Unverantwortlich

Warum es bei künftigen Datenpannen in der Medizin keine Schuldigen geben wird

Voraussichtlich am 18. September entscheidet der Bundesrat über das Patientendatenschutzgesetz (PDSG). Doch die aktuelle Fassung schützt weniger die Daten der Patienten als die Verantwortlichen möglicher Datenpannen.

Von Hartmut Gieselmann

Deutsch ist eine vielfältige Sprache: Wenn jemand will, dass sein Gegenüber ihn versteht, wählt er klare Worte. Wenn er jedoch seine Absichten verschleiern will, baut er komplizierte Sätze. Die hiesigen Datenschutzaufsichtsbehörden sind Freunde der klaren Sprache. Ihr Beschluss vom 12. September 2019 sagt kurz und knapp: Die Gematik ist datenschutzrechtlich alleinverantwortlich für die zentrale Zone der Telematik-Infrastruktur (TI).

Das von Jens Spahn (CDU) geleitete Bundesgesundheitsministerium schreibt im Entwurf des Patientendatenschutzgesetzes (PDSG) hingegen viele Paragraphen mit langen Sätzen, die selbst Juristen schwer durchschauen. Recht einfach zu verstehen ist § 311: Demnach soll die Gematik ein Sicherheitskonzept samt Vorgaben für den sicheren Betrieb der TI erstellen und deren Umsetzung überwachen.

Doch damit ist sie nicht automatisch auch datenschutzrechtlich verantwortlich. § 307 nennt als Verantwortliche an erster Stelle die „Leistungserbringer“, also Ärzte und Praxen, die die TI mit ihren Daten füttern und Patientendaten abrufen. An zweiter Stelle ist von den „Anbietern des Zugangsdienstes“ die Rede. Darunter fallen Hersteller von Sicherheitsroutern (Konnektoren) und Software-Programmen, VPN-Anbieter sowie für die Praxen tätige IT-Dienstleister.

Dass die Gematik im § 307 explizit von der juristischen Gesamtverantwortlichkeit für den Datenschutz entbunden werden soll, erfährt man erst beim Studium der langen Erläuterungen des Paragraphen. Die Gematik lege zwar „konzeptionelle und regulatorische Vorgaben, Maßnahmen zur Qualitätssicherung und zur Gefahrenabwehr“ fest. Sie sei aber nicht auf „operativer Ebene“ tätig und somit datenschutzrechtlich für die Verarbeitung der Daten nicht verantwortlich.

Schwarzer Peter

Welche Auswirkungen die Regelung im PDSG für Patienten und Ärzte haben kann, zeigt der mehr als achtwöchige Ausfall der TI von Ende Mai bis Mitte Juli. Bis heute gibt es weder von der Gematik noch irgend einer anderen Stelle eine öffentliche Auskunft zur Ursache des Ausfalls und wer dafür verantwortlich ist.

Bild: Michael Kappeler/dpa

Der Gesetzentwurf des Ministeriums von Jens Spahn (CDU) entlässt die Gematik aus der datenschutzrechtlichen Gesamtverantwortlichkeit.

Immerhin reagierte der Hersteller CGM, dessen Konnektor KoCoBox Med+ von den Ausfällen kaum betroffen war. Laut Analyse von c’t führte ein neuer DNS-Root-Anchor in der Datei „TSL.xml“ zum Ausfall der anderen Konnektoren [1]. Anders als von uns geschlussfolgert nutzte die KoCoBox damals laut CGM jedoch ebenfalls DNSSEC. Allerdings reagierten die meisten KoCoBoxen beim Update des Root-Anchors anders als die übrigen Konnektoren und fielen trotz Zertifikatsfehler nicht aus. Um derartige Ausfallrisiken künftig zu verringern, verzichtet CGM neuerdings mit dem kostenpflichtigen Software-Upgrade auf Version 2.3.24 auf DNSSEC.

Solche technischen Details lassen sich jedoch kaum von IT-Dienstleistern, geschweige denn von Ärzten und Patienten durchschauen. Und wenn sie es versuchen, ist es äußerst mühsam, an relevante Informationen zu gelangen. Beispielsweise bemängelte c’t im Januar fehlende Angaben zu Open-Source-Komponenten der KoCoBox [2]. Ein Arzt hatte damals vergeblich versucht, Informationen darüber von CGM zu bekommen. Erst die neue Fassung 2.3 des Adminstratorhandbuchs von Mitte Juli beschreibt im Anhang 9.5, wie Kunden Angaben über eingesetzte Open-Source-Bibliotheken und Quellcode der KoCoBox erhalten können. Eine lobenswerte Reaktion des Herstellers, die aber erst auf öffentlichen Druck erfolgte.

Datenpannenschutzgesetz

Sollte es künftig erneut zu Datenpannen in der TI kommen, müssen sich betroffene Ärzte und Patienten auf ein langwieriges Hin und Her einstellen. Wenn die Gematik rechtlich nicht für die Sicherheit der TI verantwortlich ist, muss sie auch keine Datenschutz-Folgenabschätzung (DSFA) abgeben, die Risiken und Auswirkungen möglicher Datenpannen detailliert beschreibt.

Den PDSG-Erläuterungen zufolge könnten allenfalls Ärzte und Praxen sowie

besagte IT-Dienstleister zu einer DSFA verdonnert werden. Zumutbar wäre dies laut PDSG-Entwurf aber erst für Firmen und Kliniken mit mehr als 20 Mitarbeitern. Beleuchten könnten diese allenfalls kleine Teilbereiche der TI. Ohne einen Hauptverantwortlichen bekommt niemand einen Gesamtüberblick und einzelne Beteiligte einer Datenpanne können Betroffene leicht abwimmeln, indem sie auf einen anderen vermeintlich Verantwortlichen zeigen. Datenpannenschutzgesetz (DPSG) wäre denn auch ein ehrlicherer Name für das PDSG.

Der Bundesbeauftragte für den Datenschutz, Ulrich Kelber, zeigte sich auf Nachfrage von c't „nicht glücklich", weil die Entbindung der Gematik von der datenschutzrechtlichen Verantwortung „nicht sachgerecht" sei. Seine Prüfung hätte in diesem Punkt jedoch ergeben, „dass der Gesetzgeber hier seine Möglichkeiten im Rahmen der geltenden Gesetze genutzt hat."

An anderer Stelle stehe der Entwurf des PDSG laut Kelber allerdings im Widerspruch zur DSGVO. Seine Hauptkritik wendet sich gegen die Einführung der elektronischen Patientenakte (ePA). Kelber kritisiert, dass Patienten die zum 1. Januar 2021 geplante ePA nur über geeignete Smartphones und Tablets einsehen und prüfen könnten. Zudem könnten sie nur entscheiden, ob ein Arzt Vollzugriff auf alle Informationen bekomme. Unterteilungen, ob beispielsweise ein Zahnarzt auch Befunde eines Psychiaters einsehen darf, sind in der ersten Phase nicht möglich.

Bild: Bernd von Jutrczenka/dpa

Der Bundesbeauftragte für Datenschutz, Ulrich Kelber, hält die aktuelle Fassung des PDSG für rechtswidrig.

Weitere Kritik übt Kelber am Authentifizierungsverfahren der ePA, das weder ausreichend sicher sei noch den Vorgaben der DSGVO entspräche. Kelber kündigte aufsichtsrechtliche Maßnahmen an, um eine europarechtswidrige Umsetzung der ePA zu verhindern. Die Mitglieder des Bundesrates sollten sich deshalb gut überlegen, ob sie ein Gesetz abnicken, das im Widerspruch zum EU-Recht steht. *(hag@ct.de)* c't

Literatur

[1] Hartmut Gieselmann, Thomas Maus, Markus Montz: Vertrauen entzogen, Warum 80.000 Arztpraxen ihre Verbindung zur Telematik-Infrastruktur verloren, c't 16/2020, S. 28

[2] Thomas Maus: Sicher wie die TI-tanic, Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik, c't 3/2020, S. 14

Weitere Infos: ***ct.de/yg94***