formationstechnik (BSI) insbesondere zur Lage der IT-Sicherheit in Kliniken belegen immer wieder, welche Lücken und Risiken immer noch bestehen auch die Patientendaten betreffend. Die Politik hat inzwischen reagiert und mit dem vom BSI betreuten Projekt KRITIS den Versuch gestartet, die IT-Sicherheitslage in sensiblen Einrichtungen wie Kliniken systematisch zu erfassen und Mindestanforderungen für die IT-Sicherheit zu formulieren.

Diese Sammlung von Datenschutzpannen muss alle aufschrecken, die in medizinischen Betrieben für die Sicherheit der Patientendaten Verantwortung tragen, insbesondere dort, wo sie manuell oder automatisiert verarbeitet werden. Dies sind insbesondere: Arztpraxen, medizinische Versorgungszentren, Kliniken, medizinische Labore, Pflegeheime usw.

Veräußerung des Innersten

Interessant ist auch die seit längerem geführte Diskussion um Fitness-Armbänder und sog. Wearables. Einerseits werden sie gepriesen als probates Spielzeug eher jüngerer, sportlich und gesundheitsaffin geprägter Menschen, um messbare Anreize zu erhalten, noch mehr Gesundheitsvorsorge zu betreiben. Großes Interesse entwickeln zudem die Krankenkassen an den Messdaten der Versicherten, weil nun persönliche Gesundheitsprofile möglich sind und großflächige Forschung. Zuschüsse beim Erwerb einer Apple Watch zum Beispiel sollen den Weg der Daten zur Kasse inzwischen ebnen.

Deutlich sind aber andererseits die Warnungen der Datenschützer an die Versicherten, nicht auch noch besonders sensible Daten für einen schnöden Vorteil und zu nicht mehr beherrschbaren Zwecken zu verkaufen. Studien machen zudem deutlich, dass selbst die ungewollte Weitergabe der Messdaten an Dritte über zahlreiche IT-technische Schwachstellen der Messgeräte möglich ist, aber kaum jemandem bewusst ist. Hierzu wäre also eine breit angelegte Aufklärung notwendig.

Normen und Regelwerke als Rahmen datenschutzrechtlich korrekter Abläufe

Weil sich die Probleme des Datenschutzes und insbesondere der Datensicherheit für medizinische Einrichtungen gerade durch den rapide zunehmenden Einsatz der IT ausgeweitet und intensiviert haben, mussten die zuständigen Fach- und Datenschutzbehörden seit ca. vier Jahren eine Fülle von neuen Regelwerken publizieren, deren sorgsame Umsetzung diese Risiken nachhaltig reduzieren können.

Die im Jahre 2011 erstmals publizierte und 2014 überarbeitete „Orientierungshilfe Krankenhausinformationssysteme“, herausgegeben von der Konferenz der Datenschutzbeauftragten von Bund und Ländern, zwang die Kliniken erstmals, ihre Verwaltungs-IT auf die aktuelle Gefahrenlage umzurüsten und datenschutzkonforme Zugriffsregeln technisch umzusetzen.

Umstellungsprozess leidet unter Gewinnorientierung

Dieser notwendige Umstellungsprozess leidet allerdings zunehmend unter der primären Vorgabe für Kliniken, möglichst gewinnorientiert zu agieren, und dennoch oft in die Verlustzone zu geraten, die für eine normenkonforme Modernisierung der Verwaltungs-IT keinen Raum lässt.

Punktuell versuchen große Kliniken wie die Universitätsklinik Frankfurt, neue Wege zur medizinisch optimalen Nutzung der elektronischen Patientenakte zu beschreiten. Diese in vorhandene KIS-Systeme eingebetteten Projekte werden auch professionell von Datenschutzbeauftragten begleitet. Zu hoffen bleibt, dass die hier gewonnenen Erkenntnisse auch die notwendige Verbreitung finden.

Ergänzend zu solchen eher abstrakten Regelwerken wie die OH-KIS haben Datenschutzverbände inzwischen auch Umsetzungshilfen erarbeitet, die einzelne datenschutzrechtliche Problembereiche in Verwaltung medizinischer Einrichtungen betreffen.

„Fast alle medizinischen Betriebe müssen externe Dienstleister einschalten wie zum Beispiel bei der Fernwartung der internen IT, als Cloud-Anbieter oder Aktenvernichter. Dieses Outsourcing löst allerdings zahlreiche Datenschutzprobleme aus.“

Fast alle medizinischen Betriebe müssen externe Dienstleister einschalten wie zum Beispiel bei der Fernwartung der internen IT, als Cloud-Anbieter oder Aktenvernichter. Dieses Outsourcing löst allerdings zahlreiche Datenschutzprobleme aus. Deshalb hat eine Arbeitsgruppe, an der unter anderem die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) und der Berufsverband der Datenschutzbeauftragten Deutschlands e.V (BvD) beteiligt waren, am 28. Januar 2015 einen sogenannten „kommentierten Muster-ADV-Vertrag für die Gesundheitswirtschaft“ publiziert, der helfen soll, die Anforderungen des § 11 BDSG für den Sonderfall sensibler medizinscher Daten einzulösen .

Es bleibt zu hoffen, dass diese Regelwerke zeitnah umgesetzt werden, um die Sicherung von Patientendaten zu gewährleisten, die besonders unter dem Schutz der ärztlichen Verschwiegenheitspflicht und der Geltung des § 203 STGB stehen. ■

Manfred Weitz
Unterriethstr. 35
65187 Wiesbaden
info@update-bdsg.com