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

Communication de données médicales à caractère personnel aux bénéficiaires de la sécurité sociale

(BLD MEDSEC)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie des normes minimales relatives à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, 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).

Nombre d'institutions de sécurité sociale disposent de données médicales concernant les assurés sociaux. En ce qui concerne ces données, les institutions ont d'une part l'obligation du secret envers des tiers et d'autre part, elles sont obligées, sous certaines conditions, à communiquer ces données à l'intéressé. Cette obligation de communication est prévue par diverses dispositions légales (voir l'annexe B).

Les assurés sociaux peuvent prendre connaissance de leurs données médicales de deux manières :

1. à leur propre demande
2. suite à une décision.

Pour ce qui concerne la communication de données médicales à la demande de l'intéressé, les différentes dispositions ne concordent pas toujours, ce qui donne lieu à un problème d'interprétation. Cette imprécision concerne surtout les deux questions suivantes :

- Quelles données médicales tombent sous le champ d'application de la loi ? (Distinction entre un dossier médical d'une part et un traitement, un fichier ou une banque de données d'autre part)
- De quelle manière faut-il communiquer ces données à l'intéressé ? (Directement ou par l'intermédiaire d'un médecin ?)

En qui concerne la communication à l'occasion d'une décision, la question se pose de savoir si des données médicales à caractère personnel peuvent être reprises dans une décision et dans quelle mesure. Cette grande diversité de dispositions légales ne favorise pas la sécurité juridique, ni dans le chef des intéressés, ni dans celui des médecins responsables. Il est dès lors utile de développer, pour la communication de données médicales, un code de bonne conduite qui soit applicable à l'ensemble des données médicales dans toutes les institutions publiques de sécurité sociale. Ce code de bonne conduite doit, d'une part, garantir de manière satisfaisante le droit à l'information de l'intéressé et, d'autre part, rencontrer les problèmes spécifiques résultant de la nature particulière des données médicales... De plus, les procédures à suivre doivent être simples et pouvoir être exécutées par les institutions de sécurité sociale sans que le travail administratif n'augmente de manière exagérée. Il est inconcevable que des obligations trop lourdes en matière de communication de données entravent le fonctionnement même de la sécurité sociale. Le point de départ, à savoir le droit des intéressés de prendre connaissance des données médicales les concernant, n'est pas contesté. Ce principe est, en effet, un des fondements d'une protection efficace de la vie privée. Il contribue en même temps et de manière importante à la transparence administrative. D'autre part, les données médicales présentent souvent des aspects très particuliers qui rendent impossible leur communication à l'intéressé comme s'il s'agissait de données administratives ordinaires. C'est la raison pour laquelle une procédure spécifique est proposée. Deux médecins jouent un rôle central dans cette procédure : le médecin-conseil de l'institution et le médecin de confiance de l'intéressé. Par le terme général de "médecin-conseil", il faut entendre tout médecin intervenant pour une institution de sécurité sociale. Le médecin de confiance est le médecin désigné par l'intéressé pour l'informer des données médicales communiquées par le médecin-conseil. Le rôle de ces médecins est précisé plus loin. Il est essentiel de tenir à l'esprit que ces propositions portent sur l'ensemble des données médicales à caractère personnel, peu importe leur forme (rapport, dossier, fichier, traitement).

Ce document propose le code de bonne conduite et les procédures pour la communication de données médicales, applicables à toutes les données médicales dans les institutions publiques de sécurité sociale. Ce code de bonne conduite et ces procédures doivent permettre d'offrir des garanties suffisantes aux bénéficiaires de la sécurité sociale, tout en respectant les obligations médico-éthiques du médecin et en limitant la charge administrative pour les institutions publiques de sécurité sociale lors de l'exécution de leurs activités.

2. La nature particulière des données médicales

Les données médicales sont en soi déjà très spéciales en ce qu'elles contiennent souvent des informations hautement confidentielles sur une personne. Elles sont également différentes de données purement administratives par d'autres aspects :

- les données administratives contiennent des informations sur un nombre restreint de variables déterminées: identité, date de naissance, sexe, salaire, statut social, etc. La nature des données médicales n'est pas préalablement déterminée et leur nombre est, en principe, illimité. L'information pourra être très différente selon la pathologie.
- les données administratives sont généralement précises et indiscutables. On n'a qu'une date de naissance, un sexe. Les données médicales, par contre, sont souvent imprécises et difficiles à interpréter. Une plainte, un symptôme ou le résultat d'un acte technique peuvent avoir des significations très diverses. Il est à peu près impossible au non-médecin d'évaluer la portée d'une collection de données médicales.
- les données administratives ne contiennent en général pas d'opinion de la part de celui qui enregistre les données. Par contre, les rapports médicaux font souvent mention de l'opinion personnelle du médecin : p.ex. sur les causes de la maladie, sur un pronostic incertain, etc. Il est souvent impossible de distinguer nettement les données médicales objectives des considérations personnelles du médecin.
- les données médicales ne sont pas "neutres" pour l'intéressé. La santé et la maladie concernent l'existence même de l'individu. La communication de données médicales peut influencer le vécu de la maladie et le comportement du malade. Le moment et la manière de communiquer les données médicales déterminent dans une large mesure la façon dont le patient les comprend et les interprète.

Pour toutes ces raisons, les médecins ont appris à être circonspects pour ce qui concerne la communication d'informations médicales à leurs patients. Il s'agit d'un aspect de l'acte médical lui-même qui ne peut être réduit à une matière purement administrative. La communication de données médicales se situe en principe dans la relation de confiance médecin-patient et non dans une relation administrative entre un ayant droit et une institution de sécurité sociale. Comme règle générale, on peut poser que les données médicales doivent être communiquées à l'intéressé par ou via un médecin qui a sa confiance et qui le connaît bien. De plus, un médecin peut, pour des considérations d'éthique, être d'avis qu'il n'est pas (ou pas encore) souhaitable de donner certaines informations au patient. Un médecin doit toujours avoir le souci du bien-être du patient et de son entourage. Il doit donc toujours disposer d'une certaine liberté de jugement pour décider quelles données il communiquera au patient et à quel moment.

3. Communication à la demande de l'intéressé

La première situation étudiée est la communication à la demande de l'intéressé: un assuré social demande de prendre connaissance des données médicales figurant dans son dossier.

3.1 Principes

La règle générale veut que les données médicales soient communiquées à l'intéressé par l'intermédiaire d'un médecin désigné par lui qui a sa confiance, le "médecin de confiance".

Le médecin qui assume cette tâche doit, dans un premier temps, décider pour lui-même s'il accepte le rôle de médecin de confiance pour une personne déterminée. Est-il disposé et en mesure d'informer l'intéressé ? En effet, le médecin de confiance ne peut pas se limiter à transmettre sans plus les données obtenues. Il doit, au contraire, s'engager à transmettre les informations à l'intéressé à la manière d'un professionnel de la santé. Le médecin de confiance doit être en mesure d'assister et de suivre le patient auquel il communique des données. Il sera de préférence le médecin traitant. Si ce n'est pas le cas, il s'acquittera de sa tâche avec le même soin qu'un médecin traitant. Dans des cas difficiles (p.ex. un diagnostic grave), la communication est laissée aux bons soins du médecin traitant ou intervient après en avoir discuté avec lui. Si nécessaire, le patient est informé de la valeur et de la signification des données communiquées. Dans tous les cas, il est tenu compte des intérêts légitimes et de la

sensibilité du patient. La communication doit également intervenir d'une manière qui ne nuit pas à la relation avec les médecins traitants. Le médecin de confiance est tenu par les mêmes obligations déontologiques que le médecin traitant.

Quelles données médicales l'institution de sécurité sociale doit-elle dès lors communiquer à l'intéressé par l'intermédiaire d'un médecin de confiance? La règle veut que l'ensemble des données soient communiquées si l'intéressé le demande. Dans une série de cas cependant, le médecin-conseil voudra éviter que certaines données du dossier médical ne soient communiquées à l'intéressé. Nous pouvons distinguer les catégories suivantes :

1. Données dont la communication peut nuire gravement à la santé du patient ou à des membres de son entourage.

   - diagnostics graves. La communication d'un diagnostic grave, avec possibilité d'issue fatale, est toujours une tâche difficile qui demande un maximum de psychologie et une approche très personnalisée du patient.

   - troubles du comportement. Les troubles psychiques peuvent évoluer en une crise aiguë lorsque le patient prend connaissance de son dossier médical, avec des conséquences parfois catastrophiques pour lui-même ou ses proches.

   - rapports médicaux dont le contenu peut être perçu comme blessant ou injurieux par une personne qui n'est pas à même d'apprécier les nuances médicales du texte

   Pour cette catégorie de "données médicales sensibles", il semble que l'intervention d'un médecin de confiance de l'intéressé offre les meilleures garanties d'une information judicieusement adaptée. Ce médecin doit avoir suffisamment de liberté de jugement pour décider quelles données (complètes ou partielles) il communiquera au patient. Le principe reste cependant que la communication portera sur l'ensemble des données et ne sera limitée que dans la mesure où elle est susceptible de nuire gravement à la santé de l'intéressé ou de ses proches.

2. Données concernant des tiers.

   Un dossier médical peut contenir des informations confidentielles sur des personnes de l'entourage de l'intéressé. Ainsi, un rapport psychiatrique peut mentionner des renseignements sur le comportement de proches. En cas d'affections héréditaires, le dossier peut mentionner des informations sur l'état de santé de membres de la famille. Il va de soi que ce genre de données ne peut pas être transmis.

3. Informations confidentielles venant du secteur traitant.

   Aucune assurance du dommage humain ne peut fonctionner sans information fournie par les médecins traitants. Habituellement, cette information est transmise via ou avec l'accord de l'intéressé. Dans certains cas, le médecin traitant peut juger que, dans l'intérêt du patient ou de tiers, il doit communiquer certains renseignements de façon confidentielle. Lorsque le médecin-conseil utilise ces données pour motiver formellement sa décision, le droit du patient à la communication de ces données ne peut être nié. Mais que se passe-t-il si le médecin-conseil ne se sert pas de ces renseignements? Doit-il tromper la confiance du médecin traitant en portant les renseignements ainsi reçus à la connaissance du patient ? Ceci pourrait aboutir à un arrêt complet de la transmission d'informations, ce qui entraverait sérieusement le fonctionnement de la sécurité sociale.

   D'un point de vue strictement juridique, on pourrait se poser des questions devant ces cas de communication confidentielle du médecin traitant au médecin-conseil. Le patient pourrait prendre cette communication de mauvaise part et même intenter une action judiciaire. L'expérience montre cependant qu'un minimum d'échange d'informations confidentielles entre les médecins traitants et les médecins-conseils est dans certains cas indispensable à un bon fonctionnement de la sécurité sociale. Si un médecin traitant devait constater une seule fois que l'envoi de ces informations au médecin-conseil se retournait contre lui, la fructueuse relation de confiance entre eux deux serait réduite à néant et la sécurité sociale privée de sérieuses informations. Une "séparation stricte du traitement et du contrôle" constitue un obstacle majeur au bon fonctionnement de la sécurité sociale.

   Des intérêts contradictoires s'affrontent ici: l'intérêt personnel de l'intéressé, ici son droit à l'information, et l'intérêt général qui postule un bon fonctionnement de la sécurité sociale. On ne peut admettre qu'un droit

strictement individuel mette en danger un système d'utilité publique majeure. La sécurité sociale protège non seulement l'individu, mais aussi la société qui, du moins en Europe, n'est plus pensable sans un système élaboré d'assurances sociales. Il faut regarder cette réalité en face et en accepter comme conséquence que, dans certaines circonstances, l'intérêt général passe avant l'intérêt individuel. Ceci peut signifier que dans certains cas, des données médicales ne seront pas communiquées à l'intéressé, pour raison d'intérêt général. Il va de soi que cet argument ne peut être invoqué à la légère, et uniquement dans des situations exceptionnelles, pour refuser à l'intéressé la communication de données médicales. Le médecin-conseil doit interpréter ces circonstances de manière restrictive.

4. Notes personnelles du médecin-conseil

   Quand il examine un patient, le médecin-conseil note ses constatations. Dans la mesure où ces notes se limitent aux constatations objectives de l'examen, il n'y aura pas d'objection sérieuse à leur communication à l'intéressé. Mais le médecin-conseil notera aussi dans son dossier, dans bien des cas, des impressions et considérations personnelles à titre d'aide-mémoire. Ce peuvent être des hypothèses provisoires, des idées et possibilités qui attendent confirmation ou élimination. La communication de ces "données" n'est d'aucune utilité et peut être source de graves méprises.

La règle générale veut donc que les données médicales soient communiquées par le médecin-conseil au médecin de confiance qui informe à son tour l'intéressé. Lorsque l'intéressé souhaite prendre connaissance de son dossier auprès de l'institution de sécurité sociale, il doit se faire assister par son médecin de confiance. Les données médicales et autres données confidentielles concernant des tiers sont au préalable éliminées du dossier. Lorsqu'un médecin-conseil a des contacts directs avec l'assuré social, p.ex. suite à un examen, il peut juger utile de communiquer directement au patient des données médicales limitées (p.ex. le rapport d'un acte technique, une radiographie, etc.). Le médecin-conseil doit s'assurer du fait qu'il ne s'agit pas de données médicales sensibles et doit, si nécessaire, commenter les données fournies. La communication à l'intervention d'un médecin de confiance n'est pas non plus requise lorsqu'il s'agit de données figurant dans les documents administratifs ou comptables. Ces documents peuvent par exemple contenir des numéros de code nomenclature ou des noms de médicaments ou des prothèses et orthèses fournies, voire même une description sommaire de certaines blessures et troubles. Dans chaque institution ou secteur de sécurité sociale, il est possible de faire une distinction entre des données médicales au sens strict, qui font partie du dossier médical et bénéficient d'une protection stricte, et des données médico-administratives, qui sont définies de manière limitative, et qui peuvent généralement être communiquées à l'intéressé sans réserve.

3.2 Directives

1. Cette procédure s'applique à toutes les données médicales des fichiers automatisés ou manuels et des dossiers médicaux.

2. La demande de communication ou de consultation de données médicales à caractère personnel doit être introduite par écrit par l'intéressé lui-même, ou s'il est juridiquement incapable, par une personne qui le représente légalement (les parents pour les enfants mineurs, les tuteurs, les administrateurs provisoires). Lorsque d'autres personnes, même munies d'une procuration de l'intéressé, demandent la communication de ses données médicales, ce sont d'autres règles qui sont d'application et qui ne sont pas traitées ici.

3. Si les nom et adresse du demandeur correspondent aux données du dossier et du registre national, on peut admettre qu'il a justifié de son identité. Dans le doute, une copie de la carte d'identité sera demandée.

4. Les données médicales personnelles sont toujours communiquées à l'intéressé par l'intermédiaire d'un médecin choisi par lui. Ce médecin a le droit de refuser cette mission. C'est pourquoi son consentement préalable à remplir ce rôle doit être demandé. Un médecin qui recevrait des informations médicales malgré son souhait de ne pas en donner connaissance au patient, devrait renvoyer à l'expéditeur les données reçues.

5. Le médecin de confiance désigné par l'intéressé (de préférence le médecin traitant) ne peut utiliser les données fournies que pour les communiquer à l'intéressé. Un médecin ne peut pas se faire désigner comme médecin de confiance s'il a l'intention d'utiliser les données à d'autres fins. Les médecins qui ont une fonction de médecin-conseil dans un service public, un organisme assureur ou une assurance privée doivent, avant d'accepter le rôle de médecin de confiance, s'assurer qu'il n'y a pas d'incompatibilité entre les deux fonctions.

6. La tâche du médecin de confiance consiste à communiquer à l'intéressé les données médicales reçues avec la même conscience qu'un médecin traitant. Le médecin de confiance peut ne pas révéler les données dont la communication présente un grave danger potentiel pour la santé du patient ou de ses proches. Le médecin-conseil rappelle dans sa lettre d'accompagnement les obligations déontologiques du médecin de confiance.

7. Les documents qui contiennent des données médicales ou autres à caractère personnel concernant des tiers, ne sont pas transmis au médecin de confiance. Les passages concernés peuvent éventuellement être rendus illisibles.

8. Les données médicales transmises confidentiellement par le médecin traitant au médecin-conseil et dont la connaissance par l'intéressé peut compromettre le bon fonctionnement de la sécurité sociale, ne sont pas communiquées au médecin choisi par l'intéressé.

9. Les données médicales qui par leur caractère sommaire, incomplet ou provisoire peuvent être source de méprise, ne sont pas communiquées au médecin de confiance de l'intéressé.

4. Communication d'office lors de la décision

L'assuré social qui fait l'objet d'une décision doit obtenir notification des motifs à la base de la décision. Cette obligation d'information peut entrer en conflit avec le secret professionnel, étant donné que la motivation fait partie de la décision qui constitue un document administratif dont les tiers peuvent également prendre connaissance.

4.1 Principes

Il faut distinguer la décision, la motivation et les constatations médicales sur lesquelles s'appuie la motivation. Si, par exemple, quelqu'un introduit auprès de l'Agence fédérale des risques professionnels (Fedris) une demande de reconnaissance de son affection comme maladie professionnelle, il peut recevoir notification d'une décision de refus de sa demande. La motivation peut être qu' « il résulte de l'examen médical que l'intéressé n'est pas atteint de la maladie professionnelle pour laquelle les indemnités sont demandées ». Les constatations médicales, c'est-à-dire tous les examens qui ont été effectués pour arriver à cette conclusion, peuvent être nombreuses: elles constituent le dossier médical.

Vu le volume et la diversité des données médicales d'un dossier, il n'est pas possible de communiquer toutes ces données comme telles in extenso; dans certains cas, il faudrait transmettre tout le dossier, car toutes les données ont pu éventuellement contribuer à la motivation. Cependant, ce que l'on cherche c'est à rendre la décision transparente et intelligible par l'intéressé. Ce but est atteint par la communication des motifs de la décision, notamment les considérations de fait qui sont à la base de la décision. La conclusion d'un examen médical répond généralement à cette exigence. Le dossier médical conserve cependant sa valeur, ne serait-ce que pour vérifier la pertinence du processus décisionnel.

Les arguments médicaux doivent être examinés par rapport aux critères juridiques à appliquer. De la confrontation de ces deux éléments, doivent logiquement ressortir les motifs pour lesquels une décision a été prise.

4.2 Directives

1. Les considérations de fait à caractère médical qui sont à la base de la décision, doivent être mentionnées dans la décision en même temps que les considérations juridiques.

2. L'ampleur de la motivation doit être en rapport avec l'importance de la décision. Lorsqu'il s'agit d'une décision mineure, un renvoi à une disposition légale ou réglementaire, ou une considération d'ordre général peut suffire. Les décisions positives qui répondent complètement à la demande de l'intéressé, peuvent également s'accompagner d'une motivation réduite, car il est à supposer que l'intéressé est déjà au courant des motifs en cause.

3. La communication de la motivation peut se faire au moyen de formulaires standard sur lesquels apparaissent les différents motifs possibles d'une décision. Les motifs retenus peuvent être marqués d'une croix. La décision doit démontrer qu'elle est le résultat d'une évaluation individuelle et elle doit contenir suffisamment d'éléments de fait pour être intelligible.

4. La motivation ne fait jamais mention de données médicales ou autres à caractère personnel concernant des tiers, même membres de la famille ou habitant sous le même toit, sauf s'il s'agit d'une personne juridiquement incapable et que la décision est communiquée à son représentant légal.

5. La mention explicite de données médicales dans la décision doit être limitée au strict minimum. Les données médicales très sensibles (diagnostics graves, pronostics fatals, diagnostics psychiatriques) ne sont jamais reprises explicitement dans une décision.

6. Si l'intéressé veut vérifier l'exactitude des motifs médicaux avancés, il peut demander la communication des données médicales de son dossier. Il invoquera à cet effet la procédure décrite ci-dessus.

5. Conclusion

Ce code de bonne conduite se veut un compromis entre des impératifs différents et souvent contradictoires: l'obligation du secret vis-à-vis de tiers et le droit à l'information de l'intéressé; l'intérêt particulier de l'intéressé et l'intérêt général; l'obligation d'information dans le chef de l'institution de sécurité sociale et les obligations déontologiques du médecin; l'obligation de motiver les décisions et les possibilités pratiques d'exécution des institutions de sécurité sociale. Les procédures proposées offrent des garanties satisfaisantes aux bénéficiaires de la sécurité sociale, respectent les obligations déontologiques du médecin et n'imposent pas une surcharge administrative exagérée aux institutions de sécurité sociale.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
1995		V1995	Première version	18/05/1995	18/05/1995
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[1];
2. La loi relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale[2];
3. La loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs[3];
4. La loi du 11 avril 1994 relative à la publicité de l'administration[4].

La plupart des institutions publiques de sécurité sociale tombent sous le champ d'application de ces quatre lois. En ce qui concerne les deux dernières, il doit s'agir d'une administration au sens de la loi. Au sein de chaque institution publique de sécurité sociale, le traitement, l'échange et la conservation de données médicales à caractère personnel 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).

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

[2] Moniteur belge 22-02-1990

[3] Moniteur belge 12-09-1991

[4] Moniteur belge 30-06-1994

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	
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	**Oui**

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