



Dr. Adrian Bachmann studierte Wirtschaftsinformatik an der Universität Zürich und verfasste dort auch seine Dissertation zum Thema Datenqualität im Software Engineering Prozess. Nach einigen Jahren im IT Projekt- und Risikomanagement bei einer grösseren Schweizer Bank berät er seit 2011 seine Kunden in Themen der Informationssicherheit und leitet entsprechende Projekte.

Kontaktadresse:

*Dr. Adrian Bachmann
Partner, IT Security Consultant
TEMET AG
Basteiplatz 5
CH-8001 Zürich
Tel: +41 79 464 01 46
E-Mail: adrian.bachmann@temet.ch
<http://www.temet.ch>*

Das elektronische Patientendossier (EPD) und die informationelle Selbstbestimmung sind zwei Themen, über die wir in den kommenden Jahren viel hören, lesen und nachdenken werden. Lasst uns darüber sprechen, weshalb das EPD zum Prüfstein für die informationelle Selbstbestimmung wird.

Am 19. Juni 2015 hat das Parlament das Bundesgesetz über das elektronische Patientendossier (EPDG) verabschiedet. Wenn das neue Gesetz im ersten Halbjahr 2017 in Kraft tritt, dann müssen Spitäler binnen dreier Jahre ihren Patienten ein elektronisches Patientendossier anbieten; andere Einrichtungen des Gesundheitswesens folgen später. Die Leistungserbringer schliessen sich hierfür in sogenannten Gemeinschaften zusammen, die sich derzeit nach geographischen (z.B. Versorgungsregionen, Kantone) und/oder organisatorischen (z.B. Besitzverhältnisse, Standesorganisationen) Kriterien bilden.

Das EPD soll die Qualität der medizinischen Behandlung stärken, die Behandlungsprozesse verbessern, die Patientensicherheit erhöhen, die Effizienz des Gesundheitssystems steigern und die Gesundheitskompetenz von Patientinnen und Patienten fördern. Gesundheitsfachpersonen (GFP) können bzw. müssen behandlungsrelevante Daten aus der Krankengeschichte zukünftig im EPD ablegen, so dass sie für andere Gesundheitsfachpersonen sowie für den Patienten selber zugreifbar werden. Wichtige datenerzeugende Systeme wie die Klinikinformationssysteme (KIS) der Spitäler oder die Praxisinformationssysteme (PIS) der Ärzte werden sich mit dem EPD für Zugriffe von aussen öffnen. Diese Öffnung bringt Sicherheitsrisiken mit sich, wie wir sie aus anderen E-Business Anwendungen kennen. Das Ausführungsrecht umfasst daher entsprechende technische und organisatorische Vorschriften zur Risikobegrenzung, deren Einhaltung bei der obligatorischen Zertifizierung einer Gemeinschaft überprüft wird. Auch von den Patienten ist ein wesentlicher Beitrag zur Sicherheit zu leisten, indem sie sich für den Zugriff auf das EPD stark authentisieren und die Integrität ihres Endgeräts sicherstellen. Für Massnahmen dieser Art können die EPD Gemeinschaften auf

bald 20 Jahre Erfahrung beispielsweise im E-Banking abstützen.

Aussergewöhnlich und ohne solches Vorbild ist die Konsequenz, mit der die informationelle Selbstbestimmung im EPD umgesetzt wird. Dieses Recht ist zwar nicht explizit formuliert, steht aber als bestimmendes Prinzip hinter zahlreichen Regelungen in Gesetz und Verordnung. Zu diesen gehört erstens, dass das Führen eines elektronischen Patientendossiers für die Patienten freiwillig ist. Zweitens hat der Patient die Hoheit über die Daten in seinem EPD, indem er beispielsweise die Erfassung spezifischer Dokumente untersagen oder die Vernichtung von bereits erfassten Daten verlangen kann. Drittens kann der Patient nicht nur sein eigenes EPD einsehen, sondern auch das Protokoll aller Zugriffe auf Dokumente in seinem EPD, was eine bisher nicht gekannte Transparenz schafft. Der Patient ist viertens verantwortlich für die Vergabe der Zugriffsrechte an Gesundheitsfachpersonen entlang von zwei Dimensionen:

In der ersten Dimension wird jedem im EPD zugänglichen Dokument eine Vertraulichkeitsstufe „nützlich“, „medizinisch“, „sensibel“ oder „geheim“ zugewiesen. Unabhängig davon, wie die initiale Klassifizierung eines Dokuments erfolgt, kann sie auf jeden Fall vom Patienten beliebig verändert werden.

In der zweiten Dimension legt der Patient fest, welche Gesundheitsfachpersonen oder welche Gruppen von Gesundheitsfachpersonen (Organisationseinheiten, z.B. Abteilungen in einem Spital) auf sein EPD zugreifen dürfen und bis zu welcher Klassifizierungsstufe dieses Zugriffsrecht gilt. Im Rahmen der Grundeinstellungen kann er auch definieren, bis zu welcher Klassifizierungsstufe ein Notfallzugriff durch Gesundheitspersonen möglich ist, ohne dass eine explizite Zugriffsberechtigung vorgängig erteilt wurde. Ferner kann der Patient ausgewählte Gesundheitsfachpersonen auf eine Sperrliste setzen, die einen EPD Zugriff durch diese GFP unabhängig von allen anderen Rechtezuteilungen unterbindet. Der Patient kann Stellvertreter (z.B. Familienangehörige oder Beistand) nominieren, die in seinem Namen auf das EPD zugreifen und auch die Berechti-

gungsverwaltung übernehmen können. Er kann überdies Gesundheitsfachpersonen dazu ermächtigen, die ihnen erteilten Zugriffsrechte an weitere Gesundheitsfachpersonen weiterzugeben.

Das oben beschriebene System der Berechtigungsverwaltung erscheint komplex und ist es auch. Die Gemeinschaften werden zwar versuchen, diese ungewohnte Aufgabe für die Patienten möglichst einfach zu gestalten. Man kann sich aber gut vorstellen, dass die Betreuung vor allem älterer Patienten und Patientinnen eine Herausforderung sein wird und dass hier ein Tätigkeitsfeld für bestehende oder neue Dienstleister im Gesundheitswesen entsteht.

Mit dem EPD steht die Schweiz vor einem Meilenstein der Digitalisierung und einem Lackmустest für die informationelle Selbstbestimmung. Wollen und können die Patienten von diesem Persönlichkeitsrecht wirklich Gebrauch machen? Wird die staatlich verordnete informationelle Selbstbestimmung die Einführung des EPD beschleunigen oder im Gegenteil behindern?

Die anstehende Einführung des elektronischen Patientendossiers wird Anhaltspunkte dafür liefern, inwiefern unsere Gesellschaft für die informationelle Selbstbestimmung reif ist. Dies ist ein weiterer guter Grund für die Hoffnung, dass sich das EPD in der vom Gesetzgeber angedachten Art und Weise rasch etablieren wird.