

Orientierungshilfe Krankenhausinformationssysteme – aus Sicht der Datenschutzbeauftragten

BvD Arbeitskreis Medizin
10.06.2011

Einleitung

- Der besondere Schutzbedarf von Gesundheitsdaten stellt hohe Anforderungen an die Umsetzung des Datenschutzes in Krankenhäusern und insbesondere an die Auswahl und Gestaltung der dort eingesetzten Datenverarbeitungssysteme. Die strafrechtlich normierte berufliche Schweigepflicht des § 203 Strafgesetzbuch setzt für alle im Gesundheitswesen tätigen Berufsheimnisträger einschließlich deren berufsmäßig tätigen Gehilfen enge Grenzen für eine zulässige Offenbarung von Patientendaten. Diese dürfen ausschließlich im befugten Umfang zugänglich sein, soweit dies zur Aufgabenerfüllung erforderlich ist und eine Weitergabe aufgrund gesetzlicher Vorgaben erlaubt ist bzw. hierzu die wirksame Einwilligung des Patienten vorliegt.
- Das vom Bundesverfassungsgericht formulierte Recht auf informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind entscheidende Maßstäbe für den datenschutzkonformen Einsatz von KIS:
Der Patient hat – eingeschränkt durch klare gesetzliche Vorgaben – das umfassende Recht, selbst über die Verwendung seiner Patientendaten zu bestimmen.
KIS müssen so gestaltet sein und betrieben werden können, dass die Vertraulichkeit der Patientendaten bei deren Anwendung im Klinikalltag gewährleistet werden kann.
- Fehlende Regelungen für den Zugriff auf Patientendaten einschließlich der Zugriffsprotokollierung stellen auch einen Verstoß gegen das Recht auf Achtung des Privat- und Familienlebens gemäß Artikel 8 der Europäischen Menschenrechtskonvention dar. Der Europäische Gerichtshof für Menschenrechte hat in seinem Urteil vom 17.10.2008 (ECHR Application No. 20511/03) im Zusammenhang mit der fehlenden Protokollierung von Zugriffen auf medizinische Daten eines Krankenhausinformationssystems einen Verstoß gegen Artikel 8 festgestellt.
- Der Arbeitskreis Medizin des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. begrüßt die Orientierungshilfe „Krankenhausinformationssysteme (KIS) datenschutzgerecht gestalten und betreiben“, die von der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 verabschiedet wurde. Sie stellt klar, dass im Informationszeitalter KIS so gestaltet werden müssen, dass auch hier die ureigene ärztliche Schweigepflicht gewahrt werden kann. Nur so ist ein vertrauensvolles Verhältnis zwischen Arzt und Patient möglich und das Persönlichkeitsrecht des Patienten wird angemessen geschützt.

A. Aufgaben eines betrieblichen Datenschutzbeauftragten im Krankenhaus

In Hinblick auf den Einsatz von KIS hat ein Datenschutzbeauftragter insbesondere folgende Aufgaben:

- Er berät das Krankenhaus als verantwortliche Stelle über einen rechtskonformen Einsatz von KIS.
- Der Datenschutzbeauftragte wirkt auf die datenschutzgerechte Gestaltung von IT-Systemen und Abläufen hin. In KIS gehören hierzu beispielsweise eine der Aufgabenerfüllung angepasste Berechtigungssteuerung oder die Abbildung organisatorischer Abläufe des Krankenhauses.
- Er führt die Vorabkontrolle beim erstmaligen Einsatz eines KIS bzw. bei wesentlichen Änderungen des KIS durch.
- Er überwacht die Einhaltung der vereinbarten Datenschutz-Vorgaben und –Maßnahmen beim Einsatz dieser Systeme. Dazu gehören beispielsweise Stichprobenkontrollen anhand der Protokollierung von Zugriffen sowie die Beratung bei der Anpassung der Berechtigungen neuer Abläufe oder Anforderungen.
- Er überwacht die Einhaltung der datenschutzrelevanten Gesetze.
- Er sensibilisiert die verantwortliche Stelle und die Beschäftigten des Krankenhauses.

B. Probleme, insbesondere beim KIS

- Die Interpretation der oft allgemeinen Formulierungen in den Datenschutzgesetzen wie „zur Aufgabenerfüllung erforderlich“ oder „Verhältnismäßigkeit“ führt immer wieder zu Diskussionen bei den Betreibern und Herstellern. Das Krankenhaus als verantwortliche Stelle muss gerade im Hinblick auf immer neue Kostenersparnis im Gesundheitswesen auch den finanziellen Aufwand für die vorgeschlagenen Maßnahmen berücksichtigen. Die KIS-Hersteller realisieren oft nur das, was klar und eindeutig gesetzlich gefordert wird oder was von den Kunden – sprich den Krankenhäusern – verlangt und bezahlt wird.
- Diese Abwägungen führen zu einem ständigen Spagat zwischen der Wahrung der persönlichkeitsrechtlichen Interessen der Patienten und dem hierzu erforderlichen Aufwand bzw. den Kosten im Krankenhaus. Der Nutzen des Patienten – nämlich ein besserer Schutz seines informationellen Selbstbestimmungsrechtes und die Gewährleistung der Vertraulichkeit – lässt sich nicht in Euro beziffern. Die Kosten einer Software-Verbesserung oder Änderung von Abläufen hingegen schon. Klare Formulierungen für die Anforderungen an die technische Umsetzung in KIS fehl(t)en bisher.
- Die reale Datenschutzpraxis im Krankenhaus weist zum Teil erhebliche Datenschutzlücken auf. Probleme bestehen einerseits darin, die Datenschutzerfordernungen im Klinikalltag sowohl praxisgerecht als auch rechtskonform abzubilden. Zum anderen sind die Möglichkeiten zur Umsetzung in KIS derzeit begrenzt. Die gegenwärtig praktisch gestaltbaren Zugriffsrechte in KIS der Krankenhäuser spiegeln oft nur unzureichend die Wirklichkeit der heutigen realen Krankenhausprozesse und -strukturen wider und erschweren somit die korrekte Umsetzung der einschlägigen datenschutzrechtlichen Anforderungen.
- KIS-Hersteller implementieren die datenschutzrechtlichen Anforderungen nicht in ihre Softwaresysteme bzw. realisieren dies nur gegen (hohen) Aufpreis. Die KIS-Hersteller sind daher aufgefordert, ihre KIS-Systeme nachzubessern, um einen praxisgerechten **und** rechtskonformen Einsatz im Krankenhausalltag zu ermöglichen.

C. Die Orientierungshilfe ist eine Hilfe für uns Datenschutzbeauftragte

- Die Orientierungshilfe konkretisiert die allgemein geltenden datenschutzrechtlichen Anforderungen sowie die Vorgaben zur ärztlichen Schweigepflicht und beschreibt die Umsetzung der hierzu erforderlichen technischen und organisatorischen Maßnahmen. Durch die klarstellenden Formulierungen erhalten wir als Datenschutzbeauftragte direkte Unterstützung bei unseren Abwägungen und Diskussionen mit allen Beteiligten auf Betreiber- und Herstellerseite.
- Die in der Orientierungshilfe dargestellten Anforderungen sind im Prinzip nicht neu – wir Datenschutzbeauftragte vor Ort fordern bei unseren Beratungen und Vorabkontrollen immer wieder bessere Möglichkeiten zur Berechtigungssteuerung sowie zur datenschutzgerechten Gestaltung von Abläufen. Uns hilft es deshalb, wenn diese Anforderungen nun auch von den Aufsichtsbehörden und Landesbeauftragten für den Datenschutz als Orientierung für einen datenschutzgerechteren Einsatz von EDV-Systemen in Krankenhäusern verabschiedet wurden.
- Sie ist auch eine Hilfe für uns, den Stellenwert des Datenschutzes gerade bei medizinischen Daten zu betonen. Nicht nur bei Facebook und Google ist das Persönlichkeitsrecht des Bürgers gefährdet. Gerade bei KIS mit besonders sensiblen medizinischen Daten muss darauf geachtet werden, dass der Kreis der "Geheimnisträger" auf das erforderliche Maß im befugten Umfang beschränkt bleibt.
- Durch die gesteigerte Sensibilität werden auch die Priorität und Bereitschaft erhöht, bestimmte Maßnahmen in den verantwortlichen Stellen zu treffen oder bei den Herstellern zu realisieren.
- Die Protokollierung von Zugriffen stellt ein gutes Instrument in Verbindung mit vereinbarten Auswertungen dar, die Einhaltung von Berechtigungsvorgaben zu kontrollieren. Dies wird in der Orientierungshilfe klar hervorgehoben. Wir Datenschutzbeauftragte erhoffen uns daher mittelfristig bessere Möglichkeiten der Protokollierungssteuerung und gute Instrumente zur Auswertung. Hier müssen die Hersteller noch einiges nachbessern.

- Wenn ein Hersteller die Anforderungen der Orientierungshilfe – auch in Teilen – erfüllt, ist dies ein eindeutiges Qualitätsmerkmal seines Produkts. Ein Beachten der Orientierungshilfe verschafft dem Hersteller dadurch klare Wettbewerbsvorteile. Das Krankenhaus kann auch im Rahmen seines Qualitätsmanagements dies als Verbesserung verwenden.
- Konkret im Alltag dient die Orientierungshilfe uns Datenschutzbeauftragten als „Checkliste“ im Rahmen einer Vorabkontrolle oder bei der Beratung für die Auswahl von IT-Systemen in Krankenhäusern.

D. Probleme im Alltag bei der Umsetzung der Orientierungshilfe

- Eine integrierte medizinische Patientenversorgung führt zu neuen Abläufen und teilweise komplizierten Strukturen im Ablauf. Diese müssen dann in eine Berechtigungsstruktur im KIS umgesetzt werden. Abläufe in Zentren mit zusammengefassten klassischen Abteilungen, Boards (z.B. für Tumoren und Infektionen), Bettenbänder usw. können mit den bisherigen KIS nicht abgebildet werden. Das Krankenhaus hat dadurch keine Möglichkeit, die Zugriffskonzepte im KIS so zu gestalten, dass sie zu den neuen Versorgungskonzepten passen.
- Ambulante medizinische Versorgungszentren (MVZ), Telemedizin, medizinische Kooperationsgemeinschaften – auch diese von der Politik gewünschten und unterstützten Formen der medizinischen Versorgung – werden hinsichtlich der Zugriffsberechtigungskonzeption bei den KIS-Herstellern noch nicht ausreichend berücksichtigt.
- Datenschutz muss im Alltag gelebt werden können. Daher müssen auch die Alltagsprobleme wie Berechtigungsvergabe (Notdienst, Springer, Bettenbänder, ...), integrierte Versorgung, Aufnahme des Patienten, Haftungsfragen datenschutzkonform **und** praxisgerecht gelöst werden.
- Datenschutz darf nicht zu mehr Bürokratie führen. Dies schadet der Akzeptanz und führt im Endeffekt zu weniger Datenschutz im klinischen Alltag. Im Mittelpunkt steht die Behandlung des Patienten – natürlich unter Beachtung seines Persönlichkeitsrechts.
- Weiterhin ungelöst sind Probleme durch die unterschiedliche Gesetzeslage je nach Träger, Bundesland oder Organisationsform. Teilweise gravierende Unterschiede in den Ausführungsgesetzen zum Datenschutz führen zu unterschiedlichen Anforderungen, die auch in den KIS abgebildet und umgesetzt werden müssen. Eine Harmonisierung auf dieser Ebene wäre wünschenswert.

E. Im Gespräch bleiben

- Die Orientierungshilfe ist für uns Datenschutzbeauftragte vor Ort zum einen eine gute Hilfe, zum anderen hat sie neue Fragen aufgeworfen. Die Handhabung der Orientierungshilfe im Alltag muss sich jetzt bewähren.
- Ohne Unterstützung der Hersteller kann das Krankenhaus viele Anforderungen aus der Orientierungshilfe nicht umsetzen. Hier haben wir nun eine Gesprächsbasis für Weiterentwicklungen.
- Auch die Orientierungshilfe selbst muss weiterentwickelt werden. In der praktischen Handhabung wird es hier sicher Anregungen und Verbesserungsvorschläge geben, die mit aufgenommen werden sollten.
- Wir Datenschutzbeauftragte vor Ort und die Aufsichtsbehörden bzw. Landesdatenschutzbeauftragten haben das gleiche Ziel:
Verbesserung des Datenschutzes durch bessere Gestaltung der KIS bei der medizinischen Versorgung, nicht nur im Krankenhaus. Gemeinsam können wir vor Ort, politisch und im Gespräch den Datenschutz voranbringen.