DATENSCHUTZ IM GESUNDHEITSWESEN

Viele Neuregelungen stehen bevor

Als Folge einer Reihe von neuen Gesetzen müssen sich Ärzte und Krankenhäuser auf neue Anforderungen im Hinblick auf Datenschutz und Datensicherheit bei der Datenverarbeitung einstellen.

Mit der fortschreitenden Digitalisierung und Vernetzung im Gesundheitswesen sind Ärzte und Krankenhäuser zunehmend gefordert, sich mit Fragen des Datenschutzes und der Datensicherheit zu befassen. Neue Gesetze, wie das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz, das zum 1. Januar 2016 in Kraft getretene E-Health-Gesetz und aktuell die EU-Datenschutzgrundverordnung (EU-DSGVO), haben Auswirkungen auf den medizinischen Bereich, auch wenn viele Detailfragen noch offen sind und etwa durch entsprechende Rechtsverordnungen konkretisiert werden müssen. Das wurde bei der Fachtagung „Datenschutz in der Medizin – Update 2016“ am 3. Februar in Hamburg deutlich.

Mit der nach vierjährigem zähen Ringen jetzt beschlossenen Datenschutzgrundverordnung *(Kasten)* sollen EU-weit geltende einheitliche Datenschutzstandards eingeführt werden, die den Anforderungen des digitalen Wandels Rechnung tragen und den Schutz des Bürgers, seiner Privatsphäre und seiner persönlichen Daten vor Missbrauch gewährleisten. Die Verordnung löst die bislang geltende EU-Datenschutzrichtlinie aus dem Jahr 1995 ab, die noch aus den Anfangsjahren des Internets stammt – als Konzerne wie Google oder Facebook noch nicht existierten und von Cloud Computing, Big Data und mobilen Apps noch nicht die Rede war. Die Richtlinie hatte den Mitgliedsstaaten zudem Spielraum bei der Umsetzung in nationales Recht zugestanden, mit der Folge einer Vielzahl nationaler Datenschutzregelungen innerhalb der EU. Diesen Flickenteppich soll die Verordnung beseitigen. Zudem ist sie – anders als eine Richtlinie – vom Zeitpunkt ihres Inkrafttretens an unmittelbar geltendes Recht innerhalb der EU.

Umsetzung Mitte 2018

Derzeit findet die technische Überarbeitung der Verordnung statt. Sie werde voraussichtlich im Juli 2018 verbindlich freigegeben, berichtete Nikolaus Schrenk, Datenschutzbeauftragter beim kbo-Klinikverbund des Bezirks Oberbayern. Bis dahin müsse der Gesetzgeber in Deutschland prüfen, welche Implikationen die EU-DSGVO hat und welche Maßnahmen hierzulande für ihre Umsetzung erforderlich sind. So müssen zum Beispiel die Auswirkungen auf das Bundesdatenschutzgesetz geprüft werden. Experten rechnen damit, dass das Gesetz stark zurückgestutzt, vielleicht sogar ganz entfallen wird. Krankenhaus- und Landesdatenschutzgesetze müssen angepasst werden.

Der in der EU-Grundverordnung ursprünglich vorgesehene Artikel 81 „Verarbeitung personenbezogener Daten für Gesundheitszwecke“ ist zwar in der letzten Fassung entfallen, dennoch gibt es eine Reihe von Regelungen, die auch für den Gesundheitsbereich relevant werden.

Ein Beispiel: Die Einwilligung des Verbrauchers in die Nutzung seiner Daten erhält mehr Bedeutung, und sie muss beweispflichtig dokumentiert werden – ein wichtiges Thema im Gesundheitswesen. Die Beweispflichtigkeit betreffe unter anderem die Unterschrift in einem technischen System, erläuterte Schrenk. Zu klären sei zudem die konkludente Einwilligung in die Datenspeicherung, etwa im Krankenhaus oder in der Arztpraxis. Schrenk zufolge ist unklar, ob die Abgabe der elektronischen Gesundheitskarte schon als Einwilligung in die technische Speicherung der Daten anzusehen ist.

Darüber hinaus gibt es Sonderregelungen für Kinder. Diese dürfen bis zu einer bestimmten Altersgrenze (13 Jahre) Internetdienste, wie et-

Foto: iStockphoto

wa Facebook, nur mit Zustimmung der Eltern nutzen. „Meine 13-jährige Tochter vereinbart ihre kieferorthopädischen Termine elektronisch“, meinte Schrenk. Im Gesundheitswesen gebe es zunehmend mehr elektronische Dienste, wie Terminvereinbarungs- oder Erfahrungsaustauschplattformen, die auch Kinder nutzten und die künftig eventuell eine Altersverifizierung benötigten.

Dauer der Datenspeicherung

Verbessert werden soll außerdem die Transparenz für die Betroffenen. So muss die Rechtsgrundlage für die Verarbeitung der Daten klar sein und angegeben werden, wie lange diese gespeichert werden. Aspekte wie leichte Verständlichkeit und Barrierefreiheit sind zu berücksichtigen – „Dinge, die wir schon lange tun müssten“, betonte der Datenschützer. Das Recht auf Vergessenwerden sowie Auskunftsrechte sind enthalten, ebenso die Verpflichtung, den Betroffenen und die Aufsichtsbehörde bei Datenpannen zu informieren. Auch das vorgesehene Recht auf Datenportierung bei offenen Diensten, das vor allem als „Consumervorschrift“ formuliert sei, betreffe das Gesundheitswesen, es werde spätestens beim Arztwechsel eines Patienten relevant, meinte Schrenk.

Für Krankenhäuser und Arztpraxen ist unter anderem die Verpflichtung zum IT-Sicherheitskonzept wichtig, die aus dem Artikel „Datensicherheit der Verarbeitung“ hervorgeht. Außerdem soll künftig eine Risiko- und Folgeabschätzung von Datenschutzverletztungen bei neuen Verfahren durchgeführt werden. Unternehmen sollen den Datenschutz durch Technik und technikfreundliche Voreinstellungen unterstützen (Privacy by Design). Bei der Auftragsdatenverarbeitung müssen Auftraggeber und Auftragnehmer künftig gleichermaßen Sorgfaltspflichten übernehmen und gemeinsam Datenschutzkonzepte entwickeln. Bei Verstößen drohen Sanktionen von bis zu 20 Millionen Euro oder maximal vier Prozent des Unternehmensumsatzes.

„Die genauen Regelungen zum Thema Gesundheit und Forschung sind noch nicht ausformuliert“, betonte Schrenk. Er rät Arztpraxen und Krankenhäusern dennoch, sich auf das Gesetz frühzeitig vorzubereiten und „nicht in Lethargie zu verfallen und zu hoffen, es wird schon nicht so schlimm werden“. Wichtig sei insbesondere das Thema Auftragsdatenverarbeitung. Krankenhäuser und Arztpraxen sollten ihre Verträge mit externen Partnern prüfen. Die Verfahrensverzeichnisse sollten auf Vollständigkeit kontrolliert und das IT-Sicherheitskonzept aktualisiert werden. Prozesse zur Folgenabschätzung könnten gleichzeitig mit dem in den Krankenhäusern schon vorhandenen Risikomanagement implementiert werden, empfahl der Experte. Meldeketten bei Datenschutzpannen sollten eingerichtet und regelmäßig getestet werden. „Wer macht was etwa bei Datenverlust? Wie sieht das gemeinschaftliche Kommunikationskonzept aus, wer gibt die Meldung nach außen?“

Viele Maßnahmen aus dem IT-Sicherheitsgesetz und dem E-Health-Gesetz lassen sich aus Sicht von Schrenk harmonisieren und „in einem Gang erledigen“. Organisationsprozesse zur Einwilligung sollten eingeübt und der Datenfluss über technische Systeme, etwa per Patientenkiosk, standardisiert werden. Gleiches gilt für Prozesse der Datenlöschung und der Rücknahme der Einwilligung. „Die Verordnung ist somit auch eine Chance für Krankenhäuser, ihre Prozesse neu zu organisieren“, erklärte Schrenk.

Sichere Webplattfomen

Wie lassen sich sichere internetbasierte Datenaustauschplattformen im Gesundheitswesen, etwa Patienten- und Behandlungsportale, gestalten? Mit dieser Frage befasst sich derzeit ein Projekt, an dem der Bundesverband Gesundheits-IT, die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS), die Gesellschaft für Datenschutz und Datensicherung und IHE Deutschland beteiligt sind. In einem 2-Phasen-Modell werden zunächst die datenschutzrechtlichen Anforderungen der Anwender erarbeitet und anschließend die organisatorischen und technischen Realisierungsmöglichkeiten geprüft, erläuterte Dr. med. Bernd Schütze, Leiter der GMDS-AG Datenschutz und IT-Sicherheit.

Beispiel Berechtigungskonzept: Wer darf wann unter welchen Umständen auf welche Daten zugreifen? Daraus ergeben sich neue Fragen, etwa nach der Art der Authentifizierung. Diese Anforderung kann durch Benutzername und Passwort, bei Internetportalen aber, um die Sicherheit zu erhöhen, auch durch eine 2-Faktor-Authentifizierung, zum Beispiel mit zusätzlicher Hardware (Token), technisch umgesetzt werden. Inzwischen sind 95 Anforderungsprofile an Datenaustauschplattformen formuliert. „Nicht jede Plattform muss allen Anforderungen genügen“, sagte Schultze. Es komme immer auf Verwendungszweck und Kritikalität der Daten an. Das Papier der Verbände soll im März veröffentlicht werden. ■

Heike E. Krüger-Brand

HINTERGRUND

Die EU-Datenschutzgrundverordnung ist Teil der europäischen Datenschutzreform, mit der innerhalb der EU einheitliche und dem Internetzeitalter angemessene Datenschutzstandards eingeführt werden sollen. Sie ersetzt als direkt anwendbares Recht nationales Datenschutzrecht und tritt zwei Jahre nach Veröffentlichung im Amtsblatt in Kraft.

Meilensteine

25. Januar 2012: Entwurf der EU-Kommission
12. März 2014: Die geänderte Fassung wird vom EU-Parlament mit großer Mehrheit angenommen.
16. Dezember 2015: EU-Parlament, EU-Rat und EU-Kommission einigen sich im „Trilog“ auf einen einheitlichen Entwurf, die technische Überarbeitung beginnt
Voraussichtlich Juli 2018: Umsetzung

Ethik-Beirat

Der EU-Datenschutzbeauftragte hat die Einsetzung eines sechsköpfigen Beirats für die ethische Dimension des Datenschutzes für den Zeitraum 1. Februar 2016 bis 31. Januar 2018 beschlossen. Aufgaben: Analyse der ethischen Dimension des Datenschutzes, Formulierung von Empfehlungen, Vorschläge für die Forschung, Förderung der interdisziplinären Zusammenarbeit, Erstellung von mindestens zwei öffentlichen Berichten, gegebenenfalls Einbeziehung anderer Experten, etwa auch für Medizin und Gesundheit.

@ EU-Datenschutzgrundverordnung: www.aerzteblatt.de/16218