Im EDI Podium vom MediData erfuhr der Datenschutz einen Lackmus-Test

Angriffe voll krimineller Energie, aber auch Riesenchancen

Das neue, revidierte Datenschutzgesetz (nDSG) steht vor der Tür. Dies bedeutet für alle Organisationen, die Daten von Kunden, Lieferanten, Geschäftspartnern und Mitarbeitenden bearbeiten, erhöhte Auskunfts-, Informations- und Meldepflichten. Die neuen Bestimmungen sollen das Risiko des Missbrauchs von Personendaten massgeblich reduzieren. Noch schwebt aber Unsicherheit wie eine diffuse Wolke über der Gesundheitsbranche. Deshalb ist jetzt der Erfahrungs- und Wissensaustausch unter Spezialisten so wichtig. Das EDI Podium wurde dieser Herausforderung mehr als gerecht.

Das revidierte Datenschutzgesetz (nDSG) tritt am 1. September in Kraft. Zum neuen Gesetz gehören auch die neue Datenschutzverordnung (DSV) und die neue Verordnung über die Datenschutzzertifizierung (VDSZ). Ziele sind mehr Transparenz bei der Bearbeitung von Personendaten, die Stärkung Betroffenenrechte und der Datenschutz-Governance sowie die Durchsetzbarkeit des nDSG mit Bewahrung des Angemessenheitsbeschlusses der EU.

Ein übersichtliches juristisches Inventar

«Ein genereller Paradigmenwechsel ist es zwar nicht», bemerkte Roman Böhni, Rechtsanwalt, MLaw bei ADLEGEM, «aber es besteht dennoch unternehmerischer Handlungsbedarf, um die neuen Anforderungen zu erfüllen. Was bleibt, ist das Verwenden von Daten unter ‹Erlaubnis mit Verbotsvorbehalt›, die Grundsätze der Datenbearbeitung, wo nur punktuelle Anpassungen erfolgen, weiterhin keine umfassende Rechenschaftspflicht und auch keine grundsätzliche Einwilligungspflicht.»

Die wichtigste Änderung im persönlichen und sachlichen Geltungsbereich ist die Bearbeitung von Personendaten natürlicher Personen durch private Personen (natürliche und juristische) und Bundesorgane (inkl. Personen, die mit öffentlichen Aufgaben des Bundes betraut sind). Zu merken gelte es, dass Kantone und Gemeinden Personen mit öffentlichen Aufgaben aufgrund kantonaler Datenschutzgesetze (DSG) beauftragen können. Im Weiteren ist der räumliche Geltungsbereich zu nennen, der Sachverhalte betrifft, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden. Der wichtigste Handlungsbedarf bestehe demnach im Klären der anwendbaren gesetzlichen Bestimmungen (nDSG, kantonale DSG und ausländisches Recht).

Datenflüsse sorgfältig überwachen

Neu ist auch das Bearbeitungsverzeichnis. Hier geht es um die Dokumentation der Datenflüsse (mit Personenbezug). Diese Vorschrift ist für Unternehmen nur zwingend, wenn sie mehr als 250 Mitarbeitende beschäftigen. Gegenstand sind insbesondere die Bearbeitung sensitiver

Der bis auf die Galerie randvolle Plenarsaal im Luzerner Regierungsgebäude zeigt klar: Das neue Datenschutzgesetz findet sehr grosses Interesse, so freut sich MediData-CEO Daniel Ebner ganz besonders, alle willkommen zu heissen.

Auf die Details kommt es an; Roman Böhni, Rechtsanwalt, versteht es, sie prima zu erklären.

Daten in grossem Umfang und das Profiling mit hohem Risiko. Es bestehen keine Vorgaben bezüglich der Form des Verzeichnisses. Bundesorgane müssen ihre Verzeichnisse dem Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) melden.

Neu besteht eine Informationspflicht bei der Beschaffung von Personendaten. Sie umfasst auch automatisierte Einzelentscheidungen. Wenn eine Rechtsfolge oder erhebliche Beeinträchtigung für die betroffene Person besteht, kann diese die Überprüfung und Auskunft durch eine verantwortliche natürliche Person des Absenders der Information verlangen. Bundesorgane müssen automatisierte Einzelentscheidungen als solche kennzeichnen. Als wichtigsten Handlungsbedarf betrachtet der Referent die Erstellung/Aktualisierung von Datenschutzerklärungen auf der Webseite, für Mitarbeitende usw.

Vorsicht bei externer Auftragserteilung

Weiteres neues Element ist die Auftragsbearbeitung. Beauftragte dürfen Daten nur so bearbeiten wie Verantwortliche. Vertraulichkeit und Berufsgeheimnisse sind zu wahren. Zu beachten sind die klare Identifikation von Auftragsbearbeitern und Subunternehmern, Due Diligence und der Abschluss eines Auftragsverarbeitungsvertrags.

Das nDSG ist sehr ernst zu nehmen. Es drohen Strafen bis zu 250 000 Franken, je nach Schwere des Vergehens oder Unterlassens. Vorteilhaft ist daher eine Datenschutz-Folgenabschätzung (DSFA) bezüglich aller geplanter Datenverarbeitungsprozesse mit hohem Risiko. Inhalt einer DSFA sind eine Schwellenwertanalyse, ein Beschrieb des Verfahrens, die Identifikation und Bewertung der Risiken sowie das Festlegen von Massnahmen zur Risikominimierung. Die Analyse ist von der Geschäftsleitung zu genehmigen und die Risikoüberwachung verlangt nach einer regelmässigen Überprüfung.

Das nDSG ändert in den Spitälern nicht viel – und doch alles

Das neue Gesetz hat sowohl für Kantone als auch für ihre Listenkrankenhäuser weitreichende Auswirkungen – obwohl auf den ersten Blick nur wenige Veränderungen erkennbar sind. Doch die Compliance-Anforderungen sind unvermeidbar und erfordern von den Spitälern umfassende Sorgfaltspflichten, die von den Kantonen für ihre Einrichtungen definiert werden. Beispielsweise in punkto Informationssicherheit, Datenschutz, Berufsgeheimnis und Geheimnisträger. Dies erläuterten André Baumgart vom Verband Zürcher Krankenhäuser VZK und Hellmuth Brandt von x-tention.

Es sind verschiedene Interessenslagen innerhalb eines Spitals, die zwingend von der Spitalleitung ausbalanciert werden müssen:

1. Die geschäftlichen Aktivitäten, bei denen möglichst viele Daten für erfolgreiche wirtschaftliche Initiativen erwünscht sind,
2. den neu gestalteten und juristisch geprägten Datenschutz mit dem Berufsgeheimnis bezüglich vieler sensibler Personendaten,
3. die IT, die Funktionen aufbaut und aufrechterhält, sowie
4. die Informationssicherheit für einwandfrei laufende Prozesse sowie die Verfügbarkeit von Daten und deren Erhalt und Integrität.

Neuer Datenschutz für Spitäler?

Die wichtigste Frage lautet: Ändert das nDSG die Gesundheitsbranche? Dazu gilt es festzuhalten, dass die Listenspitäler in ihren Leistungsaufträgen bezüglich stationärer Behandlungen dem kantonalen Datenschutzrecht unterliegen. Daher bringt das nGSG des Bundes für diese Spitäler wenig Änderungen. Im Kanton Zürich gilt das Datenschutzrecht des Bundes nur für ambulante Behandlungen.

Die Kantone sind beim Datenschutz und der Informationssicherheit schon seit einiger Zeit aktiv. Beispielsweise haben 16 Kantone ihr Datenschutzrecht bereits nach 2018 unter dem Eindruck der DSGVO revidiert, bei anderen besteht jedoch Nachholbedarf. Die Totalrevision des Datenschutzgesetzes des Bundes mit Inkrafttreten im September 2023 schafft nun ein zur DSGVO adäquates Schutzniveau im ganzen Land. Zusammenfassend kann man sagen, dass das nDSG für die Listenspitäler in vielen Bereichen nicht viel Neues bringt.

Datenschutz heisst Sorgfaltspflicht

Es gibt allerdings auch eine zweite Seite. Auch wenn das nDSG kaum Neuerungen hat, so bringt es viele, eindeutig der Geschäftsleitung zugeordnete Verantwortungen bezüglich der Sorgfaltspflichten mit sich. Insbesondere erweitern sich die Pflichten um Integrität, Nachvollziehbarkeit und Verfügbarkeit und gehen damit weit über die Wahrung des Berufsgeheimnisses hinaus.

Die Spitalleitung zeichnet sich vor allem dafür verantwortlich, dass die Grundsätze der Datenbearbeitung, die Bearbeiterpflichten und die Betroffenenrechte eingehalten werden, so dass es zu keiner Persönlichkeitsverletzung kommt. Nun liegt es in der Natur der Sache, dass kleinere und mittelgrosse Häuser Ressourcenengpässe in IT, Datenschutz und Informationssicherheit aufweisen. Hier ist externe Kompetenz gefragt. Um diesen Herausforderungen für Spitäler gerecht zu werden, hat der VZK einen verlässlichen Lösungspartner mit nachgewiesener Erfahrung im Gesundheitswesen evaluiert und mit x-tention gefunden.

Dank externer Hilfe in kurzer Zeit tüchtig zugelegt

«War die Datenschutz-Awareness 2022 noch deutlich verbesserungswürdig, zeigen die

Zürcher Spitäler heute grosse Fortschritte», stellte André Baumgart fest: «Die Projektanforderungen sind klarer definiert, ebenso die wichtigsten Massnahmen zur Umsetzung. Die Umsetzung unseres Leitfadens und damit 50–60 % der Anforderungen von ISO27001 sind Tatsache. Zahlreiche Awareness-Kampagnen wurden durchgeführt und das Personal ist bereit für die Themen Datenschutz und Security.»

Wie eine Projektumsetzung von x-tention aussieht, erklärte Hellmuth Brandt: «Gemeinsam mit der Geschäftsleitung beginnen wir mit einer Ist-Analyse, gefolgt von einer Analyse der Awareness, dem Umfang eingesetzter Standards, dem qualitativen Stand der verwendeten Technik sowie den sich ergebenden Erfahrungswerten.» – Dies alles basierend auf einem ausformulierten und in sich inhaltlich abgestimmten ISMS- und DSMS-Vorlagenset mit vorformulierten Prozessen, welche die Spitäler via VZK abrufen können. Ebenso ist es seit Kurzem möglich, einen shared Datenschutzberater oder shared CISO von x-tention via VZK zu beziehen. Des Routiniers Rezept lautet klar: «Datenschutz und Informationssicherheit täglich leben!»

Widersprüche lösen – Chancen nutzen

Innovative Technik und Datenschutz müssen kein Konfliktpotenzial bedeuten – im Gegenteil. «Wir müssen uns endlich davon lösen, Datenschutz und Nutzung von Daten als Widersprüche zu betrachten. Vielmehr müssen wir die Chance ergreifen und beides ermöglichen. Technologie kann hierbei eine wichtige Rolle

Aufmerksame Zuhörer wie Silvio Frey von Detecon erfahren die Finessen des nDSG.

spielen», das betonten Daniel von Büren, Swiss Security Officer, und Andri Puorger, Account Technology Strategist Healthcare Microsoft, in ihrem Referat «Cloud in Schweizer Spitälern – was ist dabei zu beachten?»

Heute würden noch zu viele Prozesse im Gesundheitswesen manuell ablaufen, kommunikationsmässig würden zu viele Datensilos gepflegt und die Interoperabilität sei aufgrund proprietärer Systeme und ungenügender Vernetzung suboptimal. Hier gelte es überall gezielt anzusetzen. Microsoft 365 könne mittels Cloud-Lösung für einen optimalen Behandlungserfolg sorgen: mit einfacher Zusammenarbeit zwischen Fachteams sowie hoher Behandlungsqualität durch virtuelle Untersuchungen und Kostenvorteilen aufgrund der Bündelung isolierter Workflows. «Wir bieten insbesondere die vier massgebenden Vorteile Interoperabilität, Modularität, Agilität und Extensibilität, die weitgehende individuelle Anpassung an klinikspezifische Anforderungen», unterstrich Andri Puorger. «Sicherheit, Compliance und Datenschutz sind enorm wichtig. Es gilt, vertrauliche Informationen zu schützen. Die User müssen sich auf robuste Compliance-Plattformen verlassen können und für die Patienten muss es sicher sein, dass ihre Daten privat bleiben.»

Will nun ein Schweizer Spital derartige Cloud-Services implementieren, sind aus Datenschutzgründen einige rechtliche Überlegungen angebracht. Basis ist ein passender Vertrag und dazu gesellen sich insbesondere eine Compliance- und Risikobeurteilung. Handelt es sich um ein öffentliches Spital, gilt die Regel, dass zusätzlich die kantonale Datenschutzaufsicht miteinzubeziehen ist. Ihr ist das Projekt zur Stellungnahme vorzulegen. Bei diesem Unterfangen sind teilweise rechtliche Vorgaben zu beachten, die recht streng sein können. Gut zu wissen, dass sich auch Microsoft dazu Gedanken gemacht hat und durchaus bereit ist, spezifische Amendments zu den à priori standardisierten US-Verträgen zuzulassen. Ausserdem erklärten die beiden Referenten Bereitschaft, die oft komplizierten regulatorischen Besonderheiten unseres föderalistischen Staatswesens zu respektieren und in die Cloud-Lösung zu integrieren.

Die Angriffe mehren sich

«Täglich lesen wir in Zeitungen, dass Unternehmen Unmengen an Daten durch Hackerangriffe ‹verloren› haben. Müssten hier die Unternehmen bezüglich Datenschutz mehr in die Pflicht genommen werden? Braucht es schärfere Meldepflichten und Haftbarkeiten, gerade wenn Patientendaten betroffen sind?» fragte Stefan Rothenbühler, Principal Cyber Security Analyst InfoGuard AG. In seinem Referat «Wie wir Hacker jagen – Insights aus realen Sicherheitsvorfällen» schilderte er das starke Anwachsen krimineller Attacken auf sensible Daten und probate Gegenmassnahmen.

Die 180 Sicherheits-Spezialisten aus Baar verfügen über eine über 20-jährige Erfahrung und kennen die Bedrohungen gründlich. Sie bearbeiten eine ständig steigende Zahl an Schadensfällen; dieses Jahr dürften es deutlich über 200 sein. Der Referent ging auf drei der häufigsten Betrugsfelder ein: Beim eBanking warnte er vor Fake-Anfragen und -Infos sowie Malvertising (digitaler Falschwerbung mit der Aufforderung, etwas anzuklicken), was immer raffinierter daherkomme und gab wirkungsvolle Tipps: Don't google beim Einwählen, lieber das Banken-Login als Favoriten hinzufügen, ein separates Benutzerprofil nutzen, lang dauernde Sessions abbrechen und insbesondere «Don't click that link»!

Weiter mehren sich E-Mail-Angriffe. Die Kriminellen schreckten neulich sogar nicht davor zurück, Azure-Kundenaccounts von Microsoft zu kompromittieren. Drittens ist als weitaus grösste Gefahrenquelle Ransomware zu nennen. Rothenbühler nannte als äusserst übles Beispiel den gelungenen Versuch, Ransomware in Med-Tech-Geräte zu integrieren. Rund 150 solcher Geräte gerieten in den Umlauf und der Schaden fiel entsprechend umfangreich aus. Umfassender Schutz war noch nie so wichtig wie heute.

Exakt so wie man es nicht machen darf

Sehr ungemütliche Erfahrungen haben bereits enorm viele gutgläubige Menschen mit meineimpfungen.ch gesammelt. Reto Vogt, Chefredaktor «Inside IT», zeigte, wie die Gesundheitsbranche aus diesem Skandal lernen kann oder könnte: «Technologie ist ein Mittel zum Zweck. Ohne Awareness für das Thema Datenschutz von allen Beteiligten nützt sie nichts», unterstrich er und zeigte DAS Musterbeispiel eines Total-Flops: meineimpfungen.ch., die ehemals landesweite, freiwillige Impfplattform. Sie sollte das «gelbe Büechli» digitalisieren und ersetzen. Dahinter steckten das BAG und eine Stiftung. Die Lösung befand sich in ihren Anfängen seit 2015, sie wur-

de kaum beworben und praktisch niemand interessierte sich dafür. Bis Corona kam und uns schonungslos alle Defizite punkto Digitalisierung des Gesundheitswesens brutal präsentierte.

Wegen technischer Mängel war der Datenschutz lausig, und prompt wurde die Seite gehackt. Jede/r konnte sich nämlich als medizinische Fachperson registrieren, auch BetrügerInnen. Adressen, Telefonnummern, Geburtsdaten, Krankenkasseninformationen und Impfstatus waren einsehbar und veränderbar, dito Indikatoren für die Covid-19-Impfung (wie z.B. Vorerkrankungen); 450 000 SchweizerInnen waren betroffen. Der EDÖB bemühte sich um Datenlöschung, der Kanton Aargau setzte sich als Schadensbegrenzer ein. Ihm wurde dann aber einfach – ohne vorhergehendes Einholen von Einverständnissen der User – der ganze Datensatz übermittelt unter dem Motto «Wir machen mal weiter …». – Sind die Daten nun gelöscht? Das bleibt wohl ein frommer Wunsch. Stümperhaft war auch das Zurückschicken sensibler Daten via unverschlüsselte ZIP-Datei an die Geschädigten, die das von sich aus verlangt haben.

Schlichtweg nichts gelernt(?)

Und – das ist nun wirklich grotesk. Reto Vogt brachte es auf den Punkt: «Das Gemauschel geht weiter. eHealth Suisse arbeitet an einem neuen Impfausweis, der mit dem EPD automatisch verknüpft sein soll und mit dem Doppelspurigkeiten vermieden werden sollten, wobei doch gemäss richtig praktiziertem Datenschutz die Zustimmung der BürgerInnen essenziell wäre. Man hat aus Fehlern nichts gelernt.» Ins gleiche Kapitel gehöre das Organspender-Register: «Im Januar 2022 äusserten Security-Experten Kritik am Register. Es war möglich, jede Person ohne ihr Wissen einzutragen. Das Register wurde im letzten Oktober eingestellt … verantwortlich: einmal mehr eine Stiftung im Auftrag des BAG!»

Das sei aber noch lange nicht alles. Viele Gesundheitsinstitutionen sind bereits Opfer von Cyber-Kriminellen geworden. Die Angriffe stiegen europaweit 2022 um 38 %, 2023 bereits jetzt um 78 %. Kein Wunder reagieren die BürgerInnen verärgert, ihr Vertrauen wurde missbraucht und verspielt. Daher sagen die Menschen heute: «Meine Gesundheitsdaten digitalisiere ich lieber nicht.» – Klartext Vogt: «Sind Sie da überrascht, dass auch das EPD ein Flop ist?»

Die Verantwortlichen sind aus seiner Sicht: «das Bundesamt für Gesundheit wegen fehlender Sorgfalt bei der Wahl der Stiftungen und fehlender Kontrolle von deren Arbeit, der Eidgenössische Datenschutzbeauftragte für seinen ‹Hinterzimmer-Deal› mit dem Kanton Aargau, die Geschäftsprüfungskommission des Nationalrats für das mehr als nur milde Urteil in der Sache meineimpfungen.ch. und die beauftragten Stiftungen für ihre Ignoranz und Inkompetenz in Sachen Datenschutz.»

Vogt sieht aber einen Hoffnungsschimmer: «Es ginge schon, wenn man kompetente Leute arbeiten liesse.» Ein gutes Beispiel sei die E-ID. Darüber lache die Sonne: «Es ist eine 100 % staatliche Lösung, die BürgerInnen haben Kontrolle über ihre Daten (Self-Sovereign-Identity, SSI), es bestehen eine generelle Datensouveränität und -sparsamkeit sowie eine sorgfältig erarbeitete Privacy by Design. Und so müsste es auch beim EPD sein, damit es gut kommt.»

Echter Innovationsgeist ist Gold wert

«Virtualisierung und Automatisierung sind zentrale Innovationsfelder für den Betrieb des Spitals der Zukunft», ist Dr. Daniel Heller, VR-Präsident Kantonsspital Baden AG und Klinik Barmelweid AG, überzeugt.

Angesichts der vielfältigen Herausforderungen wie wachsende Regulatorien, Fachkräftemangel, steigende Anforderungen der Patienten und unbefriedigende Tarife seien folgende Erfolgsfaktoren für ein Spital entscheidend: eine strategisch und operativ prospektive Führungsfähigkeit und -struktur inkl. effektivem Kostenmanagement, ein qualitativ hochstehendes Angebot und die Bestrebungen aller Berufsgruppen Richtung Unternehmensziel. Das hat beispielsweise im Kantonsspital Baden trotz schwierigen Umfelds regelmässig zu guten Abschlüssen geführt, währenddem mittlerweile rund zwei Drittel aller öffentlichen Spitäler rote Zahlen schreiben (vgl. dazu auch unseren aktuellen «clinicum»-Artikel über die Finanzstudie von PwC).

Massgebend seien auch die gestiegenen Kapitalkosten. Zwischen 2021 und 2023 hat das KSB 570 Mio. CHF Kapital aufgenommen: «Die Kapitalkosten haben sich vervielfacht, wenn man nicht abgesichert ist oder war. Wenn nun 150 Mio.CHF über 10 Jahre zu 0.35 % oder zu 2.55 % aufgenommen werden, macht die Zinsdifferenz über die gesamte Laufzeit 30 Mio. CHF aus», so Heller. Trotz gestiegener Umsätze, namentlich im ambulanten Bereich, bleibe es daher auch für ein fittes Spital wie das KSB anspruchsvoll, eine Erosion der immer noch erfreulichen EBITDA-Rate zu vermeiden. «Ohne Anpassungen der Tarife stationär wie ambulant und/oder Erhöhung der GWL wird es schwierig.»

Digitalisierung unbedingt vorantreiben

Ein Weg aus dem Dilemma bestehe in einer systematischen Digitalisierung. Heller zitierte aus einer McKinsey-Studie, die besagt, dass 8.2 Milliarden CHF jährliche Einsparungen möglich wären: 4 Milliarden Franken (49 %) dank patientenorientierter digitaler Gesundheitslösungen wie Online-Interaktionen, Patienten-Selbstversorgung und anderer Self-Services, 2.7 Milliarden (33 %) aufgrund von E-Health-Lösungen wie etwa der digitalen Unterstützung von Arbeitsabläufen oder Prozessautomatisierung sowie 1.5 Milliarden (18 %) durch Kosteneinsparungen mittels «Enabler-Technologien», z.B. den papierlosen standardisierten Datenaustausch oder elektronische Rezepte.

Zur besseren Digitalisierung gehört auch das Handling von Big Data. Heller: «Bis heute sind weltweit nur 6 % der klinischen Daten digital verfügbar und verwertbar. Das ist ein ‹ungehobener Schatz› an Wissen, denn medizinische Daten-Analysen erlauben präzisere Entscheide zu Therapien. Sie sind Basis für personalisierte Medizin und verringern den Zeitrahmen für klinische Studien.» Gerade hier besteht noch viel Luft nach oben.

Innovationen frühzeitig erkennen und nutzen

Zweites wichtiges Element für eine nachhaltige Spitalzukunft sind Innovationen. Hier setzte das KSB mit seinem Innovation Hub ein Monitoring auf. Damit werden regelmässig relevante Entwicklungen (Technologie, Diagnose, Therapie, Supportprozesse) bezüglich ihrer Auswirkungen beurteilt. Das KSB kooperiert zu diesem Zweck mit Partnern wie PSI,USZ, ETH, Hochschulen und anderen Leistungserbringern wie auch der Industrie. Hervorzuheben ist dabei die technologische Partnerschaft mit Siemens Healthineers, die weltweil nur wenige ausgezeichnete Kliniken pflegen dürfen, was zu einer hohen Versorgungsqualität mit ganzheitlichem Gerätemanagement und modernster Ausstattung führt. Zudem bestehen rege Kontakte mit Startups, mit denen gemeinsame Win-win-Situationen ermittelt werden.

Und das KSB blickt in die Zukunft. Zusammen mit dem Kanton Aargau und der Stadt Baden wurde ein Projektteam mit einem Vorprojekt beauftragt, Umsetzungsvarianten zu entwickeln, wie ein Innovationscluster MedTech im Raum Baden aussehen könnte. Als nächster Schritt steht der Start einer Projektstelle «HIH Do Tank zum Spital der Zukunft», bewilligt für drei Jahre, im Raum.

Künftig dürften auch die Idee von Shared Service Centers interessant werden, wie bereits von der Universität St. Gallen untersucht. Hierbei würden verschiedene (Zentrums-)Spitäler IT-Leistungen und andere Dienste gemeinsam evaluieren und einkaufen. – Spitäler bewegen sich weiter in einem höchst herausfordernden Umfeld. Daher gelte das Motto des KSB in Zukunft erst recht: innovativ, vernetzt und aufmerksam sein.

Fertig mit dem Affentheater!

Das abschliessende Podium war kurz, dafür aber umso deftiger. Die EPD-«Übung» bleibe aufgrund ungenügender Grundlagen ein Flickwerk und sei deshalb abzubrechen, neu zu starten oder zumindest umfassend zu überdenken, war sich die Runde einig. Hellmuth Brand von x-tention brachte klar zum Ausdruck, dass bei allem Digitalisieren entscheidend sei, dass die persönliche Autonomie der BürgerInnen gestärkt werde. Darin müsse auch die oberste Zielsetzung im Datenschutz bestehen. Mathias Früh, Leiter Gesundheitspolitik & Public Affairs Helsana, betonte, es sei höchste Zeit, mit der systematischen digitalen Vernetzung der Stakeholder vorwärts zu machen, ebenso sei damit aufzuhören, dass «jeder sein Ding» mache. Harmonisierung und Standardisierung seien wesentlich effizienter und nutzenstiftender.

Damit rannt er offene Türen bei Dr. Daniel Heller ein. Dieser verlangte, dass sich die staatliche Regulierung aufs Wesentliche zu beschränken hätte und den Spitälern mehr Spielraum für einen echten Qualitätswettbewerb zu bieten sei. Und «es muss doch endlich möglich sein, persönliche klinische Daten auf einer Versichertenkarte anonymisiert zu speichern, damit für Menschen, die weltweit umherreisen, die Sicherheit besteht, bei Krankheit oder Unfall sofort gut versorgt zu werden. Mit diesem Affentheater, mit den Ausreden, das gehe nicht, ist aufzuhören. In Litauen funktioniert das schon seit Langem problemlos. Wir könnten viel davon lernen.»

Bilder: Robin Kirchhofer

Weitere Informationen

www.medidata.ch