Herausforderung Gesundheitsdaten

Schutz der Gesundheitsdaten als Herausforderung

Datenschutz findet im Gesundheitsbereich grundsätzlich eine ideale Ausgangslage vor: Fast allen ist der hohe Schutzbedarf von Gesundheitsdaten bewusst. Die komplexe Organisation des Gesundheitswesens mit den vielen unterschiedlich strukturierten Akteuren stellen die Verantwortlichen jedoch vor grosse Herausforderungen. Das datenschutzrechtliche Fachwissen in den Gesundheitseinrichtungen wächst kontinuierlich. Der Dialog des Datenschutzbeauftragten mit den Akteuren im Gesundheitsbereich führt zur konstruktiven und praxisnahen Lösungsfindung.

Der Datenschutzbeauftragte begleitete die Einführung des Elektronischen Patientendossiers im Universitätsspital Zürich. In Bezug auf die Klinikinformationssysteme (KIS) hat der Datenschutzbeauftragte seinen engen Austausch mit den Spitälern fortgeführt. Besonders im Fokus standen die Dauer der Aufbewahrung für Gesundheitsdaten und der Umgang mit den Daten nach Ablauf der Aufbewahrungsfristen. Oft sehen die KIS keine Löschung vor.

Der Datenschutzbeauftragte erhielt zahlreiche Anfragen zu Datenlecks im Gesundheitsbereich. Einen weiteren Schwerpunkt bildeten Beratungen dazu, wie das Einsichtsrecht in Patientendokumentationen wahrgenommen werden kann. Zusätzlich interessieren sich Patientinnen und Patienten dafür, welche Personen im Spitalalltag auf ihre Patientendokumentationen zugreifen können.

Die technologischen Entwicklungen im medizinischen Bereich stellen etablierte Herangehensweisen infrage, auch im Bereich des Datenschutzes. So stellt sich die Grundsatzfrage nach der Anonymisierungsmöglichkeit von genetischen Daten, aber auch von Daten in der personalisierten Medizin.

Im Hinblick auf die künftigen Entwicklungen ist der fachliche Austausch mit den Forschenden wichtig. Der Datenschutzbeauftragte begleitete 2019 mehrere Forschungsprojekte zu unterschiedlichen Themen wie Emotionsanalyse in Tweets, Altersvorsorge, Arbeitsmarktbeobachtung und Durchimpfungsraten. Bei den forschenden Institutionen sind ein hohes Bewusstsein für den Schutz der Privatsphäre sowie datenschutzrechtliches Grundwissen vorhanden. Sie fragten vor allem nach Beratungen zur praktischen Umsetzung der gesetzlichen Anforderungen, gerade auch im Hinblick auf den Einsatz von technischen Mitteln wie Umfrageplattformen und Datenaustauschlösungen.

Die interdisziplinäre Zusammenarbeit der Fachpersonen aus den Bereichen Recht und Informationssicherheit ermöglicht dem Datenschutzbeauftragten die kompetente Beratung im Gesundheitsbereich.

Nie im Spital und trotzdem registriert

Der Datenschutzbeauftragte beriet eine Institution im Gesundheitswesen beim Umgang mit behandlungswilligen Personen, die ihre Meinung über einen Klinikeintritt kurzfristig änderten. Gerade bei psychischen Erkrankungen kann ein stationärer Aufenthalt mit der Angst vor Stigmatisierung verbunden sein. Es kommt daher vor, dass sich Patienten nach erfolgter Überweisung oder Anmeldung doch gegen einen Klinikeintritt entscheiden.

Bei Überweisungen durch vorbehandelnde Ärzte sind in solchen Fällen bereits medizinische Angaben zur Patientin oder zum Patienten vorhanden. Auch bei Selbsteinweisungen können vorgängig telefonische Beratungsgespräche geführt worden sein, die der medizinischen Dokumentationspflicht unterliegen. Patientendokumentationen sind gemäss gesetzlicher Regelung mindestens zehn Jahre aufzubewahren. Eine Person, die sich gegen einen Klinikeintritt entscheidet, mag aber ein Interesse an der Löschung von Einträgen haben, die sie als stigmatisierend empfindet.

Der Datenschutzbeauftragte riet der Institution, bei informellen oder rein administrativen Anfragen zunächst auf eine Erfassung im Klinikinformationssystem (KIS) zu verzichten. Sobald ein medizinisches Vorgespräch stattgefunden hat, ist dies im KIS zu dokumentieren. Ebenfalls aufzunehmen sind allfällige Unterlagen, die im Rahmen einer Überweisung übermittelt wurden. Diese Informationen sind gemäss der gesetzlichen Dokumentationspflicht aufzubewahren, selbst wenn die Behandlung vor Klinikeintritt abgebrochen wird.

Die Zusammenarbeit der Aufsichtsinstanzen verlief bei dieser Beratung sehr gut. Der Datenschutzbeauftragte konnte in dieser Sache in enger Absprache mit der Gesundheitsdirektion beraten.

Sicherheitsprüfung des Krebsregisters

Der Datenschutzbeauftragte wurde eingeladen, das Informationssicherheits- und Datenschutzkonzept des Krebsregisters Zürich zu prüfen.

Das Krebsregister entstand bereits 1980. Inzwischen wird es vom Institut für Sozial- und Präventivmedizin betrieben mit einem Leistungsauftrag der Kantone Zürich und Zug. Es ist in die Informatikstruktur des Universitätsspitals Zürich integriert und dem Informationssicherheits-Managementsystem (ISMS) unterstellt. Die Datensammlung für das Krebsregister erfolgte bislang auf freiwilliger Basis durch Ärzte, Pathologen und Spitäler. Die Daten werden personalisiert erhoben.

Ab 1. Januar 2020 sind das Bundesgesetz sowie die Verordnung in Kraft getreten, wodurch die Erfassung von Krebserkrankungen in der ganzen Schweiz und somit auch in den kantonalen Krebsregistern obligatorisch wird. Die Registrierung geschieht auch künftig über das bestehende dezentrale System. Die nationale Krebsregistrierungsstelle führt die Daten anschliessend zusammen und arbeitet sie auf. Ärztinnen und Ärzte müssen ihre Patientinnen und Patienten mündlich und schriftlich über ihre Rechte, den Datenschutz und über Art, Zweck und Umfang der Datenbearbeitung informieren. Patientinnen und Patienten können der Registrierung ihrer Daten jederzeit widersprechen.

Da es sich bei diesen Daten um höchst sensitive Personendaten handelt, berät der Datenschutzbeauftragte das Krebsregister Zürich auch in Zukunft, um die entsprechenden Anforderungen bei der Informationssicherheit und beim Datenschutz sicherzustellen.

Revision des Spital-planungs- und -finan-zierungsgesetzes

Der Datenschutzbeauftragte nahm Stellung im Rahmen der Vernehmlassung zur Revision des Spitalplanungs- und -finanzierungsgesetzes (SPFG). Die Revision beinhaltet die Aufnahme von zusätzlichen qualitativen Anforderungen an die Leistungserbringer. Damit soll der Regierungsrat mit den Leistungsaufträgen verbundene Anforderungen festlegen, beispielsweise zum Qualitätscontrolling. Der Datenschutzbeauftragte hat vorgeschlagen, dass nicht nur Vorgaben zum Qualitätscontrolling, sondern auch zum Datenschutz und zur Informationssicherheit festgehalten werden. Die Gesundheitsdirektion teilt diese Ansicht.

Spitäler sollen über die Spitalliste stärker auf ihre Pflichten zur Wahrung des Datenschutzes und der Informationssicherheit hingewiesen werden und zum Aufbau und zur Pflege von Managementsystemen verpflichtet werden, beispielsweise in Form eines Informationssicherheits-Managementsystems (ISMS). Der Datenschutzbeauftragte hielt als Anforderungskatalog für Datenschutz und Informationssicherheit zur Ergänzung im Spitallistenanhang fest:

- Es ist ein Managementsystem für Datenschutz und Informationssicherheit vorhanden und dokumentiert.
- Die Verantwortungen für Datenschutz und für Informationssicherheit sind geregelt.
- Die Verantwortlichen für Datenschutz und für Informationssicherheit sind für ihre Aufgaben geschult und verfügen über die notwendigen Ressourcen und Kompetenzen.
- Die Verantwortlichen für Datenschutz und für Informationssicherheit sind in die wesentlichen Informations- und Datenbearbeitungsprozesse und in die wesentlichen Projekte einbezogen. Die Art und Weise des Einbezugs ist in den Betriebsprozessen und im Projektmanagement geregelt.
- Die Managementsysteme für Datenschutz und Informationssicherheit werden in einem kontinuierlichen PDCA-Zyklus laufend verbessert (PDCA: Plan, Do, Check, Act).
- Die Schnittstellen und Abgrenzungen von Risikomanagement, Qualitätsmanagement und Compliance zum Datenschutz- und Informationssicherheitsmanagement sind geregelt.

Der Datenschutzbeauftragte erarbeitet einen Vorschlag für einen neuen Abschnitt über den Datenschutz und die Informationssicherheit (Datenschutz-Managementsystem) und die entsprechenden Mindestanforderungen an die Spitäler für den vollständig überarbeiteten Spitallistenanhang «Generelle Anforderungen».

Änderung des DNA-Profil-Gesetzes

Der Datenschutzbeauftragte nahm Stellung zur Änderung des Bundesgesetzes über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (DNA-Profil-Gesetz). Er kam zum Schluss, dass das neu eingeführte Verfahren zur Feststellung äusserlich sichtbarer Merkmale einer Person (Phänotypisierung) und der erweiterte Suchlauf mit Verwandtschaftsbezug (Verwandtenrecherche) hohe Anforderungen an die gesetzliche Grundlage stellen und beurteilte die Vorlage mit einigen Vorbehalten als angemessen.

Bei der Verwandtenrecherche wird in der Datenbank nach Personen gesucht, die mit der Spurgeberin oder dem Spurgeber am Tatort verwandt sein könnten. Sie ist eine Bearbeitung von sensitiven Personendaten und stellt einen starken Eingriff in die Persönlichkeitsrechte dar. Der Datenschutzbeauftragte wies darauf hin, dass keine der bisher durchgeführten Verwandtenrecherchen zu einem Ermittlungserfolg geführt hat. Deshalb beurteilte er sie als nicht ohne weiteres verhältnismässig. Weiter wies er darauf hin, dass besondere Anforderungen zu stellen sind an die Bestimmtheit der gesetzlichen Grundlage für die Bearbeitung sensitiver Personendaten. Der Datenschutzbeauftragte erachtet die Umschreibung des Gesetzeszwecks als zu wenig bestimmt und fordert eine Präzisierung.

Der Datenschutzbeauftragte wies darauf hin, dass auch die Phänotypisierung ein schwerer Eingriff in die Persönlichkeitsrechte der betroffenen Personen darstellt. Er stellte fest, dass nur die subsidiäre Anwendung dieser Massnahme verhältnismässig ist, und forderte, diese ausdrücklich im Gesetz zu regeln.

Der Datenschutzbeauftragte begrüsste, dass die Verwandtenrecherche wie auch die Phänotypisierung ausschliesslich bei Verbrechen angewandt wird. Er forderte jedoch eine Verschärfung dieser Regelung. Beide Massnahmen sollten nur bei schweren Verbrechen eingesetzt werden, für die ein Deliktskatalog zu erstellen ist. Der Datenschutzbeauftragte verlangte, dass beide Massnahmen durch das Zwangsmassnahmengericht angeordnet werden sollen, wie dies bereits heute für Massenuntersuchungen gilt.