Baden-Württembergische
Krankenhausgesellschaft e.V.

Der Landesbeauftragte für den
Datenschutz
Baden-Württemberg

Vorstellung der Checklisten der Landes-Arbeitsgruppe OH KIS als praktische Umsetzungshilfe für die Kliniken

Fachtagung Orientierungshilfe
Krankenhausinformationssysteme (OH KIS)
am 19. Juni 2013 in Neuhausen a.d.F.

Beteiligte Mitglieder der Arbeitsgruppe OH KIS BW

Friedemann Bauer	Referent beim Landesbeauftragten für den Datenschutz Baden-Württemberg, Referat V
Jürgen Flemming	IT-Leiter, IT-Risikomanagement Vinzenz von Paul Kliniken gGmbH, Stuttgart
Armin Gebert	Datenschutzbeauftragter, Hohenloher Krankenhaus gGmbH, Öhringen
Gabriele Heiss-Kaiser	Leiterin des Referats „Datenschutz im Gesundheits-, Sozial- und Bildungswesen“ beim Landesbeauftragten für den Datenschutz Baden-Württemberg
Sebastian Lau	EDV-Leitung, Agaplesion Bethesda Krankenhaus Stuttgart
Silke Mužic	Leitung KlinikenInformationsManagement, Zentrale Informations-Verarbeitung, Regionale Kliniken Holding RKH GmbH
Martin Schurer	Datenschutzbeauftragter der Universitätsklinika Heidelberg, Tübingen, Ulm
Ursula Ungerer	Stv. Geschäftsführerin, Baden-Württembergische Krankenhausgesellschaft e. V., Stuttgart

Checklisten OH KIS
Einführung/Deckblatt

vorgestellt von Ursula Ungerer

Ziel der Checkliste:

Checklisten als **Einstiegshilfe** in die Umsetzung:

- Die OH KIS ist komplex aufgebaut:
  Normativer und technischer Teil, mit vielfältigen inneren Wechselbezügen
- Die OH KIS ist sehr umfangreich.
- Der Anwender geht in der Fülle der Details schnell unter.

Ziel der Checkliste:

- Checklisten als „Schwimm“hilfe für Analyse des Ist-Zustands und des Handlungsbedarfs.
- Wichtige und für die verschiedenen Bereiche exemplarische Fragen. So wird eine schnelle Orientierung und Statusbestimmung in der Bandbreite der Thematik ermöglicht.
- Durch Kategorisierung mancher Punkte als dringender Handlungsbedarf werden erste Hinweise für die interne Priorisierung gegeben.

Hinweise:

- Checklisten sind für den **rein internen Gebrauch** in der Klinik.
- Bearbeitete Checklisten sind nicht den Aufsichtsbehörden vorzulegen.
- Aufgrund ihres verkürzenden Charakter können die Checklisten nicht die vollständigen Inhalte der OH KIS abbilden → Checklisten können OH KIS nicht ersetzen.
- Die Wertung als „besonders dringlich“ ist eine unverbindliche Wertung“ durch die Arbeitsgruppe.

Gliederung der Checklisten:

- „Deckblatt“ mit allgemeinen Hinweisen
- Rollen- und Berechtigungskonzept
- Protokollkonzept
- Reporting
- Sperr- und Löschkonzept
- Sicherheitskonzept

Gliederung der Checklisten:

Checklisten-Frage	Referenz zu den einschlägigen Stellen in der OH KIS	Bei negativer Antwort: Handlungs-empfehlung	Von den Klinikmitarbeitern zu bearbeiten: Anmerkungen
Frage zu den wichtigen Inhalten der OH-KIS	Zum vertieften Nach- und Weiterlesen	Aufzeigen des Handlungsbedarfs teilweise konkretisiert, mit Wertung, wo besondere Dringlichkeit besteht	Ja/Nein Im Falle von Nein die Ursache benennen Geplante Umsetzungs-maßnahmen

Baden-Württembergische
Krankenhausgesellschaft e.V.

Der Landesbeauftragte für den
Datenschutz
Baden-Württemberg

Checklisten OH KIS

Rollen- und Berechtigungskonzept

vorgestellt von Friedemann Bauer

Checklisten OH KIS

Rollen- und Berechtigungskonzept

- Existenz, Dokumentation, Qualität
- Detaillierungsgrad
- Reichweite (global/lokal)
- Benutzerverwaltung
- Übersichtslisten

Checklisten OH KIS

Rollen- und Berechtigungskonzept

Benutzerkategorien

Ärztliche Mitarbeiter, Pflegekräfte, Verwaltungskräfte, Ausbildungskräfte, Externe Kräfte, Administration

Grundrollen

Konsiliar, Bereitschaftsdienst, Belegarzt, Behandelnder Arzt, Honorar-Arzt,…

+ Behandlungsauftrag/Zuweisung → fachbereichsspezifische Zugriffsrechte

Häufigste Fehler: Rollen zu allgemein („Arzt“), Berechtigungen zu pauschal („abteilungsweit“) bzw. zu allgemein vergeben („Alle“)

Checklisten OH KIS

Rollen- und Berechtigungskonzept

- Wechselwirkungen
  - Protokollkonzept
  - Mandantenfähigkeit
  - Sicherheitskonzept

  (siehe auch OH Protokoll, OH Mandantenfähigkeit, Merkblätter)

- Stresstest → Konsequenzen adäquat begegnen

Checklisten OH KIS

Rollen- und Berechtigungskonzept

- Komplexität, Implementierungsaufwand, Kosten
- Bordmittel + flankierende organisatorische Maßnahmen
- Orientierung am Schutzbedarf der Daten
- Dialog suchen + Ermessensspielraum ausloten

Checklisten OH KIS
Protokollkonzept
Auswertungskonzept

vorgestellt von Armin Gebert

Protokollierung

Die datenschutzrechtliche Protokollierung ermöglicht wirksame Datenschutzkontrollmaßnahmen, indem die Zugriffe (Rollen- und Berechtigungskonzept) überprüft werden können. Das Krankenhaus muss dem Patient auf Nachfrage Auskunft erteilen können, wer auf seine Daten zugegriffen hat.

Die Protokollierung muss nachvollziehbar dokumentieren, wer wann auf welche personenbezogenen Daten in welcher Weise zugegriffen, genutzt, verarbeitet oder gelöscht hat.

Europäischer Gerichtshof für Menschenrechte 2009
ECHR Application No. 20511/03

.....in der fehlenden Protokollierung von (lesenden) Zugriffen auf medizinische Daten liegt ein Verstoß gegen Artikel 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung des Privat- und Familienlebens)

Einige Krankenhaus-Informationssysteme protokollieren schon jetzt, aber in welchem Umfang und wie strukturiert ist die Auswertung?

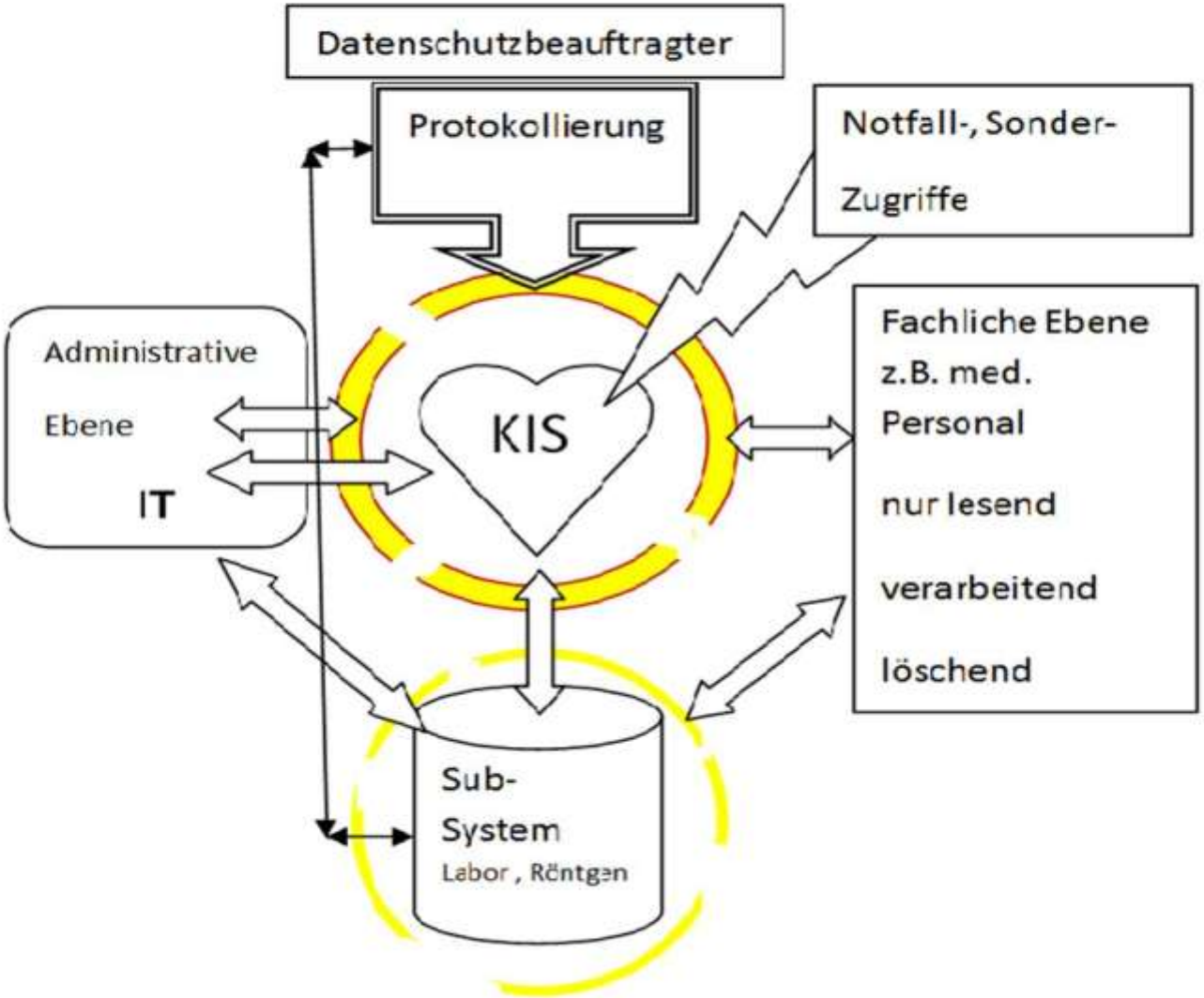
→Was muss verbessert werden?

Umsetzung:

- Erstellen eines Protokollierungskonzeptes

Das Protokollierungskonzept muss enthalten:

- Art und Umfang der Protokollierung,
- Verfahrensweisen zur Speicherung und Auswertung der Protokolldaten,
- Schutzmaßnahmen für die Rechte der Mitarbeiter,
- Aufbewahrungsdauer der Protokolldaten.


Datenschutzbeauftragter
Protokollierung
Notfall-, Sonder-
Zugriffe
Administrative
Ebene
IT
KIS
Fachliche Ebene
z.B. med.
Personal
nur lesend
verarbeitend
löschend
Sub-
System
Labor , Röntgen

Zugriffsprotokollierung - Wer, wann, worauf:

- **Zeitpunkt** des Zugriffs auf die Patientendaten (Systemzeit)
- Kennung der aufgerufenen **Transaktion** (Anzeige, Abfragefunktion, Reportname, Maskenbezeichnung)
- Kennung des jeweiligen **Benutzers**
- Identität des betroffenen **Patienten**
- **aufgerufene Transaktionen**

Keine medizinischen Daten!

Auswertungskonzept / Reporting

- Ist ein Auswertungskonzept für die Protokolldaten erstellt, und ist festgelegt, wer auf die Auswertungsdaten zugreifen darf?

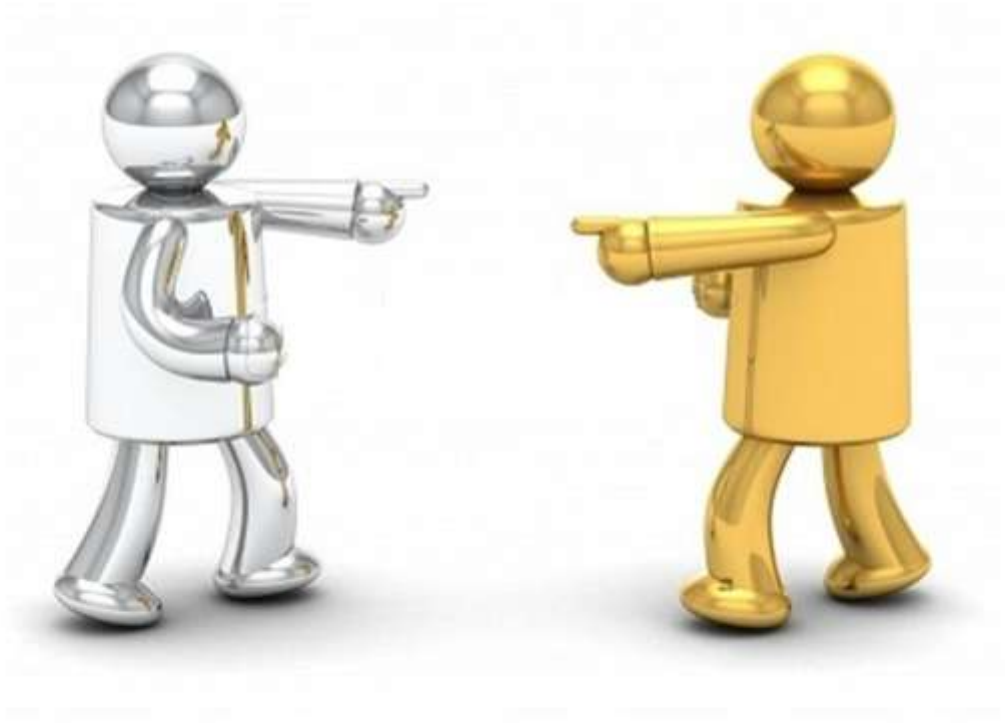
- Ist das Auswertungskonzept mit Ihrem Datenschutzbeauftragten und der Mitarbeitervertretung abgestimmt?

Umfang des Reporting:

- Ist eine stichprobenweise als auch anlassbezogene Auswertung möglich?
- Ist die Filterung nach verschiedenen Kriterien (z.B. Nutzerkennung, …) und nach fachlichen bzw. administrativen Zugriffen möglich?
- Ist bei der Protokollierung der Behandlungszusammenhang gegeben?
- Ist nachvollziehbar, wann für welche Benutzer welche Berechtigungen eingerichtet wurden?

- Ist es möglich für einen definierten Zeitpunkt und Benutzer dessen vollständige Zugriffsrechte auflisten?

- Können Sie für einen definierten Zeitpunkt nachvollziehen, welche Benutzer auf die Daten eines bestimmten Patienten zugegriffen haben oder zugreifen konnten?



Checklisten OH KIS
Sperr- und Löschkonzept

vorgestellt von Martin Schurer

Sperr- und Löschkonzept

Rechtlicher Hintergrund

§§ 23,24 **LDSG**/§ 20 Abs.2+3 **BDSG**, kirchlich analog (verkürzt):

➔ **Personenbezogene Daten (in automatisierten o.sonstigen Dateien) sind zu löschen, wenn ihre Kenntnis für die speichernde/ verantwort -liche Stelle zur Erfüllung (…) ihrer Aufgaben nicht mehr erforderlich ist.**

➔ An die Stelle einer Löschung tritt eine **Sperrung** wenn…
… Aufbewahrungsfristen einzuhalten
… schutzwürdige Interessen Betroffener
… Löschung nicht möglich

Aufbewahrungsfristen für ärztliche Dokumentation (verkürzt):

➔ … Mindestens **10 Jahre** (ärztliche Berufsordnung)

➔ … Bis zu **30 Jahre** (wg.Verjährungsfristen o. z.B. Röntgenbehandlungen)

Sperr- und Löschkonzept

Das müssen Sie sich fragen/prüfen

1. Ausgangspunkt: Wann ist bei Ihnen ein **Fall abgeschlossen**?
2. **Erfolgen** bisher in irgendeiner Weise fristengesteuerte **Löschungen/Zugriffseinschränkungen/Sperrungen** im KIS?
3. Haben Sie **Fristen und Prozesse dokumentiert** festgelegt?
4. Kann Ihr **KIS** löschen und sperren wie verlangt? Sind Löschungen endgültig?
5. Wie ist ggf. der (erforderliche) **Zugriff auf gesperrte** Daten (dokumentiert) geregelt?
6. Wie läuft das Ganze in Subsystemen (wie z.B. Laborsystem)?

Sperr- und Löschkonzept

Das müssen Sie bei Bedarf tun

1. **Sperr-/Löschkonzept** (oder auch „Fallabschlusskonzept“)
   a) Definition des Fallabschlusses
   b) Festlegen von Fristen und Prozessen (GF/Vorstand)
   c) Einführen in der Praxis
2. **Berechtigungskonzept** anpassen
   a) Zugriffe auf gesperrte Daten regeln
   b) In System und Dokumentation
3. Hinwirken bei **Systemherstellern**
   a) Fristen-/kriteriengesteuertes Löschen muss möglich sein/werden

Baden-Württembergische
Krankenhausgesellschaft e.V.

Der Landesbeauftragte für den
Datenschutz
Baden-Württemberg

Checklisten OH KIS
Sicherheitskonzept

vorgestellt von Jürgen Flemming

Die 4 Kern-Themen des Sicherheitskonzepts

1. **Anonymisierung / Pseudonymisierung**
   a. Datenbanken für Test, Schulungen etc.
   b. Export von Daten für Forschung und Lehre
2. **Verschlüsselung**
   a. Mobile Datenträger – sind die Daten darauf wirksam verschlüsselt ?
   b. Kommunikation zwischen Häusern oder mit Dritten – Verschlüsselung der Daten ?
3. **Schutzbedürftige Personen, VIP's, Mitarbeiter**
   a. Wie gut schützen Sie solche Personen vor der Öffentlichkeit und vor Kollegen oder dem Arbeitgeber ?
4. **Schutz vor unberechtigtem Zugriff und Veränderung der Daten**
   a. Physischer Zugangsschutz für das Rechenzentrum
   b. Kontrolle / Überwachung Fernzugänge (Modem, ISDN, VPN,…)

Vielen Dank für Ihre Aufmerksamkeit!