutz mit dem revidierten Datenschutzgesetz in aller Munde ist, bedeutet das nicht, dass das Arztgeheimnis nicht mehr gilt. Ich habe kürzlich einen Vertrag gesehen, der die Weitergabe von Daten einer Hausarztpraxis an einen Dienstleister regelt. Auf zehn Seiten waren alle möglichen datenschutzrechtlichen Fragen geregelt, das Arztgeheimnis wurde kein einziges Mal erwähnt. Da stimmt etwas nicht. Das Arztgeheimnis sollte im Zentrum stehen.
Der gute alte kategorische Imperativ kann auch beim Datenschutz hilfreich sein. Etwas vereinfacht und auf das vorliegende Thema angepasst: Wenn man sich als Ärztin überlegt, welchen Umgang man sich mit den eigenen Daten wünscht, wenn man selbst Patientin wäre – dann ist das eine gute Richtlinie.

Über den Autor:

Geboren 1976, studierte Michael Hochstrasser an der Universität Zürich (lic. iur. 2002, Dr. iur. 2006). 2008 erwarb er das Anwaltspatent. Michael Hochstrasser arbeitete als wissenschaftlicher Assistent an der Universität Zürich sowie als Auditor und juristischer Sekretär am Bezirksgericht Zürich. Gestützt auf seine Habilitationsschrift zum Beförderungsvertrag erteilte ihm die Universität Zürich 2015 die Venia Legendi für das Gebiet Privat- und Wirtschaftsrecht; 2021 wurde er zum Titularprofessor ernannt. Seit 2007 arbeitet er für Schiller Rechtsanwälte, seit 2014 ist er Partner.

Michael Hochstrasser ist Titularprofessor an der Universität Zürich. Er ist Mitglied des Verwaltungsrats der Carl Zeiss AG und der WintiMed AG. Weiter ist er Mitglied des Zürcher Anwaltsverbands, des Schweizerischen Anwaltsverbands, der ASDA/SVLR (Schweizerische Vereinigung für Luft- und Raumrecht), der EALA (European Air Law Association) und des Verbandsschiedsgerichts des Schweizerischen Schachbundes (Präsident).