Note de sécurité de l'information et protection de la vie privée

Synthèse et règles pratiques en matière de protection de données médicales

(sur base des discussions au sein du sous-groupe de travail « données médicales »)

(NOTE MEDSEC)

TABLE DES MATIÈRES

1. Introduction

Le présent document est destiné aux responsables, aux sous-traitants d'informations, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

Le présent document traduit les points de vue du sous-groupe de travail "Données médicales" en matière de protection des données médicales. Il a été rédigé dans le but de :

- procurer aux médecins un fil conducteur en vue de l'implémentation et de la mise en application des mesures de sécurité pour les données médicales et
- pouvoir entamer les débats avec les conseillers en sécurité de l'information et les délégués à la protection des données.

Dans le cadre de la protection des données à caractère personnel médicales, tout médecin responsable se voit attribuer dans un premier temps une mission conceptuelle, à savoir l'élaboration et la transmission d'instructions de sécurité (la détermination des objectifs de sécurité ainsi que la définition et la mise à jour continuelle du niveau de sécurité visé) au conseiller en sécurité de l'information et au délégué à la protection des données et la mise à jour de ces instructions lorsque la nécessité se présente. En particulier, tout médecin responsable a pour mission d'étudier avec le conseiller en sécurité de l'information et le délégué à la protection des données les problèmes de sécurité spécifiques de son organisation, afin d'élaborer des mesures appropriées en fonction de la situation[1]. La nature et l'étendue de ces mesures peuvent varier d'une organisation à l'autre et dépendent de nombreux facteurs tels :

- la capacité financière de l'organisation ;
- la possibilité de réaliser des changements au sein de l'organisation et la promptitude avec laquelle ces changements peuvent être réalisés.

Toutefois, il ne peut être demandé à une organisation de fournir sans délai des efforts considérables[2]. L'étalement régulier des efforts sur un intervalle acceptable peut même, dans certains cas, donner de meilleurs résultats. Les efforts fournis doivent être proportionnels à l'importance des données médicales auxquelles ils ont trait. Dans la mesure du possible, il faut éviter qu'une organisation ne doive modifier profondément ses procédures et sa manière de procéder ou que ses structures administratives soient alourdies inutilement. Toutefois, il faut tenter d'améliorer chaque année le niveau de sécurité de l'information.

Alors que le médecin responsable est dans un premier temps chargé d'une mission conceptuelle, le conseiller en sécurité de l'information et le délégué à la protection des données sont, en ce qui concerne la protection des données à caractère personnel médicales, responsables du suivi de l'application correcte des instructions reçues du médecin responsable. Le contrôle quant à l'exécution des instructions appartient au médecin responsable.

[1] Un médecin responsable peut toujours demander l'avis du sous-groupe de travail "Données médicales" pour savoir si les mesures de sécurité de l'information mises en place ou proposées sont suffisantes.

[2] Les coûts liés à la protection des données médicales doivent être inscrits au budget de la sécurité de l'information que l'organisation est tenue d'établir chaque année en vertu de l'article 7 de l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale (IPSS).

2. Points de vue quant à la protection de données médicales

2.1 Données médicales

2.1.1 Définition

Le sous-groupe de travail "Données médicales" se rallie au raisonnement suivi par le Comité de surveillance[3] lors de la définition du terme "donnée médicale". Ce raisonnement aboutit à la conclusion que tant le contexte (principe de finalité) dans lequel une donnée est utilisée que la nature de la donnée sont déterminants pour qualifier une donnée de médicale ou de non-médicale[4].

Le raisonnement du Comité de surveillance est basé sur les deux principes suivants :

- Interprétation téléologique: dans ce contexte, une notion doit être interprétée en fonction de l'objectif pour lequel elle a été définie. Dans un premier temps, il y a donc lieu de définir les objectifs à atteindre et il convient ensuite d'interpréter la notion de "donnée médicale" sur base de ces objectifs.

  Les motifs qui ont incité le législateur à placer le traitement de certaines données sous la surveillance d'un médecin sont notamment le fait que l'intervention d'un médecin offre, dans le cadre de la protection de la vie privée, pour certaines données une valeur ajoutée. Pour les données pour lesquelles cette intervention ne représente pas de valeur ajoutée, cette intervention ne semble pas requise.

  Un exemple à titre d'illustration : pour le traitement d'une adresse, l'intervention d'un médecin n'est pas nécessaire, étant donné que chacun sait en interpréter correctement le contenu. Une adresse ne constitue donc pas une donnée médicale. Par ailleurs, en plaçant une adresse sous la surveillance d'un médecin, sa protection n'augmente pas. Un diagnostic ou un code nomenclature par contre peuvent uniquement être correctement interprétés par un médecin. Il s'agit bien d'une donnée médicale.

- Univoque: soit une donnée est toujours qualifiée de médicale, soit elle ne l'est jamais. Il n'y a pas de moyen terme. En effet, il n'est pas réaliste d'affirmer qu'une adresse constitue une donnée non-médicale dans 99% des cas et que dans 1% des cas, l'exception, il faut qualifier cette donnée de médicale (p.ex. parce qu'il est possible d'en déduire un séjour dans un établissement psychiatrique[5]). Ce qui implique en effet que la donnée "adresse", si elle est enregistrée dans une banque de données, devrait être placée sous la surveillance d'un médecin. Ainsi, la presque totalité des fichiers serait placée sous le contrôle d'un médecin. Une autre solution qui consiste à regrouper ces adresses dans un fichier séparé ne constitue pas non plus une solution idéale, étant donné que chacun pourrait en conclure que le fichier concerné contient des informations confidentielles.

Il est préférable de limiter au maximum le nombre de données médicales. En effet, en classant trop de données parmi les données médicales, la protection des véritables données médicales pourrait en subir des effets négatifs.

Le médecin détermine lui-même en fonction des circonstances, au sein de son organisation, ce qui constitue et ce qui ne constitue pas une donnée médicale. La qualification d'une donnée de médicale ou non, ou en d'autres termes, le

[3] Le Comité de surveillance a défini le terme "Donnée médicale" dans son rapport d'activité 1992 (p. 34-35). Monsieur Frank Robben a précisé le raisonnement du Comité de surveillance quant à la définition de la notion "Donnée médicale" dans sa note du 19 mai 1995 sous référence A1/P2/95/150.pu qui a été adressée aux membres du sous-groupe de travail "Données médicales".

[4] Le sous-groupe de travail "Données médicales" déclare ne pas croire en une définition mais bien dans le raisonnement qui aboutit à une définition. Proposer une définition qui soit valable dans toutes les situations, semble être une mission impossible. En formulant ce point de vue, le sous-groupe de travail s'oppose clairement à ceux qui estiment que seule la nature de la donnée, et non le contexte dans lequel elle est traitée, est déterminante pour qualifier une donnée de médicale ou de non-médicale. Car cette façon de voir les choses passe outre un principe de base, à savoir le principe de finalité. Négliger cet objectif fondamental revient à qualifier toutes les données de médicales et à ainsi placer leur traitement sous la surveillance et la responsabilité d'un médecin. L'intervention d'un médecin sera finalement vaine si on le rend responsable de quasi toutes les données, étant donné que son attention pour la protection des données médicales diminuera considérablement.

[5] Un fichier comprenant uniquement des adresses de personnes séjournant dans un établissement psychiatrique est cependant à considérer comme une donnée médicale.

fait qu'elle doive faire l'objet d'une protection supplémentaire, revient au médecin qui dans ce cadre dispose des pouvoirs d'appréciation utiles. Il y a dès lors lieu d'éviter de brider ce pouvoir d'appréciation par l'élaboration de définitions précises.

2.1.2 Données médicales au sens strict et données médico-administratives

Le sous-groupe de travail "Données médicales" accepte le principe de répartir les données médicales en différentes catégories[6] de façon à pouvoir introduire différents niveaux de sécurité. Ainsi, une distinction est opérée entre les données médicales au sens strict et les données médico-administratives[7]. La décision de répartir les données médicales en différentes classes appartient à chaque institution. En effet, il est impossible de déterminer à ce niveau des règles et directives qui soient valables de manière générale.

La création de différentes catégories de données médicales permet de faire une distinction entre plusieurs types de personnel médical habilité. Par exemple :

- les personnes ayant une compétence médicale générale ont accès à l'ensemble des données médicales et sont autorisées à traiter tous les types de données médicales ;
- les personnes ayant une compétence médicale spécifique ont uniquement accès à certaines données médicales et peuvent uniquement traiter des données médicales spécifiques.

2.1.3 Accès aux données médicales

Les personnes qui interviennent dans le traitement de données à caractère personnel médicales ou qui y ont accès, doivent être désignées nominativement. Cette désignation peut avoir lieu par référence à des fonctions, à condition que les fonctions soient suffisamment précises et qu'il soit déterminé avec précision quelles personnes individuelles exercent quelle fonction[8].

Par fonction, il y a lieu ensuite de définir avec précision le contenu et la portée des autorisations d'accès[9]. Ces autorisations doivent être accordées sur base du principe de finalité. De manière concrète, ces autorisations d'accès peuvent, par exemple, être décrites au moyen de tables d'autorisation qui indiquent, par type de traitement de base (consultation, ajout, modification, suppression), qui peut les réaliser.

Le principe de la description de fonction s'inscrit dans le cadre de la réglementation relative à l'accès aux données médicales et à la portée de cet accès. Ainsi, les catégories de personnel citées ci-après ont accès aux données médicales à condition que cet accès ait été prévu dans la description de fonction: l'introduction de conclusions médicales par du personnel non-médical, la distribution du courrier médical par du personnel non-médical, le traitement de dossiers par du personnel non-médical, ...

---

[6] Un exercice pratique a été réalisé par Fedris et est commenté dans la note technique 94/3 relatif à la composition du dossier médical.

[7] Toutefois, il n'est pas toujours simple de faire une distinction entre des données médico-administratives et des données strictement médicales. En effet, certaines données médico-administratives deviennent des données médicales lorsqu'elles sont combinées à d'autres. En cas d'informatisation, la combinaison de données s'avère simple à réaliser (p.ex. data analytics). Dès lors, il y a lieu de tenir ces éléments à l'esprit lors de la répartition des données médicales en différentes catégories.

[8] A cet effet, il serait utile que les organisations élaborent dès à présent des descriptions de fonction élémentaires au moins pour les fonctions médicales (y compris médecin responsable). La meilleure façon de procéder est de demander aux collaborateurs de réaliser eux-mêmes une description de leur fonction et de les faire rationaliser ensuite par le service du personnel.

[9] Dans le cadre de l'octroi aux membres du personnel d'autorisations d'accès à des données médicales, il convient de leur demander quelles sont les données médicales dont ils ont besoin dans le cadre de l'exercice de leur fonction. Ils sont en effet les mieux placés pour déterminer les données dont ils ont besoin. Les autorisations d'accès demandées doivent par la suite être évaluées, par personne, par le médecin responsable quant à leur stricte nécessité, afin d'éviter tout usage abusif.

GROUPE D'UTILISATEURS X				
Description des données	Ajout (add / write)	Consultation (read / consult)	Modification (change / modify)	Suppression (delete / erase)
Donnée a	X	X		X
Donnée b	X		X	
Donnée c	X	X	X	X
…				

L'octroi d'autorisations d'accès relatives à des documents papier peut intervenir selon les mêmes principes que l'octroi d'autorisations relatives à des données électroniques. En effet, il suffit dans ce cas de remplacer les données a, b et c par des formulaires et d'adapter éventuellement les opérations possibles.

Il appartient au conseiller en sécurité de l'information et au délégué à la protection des données de veiller à ce que les membres du personnel respectent les autorisations telles que mentionnées dans leur description de fonction.

2.1.4 Echange de données médicales entre différents services internes (tels que comptabilité, service juridique, litiges)

La question de savoir qui peut échanger des données médicales a été examinée en détail au paragraphe 2.1.3. ("Accès aux données médicales"). En ce qui concerne la question de savoir quelles données peuvent être échangées, il appartient au médecin d'en décider. Toutefois, il est tenu de respecter à cet égard la législation en vigueur en la matière.

2.1.5 Sous-traitance de missions portant sur le traitement de données médicales

Les mêmes mesures de sécurité que celles valables pour l'organisme commettant sont d'application aux organismes travaillant en sous-traitance ou pour le compte de l'organisme commettant. Le plus prudent est de prévoir ces aspects dans un contrat et de tenir explicitement compte du cycle de vie complet de l'information (de la création à l'archivage ou la suppression). Il appartient au mandant de veiller au respect des règles de sécurité de l'information par le sous-traitant. La désignation éventuelle d'un médecin auprès du sous-traitant, si ce dernier traite des données à caractère personnel médicales pour le compte de l'organisme commettant, doit de préférence être prévue par voie contractuelle.

2.2 Dossier médical[10]

2.2.1 Dossier médico-administratif et dossier médical contenant exclusivement des documents médicaux

Il appartient à chaque organisation de décider si elle souhaite créer un dossier médico-administratif ou un dossier médical contenant uniquement des documents médicaux. Un dossier contenant tant des documents médico-administratifs que des documents médicaux doit être protégé comme s'il contenait uniquement des documents médicaux (donc la protection la plus sévère possible). Un dossier contenant uniquement des documents médico-

[10] Un médecin doit faire attention aux données qu'il reprend dans un dossier médical. Les données non pertinentes ou celles qui n'offrent pas de valeur ajoutée pour le dossier médical ne peuvent pas être reprises dans le dossier.

administratifs fait l'objet d'une protection moins sévère. L'inconvénient de mélanger un dossier médical avec un dossier médico-administratif est qu'un dossier ne peut être obtenu séparément; ce qui augmente son immobilité.

2.2.2 Un assuré social possède plusieurs dossiers médicaux au sein d'une seule et même organisation (pas d'utilisation d'un numéro d'identification unique)

Ce problème peut en premier lieu être résolu par des mesures organisationnelles qui peuvent varier d'un organisme à l'autre, par l'informatisation et par l'utilisation obligatoire du numéro de registre national. Une solution possible est la création d'un dossier médical unique par individu. Cette méthode de travail offre plusieurs avantages dont les principaux sont :

- gestion simplifiée des dossiers ;
- concentration des informations permettant de retrouver l'ensemble des données dans un seul dossier et d'éviter des décisions contradictoires. Cette concentration permettra également d'améliorer le processus de décision.

Tout dossier doit pouvoir être localisé aisément[11] et les nouveaux documents/pièces entrants pour une personne doivent toujours pouvoir être associés aux données existantes de cette personne.

L'interconnexion de plusieurs dossiers relatifs à une seule et même personne peut être réalisée par la voie électronique, de sorte que la personne qui demande un dossier puisse être avertie de l'existence d'autres dossiers pour cette même personne.

2.2.3 Circulation de dossiers médicaux

Ce problème peut être résolu par des mesures organisationnelles adéquates (par exemple en mettant les dossiers médicaux sous enveloppe ; cette enveloppe est ensuite fermée au moyen d'agrafes et pourvue d'un paraphe).

La sensibilisation du personnel en ce qui concerne les dossiers médicaux est essentielle. Encourager les membres du personnel à immédiatement renvoyer vers l'expéditeur ou transmettre à leur destinataire légitime (dans la mesure où il est connu au sein de l'organisation) les dossiers/documents/pièces qui ne leur sont pas destinés, moyennant le respect des principes généraux du secret postal.

2.2.4 Qualifications du personnel médical qui traitent/gèrent des dossiers médicaux.

Ce problème peut être résolu par la mention du profil souhaité dans la description de fonction. Ainsi, un médecin peut par exemple poser certaines conditions en matière d'aptitudes, niveau de formation et expérience aux candidats pour le traitement / la gestion de dossiers médicaux.

Lors de l'engagement ou du remplacement de membres du personnel, le service du personnel doit tenir compte de ces conditions. Pour le classement de dossiers médicaux par exemple, la personne en question doit faire preuve de précision et de discipline lors de l'exécution de son travail ; qualités que tout le monde ne possède pas.

2.2.5 Accès physique aux archives médicales (dossiers médicaux) et installation d'archives séparées pour les dossiers médicaux

2.2.5.1 Accès physique aux dossiers médicaux et aux archives médicales

[11] Peut être résolu par une gestion informatisée des dossiers. En effet, ce type de gestion permet à tout moment de savoir avec précision où se trouve un dossier.

Les mesures utiles doivent être élaborées en collaboration avec le conseiller en sécurité. Cependant, l'objectif poursuivi est de réserver l'accès aux dossiers médicaux au personnel médical habilité.

Les mesures de sécurité à implémenter doivent être fonction des risques susceptibles de se produire (p.ex.: les mesures d'accès aux archives où il est aisé de retrouver les dossiers médicaux sont différentes des mesures d'accès aux locaux où les dossiers médicaux traînent sur les bureaux). La situation est différente dans chaque organisation et chaque organisation doit prendre des mesures en fonction de sa situation spécifique. A cet égard, il est indispensable de trouver un bon équilibre entre sécurité de l'information et efficacité[12].

L'accès aux locaux où il est possible de retrouver la localisation d'un dossier médical déterminé, doit également être protégé. Seules les personnes qui sont autorisées à accéder aux dossiers médicaux peuvent savoir où se trouve un dossier médical.

2.2.5.2 Archives spéciales pour les dossiers médicaux

L'enregistrement centralisé et séparé des dossiers médicaux est à conseiller car il offre au moins deux avantages non négligeables :

- les dossiers peuvent facilement être retrouvés ;
- la gestion des accès est facilitée.

Si une organisation ne prévoit pas un espace d'archivage distinct pour les dossiers médicaux, elle doit veiller à ce que l'accès aux archives soit bien réglementé et limité au personnel médical autorisé. L'enregistrement des dossiers médicaux sur supports magnétiques constitue aussi une solution à envisager (voir force probante[13]).

2.2.6 Accès logique aux dossiers médicaux

Une solution pour ce problème doit s'envisager en fonction de la situation spécifique de l'organisation et en concertation avec le conseiller en sécurité de l'information et le délégué à la protection des données. Généralement, une adaptation du programme suffit.

2.3 Accès au bâtiment et aux locaux

L'accès aux locaux et au bâtiment constitue un problème général de sécurité de l'information et non un problème médical spécifique. La solution relève de la compétence des conseillers en sécurité de l'information. Toutefois, le médecin responsable doit examiner les problèmes éventuels avec le conseiller en sécurité de l'information.

Les réunions médicales[14] sont tenues pendant et en dehors des heures normales de travail dans des salles non-isolées: la solution la plus appropriée consiste à prendre des mesures organisationnelles adéquates, éventuellement en combinaison avec d'autres mesures techniques. L'élaboration des mesures utiles s'effectue en collaboration avec le conseiller en sécurité de l'information.

[12] Les membres du groupe de travail "Sécurité de l'information" et "Données médicales" sont d'avis que, vu l'importance des données médicales à caractère personnel et les risques y afférents, les dossiers médicaux (actifs et archivés) devaient être physiquement protégés. Les moyens de protection (p.ex. armoire, bureau, local fermé) sont à déterminer par l'organisation.

[13] Loi du 24 février 2003 concernant la modernisation de la gestion de la sécurité sociale et concernant la communication électronique entre des entreprises et l'autorité fédérale. Arrêté royal du 7 décembre 2016.

[14] Une réunion médicale est une réunion où sont examinés des dossiers médicaux.

3. Techniques de sécurité

3.1 Techniques d'authentification

Il existe plusieurs formes d'authentification, qui peuvent éventuellement être combinées afin d'obtenir un niveau de sécurité plus élevé. Trois types de preuve sont utilisables à cet égard :

1. Quelque chose que l'on sait = connaissance

   Il s'agit par exemple d'un mot de passe, d'un code pin ou d'une phrase secrète. Cette preuve doit rester secrète et ne peut donc pas être divulguée afin d'éviter le vol d'identité. Un pirate essaiera de s'approprier l'identité d'une personne en devinant son mot de passe, qui peut être retrouvé p.ex. au moyen d'un keylogger (enregistreur de frappe)[15]. C'est la raison pour laquelle les organisations qui traitent des données médicales imposent l'utilisation de mots de passe complexes[16] qui doivent être modifiés périodiquement. Idéalement, le temps nécessaire pour déceler le mot de passe devrait excéder la durée de validité des données médicales.

2. Quelque chose que l'on possède

   Ceci signifie que la preuve de l'identité est fournie en utilisant un signe de reconnaissance physique décerné par ou pour le compte du système d'autorisation. Il s'agit par exemple de tokens ou d'une carte à puce ou encore d'une clé USB. Il est fait usage d'une fonction de question/réponse : le système d'autorisation pose une question et la personne qui demande accès doit fournir la réponse adéquate au moyen du token. Le grand avantage de cette technique est qu'une personne qui souhaite se connecter doit disposer à la fois d'un code secret et d'un token et que le mot de passe calculé est modifié à chaque connexion.

3. Quelque chose que l'on est = caractéristique personnelle

   Une caractéristique d'identification unique d'une personne est enregistrée dans une base de données d'authentification[17]. Il s'agit des systèmes dits biométriques qui essaient de reconnaître les caractéristiques personnelles ou les comportements d'un utilisateur. Les techniques utilisées sont p.ex. scanner de la rétine, reconnaissance de la signature, forme de la main, empreintes digitales, reconnaissance de la voix, etc... Les inconvénients liés à ces techniques sont les suivants :

   - elles ne sont pas toujours acceptées par les utilisateurs ;
   - elles sont relativement onéreuses ;
   - elles ne sont pas toujours très fiables.

4. Authentification automatisée

   Les ordinateurs et les systèmes utilisent d'autres types d'authentification. Il peut également être fait usage d'une Public Key Infrastructure (PKI) avec utilisation de certificats. Des implémentations connues sont 802.1X et SAML[18].

Les organisations sont tenues de développer les procédures utiles au cas où un utilisateur ne retrouve plus son token (perte, vol). La méthode d'octroi de nouveaux tokens doit également être réglementée. Les techniques d'authentification peuvent uniquement être utilisées aux fins pour lesquelles elles ont été implémentées en non par

[15] Un keylogger est un programme ou un composant hardware permettant d'enregistrer les mouvements sur le clavier et même les mouvements de la souris d'un ordinateur.

[16] Un mot de passe suffisamment long compte minimum 12 caractères. Il est possible de tester la qualité d'un mot de passe sur https://www.safeonweb.be/fr/test-mot-de-passe

[17] Biométrie = la détermination de caractéristiques mesurables de personnes.

[18] Security Assertion Markup Language est un standard pour l'échange de données d'authentification et d'autorisation entre des domaines. SAML offre un cadre basé sur XML pour la création et l'échange d'informations de sécurité de partenaires en ligne. SAML est entretenu par une communauté d'internautes et les mises à jour sont effectuées de manière publique. Les intéressés sont encouragés à contribuer au développement.

exemple pour contrôler les heures de présence d'un utilisateur. Le choix de la technique d'authentification varie d'un organisme à l'autre et relève de la compétence du conseiller en sécurité de l'information en concertation avec le délégué à la protection des données.

3.2 Techniques de chiffrement

A cet égard, nous faisons référence à la politique relative au « chiffrement » (BLD CRYPT) pour de plus amples informations.

3.3 Séparation de fonctions

Selon ce principe, aucun individu ne peut, au sein d'une organisation, disposer de la compétence exclusive de sorte qu'il/elle gère entièrement le traitement d'une transaction déterminée ou d'un groupe de transactions. Ceci signifie qu'une responsabilité déterminée est partagée entre plusieurs personnes. Cette répartition sert de contrôle interne afin d'éviter toute erreur/abus. Le risque que des personnes coopèrent pour contourner ce contrôle interne est appelé collusion.

Idéalement, une séparation est opérée entre les tâches de prise de décision/autorisation, exécution, contrôle/protection, enregistrement et conservation de données médicales sans que cela ne porte atteinte à l'efficacité.

Un des moyens pour définir la séparation des processus consiste à établir une matrice de séparation de fonctions. Dans ce document, il est indiqué par processus quelle personne (dans quelle fonction) a une mission de décision, de conservation, d'enregistrement, de contrôle et d'exécution.

Pour illustrer le principe de la séparation des fonctions dans la pratique, on peut prendre l'exemple de la manière dont les nouvelles applications sont développées dans un environnement de traitement automatisé de l'information. Chaque nouvelle application à développer doit parcourir différentes phases de développement. Les principales phases sont :

- la phase d'analyse ;
- la phase de programmation ;
- la phase de test ;
- la phase de mise en production du programme testé.

Ceci permet d'éviter que la personne qui se charge de la mise en production d'une application soit la même que celle qui a conçu l'application.

Dans le cadre du traitement de dossiers médicaux, il y a lieu d'introduire le principe de la séparation de fonctions. Dans les organisations de petite taille ou de taille moyenne, il est toutefois souvent impossible de séparer parfaitement toutes les phases du processus. Il convient dès lors d'introduire une séparation de fonctions intelligente. Ceci doit être évalué en concertation avec l'instance de contrôle.

3.4 Protection de données médicales sur des supports magnétiques

Les principaux problèmes quant à l'enregistrement de données médicales sur supports magnétiques sont les suivants :

- problème de confidentialité: ce problème peut être facilement résolu par un chiffrement des données ;
- transport des supports d'information magnétiques :
    - les supports d'information doivent être envoyés dans un conteneur approprié (p.ex. clé USB dans une enveloppe spéciale à bulles, bandes magnétiques et cassettes dans un coffre scellé);
    - lors de l'envoi, l'expéditeur doit toujours veiller à disposer d'une preuve d'envoi ;

- les supports d'information doivent être accompagnés d'un formulaire d'envoi sur lequel figurent au minium les informations suivantes: nom et adresse de l'expéditeur, nom et adresse du destinataire et contenu du support d'information.

4. Règles pratiques en matière de protection de données médicales

1. Le médecin responsable s'inspirera lors de l'exécution de sa mission de sécurité de l'information :

- des normes minimales de sécurité de l'information et de protection de la vie privée à respecter par les institutions publiques de sécurité sociale en vue de leur connexion au réseau de la Banque Carrefour de la sécurité sociale ;
- des directives en matière de sécurité au niveau des organisations participant au réseau géré par la Banque Carrefour de la sécurité sociale ;
- du manuel « Sécurité de l'information sécurité sociale » ;
- du code médical de bonne conduite en matière de communication de données médicales à caractère personnel aux bénéficiaires de la sécurité sociale.

2. Dans le cadre de la protection des données médicales, les tâches sont réparties comme suit entre le médecin responsable et le conseiller en sécurité :

- la principale mission du médecin responsable se situe au niveau conceptuel, à savoir formuler les objectifs de sécurité de l'information adéquats ainsi que définir et mettre continuellement à jour (en fonction de la situation spécifique de l'organisation et de l'expérience acquise) le niveau de sécurité de l'information visé (éventuellement en collaboration avec le conseiller en sécurité de l'information et le délégué à la protection des données). Il appartient au médecin responsable d'avertir le conseiller en sécurité de l'information, le délégué à la protection des données et la personne chargée de la gestion journalière de l'organisation de la présence de risques significatifs en ce qui concerne le traitement des données à caractère personnel médicales ;
- le conseiller en sécurité de l'information et le délégué à la protection des données élaborent les mesures adéquates sur base des objectifs de sécurité de l'information formulés par le médecin responsable et du niveau de sécurité de l'information à atteindre. Ces mesures seront élaborées de préférence en collaboration avec le médecin responsable. Outre l'élaboration des mesures, le conseiller en sécurité de l'information et le délégué à la protection des données veillent au suivi de la prompte et correcte exécution[19] de celles-ci (conjointement avec le responsable de la gestion journalière qui, avant leur mise en œuvre, doit marquer son accord sur les mesures proposées) et étendent le plan de sécurité et le budget de sécurité aux mesures relatives à la protection des données médicales. Enfin le conseiller en sécurité de l'information et le délégué à la protection des données veillent à la coordination nécessaire avec le médecin responsable. Ce rôle de coordination permettra d'éviter que le responsable de la gestion journalière ne reçoive deux avis différents concernant un problème de sécurité de l'information déterminé (une telle situation est à éviter autant que possible et ne surgira que lorsque le conseiller en sécurité de l'information, le délégué à la protection des données et le médecin responsable ont chacun un avis fondamentalement différent concernant le problème constaté);
- Outre une mission conceptuelle, le médecin responsable assure également un rôle de contrôle. Il consiste à s'assurer que les mesures de sécurité de l'information élaborées ont effectivement été mises en œuvre et sont conformes aux objectifs qu'il a formulés.

3. Le médecin responsable élabore, de commun accord avec le conseiller en sécurité de l'information et le délégué à la protection des données et compte tenu de la situation spécifique, des mesures organisationnelles, techniques et

[19] Bien que le conseiller en sécurité et le délégué à la protection des données n'aient pas un rôle d'exécution, il n'est pas exclu qu'ils exécutent ou réalisent eux-mêmes certaines tâches ou activités. Cela peut survenir de leur propre initiative ou à la demande du responsable de la gestion journalière. Il va de soi que la structure organisationnelle de l'organisation et la situation spécifique constituent à cet égard un facteur crucial.

communicatives appropriées. Le conseiller en sécurité de l'information et le délégué à la protection des données sont tenus d'inscrire les mesures et les frais y afférents respectivement dans le plan de sécurité de l'information et dans le budget de sécurité de l'information (art. 7 de l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale). La décision finale quant à la mise en œuvre des mesures définies appartient au responsable de la gestion journalière de l'organisation.

4. Les personnes qui interviennent dans le traitement des données médicales ou celles qui y ont accès doivent être désignées nominativement, en vertu de l'article 26 de la loi organique de la Banque Carrefour. Cette désignation peut toutefois intervenir par référence à des fonctions, à condition que les fonctions soient décrites de manière suffisamment précise et qu'il soit déterminé avec précision quelles personnes individuelles exercent quelle fonction. De manière pratique, ce système peut être implémenté par l'élaboration et l'introduction de descriptions de fonction. Une description de fonction doit notamment comprendre les éléments suivants :

- une description précise des tâches à réaliser ;
- le contenu et la portée des autorisations d'accès ;
- la mention des qualifications ;
- ...

Ainsi, tout membre du personnel peut être autorisé à traiter des données médicales à condition que cette autorisation et sa nature figurent dans la description de fonction de la personne concernée.

5. La décision de créer différentes catégories de données médicales ainsi que la décision de créer différentes catégories de personnel médical habilité appartient à chaque organisation.

6. L'expérience nous apprend que l'automatisation des dossiers médicaux n'est pas aussi rapide que celle des dossiers administratifs. Plus encore, le support papier reste dans beaucoup de cas le support par excellence pour l'enregistrement de données médicales. S'il s'avère cependant que l'enregistrement des dossiers médicaux sous forme électronique offre un avantage au niveau de la sécurité, il y a lieu d'insister sur une accélération de l'informatisation de ces dossiers. Les aspects suivants jouent incontestablement un rôle lors du choix : l'état d'avancement de la technique, les connaissances disponibles au niveau de l'informatique et de la sécurité de l'information au sein d'une organisation et les efforts à réaliser (analyse coûts /bénéfices).

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
1996		V1996	Première version	02/12/1996	02/12/1996
2017		V2017	Adaptations dans le cadre de la réglementation GDPR	14/07/2017	14/07/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents détaillant la politique à suivre, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions normes minimales sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

1. Le Règlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[20];

La plupart des institutions publiques de sécurité sociale tombent sous le champ d'application de cette loi. Au sein de chaque institution publique de sécurité sociale, le traitement, l'échange et la conservation de données à caractère personnel médicales s'effectue sous la surveillance et la responsabilité d'un médecin. Ces médecins sont par ailleurs soumis à l'article 458 du Code pénal belge (secret médical) et au Code de déontologie médicale (Ordre des médecins).

[20] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&qid=1484310282035&from=FR

Annexe C: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	**Oui**
Sécurité des ressources humaines	**Oui**
Gestion des actifs	
Protection de l'accès	**Oui**
Cryptographie	**Oui**
Sécurité physique et protection de l'environnement	**Oui**
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	**Oui**
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	**Oui**

***** FIN DU DOCUMENT *****