2 Datenschutz – Beweggrund, Begleiter oder Bürde der digitalen Transformation?

Ingo Mleczeck

Datenschutz im Gesundheitswesen

Datenschutz im Gesundheitswesen spiegelt sich vor allem in der ärztlichen Schweigepflicht wieder und ist so alt, wie der Arztberuf selber. Um 800 v. Chr. finden sich in indischen Sanskritschriften die wohl ältesten schriftlichen Überlieferungen zur Verpflichtung der Ärzte über das, was sie von ihren Patienten erfahren, zu schweigen. Über den hippokratischen Eid und das preußische Landrecht hat sich die ärztliche Schweigepflicht bis in unser heutiges Strafrecht erhalten. Patienten müssen sich darauf verlassen können, dass Ärzte (und das Gesundheitswesen) als Basis der Arzt-Patienten-Beziehung alle Informationen vertraulich behandeln. *Gefährdet die Digitalisierung diesen Grundpfeiler medizinischen Wirkens durch unkontrollierbaren Zugriff auf Gesundheitsdaten?*

Datenschutz als Digitalisierungsbremse

Digitalisierung hat das Gesundheitswesen bereits disruptiv verändert: MRT- und CT-Technologien, Health-Apps, papierlose Visite usw. sind weitreichend etabliert. Jedoch bei anderen, bedeutenden Digitalisierungsprojekten tut man sich schwer. Im Jahr 2002 erfolgten die ersten Planungen zur bundesweiten elektronischen Gesundheitskarte (eGK) mit implementiertem elektronischem Arzneimittelrezept, Notfalldatensatz und automatischen Datenabgleich zur Aktualisierung der Stammdaten sowie Formen der elektronischen Patientenakte (ePA). 15 Jahre später haben wir lediglich eine eGK zum Auslesen der Versichertendaten mit Lichtbild des Versicherten.

Weitere Funktionalitäten stehen flächendeckend immer noch nicht zur Verfügung. Insbesondere Bedenken beim Datenschutz haben die eGK ausgebremst. Ähnlich sieht es auch bei den verschiedensten Projekten zur ePA aus. Auch hier hat sich noch keine Lösung flächendeckend durchgesetzt. Bremsend wirken sich auch bei der ePA – neben dem Informationsschutz – die Herausforderungen der Interoperabilität aus. Die Entwickler dieser Anwendungen garantieren Datensicherheit. *Kann man sich auch in der Zukunft auf die Datensicherheit verlassen?*

Datenschutz

Informationsschutz = Schutz personenbezogener Daten vor dem Zugriff Unberechtigter

Informationssicherheit = Schutz von IT-Systemen vor Datenmanipulation, -diebstahl, -zerstörung

Der Patient als Datenschützer

Soweit gesetzlich anderweitig nicht geregelt, hat jeder das Grundrecht auf die eigene Entscheidung, wer persönliche Daten erhält und wer nicht! In der analogen Welt ist dies leicht umzusetzen. Im digitalen Kontext jedoch weitaus schwieriger. Daten können kopiert, vervielfältigt, manipuliert werden. Daten sind volatil, überwinden Ländergrenzen problemlos und sind demzufolge unkontrollierbar. Daher sollte jeder sorgfältig mit seinen persönlichen digitalen Daten umgehen. Der personalisierte Werbespam durch Profiling der Internetnutzung ist bestenfalls ärgerlich. Einen Arbeitsplatz nicht zu erhalten, weil sich der potenzielle Arbeitgeber auf der Social-Media-Seite des Bewerbers informiert hat, ist gefährlich. Wenn Patienten nun Verfügungsgewalt über ihre ePA und damit ihre digitalen Gesundheitsdaten bekommen kann auch hier ein sorgloser Umgang erfolgen. Verliert man seine Bankkarte oder wird die PIN öffentlich, kann die Karte unwiderruflich gesperrt werden. Wird der Zugriff auf die eigene ePA (versehentlich) ermöglicht, können die Daten zwar erneut geschützt werden. Bis zu dieser Maßnahme sind unberechtigte Kopierzugriffe aber möglich und nicht wieder zu heilen. Die Daten sind damit unkontrollierbar geworden. *Wird sich hier ein Wandel in der Sensibilität hin zum verantwortungsvollen Umgang mit Daten ergeben oder geht man Risiken zugunsten der Bequemlichkeit ein? Nimmt man sich durch vorsichtige/reduzierte Verwendung der eigenen Gesundheitsdaten die vielfältigen Chancen der Digitalisierung?*

Big Data und das Recht auf Vergessenwerden

Nach der EU-Datenschutzgrundverordnung wird das Recht des Betroffenen auf Löschung seiner Daten auf das Internet ausgeweitet (neu: „Recht auf Vergessenwerden"). Für illegal beschaffte (Gesundheits-)Daten, die in den nichteuropäischen Rechtsraum gelangt sind, lässt sich das Recht auf Vergessenwerden nicht durchsetzen. Im europäischen Rechtsraum wird dies zur technischen Herausforderung. Schwer vorstellbar ist die Umsetzung des Rechts auf Vergessenwerden bei Big Data mit Personenbezug. Dazu muss der Betroffene in der Lage sein zu wissen, wo seine

Daten überall (legal) gespeichert sind. Da Einwilligungen zur Datenspeicherung jederzeit widerrufen werden können, muss gewährleistet sein, diese Daten (inkl. Sicherungskopien) jederzeit löschen zu können. Solange Big Data auch aus personenbezogenen Daten besteht, widerspricht dies dem Prinzip der Datensparsamkeit, dem Prinzip der Zweckbindung widerspricht Big Data ohnehin. *Lässt sich Big Data auch mit ausschließlich anonymisierten Daten nutzen? Wird sich das Recht auf Vergessenwerden durchsetzen oder bleibt es bei der These „Das Internet vergisst nicht"?*

Digitalisierung schafft Bürokratisierung

Die Verarbeitung personenbezogener Daten ist nur erlaubt, wenn eine Vorschrift dies zulässt oder die Zustimmung der Betroffenen vorliegt. Dies führt dazu, dass bereits jetzt für eine Vielzahl von Nutzungen schriftliche Einwilligungen eingeholt werden (z.B. Digitalisierung von Papierakten, Teleradiologie). Zu jeder Datenverarbeitung, die nicht durch eine Vorschrift legalisiert wird, muss der betroffene Patient über Datenarten, Zweckbestimmung Datenempfänger und Speicher-/Löschfristen informiert, sowie eine widerrufbare Einwilligung eingeholt werden. Durch digitale Transformation wird sich die Anzahl der Anwendungen erheblich erhöhen, für die eine Einwilligung der Betroffenen nötig sein wird. *Wird dies für die Betroffenen verständlich und vor allem übersichtlich und für die verantwortlichen Stellen organisatorisch durchführbar?*

Schutz vor unzulässigem Zugriff

Daten sind Rohstoff der modernen Wirtschaft. Daher gibt es viele Interessen an Daten zu gelangen. Neben den ehrenwerten Motivationen, bei denen davon ausgegangen wird, dass die Datenbeschaffung legal erfolgt, gibt es auch niedere Beweggründe: vom Datenverkauf über Datenmanipulation zur Erpressung bis hin zum Cyber-War. Dass diese Risiken real sind, beweisen die bekannt gewordenen Angriffe auf Krankenhäuser, die zu tagelangen Ausfällen der dortigen IT-Struktur geführt haben. Eine hohe Digitalisierungsrate hat eine hohe Abhängigkeit von der IT bei der Leistungserbringung zur Folge – gerade auch in Krankenhäusern. Ausfälle in der Krankenhaus-IT-Struktur können die Behandlungsprozesse unmöglich machen und damit Gesundheit der Patienten gefährden. Unabdingbar für die Digitalisierung sind daher in erster Linie IT-Sicherheitsmaßnahmen aber auch Ausfallkonzepte, die ständig validiert und trainiert werden müssen. *Sind die Leistungserbringer im Gesundheitswesen dabei gut aufgestellt und wer stellt die erforderlichen finanziellen Mittel zur Verfügung?*

Waffengleichheit

Nutzer von Anwendungen im Gesundheitswesen (Patienten oder Professionals) stehen Angreifern auf die Daten gegenüber, die in ihrem (IT-)Bereich höchst kompetent sind oder sich ihre Professionalität problemlos einkaufen können („crime as a service"). Außer dem vorsichtigen Umgang mit Gesundheitsdaten haben normale Nutzer keine echte Chance gegen professionelle Angreifer. Sie sind gezwungen, den Technologien in ihrer Sicherheit zu vertrauen. Ständig werden z.B. in Betriebssystemen Sicherheitslücken aufgedeckt, die durch Updates wieder geschlossen werden.

Die Zeitspanne zwischen Entdeckung des Risikos, Bereitstellung der Lösung und deren Implementierung bedeutet Risiko für die Daten. Der Nutzer kann nur aufmerksam beobachten um schnell die notwendigen Updates zu installieren. Das funktioniert bestenfalls bei bedeutenden Anwendungen. Bei kleineren Anwendungen ist zu befürchten, dass Sicherheitslücken spät bzw. gar nicht erkannt oder vom Hersteller verschwiegen werden. Bei professioneller Nutzung von Anwendungen liegt die Verantwortung für die Informationssicherheit beim Anwender und nicht beim Hersteller. Mit dem Risiko beabsichtigter oder unbeabsichtigter Sicherheitslücken in der Anwendung kann sich auch Zurückhaltung bei der Verwendung von digitalen Innovationen ergeben. Nutzer haben weder Einfluss auf die technische Sicherheit der Anwendung noch können sie diese überhaupt beurteilen. Dennoch müssen die Anwender die Informationssicherheit verantworten. *Lässt sich die Haftung/Verantwortung für Informationssicherheit zukünftig auf die Hersteller übertragen?*

Internet der Dinge

Das Internet der Dinge (IdD) wird bei der digitalen Transformation im Gesundheitswesen eine wesentliche Rolle spielen. Es existieren Suchmaschinen zur globalen Identifikation von ungeschützten IdD-Geräten, die dann weltweit fremdgesteuert werden können. Aus dem IdD wurde bereits eine Vielzahl von Geräten für Botnet-Angriffe miteinander vernetzt. Hier muss ein Höchstmaß an Informationssicherheit entstehen, laufend validiert und aktualisiert werden. *Spielt die Informationssicherheit eine ausreichende Rolle bei der Produktentwicklung?*

Technische Überwachung, Kontrolle und Zulassung

Gerade bei den inflationär angebotenen kostenfreien oder preiswerten Health-Apps, deren Absicht eher der Informationsbeschaffung statt dem Anwendungszweck dient, wird die Informationssicherheit keine wesentliche Berücksichtigung finden. Viele Anwender werden dies in ihrer gesellschaftlich verwurzelten Naivität nicht berücksichtigen und Daten damit unbewusst preisgeben. Informationssicherheit bereits bei der Anwendungsentwicklung von Technologien für das Gesundheitswesen zu berücksichtigen muss zwingend beachtet werden („privacy by design"/„privacy by default"). Während bei der Arzneimittelzulassung ein Höchstmaß an Studien, Tests und Genehmigungen gesetzlich verlangt werden, ist dies bei den digitalen Technologien im Gesundheitswesen nicht gegeben. Ansätze erfolgen rudimentär bei Anwendungen, die als Medizinprodukte klassifiziert werden. Aber auch hier sind die Anforderungen bei weitem nicht so hoch wie bei der Arzneimittelzulassung und konzentrieren sich eher auf den eigentlichen Anwendungszweck als auf die Informationssicherheit. Eine neutrale Zulassungsinstanz für digitale Anwendungen im Gesundheitswesen wäre sinnvoll, soweit sich die Zulassungsverfahren nicht als Bremse der Digitalisierung auswirken. *Wird die Informationssicherheit zur Anforderung und damit zum Selbstverständnis bei der Anwendungsentwicklung?*

Fazit

Das deutsche Gesundheitswesen ist volkswirtschaftlich ein bedeutender Faktor und darf der digitalen Transformation nicht hinterherlaufen. Während in der Vergangenheit der Datenschutz eher als Bremse aufgefallen ist, müssen sich Informationsschutz und -sicherheit zu selbstverständlichen Begleitern der digitalen Transformation entwickeln. Datenschutz im digitalen Gesundheitswesen muss ein laufender, ständig trainierter und immer zu validierender Prozess werden; sowohl bei den Nutzern als auch bei den Herstellern/Entwicklern. Ob Kosteneinsparungen durch Digitalisierung aufgrund der zwingenden Datenschutzmaßnahmen erzielt werden können, bleibt fraglich. Sparen durch Verzicht auf Datenschutz kann aber auch keine Lösung sein. *Wir müssen aufmerksam dafür Sorge tragen, dass die Schweigepflicht des Gesundheitswesens für die sensiblen Gesundheitsdaten dem Digitalisierungsprozess standhalten kann!*