Sichere Daten und persönliche Integrität: Die HINT AG macht sich stark für den Datenschutz im Gesundheitswesen

Datenschutz geht alle an

Datensicherheit und Datenklau füllen haufenweise Gazetten und sind heisse Themen für die Medien. Die Folgen können verheerend sein. Betroffen sind Institutionen und Privatpersonen. Im Gesundheitswesen ist eine besonders grosse Menge sensibler Daten vorhanden, das Bewusstsein bezüglich der Gefahren aber noch gering. Experten zeigten an der erstklassig besuchten Tagung in Aarau, dass gezielte Massnahmen eine gute Investition darstellen.

Urs Achermann, Security Officer HINT AG, brachte es auf den Punkt: «Eines ist allen Branchen gemein: Niemand hat so richtig Freude am Datenschutz, ausser den Security Officers. Gerade im Gesundheitswesen ist das Problem aber offensichtlich. Vorbeugen ist entscheidend.» Der Experte zeigte Beispiele: Passwörter werden als Hindernis empfunden und nicht als Zugriffsschutz gesehen. Und wenn schon Passwort, dann wünschen viele User Gruppen-Accounts: «Da ist allerdings keine lückenlose Nachverfolgung möglich, es bleibt oft ein Rätsel, wer Daten eingesehen und wer sie verändert hat.»

Auch auf Seiten von Software-Lieferanten zeigen sich Sicherheitslücken. Oft fehle hier das Verständnis für einen angemessenen Umgang mit sensiblen Daten. So bitte man etwa um Übermittlung kompletter Datensätze, um eine Fehleranalyse vornehmen zu können. «Aber das kann der Anfang einer Kette von Lecks sein», argumentierte Achermann. Denn plötzlich befinden sich heikle Daten auf einem Notebook, welches ein Mitarbeitender einer Softwarefirma mit nach Hause nimmt. Dort haben bereits mehr Menschen Einblick, die Daten bleiben auf dem Notebook, der wird später via Ebay verkauft und schon ist der theoretische Kreis von Mitwissern viel zu gross. «Wenn ich mir die Folgen vorstelle, kriege ich Bauchschmerzen. Es ist dringend nötig, dass die Verantwortlichen einer Institution ihre Lieferanten auf diese Gefahren aufmerksam machen und für ausreichenden Schutz der Daten sorgen» erklärt Achermann weiter.

Viel Geld für Medizintechnik – und für den Datenschutz?

Für Investitionen in die Medizintechnik würde sehr viel Geld aufgewendet, führte Achermann aus, «aber wie sieht es nur schon beim Basisschutz der IT aus? Es sind vielerorts auch keine Datenschutzverantwortlichen auszumachen. Zudem finde ich, der Druck von aussen nach mehr Sicherheit ist zu gering, es wird kaum Rechenschaft verlangt. Es besteht ein schlecht ausgeprägtes Sicherheits-Bewusstsein.» – Nun gäbe es drei mögliche Reaktionen: ärgern, akzeptieren oder agieren. «Ich bin eindeutig fürs Dritte. Bringen wir Licht ins Dunkel!»

Dieser Meinung schloss sich auch lic. iur. Judith Naef, Rechtsanwältin, BWL ZS (Judith Naef Rechtsanwälte AG, Baar und Zürich) an. Sie ging auf die unterschiedlichen Arten von Daten ein: allgemeine Informationen, Personendaten (z.B. von Mitarbeitenden im Spital oder Heim, von zuweisenden ÄrztInnen und von Patienten) und besondere Personendaten (z.B. medizinische Daten). Es geht um Tatsachen und Werturteile über bestimmte oder bestimmbare Personen («der Beinbruch auf Zimmer 320»). Die Daten können auf Papier, digital oder auf Datenträgern gespeichert vorkommen: in Sprache, Bild, Zeichen, Ton oder als Teil einer Tabelle, deren Inhalt mit Personen verknüpft ist.

Es geht um Menschen, nicht «nur» um Daten

«Beim Datenschutz geht es um die Menschen», betonte die Juristin, «er ist nie Selbstzweck, sondern Mittel zum Schutz der Persönlichkeit der PatientInnen. Der Persönlichkeitsschutz in Institutionen des Gesundheitswesens muss aber weiter gehen: Die Betriebe müssen umfassend die körperliche, seelische und geistige Integrität der Patienten als Ganzes schützen.» – Der Umfang der besonders sensiblen Personendaten in Spitälern

Der Datenklau geht um: Klug ist, wer sich gründlich davor schützt.

und Heimen ist riesig: Es geht etwa um die Daten über den Gesundheitszustand der Patienten, um Details aus ihrem Privat- und Intimleben, ihre religiösen und politischen Überzeugungen, die ethnische Zugehörigkeit und Sozialhilfedaten. Im Spital werden aber auch Personendaten von Mitarbeitenden und externen Personen entlang des Behandlungspfades (wie Ärztinnen und Therapeuten) oder von Netzwerkpartnern (z.B. verbundene Firmen und deren Exponenten) bearbeitet.

Die Rechtsgrundlagen, die Schutz bieten, sind in der Schweiz föderalistisch aufgebaut. Auf eidgenössischer Ebene besteht das Bundesgesetz über den Datenschutz mit zugehörigen Verordnungen, welche für Bundesbehörden und Private gelten. Jeder Kanton hat zusätzlich eigene Regelungen, welche für die Behörden des entsprechenden Kantons und alle Privaten gelten, welche eine kantonale, öffentliche Aufgabe wahrnehmen. Darunter fallen fast alle Institutionen des Gesundheitswesens. «Der Datenschutz betrifft jeden Umgang mit persönlichen Daten», bekräftigte Judith Naef, «sei es beim Beschaffen, Aufbewahren, Verwenden, Bearbeiten, Bekanntgeben, Archivieren oder schliesslich Vernichten von Daten.» Beispiele des Umgangs mit Daten sind etwa Personaldossiers, Rechnungen an Patienten, Studienresultate und natürlich in grossem Ausmass Daten bildgebender Verfahren und der Patientendokumentation.

Klare Grundsätze beachten

«Bei der vielfältigen Datennutzung sind klare Grundsätze zu beachten», hielt Judith Naef fest. Dazu gehören:

- die Rechtmässigkeit: Nur mit Einwilligung der Betroffenen oder aufgrund gesetzlicher Regelungen dürfen Daten verwendet werden.
- die Zweckbindung: Daten dürfen nur für diejenigen Zwecke gebraucht werden, für die sie erhoben wurden.
- Verhältnismässigkeit: Nur was nötig ist, was geeignet und erforderlich ist für die zu erfüllende Arbeit darf erfasst oder Dritten weitergegeben werden (etwa nachbehandelnden Ärzten, Physio- oder Ergotherapeuten).
- Weitere Merkmale sind Richtigkeit, Qualität und Integrität der Daten.
- Dabei gilt es organisatorische und technische Massnahmen zur Datensicherheit zu treffen (Schutz vor unberechtigtem Zugriff).
- Transparenz und Einsicht müssen für die Betroffenen jederzeit sichergestellt sein.
- Schliesslich ist die Verantwortung für die korrekte Datenbearbeitung zu nennen. Dafür müssen alle Mitarbeitenden einer Institution selber sorgen: Jede/r ist dafür verantwortlich.

Das Vertrauensverhältnis Arzt-Patient schützen

Besonders schützenswert ist natürlich das Patientengeheimnis. Das sei, so Naef, nicht immer so einfach zu handhaben, weil diverse Daten an unterschiedlichen Orten vorhanden und gespeichert seien. «Datenbearbeitung ist nur soweit erlaubt, als dies die oben genannten Grundsätze zulassen. Auf keinen Fall dürfen Daten ohne Wissen der Betroffenen umgenutzt, d.h. für andere als die bei der Erhebung angegebenen Zwecke eingesetzt werden. Das Vertrauensverhältnis zwischen Arzt und Patient ist im Besonderen strikte zu respektieren. Und auch hier gilt: Weil der Arzt sehr viel Persönliches von seinen Patienten erfährt, besteht ein enorm hohes Schutzbedürfnis.»

Das Patientengeheimnis, auch Berufsgeheimnis genannt, wird insbesondere im Strafgesetzbuch, im Zivilgesetzbuch, in der Strafprozessordnung und in diversen Spezialgesetzen wie dem Epidemiegesetz geregelt. Die Kantone haben entsprechende Regelungen in ihren Gesundheitsgesetzen und/oder Patientengesetzen geschaffen. Wie ein roter Faden zieht sich hier ein entscheidender Punkt durch: Betroffene müssen jederzeit Einsicht in ihre persönlichen Daten nehmen können, wo und wie auch immer diese aufbewahrt werden. Bei objektiv falschen Informationen haben die Betroffenen ein Recht auf Korrektur. Sie können zudem das Vernichten der Daten verlangen, wenn diese objektiverweise nicht mehr benötigt werden. Eine Ausnahme bilden lediglich allfällige gesetzliche Aufbewahrungspflichten für eine bestimmte Zeitdauer.

Die Schweigepflicht

Ausfluss des Berufsgeheimnisses ist die Pflicht, über alle Patientendaten zu schweigen. Ärzte und auch die von ihnen beauftsichtigen oder beauftragten Hilfspersonen haben sich kompromisslos danach zu richten. Sie dürfen keinerlei Geheimnisse offenbaren. Bei Zuwiderhandlung drohen auf Antrag bis zu drei Jahre Freiheitsstrafe oder Geldstrafen. Eine Weitergabe von Informationen ist grundsätzlich ausschliesslich mit Einwilligung der Betroffenen erlaubt. Ausnahmen kann das Gesetz regeln, etwa im Falle einer Nichtansprechbarkeit von Patienten. Hier ist es denkbar, dass Angehörige direkt informiert werden können oder sogar müssen. Eine weitere Ausnahme ist die gesetzliche Pflicht zur Weitergabe von klar eingegrenzten Informationen, beispielsweise im Falle von Epidemien zum Schutz der Bevölkerung oder im Rahmen der Rechnungsstellung an die Krankenversicherungen.

PatientInnen dürfen selbstverständlich Informationen für einen anderen Gebrauch als den ursprünglichen freigeben, sofern ihnen der Zweck der Weiterverwendung eindeutig und umfassend kommuniziert worden ist. Das kann z.B. auf Forschungszwecke oder Marketingprojekte zutreffen.

Vertretungsberechtigte Personen

Spezielle Fragen stellen sich bei urteilsunfähigen, nicht mehr ansprechbaren Patienten wie z.B. bewusstlose oder demente Personen. Welche Daten dürfen an vertretungsberechtigte Personen weitergegeben werden? Sofern vorhanden und bekannt, gilt in erster Linie eine Patientenverfügung. Ist bereits ein Beistand ernannt, so ist die weitere Behandlung mit diesem zu besprechen und seine Entscheide sind zu berücksichtigen. An dritter Stelle ist der Ehegatte Ansprechpartner. Weiter in Frage kommen können im selben Haushalt Wohnende, Nachkommen, Eltern oder Geschwister, sofern sie regelmässige Kontakte mit dem betroffenen Patienten pflegen und ihm regelmässig Beistand geleistet haben.

Davon abzugrenzen ist die Erteilung von Auskünften an nachbehandelnde Personen wie ÄrztInnen und Therapeuten. Sie dürfen nur im Rahmen des zur Therapie Nötigen gegeben werden. Kranken- und Unfallversicherer haben im Rahmen des Versicherungsobligatoriums ein eingeschränktes Einsichtsrecht. Bei privaten Versicherern gilt aber immer und unmissverständlich: Daten über den

Patienten können nur mit seiner ausdrücklichen Einwilligung weitergeleitet werden.

Bald spruchreif: das ePatientendossier

Neue Perspektiven öffnet das schweizweit geplante elektronische Patientendossier. Es soll einen schnellen, sicheren Datenzugang zu freigegebenen Patientendaten ermöglichen, welche für eine Verbesserung von Behandlungsprozessen, speziell zur Effizienzsteigerung, und für eine Erhöhung der Qualität der Leistungserbringung sinnvoll sind. Es handelt sich dabei um eine virtuelle Datensammlung, die dezentral bei den primären Leistungserbringern gespeichert ist und die dort über einen gesicherten Transfer abgefragt werden können. «Weil der Zugriff auf primäre Systeme erfolgt, kommt dem durchgängigen Datenschutz höchste Priorität zu», stellte Judith Naef fest. 2015 berät der Nationalrat als Zweitrat das Geschäft, frühestens 2017 dürfte das Gesetz in Kraft treten. Nach einer Übergangsfrist von fünf Jahren müssen alle Spitäler und weitere stationäre Leistungserbringer einer Gemeinschaft für das ePatientendossier angeschlossen sein, die auf regionaler Ebene die Vernetzung und den Datentransfer von und zu den Primärsystemen sicherstellt.

Der Bund betreibt die zentrale technische Plattform und legt organisatorische und technische Mindestanforderungen fest. Er regelt im Weiteren die Zertifizierung und die Zugriffsrechte der zu bildenden Gemeinschaften. Patienten und freipraktizierende ÄrztInnen können sich freiwillig diesem Regime unterstellen. Stationäre Leistungserbringer müssen mitmachen. Wer als Privatperson freiwillig mit dabei ist, etwa um im Notfall die Möglichkeit eines raschen Zugriffs auf überlebenswichtige Daten zu geben, kann klar definierte Berechtigungen vergeben und den Zugriff auf verschiedene Kategorien, insbesondere auf allenfalls stigmatisierende Informationen sehr selektiv handhaben. Er kann z.B. nur den Eintrag bestimmter ausgewählter Daten vorsehen. Jeder Zugriff wird automatisch protokolliert werden. «Die lückenlose Rückverfolgbarkeit ist ein tragendes Element», unterstrich Judith Naef. Für höchstmögliche Sicherheit sorgt eine spezielle Identifikationsnummer. Nur mit ihr sind ein Abfragen der Daten oder das Auffüllen des Dossiers möglich.

Datenschutz in der kantonalen Praxis

Der Schutz der Persönlichkeit ist nichts Theoretisches. Er muss dauernd vor Ort praktiziert werden. Lic.iur. Roger Lehner, Rechtsanwalt im Departement Gesundheit und Soziales (DGS) des Kantons Aargau, zeigte die Fakten, die den (juristischen) Alltag bestimmen. Fachleute im

Kompetente Referenten zeigten exakt, worauf es ankommt

lic. iur. Judith Naef

Rechtsanwältin, BWL ZS
Judith Naef Rechtsanwälte AG

Beratung und Vertretung von Institutionen des Gesundheitswesens und von Behörden

Patienten-, Arzt- und Pflegerecht, Datenschutz-, Submissions- und Personalrecht, Vertragsrecht, Projektmanagement und -beratung

- Seit 2006 selbständige Rechtsanwältin in Baar und Zürich
- 2000–2006 Leitung Rechtsabteilung Universitätsspital Zürich
- 1995–1999 Adjunktin Gesundheits- und Umweltdepartement der Stadt Zürich

lic. iur. Roger Lehner, Rechtsanwalt

Departement Gesundheit und Soziales, Kanton Aargau, Generalsekretariat

Fachspezialist im Rechtsdienst des Departements Gesundheit und Soziales (DGS)

- Seit 2008 Departement Gesundheit und Soziales, Rechtsdienst
- 2008 Anwaltspatent Kanton Aargau
- 2006–2007 Rechtspraktikum in Anwaltskanzlei und im Departement Finanzen und Ressourcen des Kantons Aargau
- 2000–2005 Studium der Rechtswissenschaften an den Universitäten Basel und Bern

Urs Achermann

Chief Information Security Officer, HINT AG

Dipl. Wirtschaftsinformatiker,
Master in Informationssicherheit
Certified ISO 27001 Lead Auditor,
ITIL Certified

- Seit 2013 Chief Information Security Officer, HINT AG
- 2011–2013 Information Security Officer, Bank Julius Bär
- 2006–2011 Information Security Officer, Holcim
- Seit 1999 spezialisiert auf IT- und Informationssicherheit, tätig als Berater, Hacker, Auditor und Sicherheitsverantwortlicher
- Seit 1993 in der Informatik tätig

DGS beschäftigen sich intensiv mit der Beratung der Leistungserbringer, des Departements selber, anderer Behörden und Privatpersonen, vielfach in Abstimmung mit der kantonalen Datenschützerin. Spezielle Aspekte werden im medizinischen Datenschutz beleuchtet; hier stehen die Patientenrechte im Zentrum. Die meisten behandelten Fälle betreffen das Abklären einer Entbindung von der beruflichen Schweigepflicht (Arzt-Patienten-Geheimnis). Schliesslich gibt es Rechtsetzungs-Projekte, aktuell ganz besonders im Rahmen von eHealth.

Die wichtigste gesetzliche Grundlage im Kanton Aargau ist das Gesetz über die Information der Öffentlichkeit, des Datenschutzes und des Archivwesens (IDAG). Die bedeutendsten Elemente werden in §8 (Bekanntgabe von schützenswerten Daten) und §12 (Datensicherheit aus organisatorischer und technischer Sicht) geregelt. Im letztgenannten Paragraphen geht es um die Zweckbindung und das Prinzip der Datenvermeidung und -sparsamkeit, vor allem beim Einsatz von IT-Systemen. Bewusst werden neutrale Formulierungen verwendet. Das Gesetz soll mit dem Fortschreiten des technischen Wandels Schritt halten können.

eHealth – der Aargau geht voran

Viele Aufgaben stammen zur Zeit aus dem aktuellen eHealth-Programm des Kantons. Er ist seit 2010 auf diesem Gebiet aktiv und setzt sich im Rahmen der Entwicklung des elektronischen Patientendossiers für einen gut vorbereiteten Start ein. «Es bestehen zwar keine Vollzugsaufgaben für die Kantone», erläuterte Roger Lehner, «aber es gibt eine Verpflichtung der stationären Leistungserbringer. Hier müssen wir die Zertifizierungsvoraussetzungen für den Datenschutz regeln. Es geht auch um die Identifikation von Fachpersonen und Patienten, um Authentifizierung, Berechtigungen und Rollenkonzepte. Wir tun das mit Mitteln des Kantons, die ihrerseits wiederum eine befristete Bundeshilfe auslösen. Die Finanzierung erfolgt auf diese Weise 1:1.»

Roger Lehners Anliegen ist ausserdem die Motivation der ambulanten Leistungserbringer zum Mitmachen beim ePatientendossier, damit ein möglichst breiter Nutzen entsteht. Die Trägerschaft, die für das bedeutende Projekt im Kanton die künftige eHealth-Gemeinschaft aufbauen soll, heisst Verein eHealth Aargau. «Sie hat ihre Arbeit bereits aufgenommen», berichtete Lehner, «und bezweckt einen Konsens zwischen Leistungserbringern und Kanton zu schaffen und die Aufgaben des Ende 2015 auslaufenden kantonalen eHealth-Programms zu übernehmen.»

Seminar «Datenschutz im Gesundheitswesen»

Viele Institutionen im Gesundheitswesen sind sich im Unklaren darüber, was es in Bezug auf die Sicherheit und den Schutz der Daten zu beachten gilt. Erfahren Sie im Rahmen eines umfassenden und praxisnahen Seminars alles Wissenswerte über die verschiedenen Aspekte des Datenschutzes im Gesundheitswesen und stellen Sie ihre eigenen kritischen Fragen.

Programm

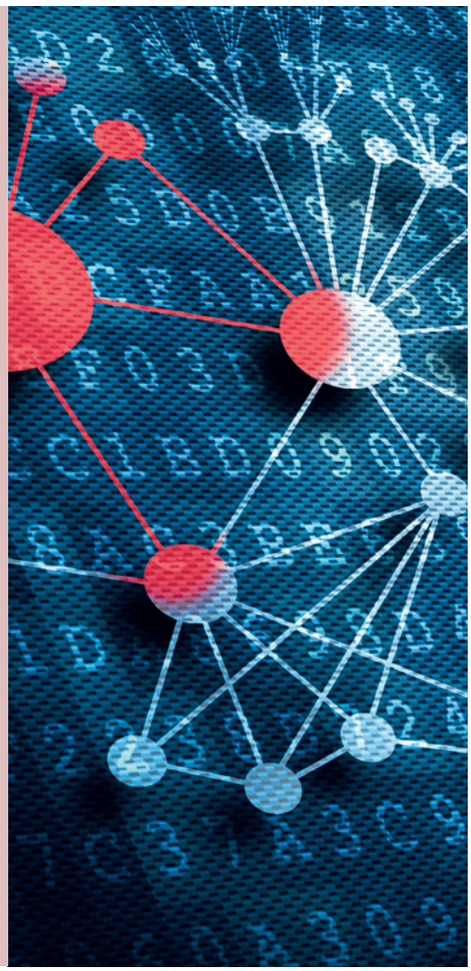
- Einführung in die Grundsätze des Datenschutzes
- Datenschutz in der klinischen Praxis
- Aktuelles zum Datenschutz aus der Gesundheitsdirektion des Kantons Aargau
- Fallbearbeitung
- Datensicherheit und IT-Hilfsmittel
- Datenschutz und Finanzen

Ort und Zeit

HINT AG, Lenzburg,
13.01.2015, 08.30–16.30 Uhr

Anmeldung

Unter www.hintag.ch oder
per E-Mail an events@hintag.ch



Konkret geht es um die Umsetzung des Zugriffs auf die sog. behandlungsrelevanten Daten – «wobei es», so der Rechtsanwalt, «interessant sein wird zu schauen, wie der Bund diese exakt definiert.» Technisch wird dabei über ein Repository Zugriff auf dezentral gelagerte Daten in Primärsystemen genommen. Zugriff haben die Patienten resp. Versicherten und alle berechtigten Fachpersonen innerhalb des Behandlungspfads. Die unmissverständlich eindeutige Identifikation des Patienten wird durch seine ID-Nummer resp. den Master Patient Index sichergestellt.

Viel Zustimmung fürs Projekt

Im Aargau herrscht Aufbruchstimmung. So hat der Grosse Rat unlängst mit einem 129:0-Entscheid grünes Licht für eHealth Aargau gegeben. Eine entsprechende Anpassung des IDAG tritt am 1. Juli 2015 in Kraft. Im befristeten eHealth-Projekt fungiert das DGS als Koordinator und Motivator. Roger Lehner: «Wir wollen Erfahrungen sammeln und suchen die intensive Zusammenarbeit mit den Leistungserbringern. Aus case studies erwarten wir Rückschlüsse, wie der Nutzen künftig zu optimieren ist. Dabei gilt es die verschiedenen Interessen der Beteiligten innerhalb des Ökosystems eHealth zu berücksichtigen: BürgerInnen, Leistungsbestimmer (Behörden), Industrie, Leistungserbringer und Versicherer.»

Bereits laufen spannende Pilotprojekte: Einerseits das Zuweisermanagement der Kantonsspitäler Aarau und Baden sowie des Spitals Zofingen, andererseits das Projekt eRezept des Aargauischen Apothekerverbands mit Argomed. Auf die Ergebnisse können wir gespannt sein. Wir werden weiter darüber berichten.

Weiter am Ball dürften auch etliche der zahlreichen TeilnehmerInnen am Info-Anlass der HINT AG bleiben. Sie haben bereits wieder am Dienstag, 13. Januar 2015 beste Gelegenheit dazu. An diesem Tag veranstaltet die HINT AG mit den am Info-Anlass aufgetretenen Experten ein ganztägiges Seminar in Lenzburg. Details dazu präsentieren wir im nebenstehenden Kasten.

Text: Dr. Hans Balmer