privatim
die schweizerischen datenschutzbeauftragten
les préposé(e)s suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

décembre 2015 / version 1.1

Exigences liées à la protection des données

Systèmes d'information clinique (SIC)

1. Introduction

1.1. Objet et objectif du guide

Le présent guide a été conçu par l'association des commissaires suisses à la protection des données (privatim). Il précise les exigences techniques relatives à l'utilisation des systèmes d'information qui découlent des lois et règlements du droit de la protection des données pour le domaine des cliniques. Il est un soutien lors de l'acquisition, de l'utilisation tout comme lors du contrôle et de l'amélioration des systèmes d'information clinique (SIC).
Le SIC est la plateforme d'information centrale d'une clinique. On y sauvegarde les données pertinentes des traitements médicaux. Le personnel d'accueil hospitalier, le service des soins stationnaires, tout comme les médecins ou autres services spécialisés sont les utilisateurs du SIC. Il peut donc s'agir d'une solution globale intégrée ou d'un ensemble de systèmes indépendants, pouvant même provenir de différentes entreprises de développement SIC.
Sur un plan institutionnel, le présent guide s'adresse aux grands hôpitaux, aux cliniques et aux homes médicalisés (> 10'000 patients par année) ainsi qu'aux entreprises de développement de SIC. Su un plan fonctionnel, il s'adresse à ceux qui décident de l'acquisition et de l'utilisation de SIC (management, direction informatique, IT-Controlling), à la direction des services de développement de SIC et aux autorités de contrôle.

1.2. Délimitation

Seules les exigences techniques les plus importantes dans les domaines du droit des personnes concernées (le droit des patients), des autorisations d'accès, des interfaces et de journalisation sont évoquées ci-après. En revanche, le présent guide ne décrit pas les mesures organisationnelles d'accompagnement, comme p.ex. le contrôle régulier des autorisations d'accès.
De même, ne le présent guide ne contient pas les exigences relatives à d'autres systèmes faisant partie de l'environnement du SIC (p.ex. la radiographie, le laboratoire etc.). Seules les exigences en lien avec les interfaces sont mentionnées.

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. Exigences formulées au SIC

2.1. Les droits des personnes concernées

Le droit de la protection des données sert à la protection de droits de la personnalité et de la sphère privée. Il oblige les personnes qui traitent des données de respecter les principes de la légalité et de la proportionnalité et offre aux personnes concernées des droits que celles-ci peuvent invoquer directement et qui doivent donc être garantis par les fonctions du SIC. Les fonctions suivantes doivent être intégrées dans le SIC :

Le droit d'accéder aux données

- Toutes les informations concernant le patient (données relatives aux personnes et à leur santé), traitées dans le cadre d'un traitement, doivent pouvoir être exportées de manière adéquate. Ceci est aussi valable pour les protocoles d'accès et de modification des données.

Le droit à la rectification et à la radiation

- Les données relatives à un traitement doivent pouvoir être radiées ou complétées (y compris les mandats de radiation et de rectification dans les systèmes référencés).
- Sous réserve de l'obligation de proposer les données aux archives compétentes, les données relatives à un traitement sont radiées ou rendues anonymes à échéance du délai de conservation.

2.2. Concept d'autorisation

Administration des comptes d'utilisateurs

- L'accès à l'administration des comptes d'utilisateurs doit pouvoir être limité: l'établissement des comptes et l'administration des autorisation d'accès ne peuvent être possibles qu'à travers des rôles prédéfinis.

Blocage des comptes d'utilisateurs

- Il doit être possible de bloquer des comptes d'utilisateurs pendant un temps déterminé.
- Les comptes d'utilisateurs doivent être bloqués après la répétition de l'utilisation d'un faux mot de passe.
- Il doit être possible de reconnaître automatiquement un compte n'ayant pas été utilisé durant une longue période et de le bloquer.
- De plus, il doit être possible de désactiver les séances après une certaine période d'inactivité.

Autorisations d'accès

- Les autorisations d'accès doivent pouvoir être attribuées sur des rôles et de fonctions (p.ex. d'après la fonction et l'unité organisationnelle). L'ampleur de l'accès d'un utilisateur ne doit découler que de l'ensemble des rôles structurels et fonctionnels qu'il occupe.
- Dans un délai défini (délai de radiation et de conservation), le système doit restreindre automatiquement l'accès aux données relatives à un traitement.
- En cas d'accès d'urgence aux données (les autorisations d'accès peuvent être élargies temporairement) le motif, la date et l'heure de l'accès, ainsi que le rôle et l'identité de l'utilisateur doivent être enregistrés.

- Lorsque le traitement concerne un collaborateur actuel ou ancien de l'institution, des restrictions spécifiques concernant l'accès doivent être mises en place.

L'authentification d'utilisateurs/les données d'accès

- L'accès au système ne peut être rendu possible que par une authentification d'utilisateur renforcée, c.à.d. les utilisateurs doivent s'authentifier sur la base d'au moins deux critères.
- Les mots de passes doivent remplir les exigences actuelles de la technique (p.ex. la visibilité et la reproduction lors de la saisie, exigences minimales concernant la complexité [longueur, caractères spéciaux, chiffres], limitation temporelle de la validité etc.).

2.3. Les interfaces

Avec l'intégration du SIC dans l'informatique hospitalière, il devient nécessaire de mettre en réseau les bases de données à travers les interfaces du SIC. Pour le support et la maintenance de l'infrastructure du SIC voire des applications, proposés par des prestataires de service externes, des interfaces au niveau des données et au niveau technique sont créées.

Illustration 1: système d'information clinique intégré

Pour ces interfaces, les exigences liées à la sécurité informatique et à la protection des données (SIPD) sont, en raison de la classification des données médicales des patients, très élevées.
Pour cette raison il convient de rédiger un concept SIPD qui remplisse les conditions suivantes :

- L'échange de données doit être détaillé (source, but à atteindre, données concernées, finalité [p.ex. agrégation dans le système de visée], base légale).
- La surveillance de l'interface doit être décrite (login, transfert, accès).
- La mise en œuvre technique de l'interface doit être décrite (procédure d'appel, push etc.).
- Les responsabilités sont définies (responsable des données dans les systèmes qui exportent des données respectivement dans les systèmes qui en importent).
- La communication est spécifiée (support, codage, procèssus de communication).

- Les rôles des utilisateurs et leurs droits dans les systèmes qui importent des données sont contrôlés.
- Les exigences liées à la radiation complète des données dans tous les systèmes sont décrites.
- Les délais de conservation et les délais de radiation sont basés sur les exigences légales et sont respectés dans tous les systèmes.
- La souche des données est fixée pour les cas d'un «rollback» ou d'un «restore».

Les exigences techniques doivent être contenues dans le concept SIPD.

L'accès externe aux données s'effectue de manière cryptée et avec une authentification renforcée.

Les données exportées du SIC doivent être rendues anonymes ou pseudonymes avant de pouvoir être utilisées dans le cadre d'un traitement non personnel. Pour des traitements non personnels (p.ex. statistiques) réguliers ou répétitifs, le SIC devrait proposer une fonction qui permet une exportation des données déjà rendues anonymes ou pseudonymes.

2.4. Journalisation et contrôle des accès

Par journalisation dans le domaine de l'informatique il faut comprendre l'établissement d'enregistrements manuels ou automatiques permettant de répondre à la question suivante: «qui a, à quel moment et par quel moyen, traité quoi, respectivement a eu accès à quelle donnée?»

Chaque traitement de données doit pouvoir être journalisé. On pense notamment aux traitements suivants:
- lecture, changement et radiation de données;
- activités d'administration du système (p.ex. journalisation de toutes les activités de maintenances du SIC);
- exportation des données;
- (ré-) activation de données bloquées par exemple en cas d'urgences médicales;
- journalisation des échecs d'accès aux données (avec annonce automatique en cas de récidive).

Les protocoles contiennent des informations sensibles et doivent être protégés en conséquence. Seules les personnes autorisées doivent pouvoir y accéder.

Les protocoles doivent être détruits à l'échéance de délais définis. Le délai de conservation doit être fixé par le responsable et s'oriente à la durée nécessaire prévue pour le traitement des données.

Les protocoles doivent être rendus pseudonymes et devraient être utilisés sans lien aux personnes concernées.

3. Annexe

3.1. Guides

- Anforderungen Berner Klinikinformationssystem (BEKIS+)

- Sektorspezifische Risikoanalyse Sektor Gesundheitswesen (BWL)
  http://www.refdata.ch/.../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

- Certification en matière de protection des données (PFPDT)
  http://www.edoeb.admin.ch/datenschutz/00756/index.html?lang=fr

3.2. Bases légales

Code pénal suisse
- article 320 CP: violation du secret de fonction
- article 321 CP: violation du secret professionnel

Lois cantonales sur la santé et/ou lois cantonales relatives aux droits des patients
- obligation de documentation (documentation du patient, antécédents médicaux)
- obligation de conservation
- secret professionnel
- droits d'accès
- restitution des dossiers médicaux

Lois sur la protection des données des cantons
- droits d'accès, droits de rectification, droits de radiation et droit au blocage
- exigences respectivement principes relatifs à la sécurité informatique et à la sécurité des données
- principes généraux du traitement des données et des responsabilités

Check-list
La check-list suivante permet d'examiner un SIC à l'aide des exigences les plus importantes.

BEKIS+	fonction / exigences	☑	commentaire
Droits des personnes concernées			
A06	Exportation des informations relatives à tous les patients	☐	
A06	Exportation des protocoles d'accès et de modifications des données	☐	
D03	Fonctions sélectives de radiation (y compris les systèmes environnants)	☐	
D03	Fonction de radiation automatique à l'échéance du délai de conservation	☐	
D03	Utilisation de fonctions de radiation fiables	☐	
D01	Restriction d'accès aux anciennes données d'un traitement, aux données de collaborateurs et sur demande du patient	☐	
Concept d'autorisation			
V02/05	Restriction de l'administration des droits d'accès	☐	
V10	Blocage temporel du compte d'utilisateur	☐	
V09	Blocage en cas de faux mot de passe	☐	
V12	Reconnaissance automatique de compte d'utilisateurs non utilisés	☐	
V11	Session-Time-Out	☐	
V04	Attribution des droits d'accès en fonction de rôles (fonction / organisation)	☐	
V01	Authentification renforcée	☐	
V06-08	Exigences techniques liées aux mots de passe	☐	
Interfaces			
-	Interfaces protégées selon le concept SIPD	☐	
D05	Cryptage et authentification renforcée en cas d'accès externe	☐	
D07	Fonction d'exportation de données rendues anonymes et pseudonymes	☐	
Journalisation			
D04	Journalisation de la lecture, de la modification et de la radiation des données	☐	
P01/P07	Journalisation des activités d'administration du système (y compris les activités de maintenance)	☐	
P02	Journalisation de l'exportation des données	☐	

P03	Journalisation de l'élargissement des droits d'accès	☐	
P04	Journalisation des échecs d'accès (y compris l'annonce automatique en cas d'atteinte d'un certain seuil)	☐	
P05	Accès restreint aux données de la journalisation	☐	