Stellungnahme der GMDS-AG DGI

zur Orientierungshilfe

„Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen“

der Datenschutzbeauftragten des Bundes und der Länder

Die Orientierungshilfe besteht aus vier Teilen:

- Begleitpapier
- Glossar
- Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus
- Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

Sie ist online zu finden unter
http://www.datenschutz-bayern.de/technik/orient/oh-kis.pdf
Das Papier ist nicht direkt rechtlich bindend. Da es bei künftigen Datenschutzbegutachtungen zu Grunde gelegt wird, muss man aber davon ausgehen, dass es den State-of-the-Art prägen wird.

Die Orientierungshilfe setzt bei der Beobachtung an, dass gegenwärtige KIS die rechtlichen Anforderungen oft mangelhaft abbilden, insbesondere die ärztliche Schweigepflicht und daraus resultierende besonders strikte Datenschutzanforderungen wie die „Datenhoheit der Fachabteilung“. Die Abbildung dieser Anforderungen durch die Rechte- und Rollenverwaltung in den gängigen KIS ist zu grob und unflexibel. Hersteller und Betreiber schieben sich als Entschuldigung oft gegenseitig den „Schwarzen Peter“ zu. Die eigentlichen Gründe sind bei den Herstellern Kosten und mangelnde Attraktivität von Sicherheitsfunktionen, bei den Betreibern die Komplexität der Maßnahmen und die Furcht vor Behinderung der Funktion in kritischen Momenten.

Aus diesem Dilemma soll die Orientierungshilfe als externe Initiative mit normativer Kraft helfen, indem sie Best-Practice-Leitlinien definiert. Diese entsprechen in großen Teilen den bereits früher publizierten Empfehlungen der AG DGI und werden grundsätzlich begrüßt.

Der Fokus der Orientierungshilfe bewusst eng gehalten und umfasst nur die Funktion eines KIS im engeren Sinne.

Hauptkritikpunkte der AG DGI (die Nummern in den Anmerkungen beziehen sich auf die technischen Anforderungen):

1. Die Empfehlungen sind z. T. vage. Es wird oft nicht unterschieden zwischen Forderungen, die mit der gegenwärtigen KIS-Technik unmittelbar erfüllt werden könnten (z. B. Kennzeichen wie in 1.7 – 1.12), Forderungen, zu deren Erfüllung bei Herstellern und Betreibern existierende, aber noch nicht eingesetzte Technik nötig wäre und die Know-How-Erwerb und somit größeren Aufwand

nach sich ziehen (z. B. kryptographische Mechanismen wie in 2.8 und 3.15, Standards oder Services wie Single-Sign-On in 2.3 und 6.2), und Forderungen, die die (Weiter-) Entwicklung neuer technischer Ansätze notwendig macht (z. B. „RFID-Armbänder“ zur Login- und Nutzer-Kontrolle). Mögliche Interoperabilitätsprobleme werden nicht thematisiert. Probleme der Standardisierung können die Erfüllung mancher der Anforderungen noch für längere Zeit verhindern (1.6, 2.7, 2.10, 2.11, 2.13, 3.1, 6.1). Z. B. erfordert eine konsistente Umsetzung von Zugriffsregelungen in „autonomen“ Subsystemen des KIS eine serviceorientierte Architektur, die neben einem zentralen Verzeichnisdienst mindestens noch einen zentralen Berechtigungsdienst bereitstellt.

2. Die Dynamik des Krankenhausbetriebs wird nicht genügend berücksichtigt. Sie bringt oft ganz kurzfristige Übernahmen von Aufgaben mit sich, die in Dienstplänen nicht schnell genug „online“ abgebildet werden können. Der Bezug auf Dienstpläne zur Zugriffsregelung, wie in 4.1 und 4.10 beschrieben, stößt daher an praktische Grenzen. Auch zeitkritische Wartungszugriffe, z. B. auf Medizingeräte, können an statischen Zugriffsregelungen scheitern.

3. Belange der medizinischen Forschung werden nicht berücksichtigt. Die Unterstützung der medizinischen Forschung ist auch im Sinne der Patienten wünschenswert (Forschung sollte stets im weiteren Sinne verstanden werden: von einfachen Auswertungen zum Vergleich von Behandlungserfolgen im Sinne des Benchmarking bis hin zur klinischen Spitzenforschung). Fast jedes medizinische Datum ist forschungsrelevant. Ein erster Schritt ist der Aufbau eines klinischen Datawarehouse oder von klinischen Registern. Hier sollte auch eine pseudonymisierte Langzeitdatenspeicherung möglich sein; die Forderung der Anonymisierung (1.15) schränkt die Brauchbarkeit der Daten zu früh ein, z. B., wenn Langzeitbehandlungen oder Spätfolgen ausgewertet werden müssten oder (auch ehemalige) Patienten für klinische Studien rekrutiert werden sollen, insbesondere wenn der Studienarzt nicht der ursprüngliche Behandler ist. Auch die Löschfristen nach 2.12 könnten in diesem Kontext ohne weitere Differenzierung kontraproduktiv sein. Im Gegenzug sollte die „Selbstbedienung“ im klinischen Datawarehouse auch bei anonymisiertem Zugriff explizit ausgeschlossen werden.

4. Eine zu weitgehende Forderung nach Pseudonymisierung kann die Sicherheit der Abläufe im Krankenhaus beeinträchtigen. Es gibt von Herstellern und Betreibern Befürchtungen, dass etwa Daten für Funktionsbereiche wie Labore, die mit dem Patienten keinen persönlichen Kontakt haben, nur pseudonymisiert bereitgestellt werden dürften. Die Arbeitsprozesse im Krankenhaus beziehen aber einen Teil ihrer Sicherheit aus der Redundanz, beispielsweise, dass der Name des Patienten in Befunden, teilweise auch in Bildern, im Klartext steht, so dass Fehler und Unklarheiten auch mal kurz per Telefon besprochen werden können. Sobald menschliche Kommunikation im Behandlungszusammenhang involviert ist, sind Pseudonyme zu fehleranfällig. Hier bietet die Orientierungshilfe wenig Unterstützung, um Erforderlichkeit und Angemessenheit abzuwägen.

5. Funktionen, die das Auskunftsrecht der Patienten unterstützen, werden nicht direkt angesprochen. Diese könnte man in 2.9 (Auskunft über die gespeicherten Daten) sowie in 3.14 (Auskunft über erfolgte Zugriffe) deutlicher herausstreichen. Ähnliches gilt für Auskunftsrechte von Mitarbeitern bezüglich der Protokollierung, siehe Punkt 7 dieser Aufzählung.

6. Die Frage, wie weit vor dem Hintergrund des §203 StGB externe Dienstleistungen genutzt werden dürfen, wird kaum behandelt. Das betrifft das Outsourcing (von Teilen) der KIS-Betreuung, etwa bei komplexen Medizingeräten, mit Fernwartung und Fernadministration, oder auch Reparaturvorgänge bei Hardware-Versagen oder hartnäckigen Software-Fehlern, wo unbeabsichtigte Einblicke des Dienstleisters in Patientendaten nicht sicher auszuschließen sind. Die in 2.8 geforderte Verschlüsselung von Speichermedien könnte in einigen dieser Fälle nicht durchzuhalten sein.

7. Die geforderten Logging- und Protokollier-Funktionen (besonders in Abschnitt 7) könnten in der Praxis wegen hohem Ressourcenverbrauch das KIS unzumutbar belasten. Welche Gesichtspunkte soll man hier zur Beurteilung der Angemessenheit beachten? Sind hier Forderungen an die Hersteller nötig? Es fehlen Hinweise darauf, dass die Mitarbeiter auch Datenschutzrechte an den protokollierten Daten haben (Mitteilung und Transparenz der Protokollierung, insbesondere, wenn die Protokollierung zu unterschiedlichen Zeiten unterschiedlich konfiguriert ist, sowie Auskunftsrechte, die evtl. auch durch Systemfunktionen unterstützt werden sollten, auch wer auf die Protokolldaten zugreifen kann bzw. zugegriffen hat). Außerdem muss vermieden werden, dass medizinische Daten in der Logdatei auftauchen (z. B. „Herr Müller-Lüdenscheid erlitt eine schwere allergische Reaktion auf den Genuss eines flambierten Hähnchenschenkels; daher Notfallzugriff erforderlich.“).

8. Beim Rollen- und Berechtigungskonzept sind einige Gruppen von Mitarbeitern nicht aufgeführt, die nicht direkt ärztliche oder pflegerische Aufgaben haben, wie verschiedene Arten technischer Assistenten und medizinischer Hilfsberufe. Dazu gehören Medizinisch-technischer Assistent (MTA, MTRA, MTLA), Anästhesietechnischer Assistent für Funktionsdiagnostik, Operationstechnischer Assistent (OTA), Pharmazeutisch-technischer Assistent (PTA), Orthopädieschuhtechniker, Zahntechniker, Hörgeräteakustiker, Augenoptiker, Physiotherapeut, Psychologe (psychosozialer Dienst), Hebamme, Masseur oder medizinischer Bademeister, Diätassistent, Ergotherapeut, Logopäde.