Kann Datenschutz töten?

Unterhält man sich als Datenschützer mit Mitarbeitern eines Krankenhauses oder mit Herstellern von Software, die medizinische und administrative Prozesse einer medizinischen Einrichtung unterstützen sollen, ist es fast zwangsläufig, dass das Thema Zugriffsrechte thematisiert wird. Oft genug wird in diesem Zusammenhang angeführt, die Vorgaben des Datenschutzes seien stark limitierend und würden die Patientenversorgung behindern, wenn nicht sogar gefährden. Die KMA (August 2011) titelte gar:"„Daten gesichert, Patient tot - Die neuen Leitlinien der Datenschützer für Krankenhausinformationssysteme gefährden Patienten und lassen den Klinikalltag unberücksichtigt".

Eine derartige Aussage kann einen verantwortungsvollen Datenschützer nicht unberührt lassen. Schließlich ist es nicht innerstes Ziel des Datenschutzes Prozesse zu behindern oder gar die Gesundheit von Patienten zu gefährden.

Seinen Ursprung findet die Thematik in der ärztlichen Schweigepflicht (MBO-Ä) und ihrer negativen Sanktion durch das Gesetz (§ 203 StGB), also nicht primär in datenschutzseitiger Gesetzgebung. Ärzte sind, wenn Sie nicht an der Behandlung beteiligt sind, grundsätzlich auch untereinander, zur Verschwiegenheit verpflichtet.

Dies wird in hochgradig arbeitsteiligen Kliniken oder rechtspersonenübergreifend (z.B. Krankenhaus – MVZ) oft als Problem empfunden, da Berechtigungskonzepte, die den jeweiligen Zugriff eines Konsiliars auf die hierfür notwendigen Daten im KIS abbilden können, nur mit Schwierigkeiten zu implementieren seien. Oft wird gar angeführt, dies sei technisch nicht zu realisieren.

Hieraus ableiten zu wollen, dass aus Gründen der Patientensicherheit generell auf die Vertraulichkeit der Daten verzichtet werden könnte, ist weder rechtskonform, noch für die Vertraulichkeit der Daten der nicht betroffenen Personen vertretbar. Die Musterberufsordnung Ärzte selbst hält ausdrücklich fest, dass die Behandlung u.a. unter Berücksichtigung des Selbstbestimmungsrechtes des Patienten zu erfolgen hat. Es ist also auch zu berücksichtigen, dass das Recht auf informationelle Selbstbestimmung gewahrt bleibt.

Im Rahmen der Rechtsgüterabwägung sollte selbstverständlich ein protokollierter und kontrollierter Zugriff auf Patientendaten ohne Auswertung eines Berechtigungskonzeptes, ein sogenannter Notfallzugriff, möglich sein. Jedoch können in der Zukunft mögliche Bedrohungen des individuellen Gutes der Gesundheit nicht zu einer kollektiven Aufgabe der Vertraulichkeit der Daten der Nichtbetroffenen führen.

In bestimmten Situationen kann die Schweigepflicht auch unter den Ärzten verschiedener Fachdisziplinen innerhalb eines Hauses im Interesse des Patienten liegen. Eine sexualmedizinische Beratung oder eine in vitro-Fertilisation ist nicht zwingend ein Alltagsthema und deren Kenntnis z.B. im Rahmen einer Traumaversorgung grundsätzlich keine zwingende Voraussetzung für den Behandlungserfolg.

Auch wenn eine Verpflichtung zu einer sorgsamen Behandlung besteht, hat der Behandelnde nicht das Recht, alle vorliegenden Informationen über den Patienten ohne dessen Wissen und Einwilligung einzusehen. Um so wichtiger wird dann natürlich eine revisionssichere Zugriffsprotokollierung, damit der Arzt im Zweifelsfalle nachweisen kann, dass er tatsächlich nicht über eine bestimmte Information verfügt hat. Die Entscheidung, wer von ihm welche Daten einsehen darf, liegt grundsätzlich erst einmal und immer noch im freien Willen des Patienten.

Grundsätzlich ist ein Berechtigungskonzept anhand der rechtlichen Vorgaben klar modellierbar. Es ist die ärztliche Schweigepflicht zu berücksichtigen und der freie Wille des Patienten ist zu respektieren. Weitere Beschränkungen sind erst einmal nicht erkennbar. Die Behandelnden können auf die notwendigen Daten im Behandlungszusammenhang zugreifen, selbst im Falle eines Notfalls. Also muss das 'Problem' Berechtigungskonzept eine andere Ursache haben, die zu finden wäre.

Moderne medizinische Versorgung ist spezialisiert, vernetzt, interdisziplinär und hochgradig arbeitsteilig. Dies führt zwangsläufig zu einer steigenden Zahl von organisatorischen und technischen Schnittstellen, die durch entsprechende Datenflüsse begleitet werden. Daher ist es nicht verwunderlich, dass der Komplexität der Versorgung eine organisatorische Komplexität folgt.

IT-Verfahren sollten dem Ziel folgen, Geschäftsprozesse zu modellieren und zu unterstützen. Hier scheint jedoch das eigentliche Problem beheimatet zu sein. Die herrschenden Prozesse der Softwarentwicklung und des Produktlebenszyklus können nur noch schwer den organisatorischen und rechtlichen Rahmenbedingungen des sich immer schneller entwickelnden Medizinsektors folgen. Dies mit der Folge, dass sich die bestehenden an der medizinischen Versorgung ausgerichteten Prozesse an den von der Software vorgegebenen ausrichten sollen. Eine derartige Vorgehensweise ist jedoch weder wirtschaftlich noch medizinisch wünschenswert, sollte doch die Versorgung des Patienten im Mittelpunkt des Geschehens stehen.

Es wäre wünschenswert, Methoden der Modellierung zu finden, die die tatsächlichen Bedürfnisse der Krankenversorgung abbilden helfen. In keinem Fall wird es stattdessen dienlich sein, die Kausalkette zu kehren und zu erklären, dass die Vorgaben des Eckpunktepapiers zu einer Behinderung des Klinikalltags beitragen würden.

Von den normativen Eckpunkten hin zu einer Checkliste werden noch Jahre vergehen. Dieser Weg ist jedoch unabdingbar, da von generell abstrakten Regelungen auf Standards abzuzielen ist. Datenschutz lebt von der konkreten technischen und organisatorischen Ausgestaltung. Nur so kann das Recht auch faktisch zur Geltung gebracht werden. Gelingt dies nicht, besteht die Gefahr, dass das Recht sich in Unrecht wendet.

Dass es sich beim Datenschutz um ein sehr hohes Gut handelt, die bestmögliche Versorgung des Patienten jedoch an oberster Stelle steht, ist kein Widerspruch. Die Vertraulichkeit von Gesundheitsdaten ist nicht nur eine gesetzliche Pflicht, sie sollte von allen Beteiligten im Sinne des Patienten als selbstverständlich angesehen werden. Integrität und Verfügbarkeit sowie Authentizität als allgemeine Sicherheitsziele sind geeignet, die Patientensicherheit weiter zu erhöhen. Die Annahme einer Gefährdung durch den Datenschutz erscheint dahingehend abwegig.

Autor: Dr. Stefan Reuschke

Grid eG
Eckerkoppel 89
22159 Hamburg
email: info@grideg.deinfo@grideg.de
Internet: www.grideg.de