
Vorwort

Die Digitalisierung des Gesundheitswesens hat vor kurzem in Deutschland begonnen und schreitet mit großen Schritten voran. Startups ebenso wie Großkonzerne entwickeln Technologien und Anwendungen, um die Gesundheitsversorgung einer alternden Gesellschaft auch in den kommenden Jahrzehnten zu gewährleisten. Fitnesstracker und andere Analysetools bieten gesundheitsbewussten Patienten die Möglichkeit, ihren Körper rund um die Uhr zu überwachen – und datenverarbeitenden Firmen und Herstellern neue Einnahmequellen.

Bei dieser rasanten Entwicklung werden die Themen Datenschutz und Datensicherheit häufig als Hindernis gesehen, was sie nicht sein müssen. Jedenfalls sind der Datenschutz und die Datensicherheit von enormer Bedeutung: Gesundheitsdaten sind hochsensibel und können in den falschen Händen großen Schaden anrichten. Gerade jetzt, wo viele Produkte und Geschäftsmodelle sich noch in der Entstehung befinden, ist der richtige Moment, um praktikable und sichere Strategien für den verantwortungsvollen Umgang mit sensiblen Gesundheitsdaten zu entwickeln.

Datenschutz ist ein Grundrecht, eine Herausforderung – und ein Wettbewerbsvorteil. Deshalb haben wir uns entschieden, ein Fachbuch als Handreichung für Hersteller, Entwickler, medizinisches Fachpersonal und interessierte Patienten herauszugeben, das sich genau dieser Herausforderung stellt. Wir möchten mit dem vorliegenden Buch praxisnahe Lösungsmöglichkeiten aufzeigen, um eine verantwortungsvolle Datenschutzpraxis schon beim Design der Produkte zu fördern. Dabei beziehen wir schwerpunktmäßig gerade auch das neue Datenschutzrecht (Datenschutz-Grundverordnung) mit ein, das ab Mai 2018 direkte Gültigkeit in allen EU-Ländern hat. Auf weitere landesspezifische Regelungen wird i. d. R. kein Bezug genommen, da diese den Rahmen dieses Buches sprengen würden.

Teil I des Buchs führt in die Entwicklung datenverarbeitender Produkte in der E-Health-Branche ein: Welche Produkte und Technologien gibt es im digitalen Gesundheitsbereich? Welche Daten werden mit welchen Methoden erhoben und zu welchen Zwecken (Kap. 1)? Wie entwickelte sich der E-Health-Markt in den vergangenen Jahren (Kap. 2)?

Teil II stellt die aktuellen Herausforderungen rund um Datenschutz und Datensicherheit bei E-Health zusammen und nennt Lösungsansätze: Welche Grundprinzipien des Datenschutzes müssen Anbieter von E-Health-Produkten einhalten (Kap. 3)? Welche rechtlichen Rahmenbedingungen beeinflussen die digitale Gesundheitsbranche in Deutschland (Kap. 4)? Welche wichtigen rechtlichen Anforderungen existieren zusätzlich international (Kap. 5)? Welche technischen Anforderungen müssen Anbieter erfüllen, um Datensicherheit zu gewährleisten (Kap. 6)?

In Teil III bieten die Ergebnisse empirischer Studien Einblicke in den aktuellen Stand von Datenschutz und Datensicherheit bei E-Health-Produkten (Kap. 7 und 8). Das Abschlusskapitel fasst gebündelt und praxisnah die konkreten technischen bzw. rechtlichen Anforderungen für die Bereiche Datenschutz und Datensicherheit zusammen (Kap. 9).

Wir hoffen, Ihnen damit eine erste Orientierung im unübersichtlichen Feld der technischen und juristischen Anforderungen an Datenschutz und Datensicherheit im Bereich E-Health zu geben. Unser großer Dank gilt Kerstin Kafke, Daniela Klette, Britt Petersen und Astrid Schwaner für die inhaltliche Mitwirkung, für viele weitere Hinweise und die umfassende Redaktion des Buches.

Hamburg
im Mai 2017

Prof. Dr. Christoph Bauer
Dr. Frank Eickmeier
Michael Eckard

E-Health: Datenschutz und Datensicherheit
Herausforderungen und Lösungen im IoT-Zeitalter
Bauer, C.; Eickmeier, F.; Eckard, M.
2018, VIII, 160 S. 13 Abb., Softcover
ISBN: 978-3-658-15090-7