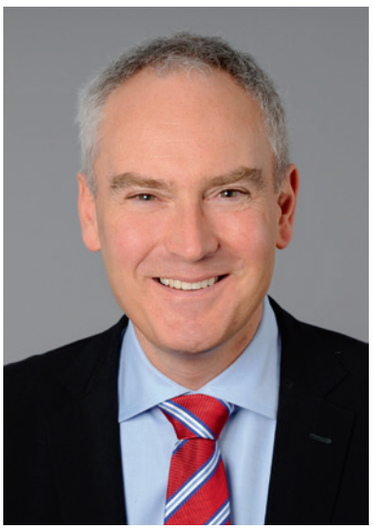
Datensicherheit und Datenschutz

«Das Konsil am Strand» – die Mobilität der Daten

Datensicherheit und Datenschutz haben im Schweizer Gesundheitswesen einen hohen Stellenwert. Täglich fallen hochsensible Daten an, die schnell, einfach aber auch sicher genutzt werden müssen. Accessability, Usability, Simplicity und Productivity sind Schlüsselbegriffe in diesem Kontext. Lassen sich diese Ansprüche in Einklang bringen? Oder bestehen gar unlösbare Zielkonflikte? Wie interagiert der Mensch mit der Technik, was wird uns die Technologie bringen und mit welchen gesetzgeberischen Anforderungen sind und werden wir in Zukunft möglicherweise konfrontiert? Wie gehen wir mit unserer Ambivalenz um, wenn wir auf Widersprüche stossen? Logicare beschäftigt sich täglich mit diesem bunten Strauss an Fragen – in der Praxis und auf der konzeptionellen Ebene.



Tobias Diener ist Geschäftsführer der Logicare AG. Nach seinem Studium der Volkswirtschaft an der Universität Zürich und einer Zweitausbildung zum Wirtschaftsinformatiker war er bei namhaften Beratungsunternehmen und als CIO in einem global aktiven Industrieunternehmen tätig. Er ist spezialisiert auf die Bereiche Prozess- und IT-Entwicklung im Schweizer Gesundheitswesen.

Datensicherheit und Datenschutz sind zwei Themen, die seit geraumer Zeit intensiv und kontrovers diskutiert werden. Die sachliche Auseinandersetzung wird bisweilen überlagert durch hysterisch anmutende Reaktionen auf der einen Seite und eine larmoyante Haltung auf der anderen Seite. Fest steht, dass sich verschiedene Anspruchsgruppen mit zum Teil divergierenden Interessen zu einem Konsens finden müssen. Und auch die Technik, das heisst die IT, muss in Einklang mit der Datensicherheit und dem Datenschutz gebracht werden. Vorweg gilt es aber festzuhalten, dass nicht die Technik das Mass aller Dinge ist: Der Mensch steht im Zentrum. Betrachten wir diesen komplexen Frage- und Anforderungskatalog nüchtern und mit der notwendigen Distanz, können wir feststellen: Es gibt noch viele unbeantwortete Fragen. Diese beziehen sich gleichermassen auf die eingesetzte Technik und etablierte Arbeitsprozesse, vor allem aber auch auf das Verhalten der involvierten Personen. Wir können jedoch gleichzeitig auch feststellen, dass Datensicherheit und Datenschutz – da nicht per se neue Themen – auf einem soliden Fundament aufbauen. Es braucht also nicht bis in die äussersten Verästelungen dieses Themenbaums Grundsatzdiskussionen und neu zu erfindende Ansätze. Die Bausteine des Fundaments sind grob zusammengefasst gesetzliche Regelungen, Gesetzesentwürfe, Verhaltens- und Prozessbeschriebe, technische Standards und Kontrollmechanismen (Audits). Es gibt also einen seriösen Fundus an (Experten-)Wissen.

«Need to know»: Wer muss Zugriff haben?

Die Diskussion über Datensicherheit und Datenschutz lässt sich exemplarisch gut am Fragekomplex rund um das elektronische Patientendossier aufhängen. Was hier diskutiert und voraussichtlich definiert wird, hat eine Strahlkraft auf weite Bereiche des Gesundheitswesens und den Umgang mit Datensicherheit und Datenschutz.

Zunächst müssen wir aber zwei Begriffe voneinander abgrenzen: die Krankengeschichte (KG) und das elektronische Patientendossier. Die KG umfasst die vollständige medizinische Dokumentation einer bestimmten Person. Das elektronische Patientendossier ist eine ad hoc-Zusammenstellung derjenigen Daten, welche für die Behandlung zu einem bestimmten Zeitpunkt durch eine Fachperson relevant sind. Das elektronische Patientendossier ist also eine Teilmenge der KG. Die Momentaufnahme eines Patientendossiers variiert dementsprechend abhängig von der Rolle der zugreifenden Person (zum Beispiel Arzt, Physiotherapeut, Psychologe). Hier stellt sich die bezüglich Datenschutz relevante Frage nach dem «Need to know»: Wer darf und wer muss Zugriff auf die Daten haben? Wie ist der Zugriff auf die Daten in Abhängigkeit vom Kontext autorisiert und geregelt? Zum Beispiel soll in einer Notfallsituation ein Vollzugriff auf die Daten möglich sein – sofern nicht im Vorfeld eine explizite Zugriffseinschränkung erfolgte. Für eine Therapiemassnahme hingegen sollen nur die hierzu notwendigen Daten eingesehen werden können.

Massnahmen auf Basis des Gesetzesentwurfs antizipieren

Im Entwurf des Bundesgesetzes über das elektronische Patientendossier (EPDG) vom 29. Mai 2013 sind die rechtlichen Voraussetzungen hierzu formuliert. Obwohl die parlamentarische Absegnung dieses Gesetzesentwurfs noch hängig ist und mit einem Inkrafttreten des Gesetzes erst in frühestens zwei Jahren

gerechnet werden kann, lassen sich einige fundamentale Elemente bereits antizipieren, die uns in Zukunft beschäftigen werden. Prima vista handelt es sich hierbei um technische und organisatorische Massnahmen, die sich auf die Datensicherheit und den Datenschutz beziehen. Konkret ist beschrieben, dass grundsätzlich immer eine Einwilligung der Patientin resp. des Patienten zur Erstellung eines elektronischen Patientendossiers vorliegen muss. Zusätzlich wird ein Patientenidentifikationsmerkmal – eine eindeutige und zufällig generierte Patientenidentifikationsnummer – beschrieben: «Der Bundesrat bestimmt die technischen und organisatorischen Massnahmen zur sicheren Ausgabe und Nutzung der Patientenidentifikationsnummer.» (EPDG Art. 4 Abs. 5).

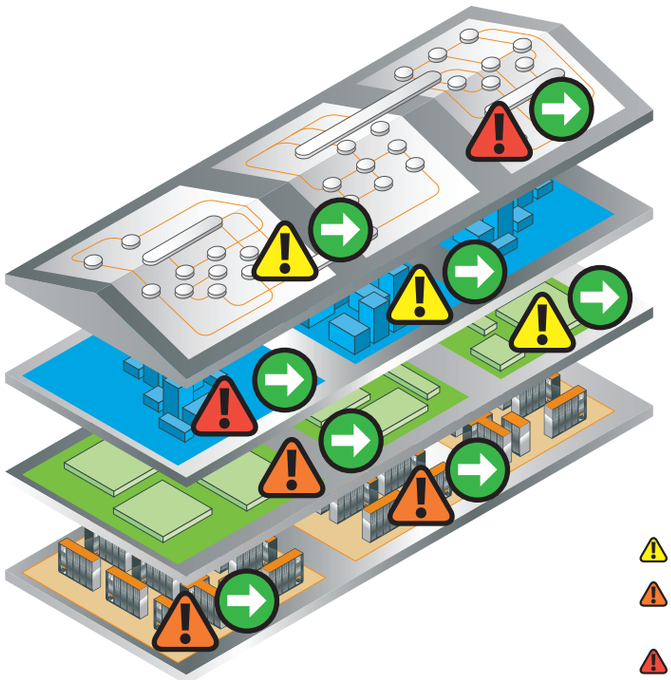
Sichere elektronische Identität

Ebenso ist der Zugriff geregelt: Sowohl Patientinnen und Patienten als auch die Gesundheitsfachpersonen müssen über eine sichere elektronische Identität verfügen. Zudem sollen gesetzliche Grundeinstellungen und Vertraulichkeitsstufen festgelegt werden. Diese – so der Gesetzesentwurf – sollen von der Patientin resp. dem Patienten jederzeit angepasst werden können. Werden in medizinischen Notfallsituationen Daten – auch ohne Zugriffsrechte – eingesehen, muss die Patientin resp. der Patient über den Zugriff informiert werden. Zwei weitere Artikel im Gesetzesentwurf beschäftigen sich mit der Modifikation der Daten und der Zertifizierungspflicht. In Artikel 10, 1b ist definiert, dass «jede Bearbeitung von Daten protokolliert wird» und dass die Protokolldaten zehn Jahre lang aufzubewahren sind. Zudem müssen die organisatorischen Einheiten von der Gesundheitsfachperson und deren Einrichtungen (Gemeinschaft) durch eine anerkannte Stelle zertifiziert sein.

Hier wird der Bundesrat die Zertifizierungsvoraussetzungen noch definieren. Dies wird unter Berücksichtigung internationaler Normen sowie anhand des aktuellen Stands der Technik erfolgen. Noch wenig Konkretes ist im Entwurf des Bundesgesetzes «Elektronisches Patientendossier» über die organisatorischen Voraussetzungen und wie der Datenschutz und die Datensicherheit zu gewährleisten sind zu erfahren. Hier ist derzeit einzig festgehalten, dass der Bundesrat dies festlegt und das Bundesamt für Gesundheit ermächtigt, die Anforderungen dem jeweiligen Stand der Technik anzupassen.

Das Konsil: Leitende Ärztin am Strand

Datenschutz und Datensicherheit beschränken sich im Gesundheitswesen beileibe nicht nur auf das elektronische Patientendossier. Ebenso wenig haben wir es hier mit einer grundsätzlich neuen Diskussion zu tun. So ist beispielsweise die Schweigepflicht im Strafgesetzbuch und im Datenschutzgesetz geregelt. Dennoch hat die Thematik eine neue Dimension, die von der Digitalisierung ausgeht: die Vernetzung und die Mobilität der Daten. Heute ist es schon Gang und Gäbe, dass geografisch weit entfernte Spezialisten zu einer Operation oder einer Diagnose, zum Beispiel via Videokonferenz, zugeschaltet werden. Plakativ ausgedrückt: Die leitende Ärztin führt das Konsil vom Strand aus. Ebenso selbstverständlich ist die Vernetzung der Leistungserbringer im Gesundheitswesen. Hier kommen die vier eingangs genannten Begriffe Accessability, Usability, Simplicity und Productivity in den Vordergrund. Und mit ihnen die vier Ebenen, auf



Risiken bezüglich Datensicherheit und Datenschutz lassen sich sowohl auf der Prozessebene als auch auf den darunter liegenden Technikebenen identifizieren. Dementsprechend vielfältig sind die Massnahmen, die es zu treffen gilt. Effektivität wird nur erreicht, wenn die Massnahmen auf allen Ebenen aufeinander abgestimmt sind.

Auf der Prozessebene adressieren die Massnahmen das Bewusstsein und Know-how der Mitarbeitenden und unterstreichen die Pflicht zum richtigen Umgang mit sensiblen Daten und Systemen. Auf den technischen Ebenen werden unter anderem Massnahmen wie Verschlüsselung, klare Login-Policies, Log-Files sowie die redundante Speicherung und Unveränderbarkeit der Daten sichergestellt.

welchen es Ansatzpunkte für die Datensicherheit und den Datenschutz gibt (siehe Grafik): Es sind dies von unten nach oben, die IT-Infrastruktur, IT-Basissysteme, IT-Anwendungen und die Prozessebene. Auf allen vier Ebenen lassen sich Risiken identifizieren: Risiken im Geschäftsprozess (auf der Prozessebene) und Risiken in der Informatik-Infrastruktur. Daraus lässt sich die dritte Kategorie Risiken ableiten: die Haftungsrisiken.

«It's the man, not the machine»

Die Feststellung mag banal klingen: Es ist immer der Mensch. Es sind Verhaltensfehler, mangelndes Know-how, fehlende Ressourcen, ungenügende Rahmenbedingungen, aber auch Zielkonflikte mit der Effizienz und der geforderten Geschwindigkeit, die zu Risiken bezüglich Datensicherheit und Datenschutz führen. Noch immer werden beispielsweise KGs per kommunem E-Mail verschickt, obwohl mit HIN (Health Information Network) eine verschlüsselte Übermittlung möglich wäre. Hier haben wir es mit der menschlichen Ambivalenz und Inkonsequenz zu tun. Die positive Botschaft lautet: Es ist ebendieser Mensch, der das korrigieren kann. Der Massnahmenkatalog ist vielseitig und bekannt. Wir sprechen von technischer Kompetenz bezüglich der Datensicherheit. Hier konzentrieren wir uns auf die drei IT-Layer (Infrastruktur, Basissysteme, Anwendungen): Server-Zertifikate, Verschlüsselung und sicherer Transport über öffentliche Netzwerke (SSL-VPN) sowie Erfassung von Metadaten und Logfiles, die den Datenzugriff protokollieren, sind nur einige der Stichworte.

Beim Datenschutz sprechen wir von Prozesskompetenz. Massnahmen sind hier unter anderem ein adäquates «Access Management»: Wer darf welche Daten zu welchem Zweck abrufen? Die Vergabe, Änderung und Löschung von Accounts erfolgt beispielsweise ausschliesslich aufgrund von schriftlichen Aufträgen. Anonyme Accounts und Gruppen-Accounts sind zu vermeiden, oder, wenn unvermeidbar, sind deren Benutzerkreise zu dokumentieren. Das sind nur ein paar Beispiele aus einem vielseitigen Strauss an Massnahmen, die es sinnvoll und im Sinne der Effektivität zu kombinieren gilt.

Logicare beschäftigt sich täglich mit dieser Thematik – in der Praxis und auf der konzeptionellen Ebene. Und wir arbeiten mit externen Expertinnen und Experten zusammen. Als Outsourcing-Partner sind wir nach ISAE 3402 zertifiziert und bieten ein kundenfokussiertes Internes Kontrollsystem (IKS).Notabene profitieren wir aber auch von den Ansprüchen unserer Kunden, indem wir ihre Bedürfnisse in soliden und pragmatischen Lösungen abbilden.

Professioneller Werkzeugkasten

Die Dynamik der Technologieentwicklung und der Mensch-Maschine-Interaktion lässt einen allerdings nicht hoffen, dass wir hier zu einer finalen Lösung kommen. Vielmehr wird sich die Thematik in der Diskussion noch akzentuieren und neue Massnahmen erfordern. Auf der anderen Seite gibt uns der bestehende Werkzeugkasten mit gesetzgeberischen Grundlagen, ausgereifter Technik und Prozess-Know-how die richtigen Werkzeuge an die Hand, um zeitgemässe und pragmatische Lösungen zu implementieren, die die Risiken substanziell minimieren lassen.

Interview mit Ueli Dummermuth, Spital STS AG Thun

«Grenze zwischen Datenschutz und Usability richtig setzen»

Ueli Dummermuth,
Leitung Informatik, Spital STS AG Thun

Welche Rolle spielt Datenschutz im Spital Thun?

Im Zuge des mobilen Datenaustauschs ist der Datenschutz in den letzten Jahren zu einem zentralen Thema in der Spitalwelt geworden. Die moderne Technik bietet uns einen Komfort und eine orts- und zeitunabhängige Flexibilität, welche den Spitalalltag äusserst vereinfacht. Wie so oft, bringen aber neue Möglichkeiten auch neue Risiken mit sich. Durch den Datenfluss über das Netz oder die Abspeicherung in einer Cloud müssen unsere Patienteninformationen besonders gut vor Missbräuchen geschützt werden. Selbstverständlich werden Daten nicht erst seit dem Anbruch des mobilen Zeitalters geschützt. Doch es ist Tatsache, dass offen herumliegende Papierakten weniger missbraucht werden als offene Logins. Daher ist das Thema Datenschutz noch wichtiger geworden, als es ohnehin schon war.

Welche Faktoren beinhaltet Ihr Datenschutzsystem?

Grundlage bildet die ICT-Governance der Spital STS AG Thun. Tragende Säulen im ganzen Ablauf sind die ICT-Strategie, die Analyse der ICT-Risiken und Security sowie das ICT-Prozessmodell. Diese Säulen ermöglichen gleichermassen Transparenz und Sicherheit bei der strategischen Steuerung unserer ICT.

Inwiefern unterscheiden sich die Anforderungen an Datensicherheitssysteme in Spitälern von anderen Unternehmen?

Im Gegensatz zu anderen Unternehmen, wo die Mitarbeitenden gewöhnlich ihren fixen Arbeitsplatz haben und nur von einem Computer aus auf gemeinsame Daten zugreifen müssen, wechselt das Spitalpersonal ständig seinen Arbeitsplatz. Beispielsweise füllen unsere Mitarbeitenden den Tagesrapport an einem Computer aus, während die Anmeldung für den Ultraschall an einer anderen Station geschieht. Weiter greifen sie während der Visite wiederum über ein anderes Gerät auf die Patientenakte zu. Die Vielfalt der verschiedenen Systeme ist in einem Spital sehr gross. Die Anforderungen an das Datenschutzsystem sind daher anspruchsvoll. Sämtliche Abläufe eines Spitalbetriebs laufen über verschiedene Systeme. Der Datenschutz muss auf all diesen Systemen gleichermassen gewährleistet sein. Alle Mitarbeitenden greifen in der Regel täglich auf mehrere Systeme zu. Das verlangt ein ausgereiftes Login-Verfahren.

Wie sieht die konkrete Umsetzung aus?

Alle neuen Mitarbeitenden werden während ihrer Einführungszeit mit den Datenschutzrichtlinien unseres Spitals vertraut gemacht. Sie erhalten eine Personalnummer und ein personalisiertes Login, welche ihnen Zugang zu den Patientendaten verschaffen. Diese Einführung erhalten alle neuen Mitarbeitenden – egal ob Temporär- oder Festangestellte. Ausserdem haben wir keine Gruppenlogins mehr. Der Zugang zu den Daten ist ausschliesslich über das persönliche Login möglich. Beim ersten Zugriff auf eine bestimmte Akte muss der Datengebrauch von der zugreifenden Person begründet werden. Zudem können wir über unser System überprüfen, wer auf welche Daten zugreift. Auf diese Weise sind – im Fall eines Missbrauchs – Rückschlüsse auf die Personen möglich.

Was sind die Anforderungen an externe Partner?

Wir sind darauf angewiesen, dass im 1st-, 2nd- und 3rd-Level-Support externe Mitarbeitende auf unsere Systeme zugreifen können. Für diese Mitarbeitenden werden spezielle Logins generiert. Die Logins sind zeitlich begrenzt und verfallen, sobald die Störung im System behoben wurde. Mit sämtlichen externen Mitarbeitenden haben wir überdies eine schriftliche Vertraulichkeitsvereinbarung. Zusätzlich ist für uns ausschlaggebend, dass wir vollstes Vertrauen in unsere externen Partner wie zum Beispiel Logicare setzen können.

Inwiefern sind die Datenschutzrichtlinien gesetzlich festgelegt? Wo gibt es Spielraum?

Der Datenschutz des Spital Thun unterliegt den kantonalen Datenschutzgesetzen. Die Datenschutzaufsichtsstelle des Kantons Bern hat KPMG mit einem Audit unseres Klinikinformationssystems beauftragt. Hieraus resultierten 42 Empfehlungen bezüglich Datensicherheit und Datenschutz. Diese Empfehlungen haben wir auf unsere gesamte IT ausgedehnt. Derzeit sind wir damit beschäftigt, die Empfehlungen in konkreten Prozess- und Verhaltensbeschrieben festzuhalten. Das heisst, wir formulieren Handlungsanweisungen und erstellen Dokumente – zum Beispiel wie der Umgang mit Passwörtern zu handhaben ist. Dabei stehen wir in einem regelmässigen Diskurs mit der Datenschutzaufsichtsstelle des Kantons Bern und übernehmen – soweit dies möglich und mit unserem internen ICT-Board abgestimmt ist – wiederum deren Empfehlungen. Schliesslich verabschiedet unsere Geschäftsleitung diese Dokumente als Weisungen. Alle Mitarbeitenden erhalten diese Weisungen in schriftlicher Form und werden in den Bereichen Informationssicherheits- und Datenschutzkonzepte (ISDS) geschult. So schaffen wir eine solide Grundlage für die Datensicherheit und den Datenschutz in unserem Haus. In diesem Prozess sind wir weit fortgeschritten: Bis Mitte 2014 werden wir für alle 42 erwähnten Empfehlungen Weisungen verabschiedet haben.

Was sind die Herausforderungen im Umgang mit den Systemen und allen Agierenden?

Die Herausforderung liegt darin, die Grenze zwischen Sicherheit und Usability richtig zu setzen. Es existieren Lücken zwischen der Haltung der Datenschützer und den Systemanforderungen in der Praxis. Zum einen müssen unsere Systeme möglichst gut vor Missbräuchen geschützt sein. Gleichzeitig darf der Zugriff aber nicht zu sehr erschwert sein. Denn im Spital sind oft wenige Sekunden entscheidend, und da ist ein schneller und einfacher Zugriff auf die Patientenakte ein absolutes Muss. Die Grenze hier richtig zu setzen ist sicherlich eine grosse Herausforderung. Die Tendenz zeigt jedoch, dass sich die Grenze in den letzten Jahren immer mehr in Richtung Sicherheit verschoben hat und durch das richtige Know-how die Usability erhalten blieb. Schliesslich sind es aber nicht nur die Systeme, in welche wir Vertrauen setzen, sondern hauptsächlich in die Menschen, mit denen wir zusammen arbeiten.