3 IT-Compliance im digitalisierten Gesundheitswesen

Thomas Althammer

Non-Compliance in der Gesundheits-IT?

Das Gesundheitswesen hat sich trotz in die Jahre gekommener Rahmenbedingungen nicht bei der Digitalisierung aufhalten lassen. Ein medizinischer Arbeitsplatz ohne IT-Unterstützung ist heutzutage undenkbar. Der geltende Rechtsrahmen ist umfangreich, die einzuhaltenden regulatorischen Vorgaben sind vielfältig. Folglich stellt der Aufbau eines umfassenden IT-Compliance-Management-Systems ein größeres Unterfangen dar (vgl. Abb. 1).

Die bisherige Gesetzeslage verlangt mitunter ein Agieren in rechtlichen Grauzonen. Strenggenommen ist es Arztpraxen mit der geltenden Interpretation der Schweigepflicht nach § 203 Strafgesetzbuch in Deutschland nur sehr schwer möglich, externe Dienstleister rechtskonform einzubinden. Im Rahmen von Schulung, Fernwartung oder Systemerweiterung ist eine Verletzung der ärztlichen Schweigepflicht jedoch fast unvermeidbar.

> **Tradierte rechtliche Rahmenbedingungen sind ein wesentlicher Hinderungsgrund für die Stellen- und Sektorenübergreifende Digitalisierung im Gesundheitswesen.**

Die Komplexität heutiger IT-Systeme verlangt eine zunehmende Spezialisierung. Kleine Einrichtungen und Praxen sind selten in der Lage, eigene IT-Kompetenz auf-

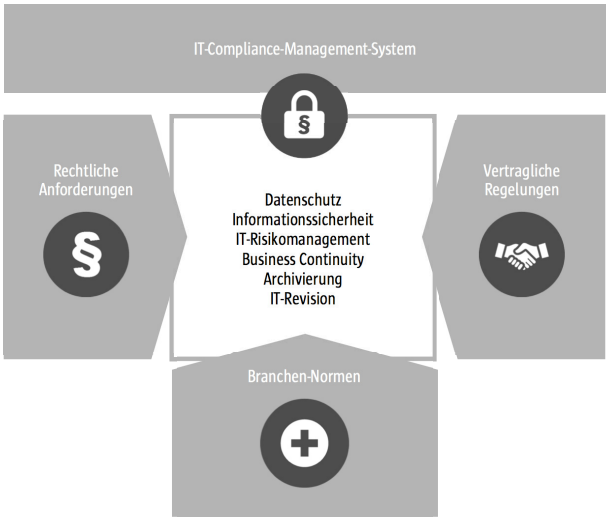

Abb. 1 Aufbau und Rahmenbedingungen für ein IT-Compliance-Management-System (eigene Darstellung)

zubauen. Doch auch Kliniken mit vergleichsweise gut ausgestatteten IT-Abteilungen übernehmen inzwischen selten mehr als die Orchestrierung des Gesamtverbunds und das Management ausgewählter IT-Systeme. Mit der zunehmenden Anzahl zu administrierenden Komponenten und Anwendungen braucht es entsprechend Spezialisten für deren Wartung und Betreuung.

Die hiesige Gesetzeslage stellt über die Schweigepflicht hinaus weitere Hürden dar: in einigen Bundesländern in Deutschland dürfen Daten nur durch ein Krankenhaus selbst oder ein anderes Krankenhaus im Auftrag verarbeitet werden. Das Einbinden externer Dienstleister ist möglich, wenn ein Patientenbezug durch den externen Dienstleister nicht hergestellt werden kann. Was sich juristisch leicht formuliert, ist IT-technisch eine extreme Herausforderung, z.B. wenn ein Rechenzentrum für den Betrieb von Krankenhausinformationssystemen eingebunden werden soll.

Neue gesetzliche Rahmenbedingungen

Bei aller Kritik an bestehenden Datenschutzgesetzen als eine Hürde bei der digitalen Transformation im Gesundheitswesen: die deutschen und europäischen Prinzipien zum Schutz von Persönlichkeit und Privatem gilt es zu verteidigen. Parallel zu einer schrittweisen Modernisierung, z.B. mit der Anfang 2017 geplanten Reformierung der Schweigepflicht im § 203 StGB, sind Potenziale bei der Entwicklung und Gestaltung von IT-Systemen im Gesundheitswesen auszuschöpfen. In ihren Grundfunktionen sind viele der am Markt erhältlichen Software-Lösungen weder als besonders datenschutzkonform noch als besonders sicher zu bezeichnen.

Heutige Konzepte zur Datenschutzkonformität in Software-Architekturen sind weit entfernt vom Potenzial eines wirklich gewollten „Privacy by Design".

Während in anderen Branchen die Sicherheit von Systemen und Produkten ein wesentliches Merkmal bei der Kaufentscheidung darstellt, spielen diese Aspekte bei der Auswahl von Hard- und Software im Gesundheitswesen (noch) keine bedeutende Rolle. Big Data geht vor Datensparsamkeit, weitreichende Zugriffe vor Kapselung in Sicherheitszonen – auch innerhalb von Software-Architekturen. Die heute verfügbaren Produkte sind über Jahre gewachsen und stehen mit ihren Strukturen neuen Anforderungen an Vernetzung und gestiegenen Bedrohungen im IT-Sicherheitsbereich gegenüber.

Die Verantwortung für die Umsetzung von Datenschutz- und IT-Sicherheitsanforderungen liegt bisher ausschließlich bei den Betreibern von IT-Systemen, also Kliniken, Arztpraxen und allen anderen Akteuren im Gesundheitswesen. Als „verantwortliche Stellen" nach den Datenschutzgesetzen sind sie für die Einhaltung datenschutzrechtlicher Belange verantwortlich. Die ab 2018 geltende Datenschutz-Grundverordnung (DS-GVO) bringt eine deutliche Verschiebung dieser klassischen Rollenverteilung mit sich.

Neben der bisher bekannten Auftrags(daten)verarbeitung kommt das Prinzip des „Joint Control" nach Art. 26 DS-GVO für Datenverarbeitung in Betracht. IT-Dienstleister werden versuchen, die Verantwortung weiterhin beim Auftraggeber zu halten. Das „Joint Control" ist der Realität aber deutlich näher, da es bei der Auslagerung von IT-Dienstleistungen häufig um eine Aufgabenverteilung und damit um eine Verlagerung der Verantwortung geht. Unabhängig von der konkreten Regelung sieht Art. 82 DS-GVO die Haftung bei allen Parteien einer Auftragsverarbeitung und ermöglicht die Durchsetzung von Schadensersatzansprüchen explizit auch gegenüber Auftragnehmern.

Traditionelle Schutzmaßnahmen haben ausgedient

Anbieter von Produkten und Dienstleistungen für das digitale Gesundheitswesen sind in der Pflicht, ihr Lösungsangebot der neuen Gesetzeslage anzupassen. Handlungsbedarf ergibt sich auch durch eine andere Entwicklung: In Zeiten, in denen Crypto-Viren ganze Krankenhausbetriebe zum Stillstand bringen und selbst der Bundestag erfolgreich „gehackt" werden kann, scheinen klassische Mittel zur Gewährleistung der IT-Sicherheit nicht mehr auszureichen.

Parallel zu diesen neuen Angriffsvektoren rollt eine Welle von Sicherheitslücken auf unsere Netzwerke zu: Das als „Internet der Dinge" (IoT) beschriebene Szenario ist längst Realität. Die Zahl „intelligenter" Geräte in internen Netzwerken wächst rasant. Viele dieser Geräte lassen sich nicht zentral verwalten und sind vor Angriffen nicht ausreichend geschützt. Wöchentliche Patches und automatische Aktualisierungen haben Betriebssysteme in den letzten Jahren deutlich sicherer gemacht. Beim IoT fehlt es an derartigen Konzepten und so werden vernetzte Kopierer, Heizungssteuerungen oder Telefonanlagen möglicherweise Einfallstore für IT-Angriffe darstellen.

Sind wir in der Lage, mit den bisherigen Methoden Datenschutz und IT-Sicherheit in einer vernetzten Welt zu organisieren?

Die Gesundheits-IT von morgen wird sich nicht wie bisher abgeschottet in separaten Netzwerken betreiben lassen. Wer trägt die Verantwortung für ein ungeschütztes Gerät? Wie organisieren wir Verfügbarkeit, Integrität und Vertraulichkeit, wenn Vitaldaten in der vernetzten Nachsorge zwischen Klinik, Hausarzt und mittels App beim Patienten selbst kontrolliert werden?

Digitale Transformation im Gesundheitswesen wird sich am Patienten orientieren. Bisherige Sicherheitszonen werden durchlässiger, Zuweiser- und Patientenportale werden sich öffnen oder ganz ersetzt werden durch den direkten Zugriff auf relevante Kernanwendungen. Welche Hürden es dabei zu überwinden gibt, zeigen heute schon Projekte im Krankenhaus-Umfeld, den Zugriff auf Patientenakten über Smartphones von Ärzten zu realisieren. Allein die Gestaltung und Formulierung entsprechender Richtlinien und Betriebsvereinbarungen stellt Unternehmen vor Herausforderungen.

IT-Compliance als Maßstab

Die strategische Verankerung von IT-Compliance-Konzepten in Zeiten großer gesetzlicher und technischer Veränderungen ist unausweichlich für eine gelungene digitale Transformation im Gesundheitswesen. Produkte und Dienstleistungen werden den Prinzipien des „Privacy by Design" und „Privacy by Default" folgen müssen, um auf der einen Seite den rechtlichen Anforderungen zu genügen, um auf der anderen Seite aber auch den aktuellen Gegebenheiten unserer IT-Welt begegnen zu können. Die Datenschutz-Grundverordnung erscheint damit als zentraler Baustein einer Compliance-Organisation in ihren Kerngedanken auf der Höhe der Zeit.

Anbieter wie Betreiber im Health-IT-Umfeld sind gut beraten, sich auf die neuen Herausforderungen einzustellen und ihre Produkte und Services entsprechend anzupassen. IT-Sicherheit sollte sehr viel mehr dezentral und anwendungsbezogen gedacht werden. Dabei ist aber auch der Gesetzgeber gefragt: die Einwilligung als Legitimation datenschutzrechtlicher Hürden kann maximal ein Hilfskonstrukt und keine dauerhafte Lösung für alle IT-Compliance-Fragen darstellen.