

«Eine patientenzentrierte Betreuung ohne Datenschutz ist nicht möglich»



Ob Überwachung von Mitarbeitenden im Homeoffice oder Contact-Tracing-App des Bundes: Über den Datenschutz wird in der Schweiz aktuell heiss diskutiert. Wie lässt sich Datenschutz im Gesundheitswesen einfach umsetzen? Wir haben mit HIN Datenschutzexperte Christian Peter dazu ein Interview geführt.

Herr Peter, ist Datenschutz – gerade im Licht der aktuellen Krise – nicht ein Luxusproblem?

Wenn Sie Luxus mit etwas in Verbindung bringen, das nicht zwingend nötig ist und nur bestimmten Personen vorbehalten ist, dann ist Datenschutz kein Luxus. Datenschutz ist Persönlichkeitsschutz. Darauf haben alle Leute zu jeder Zeit Anspruch. Wenn Sie hingegen mit Luxus in erster Linie qualitativ hochwertige Güter in Verbindung bringen, dann könnte man die Frage eventuell bejahen. Eine medizinische Dienstleistung kann nur hochwertig sein, wenn sie auch dem Datenschutz die nötige Beachtung schenkt.

Datenschutz als Qualitätsmerkmal einer medizinischen Dienstleistung: Wie muss ich mir das vorstellen?

Das Streben nach Exzellenz ist im Gesundheitswesen weit verbreitet. Dazu gehört grundsätzlich auch, die Rechte der Patienten zu respektieren. Leider wird gelegentlich vergessen, dass auch Datenschutz Persönlichkeitsschutz ist und wir dem Patienten nur gerecht werden können, wenn wir seine informationelle Selbstbestimmung achten. Und Datenschutz ist nichts anderes als die Umsetzung der informationellen Selbstbestimmung.



Christian Peter

Christian Peter ist promovierter Jurist mit einem CAS Information Security and Risk Management. Seit 2004 unterstützt er Spitäler, Verbände, Praxen und Kliniken nicht nur bei allen Fragen des Spital- und Gesundheitsrechts, sondern insbesondere auch im Datenschutzrecht. Bei der Health Info Net AG (HIN) ist er als Datenschutzexperte für die entsprechenden Schulungsangebote verantwortlich. Er hat Lehraufträge an verschiedenen Fachhochschulen und publiziert regelmässig.

Können Sie für die Leser kurz beschreiben, was «informationelle Selbstbestimmung» bedeutet?

Es ist wichtig, dass die Menschen die Möglichkeit haben, personenbezogene Informationen selbstbestimmt zu steuern. Dass wir selbstbestimmt über medizinische Eingriffe entscheiden, hat sich durchgesetzt. Wir werden durch die Behandelnden aufgeklärt, entscheiden dann aber selber, ob wir den Eingriff wollen oder nicht. Beim Umgang mit personenbezogenen Daten muss auch so vorgegangen werden: Die Betroffenen sollen darüber ins Bild gesetzt werden, was man mit ihren Daten machen möchte. Aufgrund dieser Informationen wägt ein Betroffener dann ab und entscheidet, ob er die Datenbearbeitung will oder nicht.

Das klingt aber doch eher nach einem «Luxusproblem», wenn man als Patient dringend ärztliche Hilfe benötigt. Kann es die Qualität einer medizinischen Behandlung konkret beeinflussen, wie viel Aufmerksamkeit ein Arzt, eine Ärztin dem Datenschutz beimisst?

Durchaus! Je nach Beziehung zu einer anderen Person geben wir mehr oder weniger Informationen Preis. So steuern wir auch unsere Selbstdarstellung in der Öffentlichkeit. Im Behandlungsverhältnis offenbaren sich die Patienten und geben persönlichste Informationen Preis, welche zum Teil nicht einmal ihre Lebenspartner kennen. Dies führt zu einer Verantwortung, der man sich bewusst sein muss. Befürchtet der Patient einen Vertrauensbruch, teilt er der Ärztin oder dem Arzt wesentliche Informationen (zum Beispiel über bestimmte gesundheitsrelevante Verhaltensweisen) nicht mit. Dies hat unmittelbare Auswirkungen auf Qualität und Erfolg der Behandlung. Dies gilt es zu verhindern.

Kann ich als Patient nicht voraussetzen, dass mein Hausarzt sich an das Berufsgeheimnis hält?

Grundsätzlich müssen Sie als Patient darauf vertrauen können, dass Ihre Gesundheitsdaten die Praxis Ihres Hausarztes nur mit Ihrem Wissen und Einverständnis verlassen, etwa wenn er Sie an einen Spezialisten überweist. Die Digitalisierung schafft hier jedoch neue Realitäten. Wenn Ihr Hausarzt beispielsweise die Dossiers seiner Patienten in der Cloud aufbewahrt oder für seine Praxis-IT einen externen Dienstleister beauftragt, dann wird es für ihn als IT-Laie schwierig, die Verantwortung wahrzunehmen, die ihm aus Berufsgeheimnis und Datenschutzgesetz erwächst.

Wie kann denn im hektischen Praxisalltag und angesichts der fortschreitenden Digitalisierung diese informationelle Selbstbestimmung gewährt und das Vertrauen der Patienten hochgehalten werden?

Es ist viel einfacher als man denkt. Es gibt zwei Bereiche, denen man sich annehmen muss: der Infrastruktur und dem eigenen Verhalten. Bei der Infrastruktur muss man sicherstellen, dass das IT-System geschützt ist. Das [11-Punkte-Programm der FMH](#) gibt hier gute Anhaltspunkte. So muss zum Beispiel die ganze ICT-Umgebung mit einer Firewall geschützt sein, jedes Endgerät vor Schadsoftware. Daten müssen regelmässig gesichert werden, damit sie wiederhergestellt werden können, wenn sie versehentlich gelöscht worden sind oder wenn ein Angreifer die Daten willentlich zerstört hat.

Und wenn, wie Sie angesprochen haben, Daten an den Patienten oder eine andere Gesundheitsfachperson übermittelt oder einem IT-Dienstleister anvertraut werden?

Dann muss sichergestellt werden, dass sicher mit Kolleginnen und Kollegen oder den Patienten per E-Mail kommuniziert wird. E-Mails mit Patientendaten sollten ausschliesslich verschlüsselt verschickt werden. Hier bietet sich die [Lösung von HIN](#) an, die im Gesundheitswesen weit verbreitet ist und eine Verschlüsselung bietet. Wenn man – was in vielen Fällen ja Sinn macht – die IT spezialisierten Dienstleistern in die Hände gibt, sollte man sich vertraglich entsprechend absichern. Die FMH stellt auch hierfür nützliche [Hilfsmittel wie einen Rahmenvertrag](#) bereit.

Gibt es noch weitere Punkte zu beachten betreffend Infrastruktur?

Auch beim Einrichten der Praxis kann man auf Datenschutzkonformität achten. Bildschirme sollten so positioniert werden, dass die Patienten nicht darauf blicken können, und die wartenden Patienten sollten die Gespräche am Telefon nicht mithören können. Neben diesen, die Infrastruktur betreffenden Massnahmen, sollte man aber das Augenmerk auch auf das eigene Verhalten oder den gelebten Datenschutz richten.

Was verstehen Sie unter «gelebtem Datenschutz»?

Wem gebe ich am Telefon Auskunft über die Patienten, sperre ich den Bildschirm, wenn ich den Arbeitsplatz verlasse, spreche ich so laut, dass andere Patienten mithören können und klicke ich auf jeden Link, der mich in einer E-Mail anblinkt? Bei all diesen Tätigkeiten muss ich mir überlegen, ob ich hierbei nicht das Vertrauen der Patienten missbrauche. Aus einem solchen Bewusstsein heraus lebe ich dann ganz automatisch [Prinzipien wie Sparsamkeit und Verhältnismässigkeit](#), sodass ich beispielsweise einer Versicherung nur die unbedingt erforderlichen Informationen weitergebe.

Lässt sich ein solches Verhalten trainieren?

Durch kontinuierliche Sensibilisierung oder Schulungen können alle Mitarbeitenden ihr Sensorium schärfen. In den Awareness-Schulungen von HIN zum Beispiel wird an Hand von Beispielen gezeigt, wo Gefahren lauern und wie man diesen einfach begegnen kann. Es stehen nicht die Normen und Herausforderungen im Zentrum, sondern die Lösungen. Mit einer einfachen Tastenkombination kann der Bildschirm gesperrt werden, mit einem besseren Headset und leiserem Sprechen kann am Telefon die unrechtmässige Weitergabe von Patientendaten verhindert werden. Oder es kann gezeigt werden, wie Kriminelle an Passwörter kommen, und mit welchen Mitteln [man sich dagegen wappnen kann](#). Dieses Wissen können Mitarbeitende im beruflichen und persönlichen Alltag nutzen.

Sie unterrichten seit über zehn Jahren Gesundheitsfachpersonen im Bereich Datenschutz. Welches sind die Gründe dafür, dass es zu Datenschutzverletzungen kommt?

Es ist oft Unachtsamkeit. Niemand verstösst mit Wissen und Willen gegen den Datenschutz, dafür liegen die Patienten den Gesundheitsfachpersonen zu fest am Herzen. Vielmehr realisiert man gar nicht, dass ein Handeln aus Sicht des Datenschutzes problematisch ist. Hier kommt der [Awareness-Gedanke](#) ins Spiel. Die Gesundheitsfachpersonen müssen ein Sensorium entwickeln, woraus Datenschutzverletzungen resultieren können. Da möchte ich auch bei meinen Schulungen ansetzen. Den Leuten aufzeigen, dass eine patientenzentrierte Betreuung ohne Datenschutz nicht möglich ist, und wenn man vom Nutzen des Datenschutzes überzeugt ist, fällt es einem auch einfach, Datenschutzrisiken zu erkennen. Hier helfe ich und zeige natürlich auch auf, wie mit einfachen Mitteln datenschutzkonformes Handeln möglich ist.

Was möchten Sie mit Ihrem Engagement für den Datenschutz bewirken?

Wenn sich die Menschen im Nachgang an ihrem eigenen Arbeitsplatz mehr mit dem Datenschutz und somit mit den Rechten der Patienten auseinandersetzen und allenfalls für den ganzen Betrieb Verbesserungen anregen, habe ich mein Ziel erfüllt. All diejenigen Betriebe, welche sich die wichtigsten Vorgaben zu Herzen nehmen, können dies auch mit dem [HIN Label](#) «Ihre Daten im Vertrauen» nach aussen kundtun. Für die Patienten ist dann klar ersichtlich, dass sie sich in einem Betrieb befinden, dem Datenschutz wichtig ist. In einem Betrieb, für den Datenschutz kein überbeuertes Gut für wenige ist, sondern Teil einer qualitativ hochstehenden Dienstleistung.