Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

P R E S S E E R K L Ä R U N G

2. Juni 2009

Papierloses Krankenhaus = gläserner Patient ?

Datenschutz-Risiken der elektronischen Patientenakte

Das papierlose Krankenhaus setzt sich durch. Datenschutzrechtliche Prüfungen im UKE und bei Asklepios sowie Workshops mit den Datenschutzbeauftragten der Hamburger Krankenhäuser offenbarten erhebliche Missbrauchsgefahren bei der Nutzung der elektronischen Patientenakten.

Die Versuchung für Klinikmitarbeiter, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen, privat zu nutzen oder womöglich an Medien zu verkaufen, ist kein Hirngespinst besonders misstrauischer Datenschützer. Missbrauch gab es schon bei der Papierakte. Bei der elektronischen Patientenakte ist dieser jedoch ungleich leichter - wie auch der Fall einer prominenten Patientin im UKE in der jüngeren Vergangenheit zeigte.

Die konventionelle Patientenakte aus Papier ist einmalig, liegt zur selben Zeit nur an einem Ort und kann nur von einer Person zugleich gelesen werden - ein physikalisches Gesetz.
Die elektronische Patientenakte kann dagegen prinzipiell **von sehr vielen Krankenhausmitarbeitern gleichzeitig gelesen**, gespeichert, kopiert und übermittelt **werden** - auf Knopfdruck am Arbeitsplatz, ohne Aktensuche, Nachfragen, Transport, Durchsuchen usw. Das ist ihr Vor-

www.hamburg.datenschutz.de
E-Mail: mailbox@datenschutz.hamburg.de
Klosterwall 6 - D-20095 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00
Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 53D9 64DE 6DAD 452A 3796 B5F9 1B5C EB0E).

teil, gerade auch ihr medizinischer: sekundenschnelle, aktuelle, vollständige Informationen für die optimale Behandlung des Patienten.

Das ist aber auch ihr Risiko: **Kann sichergestellt werden, dass** wirklich **nur diejenigen Krankenhausmitarbeiter/innen Zugriff** auf die sensiblen Daten **bekommen**, **die** tatsächlich **mit der Behandlung des Patienten** und ihrer verwaltungsmäßigen Abwicklung **zu tun haben?** Das Hamburgische Krankenhausgesetz fordert genau das - und zwar nicht nur als Gebot (zugreifen dürfen), sondern als technische Bedingung (zugreifen können). Während die Papierakte dies durch ihre Einmaligkeit und örtliche Gebundenheit in wesentlichen Zügen bereits erfüllt, müssen bei der elektronischen Form erst entsprechende Zugriffsregelungen etabliert werden.

Die bestehenden Konzepte für den Zugriff auf elektronische Patientenakten folgen jedoch einer ganz anderen Logik: **Der Zugriff wird allen Ärzten, Schwestern und Funktionskräften eingeräumt, die *in Zukunft wahrscheinlich oder möglicherweise* mit der Behandlung des Patienten zu tun haben könnten**: Bei der Aufnahme in das Krankenhaus wird der Patient auf die elektronische Bearbeitungsliste der behandelnden *Fachabteilung (z.B. HNO)* gesetzt. Statt des einen behandelnden Arztes (und seines Vertreters) können dadurch alle Ärzte derselben Fachabteilung, alle für alle Stationen der Abteilung zuständigen Stationsärzte und Schwestern / Pfleger auf den gesamten Datenbestand des Patienten zugreifen - egal, ob sie den Patienten während seines Aufenthalts tatsächlich kennenlernen oder nicht. Die Akte „liegt“ nicht mehr beim Patienten im Stationszimmer zur Einsichtnahme bei einem konkreten medizinischen Bedarf, sie steht „im Netz“, im Krankenhausinformationssystem (KIS), grundsätzlich abrufbar per Knopfdruck von allen Mitgliedern der behandelnden Einheit.

In einem großen Krankenhaus stellten wir fest, dass am selben Tag 20 Ärztinnen und Ärzte auf die Daten von 50 stationären und 50 ambulanten Patientinnen und Patienten ihrer Fachabteilung zugreifen konnten. Hinzu kommt, dass im modernen Krankenhaus interdisziplinär gearbeitet wird, viele Ärztinnen und Ärzte deswegen mehreren Fachabteilungen (mit den entsprechenden Zugriffsrechten) zugeordnet sind. Schwestern sind zur Flexibilisierung und „Verschlankung“ des Personaleinsatzes nicht mehr nur für „ihre“ eine Station zuständig, sondern ggf. auch noch für mehrere andere. Das vervielfältigt die Zugriffsmöglichkeiten, ohne aber die Kapazität für konkrete Patientenkontakte zu erhöhen.

Und weiter: Wird für die Behandlung ein abteilungsfremder Spezialist benötigt (sog. Konsil), erscheint dies nicht in dessen persönlicher Arbeitsliste, sondern in der Abteilungsliste, auf die

alle Mitarbeiter/innen der Abteilung zugreifen können. Die Abteilung soll selbst die freien, kompetentesten Experten auswählen. **Selbst nach der Übernahme der Aufgabe durch einen der Spezialisten ist eine Ausblendung der Patientendaten für die anderen nicht sichergestellt.** Dieses Konzept gilt auch für klinikübergreifende Fachkräfte-Pools wie **Anästhesisten, Physiotherapeuten, Sozialdienste** und teilweise auch Notfallaufnahmen. Sie haben in einzelnen Krankenhäusern Zugriff auf die Daten aller Patienten.

Und weiter: Neben den medizinisch und pflegerisch tätigen Krankenhausmitarbeiter/innen erhalten auch viele Funktionskräfte Zugriffsrechte für die Patientendaten. Dies ist besonders bei zentralen Einheiten wie **„Casemanagement" / Patientenverwaltung / Abrechnungsstelle** bedeutsam, weil sie einerseits auch medizinische Details aus der Patientenakte verarbeiten und andererseits Zugriff auf Daten aller Patienten des Krankenhauses haben. Die aus Zeiten der Papierakte bekannte Zuständigkeitsbeschränkung nach Anfangsbuchstaben der Patientennamen ist entfallen.

Und weiter: Die allgegenwärtige EDV muss von IT-Sachverständigen gepflegt und aktualisiert werden. Aus diesem Grunde haben zusätzlich immer auch mehrere Personen der **IT-Abteilung** nicht nur Zugriff auf die Systemdateien, sondern auch - mehr oder weniger - freien Zugriff auf Patientendaten. Und dies gilt nicht nur für schweigeverpflichtete Mitarbeiter des Krankenhauses, sondern auch für die **Techniker der Software-Hersteller**. Die Systeme von elektronischen Patientenakten sind so komplex, dass das Krankenhaus leicht in eine Abhängigkeit vom Hersteller gerät und auch die Übersicht darüber verliert, auf welche Daten die Mitarbeiter der Hersteller zugreifen und was sie mit ihnen machen. Nicht selten wurde der Datenschutzbeauftragte bei seinen Prüfungen direkt an die Vertreter der Software-Hersteller verwiesen. Manchmal drängte sich die Frage auf, ob das Krankenhaus seine Funktion als datenschutzrechtlich verantwortliche Stelle auch in der Realität noch voll wahrnimmt und überhaupt wahrnehmen kann.

Und weiter: Die aufgezeigten Datenschutzrisiken bestehen fort, solange ein Datenzugriff möglich bleibt. Die vom Hamburgischen Krankenhausgesetz geforderte **Sperrung der Patientendaten nach Abschluss der Behandlung** und Abrechnung wird vom größten einschlägigen Software-Hersteller technisch nicht oder **kaum unterstützt**. Wer Zugriffsrechte hatte, behält sie - jedenfalls als Arzt. Nur die modernsten Systeme erlauben eine Befristung der Zugriffsrechte.

Je weiter die Entwicklung zur integrierten, alle Subsysteme umfassenden elektronischen Patientenakte fortschreitet, desto größer werden tendenziell die beschriebenen Datenschutzrisiken.

Zwar ist eine flächendeckende Dokumentation aller Datenzugriffe technisch möglich, eine flächendeckende Auswertung dieser Protokolldaten zur Entdeckung von Missbräuchen ist praktisch jedoch nicht zu realisieren. Es wird vor allem darauf ankommen, die Logik der Zugriffsberechtigungskonzepte umzustellen auf eine stärkere Bindung an den konkreten Behandlungszusammenhang, auf eine deutliche Verringerung der Lücke zwischen „zugreifen können“ und „zugreifen dürfen“. Hierbei sind nicht nur die Krankenhäuser als Anwender, sondern auch die **Software-Hersteller in der Pflicht**. Nur Systeme, die in der Lage sind, die datenschutzrechtlichen Anforderungen zu erfüllen, werden sich in diesem besonders sensiblen Segment dauerhaft am Markt halten können. Wesentlich dabei sind:

- Einführung einer behandlungs- bzw. patientenbezogenen statt (oder zusätzlich zu) einer „rollenbasierten“ bzw. abteilungsbezogenen Zugriffslogik
- Transparenz für den Patienten und Möglichkeiten für seine aktive Mitwirkung (wer kann auf meine Daten zugreifen, wer hat zugegriffen, wen will ich zum Zugriff ermächtigen?)
- Berücksichtigung der speziellen Belange besonderer Patientengruppen wie Prominente oder Krankenhausmitarbeiter ohne Schaffung medizinischer Risiken
- Ausreichende Systemtransparenz um einen verantwortlichen Betrieb durch das Krankenhaus zu ermöglichen.

Die gesetzlichen Datenschutzregelungen zur **elektronischen Gesundheitskarte** tragen dem bereits weitgehend Rechnung. Der Wille des Gesetzgebers ist deutlich. Für die krankenhausinterne elektronische Patientenakte gibt es dagegen keine spezifischen gesetzlichen Vorgaben. Wie beide Zugriffs-Logiken in Zukunft zusammengeführt werden können, bleibt weitgehend ungeklärt.

Kontakt/Rückfragen:

Dr. Hans-Joachim Menzel, Tel. 428 54 – 4049

Ulrich Kühn, Tel. 428 54 – 4054