3.3 Datenschutz und Sicherheit von E-Health

C. Bauer und F. Eickmeier

Zusammenfassung

Daten aus E-Health-Anwendungen sind sensitive Daten und unterliegen gemäß den Datenschutzgesetzen einem besonders hohen Schutz. Für den Datenschutz bei E-Health ist vor allem relevant, ob und welche Informationen an andere Personen weitergegeben werden und wie sie als sensitive Daten hoch gesichert werden. Zu der rechtlichen Frage, wann welche Daten weitergegeben werden und der technischen Frage, wie sie gesichert werden, gibt es hohe rechtliche Anforderungen an die Einwilligung, die Verträge und hohe technische Anforderungen der Datensicherheit. Darüber hinaus sind hohe Anforderungen an die Transparenz der Datenverarbeitung und die Informationen an die Verbraucher einzuhalten.

Grundprinzipien des Datenschutzes bei E-Health

Datenschutz ist Grundrechtsschutz

Der Datenschutz, der in der Form des Rechtes auf informationelle Selbstbestimmung im Grundgesetz verankert ist, ist ein Grundrechtsschutz – er dient dem Schutz der Freiheit des Einzelnen (DIVSI 2016, Dix 2012). Auf ein Individuum bezogen ist das Ziel des Datenschutzes, „den Einzelnen vor Beeinträchtigungen seiner Persönlichkeitsrechte durch den Umgang mit seinen personenbezogenen Daten zu schützen. Das Recht des Datenschutzes bezweckt damit Persönlichkeitsschutz und insoweit auch Schutz der Privatsphäre.“ (Pramann 2016). Unter Privatsphäre versteht man das Ausmaß, in dem ein Mensch anderen „Zutritt zu seiner Welt gewährt“. Privatsphäre ist lebensnotwendig, da nur sie Raum für Muße und Kreativität, für die Herausbildung von eigenständigem Denken und Handeln bietet. Für den Datenschutz bei E-Health ist von den verschiedenen Formen der Privatsphäre vor allem die informationsbezogene Privatsphäre relevant, die sich auf die Kontrolle einer Person darüber bezieht, ob und welche Informationen an andere Personen weitergegeben werden (Trepte 2012). Das überindividuelle Ziel des Datenschutzes ist „die Begrenzung jener Machtungleichgewichte, die durch die Informationsballung bei einzelnen Akteuren bestehen“ also „der Schutz vor Datenmacht“. Dieses zentrale Motiv richtet sich vor allem gegen die Datenmacht des Staates, aber zunehmend auch von Unternehmen, die dank ihrer technikbasierten Geschäftsmodelle Datenmacht gewinnen, und sogar von Nutzern mancher Onlinedienste, die durch den Zugang zu Informationen über andere Nutzer ebenfalls Datenmacht erhalten (Lewinski 2012).