

Anmerkungen zum Umgang mit der Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder

Berlin, Oktober 2011

Der Bundesverband Gesundheits-IT (bvitg) e.V. vertritt in Deutschland die führenden IT-Anbieter im Gesundheitswesen und repräsentiert mit seinen Mitgliedern 90 Prozent des stationären, des ambulanten sowie des zahnmedizinischen IT-Marktes. Das Produktportfolio unserer Mitglieder umfasst sämtliche in den Krankenhäusern eingesetzten IT-Lösungen, von Primärsystemen über Sekundär- und Spezialsystemen hin zu Archivierungslösungen.

Die von den Datenschutzbeauftragten abgestimmte Orientierungshilfe befasst sich mit dem datenschutzkonformen Umgang mit Patientendaten in entsprechenden Einrichtungen und leitet hieraus Anforderungen an die Gesamtheit aller eingesetzten Informationssysteme in den Einrichtungen ab. Die Summe aller Systeme in einer Einrichtung bildet laut Orientierungshilfe das Krankenhausinformationssystem – KIS. Die Orientierungshilfe erweitert folglich die Definition der KIS um die Sekundär- und Spezialsysteme und weicht durch die Zusammenfassung unterschiedlicher, in der Regel über Schnittstellen kommunizierender, Systeme von unserem Verständnis eines KIS ab. Die damit im Zusammenhang stehenden Anforderungen stellen in deren Umsetzung hohe technische Hürden auf.

Alle Betreiber, aber auch alle Hersteller entsprechender IT-Lösungen für Einrichtungen des Gesundheitswesens, sind in der Regel direkt, mindestens aber indirekt von der Orientierungshilfe und deren Auswirkungen betroffen.

Die Orientierungshilfe erfüllt in erster Linie die Funktion, im Falle einer Prüfung der Einrichtung den Prüfern einen Leitfaden an die Hand zu geben, um im Umfeld der unterschiedlichen Regelungen und deren Interpretationen auf Bundes- und Landesebene vergleichende und einheitliche Prüfstandards zu etablieren. Sie soll aber auch eine Hilfestellung für den datenschutzkonformen Betrieb der KIS sein. Adressaten sind folglich neben den Mitarbeitern der Datenschutzbeauftragten des Bundes und der Länder alle Betreiber und auch Hersteller von Krankenhausinformationssystemen im o.g. Sinne, denn letztere sind es, die die technischen Anforderungen anbieten können müssen, um die aufgrund der Umsetzung der Anforderungen aus der Orientierungsrichtlinie geänderte Nachfrage im Sinne ihrer Kunden bedienen zu können.

Die Orientierungshilfe gliedert sich in zwei zentrale Bereiche:

1. Die „Normativen Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus“, die auf einem abstrakten Niveau 41 Anforderungen an Krankenhäuser und ihre IT-Systeme für einen datenschutzkonformen Betrieb formuliert und
2. die „Technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“, die dann diese in technische und organisatorische

Anforderungen an Hersteller und Betreiber von Krankenhausinformationssystemen übersetzt. Das Dokument enthält immerhin 142 detaillierte Anforderungen, die seitens der Betreiber und/oder der Hersteller einzuhalten sind.

Grundsätzliches

Der Bundesverband Gesundheits-IT (bvitg) e.V. begrüßt ausdrücklich das Bestreben der Datenschutzbeauftragten des Bundes und der Länder, Konsens über Regelungen zum Einsatz und Betrieb von Krankenhausinformationssystemen herzustellen. Aus diesem Grunde haben wir den uns vorab zur Kommentierung zur Verfügung gestellten Entwurf der Orientierungshilfe detailliert innerhalb unserer AG-Datenschutz geprüft und umfangreich kommentiert, uns eng mit unseren Partnern, den Bundes- und Landesdatenschutzbeauftragten und der DKG ausgetauscht und uns in mehreren öffentlichen Veranstaltungen zur Orientierungshilfe konstruktiv geäußert.

Wir müssen heute feststellen, dass die Orientierungshilfe in ihrer jetzigen Fassung als erster Schritt gewertet werden kann: Es zeigt sich bereits und es wird sich auch in Zukunft noch zeigen, dass die Anforderungen an die Betreiber und Hersteller in weiten Teilen noch zu unklar und wenig aufeinander abgestimmt sind. Sie widersprechen in mancherlei Hinsicht den heutigen Versorgungsrealitäten und bauen Hürden auf, die einer effektiven und effizienten Prozesssteuerung in komplexen Einrichtungskonglomeraten widersprechen. Eine wortgetreue Umsetzung der formulierten Anforderungen ist technisch nicht immer möglich und im Sinne der Patientensicherheit auch nicht immer wünschenswert.

Der bvitg stellt sich der Diskussion und arbeitet schon jetzt aktiv an der Evaluation der Orientierungshilfe. So wird in Kürze das Ergebnis eines Stresstests veröffentlicht, der den dringenden Klärungs- und Handlungsbedarf beispielhaft aufzeigt. Wir appellieren an alle, sich konstruktiv mit der Orientierungshilfe auseinanderzusetzen. Und wir appellieren an die Verfasser der Orientierungshilfe, den Dialog weiter aufrechtzuerhalten und die Hersteller, die Datenschutzbeauftragten aus den Einrichtungen ebenso wie die Direktoren und IT-Leiter aus den Häusern bzw. deren jeweilige Verbände in den Konsensprozess aktiv einzubinden, ihnen also mehr Mitwirkungsmöglichkeiten zu ermöglichen, als es eine bloße Kommentierung bieten kann. Wir sind überzeugt, dass nur so Akzeptanz hergestellt werden kann und auch nur so in den jeweiligen Einrichtungen die informationelle Selbstbestimmung der Patientinnen und Patienten *und* der Mitarbeiterinnen und Mitarbeiter geschützt bleiben wird, bei gleichzeitiger effektiver und effizienter Versorgung und hoher Patientensicherheit.

Dieser Dialog muss aber neben all den organisatorischen und technischen Implikationen insbesondere das Bewusstsein für den Datenschutz in einem fundamental anderen medizinischen Umfeld, das ganz wesentlich auf Vertrauen zwischen Behandler und Behandelten setzt, schärfen. Es darf nicht sein, dass Datenschutzkonzepte aus einem Umfeld mit einer Misstrauensvermutung in ein durch Vertrauensnotwendigkeit zwischen Behandler und Behandeltem geprägtes Umfeld „eins zu eins“ übertragen werden. Es darf auch nicht sein, dass das unreflektierte Festhalten an datenschutzrechtlichen Anforderungen, die eben nicht für das medizinische Umfeld definiert worden sind, im Extremfall die Sicherheit der Patienten gefährdet.

Auswirkung der Orientierungshilfe für die Krankenhäuser

Die Orientierungshilfe erhebt den Anspruch, für das Thema Datenschutz in den Einrichtungen zu sensibilisieren. Und: Sie erhebt den Anspruch, Hilfsinstrument bei der Frage zu sein, mit welchen Maßnahmen die datenschutzrechtlichen Bestimmungen bei dem Betrieb von KIS eingehalten werden können. Dabei kommt es auf das Ziel an! Verstehen Sie die Orientierungshilfe als Anregung und Anstoß. Wenn Sie mit anderen organisatorischen und/oder technischen Lösungen das gleiche Ziel erreichen, sind Sie ebenfalls auf der sicheren Seite!

Die Orientierungshilfe hat weder ein Gesetz verändert, noch hat sie Gesetzeskraft! Auch wenn der Titel „Normative Eckpunkte“ zunächst anderes vermuten lässt. Die Orientierungshilfe dient zu aller erst den Datenschutzbeauftragten und deren Mitarbeitern, um für anstehende Prüfungen einheitliche Prüfkriterien anwenden zu können. Übrigens: Ein Rückschluss dergestalt, dass die Verabschiedung der Orientierungshilfe Indiz für mehr Prüfungen ist, ist aus unserer Sicht nicht plausibel.

Und dennoch raten wir Ihnen, die Orientierungshilfe zum Anlass zu nehmen, sich innerhalb der Einrichtungen intensiv mit den Anforderungen als Hersteller und als Betreiber zu befassen. Hierbei sollte Folgendes immer beachtet werden:

Datenschutz kann nicht gekauft werden. Datenschutz ist immer ein Zusammenspiel zwischen persönlicher Verantwortung, organisatorischen Regelungen und baulichen und softwaretechnischen Maßnahmen! Die folgenden Beispiele aus der Praxis verdeutlichen das:

1. Eine Verschlüsselung aller Patientendaten nützt nichts, wenn diese vom Bildschirm für die Öffentlichkeit ablesbar sind, weil bspw. hinter den Terminals ein Warteraum ist, der nur durch eine Glasscheibe getrennt ist.
2. Die Möglichkeiten für eine Pseudonymisierung von VIP-Patienten in der Software nützt nichts, wenn intern dann jeder das Recht bekommt, die Klarnamen zu lesen.
3. Ein Gruppen- und Rollenorientiertes Rechtekonzept bringt keinen Nutzen, wenn nicht zusammen mit dem Personal eine Rollenaufteilung gefunden wird, die sich auch in den Arbeitsabläufen widerspiegelt und damit auch ohne Behinderung dieser Abläufe gelebt werden kann.
4. Was nützen dedizierte Abfragen, um Datenschutzprobleme zu identifizieren, wenn kein ausgebildetes Personal zur Verfügung steht, um diese unter Wahrung der Beschäftigtenrechte auszuwerten?

Die Lösungen unserer Mitgliedsunternehmen können die notwendigen Funktionen abbilden und die Träger der Einrichtungen maßgeschneidert unterstützen. Die Einhaltung der datenschutzrechtlichen Bestimmungen und Anforderungen kann indes ausschließlich durch den datenschutzkonformen Betrieb des eingesetzten KIS in Verantwortung des Trägers der jeweiligen Einrichtungen gewährleistet werden.

Also: Befassen Sie sich mit der Thematik in Ihren Einrichtungen, analysieren Sie die KIS und identifizieren Sie Schwachstellen im Betrieb. Beraten Sie gemeinsam mit Ihrem Hersteller, welchen Beitrag er Ihnen zur Lösung leisten kann.

Was wir tun

Aktuell werden die Anforderungen im Detail geprüft und es sind schon einzelne Anforderungen identifiziert worden, die so kaum oder nur mit unverhältnismäßig hohem Aufwand realisiert werden können. So ist z.B. die Forderung, dass Löschanfragen zwischen allen patientendatenhaltenden Systemen automatisch abgeglichen werden, auf Basis heute existierender Standards nicht zu realisieren. Andere Anforderungen, wie bspw. das Recht des Patienten, den Zugriff auf Informationen aus vorherigen Behandlungen zu verbieten, müssen auch in ihrer Auswirkung auf die medizinische Arbeit beurteilt werden.

Diese Fragen werden vom bvitg gemeinsam mit seinen Partnern thematisiert und in die Novellierung der Orientierungshilfe als Stellungnahme der Industrie mit dem Ziel einfließen, die Orientierungshilfe für alle Beteiligten handhabbarer zu machen. Wir stehen auch im Dialog mit der DKG, um gemeinsame Standpunkte zu definieren und festzustellen, welcher Aufwand notwendig ist, um die Prozessabläufe in den Einrichtungen an die Anforderungen aus der Orientierungshilfe anzupassen.

Ferner wurden die bestehenden Sicherheitsmechanismen der Softwarelösungen herstellerseitig in Relation zu den Anforderungen überprüft und untersucht, wie welche Anforderungen umgesetzt werden können. Dabei sind technisch anspruchsvolle und auch klärungsbedürftige Punkte identifiziert worden. Allerdings werden konkrete Implementierungen davon abhängig gemacht, was in den Krankenhäusern tatsächlich genutzt werden soll und kann. Es wird sich zeigen, welche Anforderungen letztlich auch implementiert werden. Eines steht aber schon jetzt fest: Alle in der Orientierungshilfe genannten Anforderungen sind in Summe so nicht umsetzbar. Das hingegen, was unproblematisch und ohne Eingriff in den Prozessablauf schon jetzt seitens der Hersteller getan werden kann, wird schnellstmöglich erfolgen.

Zusätzlich wird herstellerseitig geprüft, ob spezielle Angebote zum Thema Datenschutz gemacht werden können, um die Datenschutzbeauftragten in den Einrichtungen zu unterstützen und die IT-Abteilungen zu entlasten.

Was Sie in Ihren Einrichtungen tun können

Bitte prüfen Sie die Orientierungshilfe dahingehend, an welcher Stelle Eingriffe in Ihre Arbeitsabläufe vorgenommen werden, die aus Ihrer Sicht nicht umsetzbar sind. Bewerten Sie, welche organisatorischen Änderungen durchgeführt werden müssen, um die Anforderungen zu realisieren und nicht zuletzt: fragen Sie Ihre Mediziner, wie diese die Auswirkungen auf ihre Arbeit sehen. Nur Sie als Leistungserbringer können die Auswirkungen auf Ihre Abläufe beurteilen und Sie sind als Betreiber der Systeme in einer nicht delegierbaren Verantwortung. Beachten Sie dabei, dass Patientendaten nicht nur im KIS sondern auch im PACS, dem Laborsystem und evtl. noch an weiteren Stellen gespeichert werden.

Kommunizieren Sie Ihre Ergebnisse über Ihre Gremien und Vereinigungen, aber bitte auch mit uns, dem bvitg. Nur so sind wir in der Lage, den seitens der Datenschutzbeauftragten angebotenen Dialog mit einer Stimme für einen pragmatischen, umsetzbaren Datenschutz im medizinischen Bereich zu führen.

Beteiligen Sie sich an angebotenen Kundenworkshops zum Datenschutz und nehmen Sie das Thema Datenschutz auf Ihre Agenda. Und: schaffen Sie auch bei Ihrem Personal ein Bewusstsein dafür, dass Datenschutz auch ein Teil der Patientensicherheit ist.