privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Dezember 2014 / Version 1.0

Datenschutztechnische Anforderungen

Klinikinformationssysteme (KIS)

1. Einleitung

1.1. Gegenstand und Ziele dieser Hilfestellung

Die vorliegende Hilfestellung wurde von der Vereinigung der schweizerischen Datenschutzbeauftragten (privatim) erstellt. Sie konkretisiert die wesentlichen technischen Anforderungen, die sich aus den geltenden datenschutzrechtlichen Gesetzen und Regelungen für den Einsatz von Informationssystemen in Kliniken ergeben. Sie hilft bei der Beschaffung, im Betrieb sowie bei der Kontrolle und Verbesserung von Klinikinformationssystemen (KIS).
Bei einem KIS handelt es sich um die zentrale Informationsplattform der Klinik. Darin werden die relevanten Daten zu einem Behandlungsfall bearbeitet. Nutzende sind unter anderem das Aufnahmepersonal, der pflegerische Stationsdienst sowie Ärztinnen und Ärzte oder andere Fachabteilungen. Dabei kann es sich sowohl um eine integrierte Gesamtlösung als auch einen Verbund selbständiger Systeme, gegebenenfalls von unterschiedlichen Herstellern, handeln.
Die Hilfestellung richtet sich institutionell an die grösseren Spitäler, Kliniken und Pflegeheime (> 10‘000 Patientinnen und Patienten pro Jahr) sowie an die Entwicklerfirmen von KIS. Funktional richtet sie sich an die Entscheidungsträger für Beschaffung und Betrieb von KIS (Management, IT-Leitung, IT-Controlling), an die Leitungen der Entwicklungsabteilungen von Anbietern von KIS und an die Kontrollbehörden.

1.2. Abgrenzung

Es werden nur die wichtigsten technischen Anforderungen für die Bereiche Betroffenenrechte (Rechte der Patienten), Zugriffsberechtigungen, Schnittstellen und Protokollierung beschrieben. Auf die Beschreibung begleitender organisatorischer Massnahmen, wie z.B. die regelmässige Kontrolle der Zugriffsrechte, wird verzichtet.
Anforderungen an weitere an das KIS angebundene Systeme (z.B. Röntgen, Labor etc.) sind nicht Inhalt dieses Dokuments. Es werden lediglich Anforderungen im Zusammenhang mit den Schnittstellen aufgeführt.

Arbeitsgruppe ICT
privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati
c/o Datenschutzbeauftragter des Kantons Zürich
Postfach, CH-8090 Zürich
Tel. +41 (43) 259 39 99, Fax +41 (43) 259 51 38
geschaeftsstelle@privatim.ch, www.privatim.ch

2. Anforderungen an KIS

2.1. Rechte der Betroffenen

Der Datenschutz dient dem Schutz der Persönlichkeitsrechte und der Privatsphäre. Er verpflichtet die Datenbearbeiter zu rechtmässigem und verhältnismässigem Handeln und verleiht den betroffenen Personen durchsetzbare Rechte, die durch Systemfunktionen des KIS unterstützt werden müssen. Folgende Funktionen müssen im KIS integriert sein:
Auskunftsrecht

- Alle Patienteninformationen (Stamm- und Gesundheitsdaten) zu einem Behandlungsfall müssen zweckmässig exportiert werden können, dies beinhaltet auch die Zugriffs- und Änderungsprotokolle.

Berichtigungs- und Löschrecht

- Falldaten müssen gelöscht und ergänzt werden können (inkl. Lösch- und Berichtigungsaufträge in referenzierte Systeme).
- Falldaten werden nach Ablauf festgelegter Aufbewahrungsfristen bzw. Ablieferung an Archive unwiderruflich gelöscht oder anonymisiert.

2.2. Berechtigungskonzept

Verwaltung der Benutzerkonten

- Der Zugang zur Verwaltung von Benutzerkonten muss eingeschränkt werden können: Das Einrichten der Konten und Verwalten der Zugriffsrechte darf nur durch eine definierte Rolle möglich sein.
- Das System muss die Zugriffe auf Falldaten nach Ablauf definierter Fristen (Lösch- und Aufbewahrungsfristen) automatisch einschränken.
- Bei einem Notfallzugriff (bestehende Zugriffsrechte können temporär ausgeweitet werden) auf Daten müssen der Grund, Datum und Zeit des Zugriffes, Rolle und die zugreifende Benutzer-ID protokolliert werden.
- Bei Eröffnung eines Behandlungsfalls für aktuelle oder ehemalige Mitarbeitende der Institution müssen spezifische Einschränkungen des Zugriffs erfolgen.

Sperrung der Benutzerkonten

- Es muss möglich sein, Benutzerkonten für definierbare Zeiten zu sperren.
- Benutzerkonten müssen nach wiederholter fehlerhafter Passworteingabe gesperrt werden.
- Es muss möglich sein, über längere Zeit unbenutzte Benutzerkonten automatisch zu erkennen und zu sperren.
- Es muss ebenfalls eine Möglichkeit geben, Sitzungen nach einer bestimmten Zeit der Inaktivität zu deaktivieren.

Zugriffsberechtigungen

- Zugriffsberechtigungen müssen rollenbasiert (z.B. nach Funktion und Organisationseinheit) vergeben werden können. Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben.

Benutzerauthentifikation / Zugangsdaten

- Der Zugriff zum System darf nur mittels starker Benutzerauthentifikation möglich sein, d.h. Benutzer müssen sich basierend auf mindestens zwei Faktoren authentisieren.
- Die Anforderungen an die Passwörter sind gemäss aktuellem Stand der Technik umzusetzen (z.B. Sichtbarkeit und Kopierbarkeit bei der Eingabe, Mindestanforderungen betreffend Komplexität (Länge, Sonderzeichen, Zahlen), zeitliche Beschränkung der Gültigkeit etc.).

2.3. Schnittstellen

Mit der Integration der KIS in die IT-Umgebungen der Spitäler besteht ein Bedürfnis, die vorhandenen Datenquellen miteinander über Schnittstellen mit dem KIS zu vernetzen. Für Support und Wartung der KIS-Infrastruktur und der Applikationen durch externe Dienstleistende werden nebst den Datenschnittstellen auch technische Schnittstellen implementiert.

Abbildung 1: Integriertes Klinikinformationssystem

Die Anforderungen von Informationssicherheit und Datenschutz (ISDS) an diese Schnittstellen sind aufgrund der Klassifizierung der medizinischen (Patienten-)Daten entsprechend hoch.
Aus diesem Grund ist für die Schnittstellen ein ISDS-Konzept zu erstellen, das:

- den Datenaustausch im Detail beschreibt [Quelle, Ziel, Datenfelder, Zweck (Bsp.: Aggregation im Zielsystem), gesetzliche Grundlage]
- die Überwachung der Schnittstelle beschreibt (Logging, Transfer, Freigabe)
- den technischen Betrieb der Schnittstelle beschreibt (Abrufverfahren, Push, etc.)
- die Verantwortlichkeiten definiert (Dateneigner bzw. Datenverantwortlicher in Quell- und Zielsystemen)
- die Kommunikation spezifiziert (Medium, Verschlüsselung, Kommunikationsprozess)
- die Benutzerrollen und -rechte im Zielsystem überprüft

- die Anforderungen an eine konsistente Datenlöschung in allen Systemen beschreibt
- die Aufbewahrungs- und Löschfristen basierend auf den gesetzlichen Vorgaben konsistent über alle Systeme umsetzt
- den Datenstamm festlegt für ein Rollback- oder Restoreszenario

Die technischen Anforderungen sind aus dem ISDS-Konzept abzuleiten.

Externer Zugriff auf die Daten erfolgt verschlüsselt und mit einer starken Authentifizierung.

Aus dem KIS exportierte Daten müssen vor allfälligen nicht personenbezogenen Auswertungen anonymisiert oder pseudonymisiert werden. Für regelmässige oder wiederkehrende Auswertungen sollte das KIS die Funktionalität für einen entsprechenden anonymisierten oder pseudonymisierten Export anbieten.

2.4. Protokollierung und deren Auswertung

Unter Protokollierung beim Betrieb von IT-Systemen ist die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Frage beantworten lässt: "Wer hat wann mit welchen Mitteln was veranlasst, beziehungsweise worauf zugegriffen?"

Jede Datenbearbeitung muss protokolliert werden können. Denkbar sind folgende Datenbearbeitungen:

- Lesen, Verändern und Löschen von Daten
- Systemadministrationstätigkeiten (z.B. Protokollierung aller KIS-Wartungsvorgänge)
- Datenexport
- (Re-)Aktivierung gesperrter Daten beispielsweise in medizinischen Notfällen
- Protokollierung fehlgeschlagener Zugriffsversuche (mit automatischer Meldung bei mehrfach fehlgeschlagenen Zugriffsversuchen)

Die Protokolle enthalten sensible Informationen und müssen entsprechend gut geschützt sein. Nur autorisierte Personen dürfen Zugriff haben.

Die Protokolle müssen nach einer klar definierten Frist vernichtet werden. Die Aufbewahrungsfrist muss vom Verantwortlichen festgelegt werden und orientiert sich an der für die Aufgabenerfüllung erforderlichen Dauer.

Die Protokolle sind zu pseudonymisieren und sollten sich ohne Personenbezug auswerten lassen.

3. Anhang

3.1. Hilfestellungen

- Anforderungen Berner Klinikinformationssystem (BEKIS+)

- Sektorspezifische Risikoanalyse Sektor Gesundheitswesen
  http://www.refdata.ch/downloads/company/download/schlussbericht_risikoanalyse_gesundheitswesen.pdf

- Orientierungshilfen Krankenhausinformationssysteme (OH KIS)
  Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
  http://www.lfd.niedersachsen.de/download/57482/Orientierungshilfe_Krankenhausinformationssysteme_Version_2.pdf

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

- Zertifizierungsanforderungen EDÖB
  http://www.edoeb.admin.ch/datenschutz/00756/index.html?lang=de

3.2. Rechtliche Grundlagen

Schweizerisches Strafgesetzbuch
- Artikel 320 StGB: Amtsgeheimnis
- Artikel 321 StGB: Berufsgeheimnis

Gesundheits- und / oder Patienten(rechts)gesetze der Kantone
- Dokumentationspflicht (Patientendokumentation, Krankengeschichte)
- Aufbewahrungspflicht
- Schweigepflicht
- Einsichtsrechte
- Herausgabe der Behandlungsunterlagen

Datenschutzgesetze der Kantone
- Auskunfts-, Einsichts-, Berichtigungs-, Lösch- und Sperrrechte
- Anforderungen an bzw. Grundsätze der Informationssicherheit, Datensicherheit
- Allgemeine Grundsätze der Datenbearbeitungen und Verantwortlichkeiten

3.3. Checkliste

Mit folgender Checkliste kann ein KIS anhand der wichtigsten Anforderungen geprüft werden.

BEKIS+	Aufgabe / Anforderung	☑	Kommentar
Rechte der Betroffenen			
A06	Export aller Patienteninformationen	☐	
A06	Export der Zugriffs- und Änderungsprotokolle	☐	
D03	Löschung auf Wunsch der Patientin / des Patienten (inkl. Umsysteme)	☐	
D03	Automatische Löschfunktion nach Ablauf der Aufbewahrungsfristen	☐	
D03	Verwendung sicherer Löschfunktionen (z.B. Überschreiben)	☐	
D01	Zugriffeinschränkung bei alten Falldaten, Mitarbeitenden und auf Wunsch der Patientin / des Patienten	☐	
Berechtigungskonzept			
V02/05	Eingeschränkte Verwaltung der Benutzerrechte	☐	
V10	Zeitliche Sperrung der Benutzerkonten	☐	
V09	Sperrung bei falscher Passwort-Eingabe	☐	
V12	Automatische Erkennung veralteter (unnötiger) Benutzerkonten	☐	
V11	Session-Time-Out	☐	
V04	Rollenbasierte Berechtigungsvergabe (Funktion / Organisation)	☐	
V01	Starke Authentifizierung	☐	
V06-08	Technische Anforderungen an die Passwörter	☐	
Schnittstellen			
-	Geschützte Schnittstellen gemäss ISDS-Konzept	☐	
D05	Verschlüsselung und starke Authentifizierung bei externem Zugriff	☐	
D07	Exportfunktion von anonymisierten und pseudonymisierten Daten	☐	
Protokollierung			
D04	Protokollierung beim Lesen, Verändern und Löschen von Daten	☐	
P01/P07	Protokollierung der Systemadministrationstätigkeiten (inkl. Wartungsvorgänge)	☐	
P02	Protokollierung der Datenexporte	☐	
P03	Protokollierung der Ausweitung der Zugriffsrechte	☐	
P04	Protokollierung der fehlgeschlagenen Zugriffsversuche (inkl. automatische Meldung beim Erreichen eines Schwellwertes)	☐	
P05	Geschützte Protokolldateien	☐	