Vorstellung der OH KIS

Zielsetzung – Umsetzungsbedarf - Stand der Überarbeitung

Fachtagung von BWKG und LfD BW zur Orientierungshilfe Krankenhausinformationssysteme am 19. Juni 2013 in Neuhausen a.d.F.

Ursula Ungerer
Stv. Geschäftsführerin der
Baden-Württembergischen
Krankenhausgesellschaft e.V.

Gabriele Heiss-Kaiser
Ministerialrätin
beim Landesbeauftragten für den
Datenschutz Baden-Württemberg

Teil I : **Frau Heiss-Kaiser (LfD BW)**

Rückschau
Erstellen der OH KIS
Zielsetzung und Inhalt der OH KIS
Verbindlichkeit der OH KIS - Umsetzungsbedarf
Aktivitäten auf Landesebene

Teil II : **Frau Ungerer (BWKG)**

Anwendungsbereich der OH KIS
Zugriffsbegrenzung als Kernprinzip des Datenschutzes
Projekt Umsetzung der OH KIS
Wichtige Forderungen an die Hersteller
Klarstellungen innerhalb der AG OH KIS (BW)
Anliegen an die UAG

Teil III: **Frau Heiss-Kaiser (LfD BW)**

Aktivitäten auf Bundesebene

Rückschau

Weshalb eine Orientierungshilfe?

Entschließung der 78. Sitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009

- Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.
- Nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit hin (Protokollierung).
- Erstellen einer Orientierungshilfe, die bundesweit Mindestanforderungen an eine datenschutzgerechten Betrieb von Krankenhausinformationssystemen formuliert.

Erstellen der OH KIS

- Konstituierung der UAG KIS am 25.11.2009 unter Federführung des LfD Berlin unter Beteiligung einiger Landesdatenschutzbehörden sowie der Datenschutz-beauftragten der EKD und der Diözesanbeauftragten der norddeutschen Bistümer

- Einbindung von DKG und KIS-Herstellern

Erstellen der OH KIS

- 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17.03.2011
- Sitzung der Obersten Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 04./05.05.2011
- Tagung der Datenschutzbeauftragten der EKD am 04.05.2011
- Sitzung der Konferenz der Datenschutzbeauftragten der Katholischen Kirche Deutschlands am 31.05.2011

Zielsetzung und Inhalt der OH KIS

Die Orientierungshilfe basiert auf den geltenden rechtlichen Vorgaben, insbesondere Krankenhausgesetze, Datenschutz-gesetze, Berufsrecht, Strafrecht.

- Die Umsetzung der rechtlichen Vorgaben soll mit der Orientierungshilfe erleichtert werden.

- Orientierungsrahmen sowohl für Krankenhausbetreiber als auch für KIS-Hersteller

Zielsetzung und Inhalt der OH KIS

Wesentliche Aussage:

- Mit der Nutzung der modernen Informationstechnik im Krankenhaus gehen mögliche Gefährdungen für die Datensicherheit und das von der ärztlichen Schweigepflicht geschützte Arzt-Patientenverhältnis einher.
  Den Gefährdungen muss mit geeigneten und angemessenen technischen und organisatorischen Maßnahmen begegnet werden.
- Die Orientierungshilfe bietet konkrete und handhabbare Lösungsansätze. Alternative Maßnahmen, die die gleiche Schutzwirkung erzielen können, sind möglich.

Zielsetzung und Inhalt der OH KIS

- *Begleitpapier* einschließlich *Glossar*

- *Normative Eckpunkte* (Teil I)

  Konkretisierung der Eckpunkte, die sich aus den datenschutzrechtlichen Regelungen und den Vorgaben der ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben.

- *Technische Anforderungen* (Teil II)

  Beschreibung von Maßnahmen zur technischen Umsetzung der rechtlichen Vorgaben einschließlich der ärztlichen Schweigepflicht.

Verbindlichkeit der OH KIS - Umsetzungsbedarf

- Die Orientierungshilfe ersetzt nicht die für die Krankenhäuser geltenden rechtlichen Regelungen.

- Sie bildet im Rahmen der Kontroll- und Beratungstätigkeit des LfD BW den Maßstab für die Bewertung eingesetzter Verfahren.

Verbindlichkeit der OH KIS – Umsetzungsbedarf

- Die Umsetzung der rechtlichen Anforderungen unter Zuhilfenahme der Orientierungshilfe ist zwingend.

- Bei Defiziten ist zu klären, welche notwendigen Maßnahmen zu veranlassen sind.

Aktivitäten auf Landesebene

- Bildung einer Arbeitsgruppe unter Beteiligung der BWKG, Datenschutzbeauftragter und IT-Verantwortlicher einiger Krankenhäuser und des LfD BW
  (insgesamt 11 Sitzungen seit Anfang 2012).

- Diskussion der OH KIS mit dem Ziel, ein gemeinsames Verständnis zu schaffen.

- Ergebnisse sind in die Evaluation der OH KIS eingeflossen.

- Erstellen von Checklisten.

Aktivitäten auf Landesebene

Aktivitäten des LfD BW

- Informations- und Beratungsgespräche bei Krankenhäusern unterschiedlicher Größe

- Referenzkrankenhaus

Anwendungsbereich der OH KIS:

- KIS sind die elektronischen informationsverarbeitenden Systeme zur Verarbeitung der medizinischen und administrativen Patientendaten im Krankenhaus
- Zumeist gibt es ein führendes System + verschiedene weitere Systeme wie das PACS, Laborsystem, usw.
- In manchen Krankenhäusern sind jedoch auch das medizinische und das administrative System von unterschiedlichen Anbietern

Anwendungsbereich der OH KIS:

- Von der OH KIS nicht tangiert sind die Bereiche, in denen eine Klinik nach wie vor ausschließlich papiergebunden arbeitet.

- Die OH KIS spricht zwar von Krankenhäusern. Für die elektronische Verarbeitung von Patientendaten in – Vorsorge- oder Rehakliniken gelten jedoch die gleichen Grundsätze.

Zugriffsbeschränkung als Kernprinzip im Datenschutz

Grundsatz der Erforderlichkeit (z.B. § 28 BDSG):

- Sachlicher Grund für eine Datenverarbeitung,
  „nur der darf Zugriff haben, der Daten auch braucht“
  → Zugriffskonzept,
  → OH KIS: Überwachung der Zugriffe (Protokollierung)

- Zeitliche Begrenzung der Zugriffsberechtigung und der Speicherung
  „nur so lange, wie erforderlich“
  → Zugriffskonzept, Löschkonzept

Zugriffsbeschränkung als Kernprinzip im Datenschutz

Grundsatz der Datensparsamkeit (z.B. § 3a BDSG)

- Datenverarbeitungssysteme sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu nutzen
- Anonymisierung oder Pseudonymisierung, soweit dies nach Verwendungszweck möglich ist und im Verhältnis zum Schutzzweck keinen unverhältnismäßigen Aufwand darstellt.

Zugriffsbeschränkung als Kernprinzip im Datenschutz

- Das Behandlungsinteresse des Patienten hat Vorrang vor dem Geheimnisschutz. Bei der Detailausgestaltung der Prozesse muss jedoch dem Geheimhaltungs-interesse Rechnung getragen werden.
- Erforderlichkeit, Verhältnismäßigkeit - unbestimmte Rechtsbegriffe, die ausgelegt werden müssen.
- Die OH KIS nimmt eine konkretisierende Interpretation der gesetzlichen Vorgaben aus **Sicht der Datenschutzbehörden** vor.

Ausgangssituation einer Umsetzung:

- KIS-Systeme sind gewachsene Systeme, die von den Herstellern kontinuierlich erweitert und ausgebaut wurden
- Sinnvoll:

  Anforderungen → Entwicklung des KIS-Systems

- Realität:

  bestehendes System → Anforderungen der OH KIS schlagen nun im Nachhinein „ein“ .

Projekt „Umsetzung der OH KIS“:

Umsetzung der OH KIS ist **Gemeinschaftsaufgabe:**

⇔ es müssen ganz unterschiedliche Bereiche der Klinik zusammenarbeiten:

- IT-Bereich als technischer Umsetzer
- Klinikleitung
  - Kosten für die Umsetzung können ganz erheblich sein
  - Die Umsetzung ist eng mit innerorganisatorischen Gestaltungsfragen verbunden (Zugriffskonzept, wie arbeiten Abteilungen und Berufsgruppen zusammen).
- Datenschutzbeauftragter der Klinik

Projekt „Umsetzung der OH KIS“:

Sofern noch nicht geschehen:

- Bildung einer Projektgruppe zur Umsetzung der OH KIS, Festlegung von Verantwortlichkeiten
- Abgleich des „Ist“ mit den Anforderungen der OH KIS
- Checklisten der AG KIS als Hilfestellung zum Einstieg und zur Priorisierung
- Feststellung des „Deltas“
- Arbeitshilfen der DKG zur Umsetzung

Projekt „Umsetzung der OH KIS“:

- Priorisierung der „Baustellen“ nach Bedeutung und Umsetzbarkeit

- Bei jeder „Baustelle“ Prüfung:

  - Bietet mein KIS-System die Funktion, habe ich sie aber bislang nicht genutzt?

    Bsp: Einrichtung von Zugriffsberechtigungen.

  - Fehlen in meinen KIS-System grundlegende Funktionen?

    Bsp.: Möglichkeit zur Löschung und Sperrung von Daten

Projekt „Umsetzung der OH KIS“:

- Gespräch der Klinik mit dem Hersteller
  - Hat dieser bereits eine Lösung entwickelt?
  - Ist eine individuelle Lösung erforderlich?

- DKG plant Gespräche mit den Herstellern

→ DKG übermittelt dem Bundesverband BVITG in Kürze die Arbeitsfassung der DKG-Umsetzungsempfehlung mit der Bitte um ein Gespräch.

Wichtige Forderungen an die Hersteller

- Schaffung von Schnittstellen
- Fallbezogene Zugriffsmöglichkeit
- Fallnummernbezogene Gestaltung des Notfallzugriffs, der zeitgesteuert ist.
- Protokollierungsmöglichkeit für lesende Zugriffe.
- Unterscheidung zwischen administrativ und medizinisch abgeschlossenen Fällen.

Wichtige Forderungen an die Hersteller

- Sperrung und Löschung müssen als Funktionen vorhanden sein.
- Die Software muss eine zeitliche Begrenzung der Zugriffsberechtigung ermöglichen bzw. für jedes einzelne Dokument bzw. einzelne Dokumentengruppe muss eine Löschfrist parametrisierbar sein.
- Revisionssichere Protokollierung
- Möglichkeit einer Protokolldatenbank mit Berechtigung der Zugriffe
- Einfache Möglichkeit zum Anonymisieren und Pseudonymisieren

Klarstellungen innerhalb der AG OH KIS (BW)

- OH KIS fordert Protokollierung, „wer“ „wann“ „welche“ personenbezogenen Daten in welcher Weise verarbeitet hat.

  → unter „welche Weise“ können auch Modifikations-kategorien (z.B. angelegt, gelesen, gedruckt, geändert) verstanden werden

  → Es muss nicht der Inhalt von Änderungen protokolliert werden – zulässig ist auch die Speicherung von Versionen (vgl. auch § 630f Abs. 1 BGB)

  → Änderungen an bloßen Entwürfen müssen nicht protokolliert werden.

Klarstellungen innerhalb der AG OH KIS (BW)

- Behandlungsfall

  Der Behandlungsfall ist maßgeblicher Anknüpfungspunkt die Dauer von Zugriffsberechtigungen.

  → Die Klinik hat hier Spielraum, was als Behandlungsfall definiert wird (z.B. Abrechnungsfall, eng zusammenhängende Behandlungszyklen)

  → Wichtig ist, dass die Klinik intern festlegt, wann ein Behandlungsfall abgeschlossen ist.

Klarstellungen innerhalb der AG OH KIS (BW)

- Trennung der KIS-Administration in technische Administration, Anwendungsadministration und Berechtigungsverwaltung

  → Nur wenn dies in der Klinik personell realisierbar ist.

  → KIS-Hersteller müssen die technische Möglichkeit für die Trennung bereitstellen.

Klarstellungen innerhalb der AG OH KIS (BW)

- Keine Unterscheidung zwischen Mitarbeitern und sonstigen schützenswerten Patientengruppen (z.B. VIP) erforderlich

→ In beiden Fallgruppen können gleichermaßen alternative Gestaltungsmöglichkeiten wie Schutz über Verfahrensabläufe, Zugriffsbeschränkungen, teilweise Pseudonymisierung genutzt werden. Die Patientensicherheit bleibt im Vordergrund.

Anliegen, die aus der KIS-AG BW an die UAG der Datenschutzbehörden transportiert wurden

- Hinzuziehung von Patientenunterlagen der Vorbehandlungen im gleichen Krankenhaus

  Derzeitige OH KIS:

  - Allgemeiner Hinweis an Patienten bei Aufnahme, dass er Hinzuziehung widersprechen kann.
  - Der Arzt soll den Patienten dann zusätzlich auf mögliche Risiken eines Widerspruchs hinweisen.

Anliegen, die aus der KIS-AG BW an die UAG der Datenschutzbehörden transportiert wurden

⇨ Position der Krankenhausseite:

- ✓ Der Patient wird durch eine Entscheidung über eine Hinzuziehung/Widerspruch meist überfordert.
- ✓ Vergleichbarer Sachverhalt wie bei Arztbriefen → Patient geht regelhaft von einer Hinzuziehung aus. Wenn er dies nicht will, wird er von sich aus aktiv.
- ✓ Solange der Arzt keinen Einblick hat, kann er auch nicht die Erforderlichkeit und die Folgen einer Nichthinzuziehung beurteilen. Neue Haftungsrisiken.

Anliegen, die aus der KIS-AG BW an die UAG der Datenschutzbehörden transportiert wurden

- Sperrung

  Deutliche Klarstellung, dass eine Sperrung keine aktive elektronische Kennzeichnung als „gesperrt“ voraussetzt, sondern dass die Definition des Endes einer Zugriffsberechtigung im Rahmen des Zugriffskonzepts ausreichend ist.

Anliegen, die aus der KIS-AG BW an die UAG der Datenschutzbehörden transportiert wurden

- Umfang der Protokollierung als Missbrauchskontrolle

OH KIS:	Auch das Ergebnis einer Suchabfrage muss protokolliert werden.
Krankenhäuser:	Ausreichend ist, wenn statt Ergebnis die Suchparameter und Folgeaktion protokolliert werden. (Verhältnismäßigkeit von Aufwand und Nutzen!)

Anliegen, die aus der KIS-AG BW an die UAG der Datenschutzbehörden transportiert wurden

- Mandantentrennung

  Ein gemeinsames KIS mehrerer Krankenhäuser oder Unternehmen wie MVZ setzt eine Mandantentrennung voraus

  OH KIS: logische oder physische Trennung

  Krankenhäuser: Lösung über Zugriffsberechtigungen muss zulässige Alternative sein.

Wichtige Anliegen, die an die UAG der Datenschutzbehörden transportiert wurden

- Gemeinsamer Stammdatensatz ambulant/stationär

  OH KIS: getrennte Datenhaltung im KIS für ambulante, in Nebentätigkeit behandelte Privatpatienten

  Krankenhäuser: Möglichkeit eines gemeinsamen Stammdatensatzes für die stationäre und ambulante Versorgung in einem Krankenhaus soll gegeben sein.

Wunsch an den Gesetzgeber: Zulässige Nutzung des Wirtschaftlichkeitspotentials einer Konzerndatenbank

Aktivitäten auf Bundesebene

- Gespräche mit der DKG
- Arbeitshilfen der DKG
- Bisherige Erfahrungen mit der Orientierungshilfe bzw. deren Umsetzung zeigen, dass eine Fortschreibung notwendig und sinnvoll ist. Einzelne Anforderungen werden
  - modifiziert
  - inhaltlich präzisiert
  - gestrichen
  - neu aufgenommen

Überarbeitung der OH KIS

beispielhafte Überarbeitungsvorschläge

- Normative Eckpunkte → Rechtliche Rahmenbedingungen
- Sperrung → Unterscheidung zwischen Einschränkung der Zugriffsrechte auf Daten vs. Sperrung der Daten anstelle der Löschung von Daten
- Notfallzugriff → Sonderzugriff
- VIPs etc. → Die Festlegung trifft die Klinikleitung … auf Antrag des Patienten

Überarbeitung der OH KIS

beispielhafte Überarbeitungsvorschläge

- **Umgang mit Vorbehandlungsdaten**

„Bei der Aufnahme kann der Patient der Hinzuziehung von Daten aus früheren abgeschlossenen Behandlungsfällen in demselben Krankenhaus ganz oder teilweise widersprechen. Hierauf und auf die mit einer derartigen Beschränkung verbundenen Risiken ist der Patient bereits bei der administrativen Aufnahme in allgemeiner Form (z.B. durch ein Merkblatt) hinzuweisen.“ → gestrichen

Überarbeitung der OH KIS

beispielhafte Überarbeitungsvorschläge

- **Protokollierung („revisionssicher“)**

Vorgesehene Protokollierungen dürfen nicht umgangen werden können *(von denjenigen, die durch die Protokolle kontrolliert werden sollen)* und eine nachträgliche Veränderung von Protokollen darf nicht möglich sein.

Überarbeitung der OH KIS

beispielhafte Überarbeitungsvorschläge

- **Mandantenfähigkeit**

Mandant = abgeschlossener Datenhaltungs- und Verarbeitungskontext einer im datenschutzrechtlichen Sinne verantwortlichen Stelle

Ein Verfahren ist "mandantenfähig", wenn Patientendaten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können.

siehe auch Orientierungshilfe Mandantenfähigkeit - Version 1.0 vom 11.10.2012. (Diese Orientierungshilfe ist durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zustimmend zur Kenntnis genommen worden.)

Überarbeitung der OH KIS

- Fortschreibung der OH KIS vorbehaltlich der zustimmenden Kenntnisnahme der neuen Fassung der UAG durch die Gremien im schriftlichen Verfahren.

- Die neue Fassung der Orientierungshilfe steht voraussichtlich ab *Ende 2013 / Anfang 2014* zur Verfügung und kann dann unter www.baden-wuerttemberg.datenschutz.de heruntergeladen werden.

Vielen Dank für Ihre Aufmerksamkeit!