Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique OFSP
Unité de direction Assurance maladie et accidents

CH-3003 Bern
OFSP

Aux assureurs LAMal et à leurs réassureurs

Référence du document:
Notre référence:
Dossier traité par : Lp
Berne, 17 décembre 2015

Circulaire n° :	**7.1**
Entrée en vigueur :	**1er janvier 2016**

Assureurs-maladie : organisation et processus conformes à la protection des données

1. Contexte

Les enquêtes sur la protection des données réalisées par l'OFSP et les mesures de contrôles qu'il a prises jusqu'à présent, ont montré que les assureurs-maladie garantissent la protection des données dans une large mesure, malgré des structures organisationnelles très disparates. Il ressort toutefois également que des améliorations sont possibles dans certains domaines sensibles. C'est pourquoi les recommandations formulées dans le passé sont toujours valables :

- L'OFSP recommande aux assureurs d'élaborer un concept (stratégie) en matière de protection des données.
- Chaque assureur doit tenir une liste des fichiers. Pour chaque fichier comportant des données personnelles sensibles, il faut un règlement de traitement (description des processus, y c. des responsabilités, des autorisations, du flux des données et des mesures techniques visant à garantir la sécurité des données). Ce règlement de traitement doit être régulièrement actualisé.
- L'OFSP conseille aux assureurs de désigner un conseiller à la protection des données, dont les tâches doivent être consignées dans un cahier des charges.
- Les conseillers à la protection des données doivent disposer des connaissances techniques nécessaires.
- Un service spécialisé doit régulièrement mener des audits externes sur la protection des données et soumettre les résultats aux autorités de surveillance.

Office fédéral de la santé publique
Schwarzenburgstrasse 157, 3003 Berne
Tél. +41 58 463 70 66, fax +41 58 462 90 20
www.bag.admin.ch

L'OFSP conseille aux assureurs-maladie de prendre et d'appliquer régulièrement d'autres mesures pour conformer leur organisation et/ou leurs processus aux exigences en matière de protection des données. Pour encourager ce développement, la présente circulaire et ses annexes 1 à 8 renvoient les assureurs aux dispositions en vigueur sur la protection des données qui ressortent des différents actes fédéraux[1]. Les dispositions plus récentes apparaissent en caractères gras.

Suite à l'introduction des forfaits par cas liés au diagnostic (SwissDRG) résultant du nouveau financement hospitalier, le Conseil fédéral a adapté les articles **59 ss** OAMal. Ces modifications concernent notamment la protection des données dans le cadre de la facturation dans le cas d'un modèle de rémunération de type DRG. Elles sont expliquées dans l'annexe 8.

2. Concept de protection et de sécurité des données

Art. **84*b*** LAMal /art. 2, 3, 4, 5, 7 LPD / art.8 à 10, 20 et 21 OLPD

L'OFSP recommande à tous les assureurs-maladie d'élaborer un **concept de protection et de sécurité des données** complet et global. La sécurité des données est un aspect essentiel de la protection des données.

Un concept de ce type donne des informations sur la stratégie, à moyen et à long terme, de mise en œuvre de la protection et de la sécurité des données au sein de l'entreprise. Il décrit comment sont organisés la protection des données ainsi que les flux de données conformes à la protection des données. En outre, c'est sur cette base que l'on peut notamment définir les tâches des personnes responsables de la protection et des fichiers.

Même si la loi ne prescrit pas un concept de ce type, celui-ci constitue l'un des fondements de la protection et de la sécurité des données dans l'entreprise. Sur cette base, on peut intégrer la protection des données dans les processus à l'interne. Le concept de protection et de sécurité des données ou des volets de celui-ci pourront par la suite être concrétisés dans des directives à l'attention des collaborateurs, dans des directives de sécurité et de protection de l'information pour l'informatique et d'autres domaines ainsi que dans des règlements de traitement des données (art. 11 et 21 OLPD, art. **84b** LAMal).

La mise en œuvre du concept de protection et de sécurité des données nécessite également des mesures techniques et organisationnelles. Pour ce faire, les assureurs-maladie doivent mettre les ressources nécessaires à disposition pour exécuter ces mesures techniques et organisationnelles (art. 7 LPD).

Un guide élaboré par le PFPDT concernant les mesures techniques et organisationnelles liées à la protection des données ainsi que des informations sur les points que doit contenir un règlement de traitement, peuvent être consultés sous le lien suivant :

http://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=fr

[1] Cf. annexes 1 et 2

3. Règlement de traitement

Art. **84*b*** LAMal / art. 21 OLPD

L'art. 21 OLPD prescrit aux assureurs-maladie qu'ils doivent établir un règlement de traitement *pour les fichiers automatisés qui contiennent des données personnelles sensibles ou des profils de la personnalité*, ou qui sont connectés à d'autres fichiers. Ce règlement doit contenir des informations sur l'organisation interne de l'assureur ainsi que sur la structure dans laquelle la liste des fichiers ou le système de traitement automatisé s'inscrit. Il décrit les *procédures* de traitement et de *contrôle* des données, et contient tous les documents relatifs à la planification, à l'élaboration et à la gestion du fichier ainsi qu'aux outils informatiques utilisés. Il règle notamment la *nature et l'étendue des droits d'accès aux données personnelles*. Le règlement doit être mis à jour régulièrement et être mis à la disposition du PFPDT sous une forme intelligible. Il doit être notamment adapté aux processus relatifs au traitement des données et aux contrôles des factures dans le cas d'un modèle de rémunération de type DRG (voir annexe 8).

S'assurer que le règlement de traitement est *complet* et *mis à jour* est une des tâches principales du *conseiller à la protection des données* auprès de l'assureur. Cette tâche constitue la base d'une gestion et d'une utilisation conformes à la loi d'un fichier contenant des données personnelles sensibles.

L'art. **84*b*** LAMal répète et souligne ces obligations, qui existent déjà en vertu de l'OLPD et auxquelles sont tenus les assureurs. Il précise par ailleurs que les règlements de traitement doivent être *soumis à l'appréciation du PFPDT et être rendus publics*.

En raison de cette disposition, les assureurs doivent soumettre *automatiquement pour avis* au PFPDT leurs règlements de traitement. Cela vaut également pour les règlements adaptés aux processus relatifs au traitement des données et aux contrôles des factures dans le cas d'un modèle de rémunération de type DRG. Le règlement est cependant applicable dès que l'assureur le déclare contraignant.

En outre, les assureurs doivent publier leur règlement de traitement sur Internet ou sous une autre forme, afin d'informer les *personnes intéressées*. Cette obligation de publication est néanmoins indépendante de l'évaluation effectuée par le PFPDT. Une communication du règlement sur demande ne suffit pas. L'assureur peut excepter de la publication des secrets d'affaires.

Un règlement de traitement peut être valable pour plusieurs fichiers de données s'il est effectivement appliqué pour les fichiers décrits et qu'il remplit, pour chacun d'entre eux, les exigences énumérées à l'art. 21, al. 2, OLPD.

4. Abandon de la déclaration des fichiers – désignation du conseiller à la protection des données

Art. 11*a*, al. 5, let. e LPD / art.12*a* OLPD

La LPD permet l'autorégulation de l'entreprise dans le domaine de la protection des données : il incombe à l'assureur de veiller à ce que les principes et les exigences relatifs à législation en la matière soient respectés. En tant que maître des fichiers, l'assureur est dispensé de l'obligation de les déclarer s'il a désigné un **conseiller à la protection des données** *indépendant, chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers*, et qu'il a *communiqué son nom au PFPDT*.

Le conseiller à la protection des données n'est, concernant sa désignation, pas responsable de la protection des données au sein de l'entreprise mais, comme son nom l'indique, a un *rôle de conseiller* ou celui d'un organe de surveillance. La responsabilité du respect des dispositions en matière de protection

des données incombe dans tous les cas au maître du fichier, c'est-à-dire à l'assureur-maladie ou à son organe directeur (art. 16, al. 1, LPD).

Le conseiller à la protection des données doit exercer sa fonction de manière indépendante, tant sur le plan organisationnel que technique. Tout risque de conflit d'intérêts doit être évité de par sa position organisationnelle au sein de l'entreprise. C'est pourquoi son poste devrait se situer en dehors de toute ligne hiérarchique et être rattaché de préférence à un service de l'état-major, à une division juridique ou informatique, ou être un poste externe. Son rôle et sa fonction doivent être définis dans un *cahier des charges*.

Vous trouverez de plus amples informations à l'annexe 3 et dans les recommandations du PFPDT à l'adresse suivante :

http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr

5. Externalisation

Art. 6 LSAMal / art. 84 LAMal / art. 10*a* LPD

L'externalisation consiste à confier à un prestataire externe (externalisation externe à l'entreprise) ou à une société du même groupe d'assureurs (externalisation interne dans le groupe) des prestations fournies jusque-là par les assureurs eux-mêmes ou qu'ils doivent fournir selon la loi.

Le traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie, que *seuls les traitements que le mandant serait en droit d'effectuer lui-même soient effectués et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise* (art. 10*a* LPD). Cela doit être mentionné par écrit dans la convention.
L'art. 84 LAMal habilite les assureurs-maladie à faire traiter par des tiers des données personnelles, y compris les données sensibles et les profils de la personnalité.

L'assureur doit choisir le prestataire avec soin, le renseigner et le surveiller. Il doit auditer régulièrement les prestataires. Les interfaces, les responsabilités, les compétences et les questions de responsabilité doivent être réglées et définies précisément dans un contrat. La fonction externalisée doit être intégrée dans le système interne de contrôle de l'assureur.

Le contrat doit clairement définir le but du traitement des données et spécifier l'obligation faite au prestataire de traiter les données uniquement *dans le but et selon les instructions fixés*. On exclut ainsi toute utilisation aux propres fins du prestataire ou au profit d'un tiers. Le prestataire et ses collaborateurs, ainsi que le personnel auxiliaire et les tiers mandatés par le prestataire, doivent également être soumis au *secret professionnel* ainsi qu'au droit spécifique à la protection des données de l'assureur. Les collaborateurs du prestataire, ainsi que le personnel auxiliaire et les tiers mandatés par le prestataire, doivent s'engager contractuellement à respecter le secret, le cas échéant en signant chacun un contrat. Si les tâches du médecin-conseil sont externalisées, les collaborateurs du prestataire doivent être soumis au secret professionnel du médecin-conseil en signant individuellement une déclaration de confidentialité.

Le devoir de garder le secret pour les collaborateurs de prestataires externes actifs dans le domaine de l'informatique (p.ex. administrateur de bases de données ou du réseau) doit aussi être réglé par le biais d'une déclaration de confidentialité avec signature individuelle, car ils bénéficient de droits d'accès et de traitement très étendus.

L'assureur doit s'assurer que le prestataire *garantit la sécurité et la protection des données*. Les standards appliqués pour l'échange des données et les exigences que le prestataire doit remplir en matière

de sécurité doivent être définis par écrit. *Les données personnelles des assurés doivent être protégées contre toute utilisation non autorisée par des mesures techniques, personnelles et organisationnelles adaptées.* Le prestataire doit pouvoir garantir la protection des données en tout temps (art. 7 LPD ; art. 8 et 9 OLPD). Le contrat doit indiquer les conséquences auxquelles s'expose le prestataire qui ne respecte pas les clauses en matière de protection des données et de résiliation du contrat (peines conventionnelles, mise à disposition immédiate des données, résiliation du contrat, élimination complète des données).

Le prestataire doit régulièrement informer l'assureur du traitement des données. L'assureur, son service interne et externe de révision ainsi que l'OFSP doivent pouvoir consulter et vérifier en tout temps, de manière exhaustive et librement le secteur externalisé. L'assureur doit fixer contractuellement un droit de regard, un droit d'émettre des directives et un droit de contrôle afin de pouvoir assumer un controlling réglementaire vis-à-vis du prestataire. L'assureur doit effectivement et régulièrement faire valoir ces droits de contrôles p. ex. dans le cadre d'un audit.

L'obligation qu'a l'assureur d'informer les personnes concernées demeure, étant donné qu'il reste maître des fichiers même lorsque des données personnelles sont traitées par un tiers (art. 8, al. 4, LPD). L'assureur doit donc avoir accès à tout moment aux données, accès que doit lui garantir le prestataire.

Dans le contrat pour le domaine externalisé et dans le dispositif de sécurité, l'assureur doit prendre les dispositions nécessaires le protégeant d'un départ soudain et inattendu du prestataire et qui lui permettent de poursuivre l'externalisation du secteur en garantissant la sécurité des données.

Il faut renoncer, dans la mesure du possible, à externaliser à l'étranger des domaines comportants des données sensibles. Si, exceptionnellement, tel est le cas, l'assureur doit notamment veiller à respecter l'art. 6 LPD. La communication transfrontière de données n'est possible qu'à certaines conditions et en informant le PFPDT. Les données personnelles ne peuvent pas être communiquées à l'étranger, si cela portait gravement atteinte à la personnalité de la personne concernée, notamment parce qu'une législation étrangère assurant un niveau de protection approprié manque (art. 6, al. 1, LPD). Vous trouverez une liste des Etats sous :

http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr

S'il manque une législation assurant un niveau de protection approprié des données personnelles, celles-ci ne peuvent être communiquées à l'étranger que si les conditions alternatives de l'article 6 alinéa 2 lettres a-q LPD sont remplies.

Des précautions doivent être prises lors de l'utilisation de l'informatique en nuage (cloud computing). Pour plus d'informations voir sous le site du PFPDT :

http://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=fr

En tant que maître du fichier, l'assureur continue de porter la pleine responsabilité en matière de protection des données pour le secteur externalisé. Les assureurs doivent informer de manière exhaustive les assurés de leur pratique d'externalisation.

A l'exception de l'alinéa relatif au droit de regard et de contrôle de l'assureur, ces prescriptions sont également applicables à un assureur qui recourt aux services d'un prestataire externe certifié pour la mise en œuvre d'un service de réception des données selon l'art. **59*a*** OAMal (voir annexe 8). Les droits de regard, d'émettre des directives et de contrôle de l'assureur, mentionnés ci-dessus, ont une applicabilité limitée au service de réception des données. L'assureur ne peut ni contrôler, ni avoir accès à des données dont la confidentialité est garantie par le service de réception des données.

Pour l'application du droit d'accès selon l'art. 8 LPD, une procédure de traitement des données doit être mise sur pied qui garantit que l'assureur n'ait pas accès à des données auquel il n'a pas droit.

6. Indépendance du médecin-conseil et du service de médecin-conseil

Art. 321 CP / art. 57, 56 et 42, al. 5 LAMal

Conformément à l'art. 57 LAMal, le médecin-conseil correspond à un *organe particulier de l'assurance-maladie sociale*. Ses tâches sont précisées à l'art. 57, al. 4 et 5 : le médecin-conseil donne son avis à l'assureur sur des questions médicales ainsi que sur des questions relatives à la rémunération et à l'application des tarifs. Il exerce également une fonction de surveillance et de contrôle. Il examine si les conditions de prise en charge d'une prestation sont remplies (art. 57, al. 4, LAMal). Il lui incombe de contrôler l'efficacité, l'adéquation et le caractère économique du traitement au sens des art. 32 et 56 LAMal. Sa compétence se limite à *répondre à des questions médicales*. En termes techniques, l'assureur ne peut lui donner de directive. Le médecin-conseil évalue les cas *en toute indépendance*, ne transmet aux organes compétents des assureurs que les indications *dont ceux-ci ont besoin* pour décider de la prise en charge d'une prestation, pour fixer la rémunération, pour calculer la compensation des risques ou motiver une décision. Ce faisant, il respecte les droits de la personnalité des assurés (art. 57, **al. 7**, LAMal). Le fournisseur de prestations est fondé *lorsque les circonstances l'exigent, ou astreint dans tous les cas*, si l'assuré le demande, à ne fournir les indications d'ordre médical *qu'au médecin-conseil* de l'assureur (art. 42, al. 5, LAMal).

L'indépendance, prescrite par la loi, du médecin-conseil doit également se répercuter dans l'*organisation du service du médecin-conseil*. Cette indépendance appelle l'élaboration d'un *propre règlement de traitement*, qui délimite clairement les compétences et les tâches du médecin-conseil et de ses auxiliaires.

Les locaux du service de médecin-conseil doivent être suffisamment séparés et doivent pouvoir être fermés. Le courrier ne doit être ouvert que par le service du médecin-conseil, et il faut s'assurer en tout temps qu'aucune information médicale ne puisse sortir de ce service. Il est indispensable d'installer un réseau indépendant pour le téléphone et le télécopieur. Le système informatique doit être physiquement organisé de sorte que les documents établis par le service du médecin-conseil sont archivés seulement sur son propre disque et qu'ils ne sont accessibles qu'aux collaborateurs de ce service. Le médecin-conseil doit avoir en outre la compétence de recruter son propre personnel. Il doit veiller à ce que la subordination *technique et organisationnelle* des auxiliaires ainsi que leur *taux d'occupation* n'entraînent *pas de conflit d'intérêts*. Il faut installer des places de travail séparées dans le service des prestations et dans le service du médecin-conseil pour les spécialistes qui contrôlent les factures de type DRG (p. ex. spécialistes en codage médical) et qui exécutent leurs tâches alternativement pour le service des prestations et pour le service du médecin-conseil. Ce n'est que de cette façon qu'il peut être garanti que les informations médicales destinées au service du médecin-conseil ne sortent pas de ce service.

Le médecin-conseil et ses auxiliaires sont punissables en cas de violation du secret professionnel au sens de l'*art. 321 du code pénal (CP)*. Un auxiliaire se rend punissable s'il utilise les données personnelles obtenues dans le cadre de son activité auprès du médecin-conseil pour une autre activité auprès du même assureur ou d'un autre. L'assureur doit spécifier (sur une liste) ses collaborateurs qui sont employés comme auxiliaires du médecin-conseil et les rendre expressément attentifs à leur position et leurs obligations. Il est conseillé de leur faire signer une déclaration de confidentialité.

Afin de ne pas se voir reprocher une sélection des risques, les médecins-conseils au sens de l'art. 57 LAMal ne doivent pas procéder à une évaluation des risques dans les nouveaux contrats d'assurance LCA.

7. Degré de détail lors de la facturation

Art.42, **al. 3 – 5,** 57, al. 4 et 6 LAMal / art. **59, 59a, 59a** ^{bis} OAMal

Selon l'art. 42, al. 3, LAMal, le fournisseur de prestations doit remettre au débiteur de la rémunération une facture détaillée et compréhensible (1ère phrase). Il doit lui transmettre toutes les indications nécessaires lui permettant de vérifier le calcul de la rémunération et le caractère économique de la prestation (2ème phrase). L'art. 42, **al. 3** ^{bis}, LAMal, prévoit en particulier que les fournisseurs de prestations doivent faire figurer dans la facture au sens de l'al. 3 les diagnostics et les procédures sous forme codée, conformément aux classifications actuelles (pour l'application de cette disposition liée à la facturation dans le cas d'un modèle de rémunération de type DRG voir l'art. **59*a*** OAMal et l'annexe 8). Actuellement, cette disposition n'est applicable que dans le domaine des traitements hospitaliers somatiques aigus.

Actuellement, la transmission systématique des diagnostics et des procédures n'est admise que dans le domaine des traitements hospitaliers somatiques aigus parce que pour d'autres traitements hospitaliers il manque des dispositions d'exécution sur la collecte, le traitement et la transmission des données dans le respect du principe de la proportionnalité (art. **59a**^{bis} OAMal). Dans le domaine des traitements ambulatoires, ce sont les dispositions des conventions tarifaires (p.ex. TARMED) qui s'appliquent.

En outre, l'art. 42, **al. 4,** LAMal prévoit que l'assureur peut exiger des renseignements supplémentaires d'ordre médical. Selon l'art. 42, al. 5, LAMal, le fournisseur de prestations est fondé lorsque les circonstances l'exigent, ou astreint dans tous les cas, si l'assuré le demande, à ne fournir les indications d'ordre médical qu'au médecin-conseil de l'assureur. Cela suppose que l'assureur informe l'assuré qu'il va demander des renseignements supplémentaires d'ordre médical au fournisseur de prestations et que celui-ci ne pourra les fournir qu'au médecin-conseil de l'assureur si l'assuré le demande.

Dans ces cas, les fournisseurs de prestations doivent donner aux médecins-conseils les indications dont ils ont besoin pour remplir leurs tâches (art. 57, al. 6, 1ère phrase, LAMal). Ces dernières comprennent en particulier l'avis à l'assureur sur des questions relatives à la rémunération et à l'application des tarifs ainsi que le contrôle des conditions de prise en charge d'une prestation (art. 57, al. 4, LAMal). Selon la doctrine, les fournisseurs de prestations ont en vertu de ces dispositions légales aussi bien l'obligation que l'autorisation de révéler des informations. Dans les situations de l'art. 42, al. 3, 2 ^{ème} phrase, **al. 3**^{bis} **1** ^{ère} **phrase** et **al. 4**, LAMal, ainsi que dans celles de l'art. 57, al. 6, 1ère phrase, LAMal, le fournisseur de prestations est, dans sa relation avec l'assureur-maladie, délié du secret professionnel dans la mesure où cela est nécessaire pour le cas concret. La transmission des informations n'est pas laissée au bon vouloir du fournisseur de prestations. Il s'agit d'une obligation légale de ce dernier à l'égard de l'assureur2. Ces dispositions, imposant aux fournisseurs de prestations l'obligation de transmettre toutes les données pertinentes pour les prestations, ont une grande portée. Les assureurs ont par conséquent le droit d'exiger une facturation détaillée dans le sens des explications qui précèdent et de ne procéder à aucun paiement jusqu'à sa réception.

8. Suite des travaux

L'OFSP vérifiera, lors de contrôles réguliers menés par la section Audit, si les prescriptions en matière de protection et de sécurité des données sont conformes à la présente circulaire. Il est prévu que des audits spéciaux continuent à être réalisés par échantillonnages pour examiner la manière dont les assureurs-maladie traitent les données personnelles liées au diagnostic.

---

[2] Datenschutz im Gesundheitswesen, éditeur: B. Hürlimann/R. Jacobs/T. Poledna, Kapitel Datenschutz in der obligatorischen Krankenpflegeversicherung de G. Eugster/R. Luginbühl, p. 98 sv, Schulthess 2001

Dans cette perspective, nous rappelons aux assureurs que toute violation de l'obligation de garder le secret (art. 33 LPGA) par des personnes qui participent à l'application de la loi sur l'assurance-maladie sociale est un comportement punissable (contravention) sanctionné par une amende (art. 54, al. 1, let. d, et al. 2, LSAMal) et que le non-respect des prescriptions légales en matière de protection des données entraîne des mesures de surveillance au sens des art. 38 et 39 LSAMal. L'OFSP peut informer le public sur les mesures qu'il a prises et les sanctions qu'il a prononcées (art. 37 LSAMal).

La présente circulaire comporte, aux chiffres 5 et 8 ainsi qu'aux annexes 1, 2, 6, 7 et 8, les adaptations nécessaires suite à l'entrée en vigueur de la LSAMal et de l'OSAMal. Cette circulaire remplace la circulaire 7.1 du 1er novembre 2014.

Responsable de l'Unité de direction
Assurance maladie et accidents

Oliver Peters
Vice-directeur
Membre de la direction

Division Surveillance de l'assurance
La Cheffe

Helga Portmann

Annexes : Annexes 1 à 8

Annexe 1 : Bases légales, dispositions principales

- Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA ; RS 830.1)
- Ordonnance du 11 septembre 2002 sur la partie générale du droit des assurances sociales (OPGA ; RS 830.11)
- Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal ; RS 832.10)
- Ordonnance du 27 juin 1995 sur l'assurance-maladie (OAMal ; RS 832.102)
- Loi fédérale du 26 septembre 2014 sur la surveillance de l'assurance-maladie sociale (LSAMal ; RS 832.12)
- Ordonnance du 18 novembre 2015 sur la surveillance de l'assurance-maladie sociale (OSA-Mal ; RS 832.121)
- Ordonnance du 12 avril 1995 sur la compensation des risques dans l'assurance-maladie (OCOR ; RS 832.112.1)
- Ordonnance du 14 février sur la carte d'assuré pour l'assurance obligatoire des soins (OCA ; RS 832.105)
- Ordonnance du Département fédéral de l'intérieur (DFI) du 29 septembre 1995 sur les prestations de l'assurance des soins (OPAS ; RS 832.112.31)
- Ordonnance du DFI du 20 mars 2008 concernant les exigences techniques et graphiques relatives à la carte d'assuré pour l'assurance obligatoire des soins (OCA-DFI ; RS 832.105.1)
- Ordonnance du DFI du 13 novembre 2012 sur l'échange de données relatif à la réduction des primes (OEDRP-DFI) (RS 832.102.2)
- Ordonnance du DFI du 20 novembre 2012 sur les fichiers de données pour la transmission des données entre fournisseurs de prestations et assureurs (RS 832.102.14)
- Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1)
- Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11)
- Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD ; RS 235.13)

Annexe 2 : Commentaires sur les principes et les exigences concernant le traitement des données

Art. 28, 31, 32, 33, 47 LPGA / art. 8, 9 OPGA / art. 42 **al. 3 à 5**[3], 42*a*, **57 al.** 6, **7**[4] et 8, 82, **84**[5], **84*a***[6], **84*b***[7] LAMal / art. 6*a*, **28**[8], **59**[9], **59*a ss***[10], 76, 120 OAMal / art.2, 3, 4, 5, 7, 8, **9**[11], 10*a*, 11, 11*a*, 16, 17, **18*a***[12], **18*b***[13], 19, 20, 22, 25, 27, 35 LPD / art.1, 2, 8, 9, 10, 12*a*, 12*b*, 16, 18, 20, 21, 22, 23, **24**[14], 28, 34, 35 OLPD / OCPD

- Les assureurs-maladie qui pratiquent l'assurance-maladie obligatoire et l'assurance d'indemnités journalières selon la LAMal sont habilités, dans le cadre des dispositions légales, à traiter ou à faire traiter les données personnelles sensibles[15] et les profils de la personnalité[16] des assurés. Pour ce faire, ils se basent notamment sur les art. 42, **al. 3 à 5**, 42*a*, 56, 57, al. 4, 6 et 7, 58, al. 3, **59**, 82, 83, **84, 84*a* et 84*b***, LAMal. Ils sont ainsi tenus de respecter les principes légaux de protection des données tels que la *légalité*, la *proportionnalité*, la *finalité*, la *bonne foi*, *la transparence*, l'*exactitude* et la *sécurité des données* (art. 4, 5 et 7 LPD).

- Les assureurs, en tant qu'organes d'exécution de l'assurance-maladie sociale, assument une tâche de la Confédération au sens de l'art. 2, al. 1, let. b et art. 3, let. h, LPD, et sont donc soumis au **principe de la légalité,** qui prévoit qu'une base légale est nécessaire aux assureurs pour traiter des données personnelles. Des *données personnelles sensibles* et des *profils de la personnalité* au sens de l'art. 3 LPD ne peuvent être traités que si une loi formelle le prévoit expressément. De telles données peuvent également être traitées au cas par cas, si la personne concernée a donné son *consentement* ou a rendu ses données accessibles à tout un chacun et ne s'est pas opposée formellement à leur traitement (art. 4, al. 1, et 17, al. 2, let. c, LPD). L'art. **84** LAMal constitue notamment la base légale formelle du traitement des données. Selon celle-ci, les assureurs peuvent traiter des données personnelles uniquement dans le cadre des tâches qui leur ont été assignées par la loi (art. **84** LAMal). Dans la liste, non exhaustive, des tâches d'exécution, le calcul de la compensation des risques a été ajouté (art. **84, let. i**, LAMal).

- Le **principe du traitement de données basé sur la bonne foi** (art. 4, al. 2, PLD) exige que celui-ci soit *transparent* pour la personne concernée, c'est-à-dire que toute collecte de données et tout traitement ultérieur de données soient *reconnaissables* pour la personne concernée ; celle-ci devrait donc s'y attendre, en fonction des circonstances, ou en être dûment informée.

---

[3] Art. 42, al. 3[bis] et 4 LAMal : en vigueur depuis le 1.1.2013

[4] Art. 57, al. 7, LAMal (complété) : en vigueur depuis le 1.1.2012

[5] Art. 84, phrase d'introduction (modification en vigueur depuis le 1.1.2016) et let. i, LAMal (en vigueur depuis le 1.1.2012)

[6] Art. 84*a*, al. 1, phrase d'introduction (modification en vigueur depuis le 1.1.2016)

[7] Art. 84*b* LAMal : en vigueur depuis le 1.1.2012

[8] Art. 28 OAMal : en vigueur depuis le 1.1.2009

[9] Art. 59, plusieurs alinéas en vigueur depuis le 1.1.2009 resp. le 1.1.2010 resp. le 1.1.2013

[10] Art. 59*a*, 59*a*[bis] 59*a*[ter] OAMal: en vigueur depuis le 1.1.2013

[11] Art. 7*a* LPD (abrogé) et art. 9 LPD (modifié) à partir du 1.12.2010

[12] Art. 18*a* LPD : en vigueur depuis le 1.12.2010

[13] Art. 18*b* LPD : en vigueur depuis le 1.12.2010

[14] Art. 24 OLPD (modifié) à partir du 1.12.2010

[15] Art. 3 LPD : on entend par données sensibles les données personnelles sur les opinions et activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, des poursuites ou sanctions administratives.

[16] Art. 3 LPD : on entend par profil de la personnalité, un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

Les personnes concernées doivent être informées de la collecte et du traitement des données sensibles et des profils de la personnalité les concernant (art. **14** LPD).

- Le **principe de la proportionnalité** exige que seules peuvent être collectées et traitées les données personnelles qui *sont uniquement celles qui sont objectivement nécessaires et appropriées au but indiqué* (art. 4, al. 2, LPD). Les données personnelles peuvent être conservées uniquement dans les proportions et la durée fixées par la loi. Pour le traitement des données des assurés, les assureurs sont obligés de régler de manière très restrictive les accès utilisateurs de leur collaborateurs selon les fonctions de ces derniers.

- Des données personnelles ne doivent être traitées que *dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances* (**principe de la finalité** ; art. 4, al. 3, LPD). Les données personnelles ne peuvent pas être utilisées dans un autre but que celui qui a été défini lors de leur collecte.

- Celui qui traite des données doit s'assurer qu'elles sont correctes (**principe de l'exactitude des données** ; art. 5, al. 1, LPD). Les personnes concernées par ce traitement *peuvent requérir la rectification de données inexactes* (art. 5, al. 2, LPD). En outre, toute personne peut demander des informations sur *toutes* les données la concernant (art. 8 LPD). Ainsi, la personne assurée peut, en tout temps et indépendamment d'une quelconque justification d'un intérêt, obtenir de l'assureur une copie du dossier complet la concernant. Les exceptions sont réglées à l'art. 9 LPD.

- Les assureurs-maladie doivent *tenir un inventaire de tous les* ***fichiers*** et les *déclarer* auprès du PFPDT *pour leur intégration dans le registre* (art. 11*a* LPD ; art. 16 OLPD). Ils sont exemptés de ce devoir s'ils ont désigné un *conseiller à la protection des données indépendant* chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers[17], ou s'ils se sont soumis à une *procédure de certification* au sens de l'art. 11 LPD, ont obtenu un label de qualité et ont communiqué le résultat de la procédure de certification au PFPDT (art. 11*a*, al. 2 et 5, let. e et f LPD)[18].

- Tous les collaborateurs de l'assureur sont **tenus de garder le secret**, conformément à l'art. 33 LPGA. Le non-respect de cette obligation peut entraîner des poursuites pénales (art. 54, al. 1, let. d, LSAMal). En outre, les collaborateurs autorisés doivent avoir accès uniquement aux données personnelles dont ils ont clairement besoin pour accomplir leur tâches (art. 9, al. 1, let. g OLPD). Enfin, *le médecin-conseil et son personnel auxiliaire* sont astreints au **secret professionnel**, en vertu de l'art. 321 du code pénal (CP ; RS 311.0) et sont par conséquent soumis à l'obligation de garder le secret par rapport à ce qu'a pu leur confier le patient.

- La **transmission de données personnelles** à des services extérieurs n'est admise que dans un *cadre très restreint*. A cet égard, les articles suivants sont à prendre en compte : art. ***84a*** LAMal (Communication de données) par dérogation à l'art. 33 LPGA (Obligation de garder le secret) et 82 LAMal (Assistance administrative dans des cas particuliers) par dérogation aussi à l'art. 33 LPGA, art.120 OAMal (Obligation pour les assureurs d'informer sur la communication des données et sur l'assistance administrative), art. 32, al. 2 LPGA (Assistance administrative) et 47 LPGA (Consultation du dossier). L'art. ***84a*** LAMal règle de manière exhaustive les conditions auxquelles les organes cités dans cette disposition (et uniquement ceux-ci) peuvent communiquer des données personnelles à des tiers clairement définis, en dérogation à l'obligation de garder le secret (art. 33 LPGA). Ainsi, une compagnie d'assurance appartenant au même groupe que l'assureur, qui propose des assurances selon la LCA constitue un *tiers* au sens de l'art. 84*a*, al. 5, LAMal. Si l'assureur-maladie propose de telles assurances selon la LCA, les

[17] Cf. annexe 3

[18] Cf. annexe 4

principes susmentionnés s'appliquent (en particulier le traitement conforme aux principes de la bonne foi et de la finalité). *Des modes de traitement séparés* doivent être mis sur pied pour les domaines dans lesquels les mêmes flux (automatisés) d'informations concernant des données personnelles relevant de l'assurance obligatoire des soins et des assurances selon la LCA recèlent un potentiel d'abus. Les dispositions de la LPD susmentionnées doivent également être prises en compte dans le cadre de l'art. **84*a*** LAMal, pour autant qu'aucune exception ne soit prévue dans la LAMal.

- En cas de **restructuration ou de fusion**, il existe le risque que des personnes non habilitées puissent avoir accès à des données personnelles, qu'un trop grand nombre de données soient transmises (prématurément ou aux mauvaises personnes) ou que des données personnelles ne soient pas utilisées conformément au but initialement prévu. Au cours de toutes les phases d'une restructuration ou d'une fusion, il faut donc veiller à ce que les données personnelles transmises continuent d'être *traitées uniquement dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances* (art. 4, al. 2, LPD) et que *seules* les personnes *habilitées* aient accès à ces données. Les recommandations du PFPDT sur la transmission des données dans le cadre du regroupement d'entreprises sont disponibles à l'adresse suivante :

  http://www.edoeb.admin.ch/datenschutz/00626/00743/00746/index.html?lang=fr

Annexe 3 : Aide-mémoire relatif au cahier des charges du conseiller à la protection des données

Art.11*a*, al. 5, let. e LPD / art. 12*a s* OLPD / art. 8 LPD

1. Finalité de la fonction

- Garantir le respect des dispositions légales en matière de protection des données au sein de la compagnie d'assurance-maladie.
- Servir de personne de référence vis-à-vis du PFPDT/de l'OFSP.

2. Compétences et responsabilité

- Contrôler le traitement des données personnelles ;
- Proposer des mesures s'il existe un risque que des prescriptions sur la protection des données ont été violées ;
- Exercer sa fonction de manière indépendante sur le plan technique et organisationnel, sans recevoir d'instructions ou de sanctions de la part du maître du fichier ;
- Ne pas exercer d'activité incompatible avec les tâches de conseiller à la protection des données ;
- Disposer des ressources nécessaires à l'accomplissement des tâches prévues ;
- Avoir accès à tous les fichiers, traitements et informations nécessaires à l'accomplissement des tâches prévues : droit illimité de consulter la documentation, droit d'exécution concernant les systèmes de traitement des données, droit d'accès vis-à-vis des responsables du traitement des données ;
- Dresser un rapport sur la situation en matière de protection des données à l'intention du maître du fichier (organe directeur).

3. Tâches principales

- Contrôler si tous les contrats et projets comportant un traitement de données personnelles respectent les dispositions légales et internes relatives à la protection des données ; effectuer une analyse des risques (risque de transmettre, d'effacer et de traiter des données de façon non intentionnelle ou non justifiée, de perdre des données ou risque d'erreur technique) ; Proposer des mesures pour corriger les violations de la protection des données ;
- Emettre des instructions et des directives relatives à la protection et la sécurité des données. Actualiser régulièrement les règlements de traitement des données ainsi que les fichiers qui contiennent des données personnelles sensibles.
- Contrôle permanent et adaptation continue des directives internes de protection des données à l'évolution du droit.
- Former et soutenir les collaborateurs dans tous les aspects de la protection des données. Garantir la transmission rapide des informations entre le conseiller à la protection des données et la division touchée par une violation de la protection des données ;
- Assurer l'envoi d'une réponse correcte dans les délais à toute demande de renseignements, conformément à la législation sur la protection des données ;
- Dresser l'inventaire des fichiers utilisés dans l'entreprise. Il est recommandé de recenser les fichiers ainsi que les traitements de données existants et prévus au moyen d'un formulaire uniformisé, ce qui permet de contrôler l'effectif, les mutations et les suppressions. Le conseiller à la protection des données doit en tout temps avoir la vue d'ensemble sur les données, leur emplacement dans telle ou telle division et dans quels domaines elles sont traitées. L'inventaire des fichiers utilisés doit être mis à la disposition du PFPDT ou de la personne concernée qui en a fait la demande, conformément à l'art. 8 LPD.

Annexe 4 : Protection des données : systèmes de gestion et certifications

Art. 59a, al. 6 OAMal / art.11 et 11*a*, al. 5, let. f LPD / OCPD

Afin d'améliorer la protection et la sécurité des données, les assureurs-maladie qui traitent des données personnelles peuvent soumettre leurs systèmes, leurs procédures et leur organisation à une évaluation effectuée par des organismes de certification agréés et indépendants (art. 11 LPD). Un service de réception des données selon l'art. **59*a*, al. 4** OAMal doit être certifié (art. **59*a*, al. 6** OAMal). Ces organismes de certification indépendants doivent être agréés par le service d'accréditation suisse SAS (voir annexe 8 pour plus d'informations).

La certification de l'organisation et des procédures au sens de l'Ordonnance sur les certifications en matière de protection des données (OCPD) est exposée dans les nouvelles directives émises par le PFPDT sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir (art. 4 al. 3 OCPD) et le code de bonne pratique pour la gestion de la protection des données (annexe aux directives), consultables sous

http://www.edoeb.admin.ch/datenschutz/00756/00974/index.html?lang=fr

Les directives s'appuient sur les normes internationales relatives aux systèmes de gestion, en particulier d'ISO/CEI 27001:2013 (sécurité de l'information).

La certification au sens de l'OCPD, soit la mise en place et le maintien à long terme d'un système de gestion de la protection des données (SGPD) fiable et implémenté dans les processus de l'entreprise, tend à réduire les coûts par une approche systématique dans le traitement des données personnelles. De plus, elle accroît la sécurité dans l'utilisation des données personnelles (p. ex. pour l'application des dispositions des articles **59 ss** OAMal relatives au traitement et à la conservation des données relatives au diagnostic) et garantit une surveillance constante des processus de l'entreprise en matière de protection des données en vue de leur amélioration permanente. Enfin la certification peut promouvoir l'image et la confiance auprès des partenaires, des personnes assurées, des autorités et des instances officielles (label de qualité).

En outre, les assureurs ne sont pas tenus de déclarer leurs fichiers au PFPDT s'ils se sont soumis à une procédure de certification au sens de l'art. 11 LPD, ont obtenu un label de qualité et ont communiqué le résultat de la procédure de certification au préposé (art. 11*a*, al. 5, let. f, LPD). Cette procédure est surtout recommandée aux petits assureurs-maladie qui ne disposent pas d'un conseiller à la protection des données au sein de leur entreprise (au demeurant, une certification est obligatoire dans le domaine d'application de l'art. 59a OAMal; voir l'annexe 8).

Le choix de procéder à une certification, qui peut être effectuée pour l'entreprise dans son ensemble ou seulement pour certaines procédures, resp. certains domaines, incombe à l'assureur. La certification et le maintien de sa validité imposent certaines contraintes financières et en ressources personnelles.

L'investissement pour une certification dépend de son ampleur (pour l'ensemble de l'entreprise ou pour certaines procédures, resp. certains domaines) ainsi que de la taille et de l'organisation de l'assureur. A cela s'ajoutent les ressources personnelles nécessaires à l'élaboration de la documentation relative à la certification et à l'implémentation du système de gestion de protection des données.

Pour le maintien de sa validité, les coûts des audits intermédiaires annuels et les ressources personnelles à prévoir pour l'exécution des audits intermédiaires ainsi que pour l'actualisation régulière de la documentation et le contrôle périodique de l'application correcte du système de gestion de la protection des données (audit interne, management review, etc) sont à prendre en considération. Pour

l'exécution de ces tâches, l'assureur devrait désigner un conseiller à la protection des données[19]. De plus, les coûts de recertification (tous les trois ans) ne doivent pas être oubliés.

Le lien suivant donne la possibilité de rechercher des organismes agréés par le service d'accréditation suisse SAS pour la certification des systèmes de management :

http://www.seco.admin.ch/sas/00206/index.html?lang=fr

[19] Voir annexe 3

Annexe 5 : Gestion des cas

Différents assureurs-maladie proposent une gestion des cas (*case management*).

La gestion de cas donne lieu au traitement de données personnelles sensibles. Les gestionnaires agissant aussi bien dans l'intérêt de la personne concernée que dans celui de l'assureur, des conflits d'intérêts peuvent survenir. Il importe donc d'observer scrupuleusement les **principes de la transparence et de la finalité (art. 4, al. 2 et 3 LPD)**. Il faut en particulier noter que les assureurs recourent à une gestion de cas pour réduire autant que possible les coûts liés à un accident ou à une maladie et pour prendre en charge la personne concernée de manière à ce qu'elle guérisse le plus vite possible.

Afin que les gestionnaires de cas puissent procéder légalement au traitement des données, il est essentiel qu'ils informent la personne concernée de leur fonction, de leurs objectifs, de la finalité du traitement des données en question ainsi que de leur commanditaire, l'assureur-maladie. Les données personnelles peuvent être utilisées uniquement à des fins qui peuvent être reconnues par la personne concernée. Le gestionnaire de cas ne peut donc pas se contenter d'être une sorte de « bienfaiteur » pour la personne concernée se trouvant dans une situation difficile. Il doit également respecter le principe de transparence en fournissant les informations nécessaires.

La subordination technique et organisationnelle du gestionnaire de cas et de ses collaborateurs doit être contrôlée et corrigée auprès de nombreux assureurs. *Les gestionnaires de cas ne peuvent plus être intégrés dans la division des prestations mais doivent être subordonnés aux médecins-conseils.* En ce qui concerne la subordination technique et organisationnelle ainsi que le taux d'occupation fixé pour la gestion d'un cas, il faut veiller à concevoir les postes des gestionnaires et de leurs collaborateurs de manière à ce qu'ils n'entraînent *aucun conflit d'intérêts*. Ils ne peuvent pas être chargés de différentes tâches incompatibles les unes avec les autres. En outre, les salaires (et bonifications) des gestionnaires ne doivent pas être fixés en relation avec les coûts épargnés par l'assureur.

Annexe 6 : Questionnaires relatifs à l'état de santé

Art. 5 Cst. / art. 5, let. i LSAMal / art. 61, al. 1 OSAMal / art. 6*a*, al. 1 OAMal

Les questions concernant l'état de santé des personnes requérant leur affiliation à l'assurance obligatoire des soins sont contraires à la LSAMal et au principe de proportionnalité. Il est illégal de recueillir de cette manière des informations relatives à l'état de santé.

Les assureurs n'ont pas le droit de s'informer, lors de l'admission de personnes tenues de s'assurer dans l'assurance obligatoire des soins, sur l'état de santé de celles-ci. Cette interdiction découle de l'obligation d'accepter toute personne astreinte à s'assurer selon l'article 5, let. i, LSAMal, et du principe de proportionnalité énoncé à l'art. 5 de la Constitution fédérale suisse (Cst.) du 18 avril 1999.

Les questions concernant l'état de santé ne peuvent être posées au moment de l'admission que si la personne tenue de s'assurer signale expressément son intérêt à conclure une assurance complémentaire ou une assurance d'indemnités journalières. Le questionnaire correspondant devra porter exclusivement sur les assurances non obligatoires, et le préciser clairement. Ainsi, les formulaires d'affiliation comportant des questions relatives à la santé doivent être strictement séparés du formulaire d'affiliation pour l'assurance obligatoire des soins.

Les assureurs doivent veiller à ce que les intermédiaires d'assurance mandatés par eux ne s'informent pas de l'état de santé d'une personne intéressée à une affiliation.

Au cas où des données sur l'état de santé auraient déjà été obtenues de cette manière, il faut détruire immédiatement ces informations recueillies illégalement et, le cas échéant, les fichiers exploités de manière illégale sur cette base.

Annexe 7: Clauses d'autorisation / procurations générales

Art. 321 CP / art. 28, al. 3, 33 et 43, al. 3 LPGA / art. 3, let. c, chiffre 2, 4, al. 5, et 12ss LPD / art. 5, let. i LSAMal / art. 42, al. 3, 84*a* LAMal / art. 6*a*, al. 1 OAMal

1. Procuration, clause de consentement

Conformément à l'article 33 LPGA, les assureurs sont tenus de garder le secret à l'égard des tiers. Ils ne peuvent communiquer des données que si les conditions de l'article 84*a* LAMal sont remplies. Les fournisseurs de prestations et leurs auxiliaires sont soumis au secret professionnel (art. 321 CP) ; les autres acteurs du domaine de la santé (autres assureurs sociaux, assureurs privés) sont également soumis à l'obligation de garder le secret (art. 33 LPGA, art. 12ss LPD). Dans la pratique, *nombreux sont les assureurs qui exigent des assurés la signature d'une procuration les autorisant à requérir des renseignements auprès de tiers ou à livrer des informations à des tiers. Une telle procuration doit remplir les conditions légales, notamment celles de l'article 4 LPD.* Le traitement des données de l'assuré ne peut ainsi être opéré que si ce dernier a donné *librement son consentement éclairé*. Le consentement est éclairé si la personne, au moment où elle donne son autorisation, a été dûment informée, c'est-à-dire qu'elle est *en mesure de déterminer la portée de l'autorisation*, les données qui peuvent être transmises, le cercle des personnes qui peuvent communiquer ces données et / ou auxquelles ces données peuvent être communiquées ainsi que le but du transfert de données. Les données relatives à la santé sont *des données sensibles* au sens de l'article 3, let. c, chiffre 2, LPD. Leur traitement exige par conséquent le *consentement explicite de l'assuré* (art. 4, al. 5, LPD).

2. Procuration demandée lors de l'affiliation

Conformément à l'article 5, let. i, LSAMal, les assureurs doivent, dans les limites de leur rayon d'activité territorial, accepter toutes les personnes tenues de s'assurer sans égard à leur état de santé. Les questionnaires de santé sont interdits (voir annexe 6). Etant donné que les assureurs sont autorisés à demander dans le formulaire d'affiliation toutes les données nécessaires à l'admission dans l'assurance obligatoire des soins ou au changement d'assureur (art. 6*a*, al. 1, OAMal), *une procuration est superflue.* En effet, l'assureur doit obtenir de l'assuré lui-même tous les renseignements nécessaires.

3. Procuration demandée lors d'un cas de prestations

En vertu de l'article 28, al. 3, LPGA, et sous réserve de l'article 42, al. 3, LAMal, *la procuration doit toujours se référer à un cas de prestations particulier.* Dans le document qu'il soumet à l'assuré pour signature, l'assureur doit expressément indiquer le cas d'assurance (maladie / accident, date) pour lequel la procuration est demandée. Une procuration délivrée pour des cas de prestations futurs n'est par conséquent pas valable.

La procuration doit respecter le principe de la proportionnalité : l'assureur ne peut pas obtenir davantage d'informations que celles dont il a impérativement besoin pour remplir ses tâches conformément à la LSAMal et à la LAMal. De même, il ne peut porter à la connaissance de tiers plus de renseignements que ceux qui sont absolument nécessaires à ces derniers.

La procuration peut être révoquée par l'assuré en tout temps ; celui-ci doit être explicitement informé de ce droit.

Il n'est pas correct d'indiquer dans la procuration que le défaut de signature de ce document entraîne la suspension ou la suppression du droit aux prestations. Si l'assuré refuse à tort de signer la procuration, l'assureur doit lui adresser une mise en demeure écrite pour lui rappeler son devoir de collaboration et

l'avertir des conséquences juridiques. L'assureur impartira à l'assuré un délai de réflexion convenable (art. 43, al. 3, LPGA).

4. Consentement en cas de Case Management

Dans les assurances impliquant un « Case Management » (voir annexe 5), le volume des données échangées entre l'assureur qui pilote le traitement et les fournisseurs de prestations est plus important que dans les autres assurances. A cette fin, l'assuré doit donner son consentement explicite.

L'assuré devra être renseigné précisément sur les données qui seront transmises, sur l'identité du destinataire et sur le but que poursuit l'échange de données. Il doit en outre pouvoir révoquer son consentement en tout temps et être informé de ce droit.

Annexe 8: Facturation dans le cas d'un modèle de rémunération de type DRG

Art.42, **al. 3**[bis] LAMal / art.**59, 59*a*** OAMal **et disposition transitoire de la modification du 4 juillet 2012 /**
Ordonnance du DFI du 20 novembre 2012 sur les fichiers de données pour la transmission des données entre fournisseurs de prestations et assureurs / OCPD

1. Transmission systématique des données

L'art. 42, **al. 3**[bis] LAMal a concrétisé le principe de la transmission systématique des données entre fournisseurs de prestations et assureurs. La transmission des données dans le cas d'un modèle de rémunération de type DRG a été précisée par les dispositions de l'art. 59a OAMal. Les fournisseurs de prestations doivent faire figurer dans la facture les diagnostics et les procédures sous forme codée, conformément aux classifications contenues dans l'édition suisse correspondante publiée par le département compétent.

Pour qu'un assureur puisse recevoir les factures ainsi que les fichiers de données administratives et médicales, il doit impérativement disposer d'un service de réception des données certifié selon l'art. **59*a*, al. 6** OAMal.

La procédure de certification du service de réception des données doit être effectuée selon l'art. 11 LPD et l'art. 4 OCPD. La certification est valable trois ans. Le domaine certifié comprend toutes les procédures de traitement de données visant la réalisation de l'art. **59a** OAMal. Il faut donc que les processus électroniques de traitement des factures, les procédures de traitement des factures sur papier ainsi que celles effectuées par des prestataires externes soient certifiés.

L'organisme de certification peut suspendre ou révoquer une certification lorsque des manquements graves sont constatés (art. 9 ss OCPD). Dans les deux cas, les conditions de l'art. **59a, al. 6** OAMal ne seraient plus remplies et les factures de type DRG ne pourraient plus être transmises à l'assureur. L'assureur ne pourrait pas non plus exiger leur transmission au médecin-conseil, car la transmission des factures de type DRG au médecin-conseil n'est plus admise depuis le 1er janvier 2014. Sont réservées les mesures du droit de la surveillance de l'OFSP au sens des art. 37, 38 et 39 LSAMal ainsi que les sanctions pénales selon l'art. 54, al. 1, let. d, et al. 2 LSAMal.

Les fournisseurs de prestations doivent transmettre simultanément avec la facture les fichiers de données avec les indications administratives et médicales au service de réception des données de l'assureur (art. **59*a*, al. 3** OAMal). Pour que le fichier avec les données administratives et celui avec les données médicales puissent être réunis après un triage, le fournisseur de prestations doit les munir d'un numéro d'identification (Art. **59a, al.1** OAMal).

2. Contenu de la facture

Selon l'art. 42, **al. 3**[bis] LAMal en relation avec l'art. **59*a*, al. 2** OAMal, les fournisseurs de prestations doivent coder les diagnostics et les procédures conformément aux classifications mentionnées pour la statistique médicale des hôpitaux au chiffre 62 de l'annexe à l'ordonnance du 30 juin 1993[20] sur les relevés statistiques et les faire figurer sous forme codée dans la facture.

[20] RS 431.012.1

De plus, l'art. **59*a*, al. 3,** OAMal stipule que les fournisseurs de prestations doivent transmettre simultanément avec la facture les fichiers de données avec les indications administratives et médicales visées à l'art. 59 **al. 1** OAMal, au service de réception des données de l'assureur. La même disposition prévoit que l'assureur doit garantir que seul le service de réception des données obtienne l'accès aux indications médicales.

La structure uniforme des fichiers de données, leur étendue et leur contenu sont fixés dans l'**ordonnance du DFI du 20 novembre 2012 sur les fichiers de données pour la transmission des données entre fournisseurs de prestations et assureurs**.

3. Service de réception des données

Le service de réception des données certifié a pour fonction de réaliser un triage complètement automatisé des factures au moyen des données de la facture, y compris avec les indications médicales et administratives. Le triage se fait selon des paramètres que l'assureur fixe préalablement. Les paramètres doivent être fixés de manière à ce que le principe de la proportionnalité selon la LPD soit pris en compte et qu'un contrôle efficace de la facture et du caractère économique des prestations puisse être réalisé.

Après le triage effectué par le service de réception des données certifié, seules les factures qui présentent des particularités selon le paramètre fixé sont transmises au service compétent de l'assureur pour un contrôle plus approfondi. Durant tout le contrôle par le service compétent de l'assureur, la protection des données doit être garantie à tout moment selon l'art. **59*a*^{ter}, al. 1** OAMal. Avant que le service de réception des données se mette à exploiter le MCD pour le triage, il faut qu'il soit garanti par ce service que le MCD appartienne à une facture qui concerne une personne effectivement assurée auprès de l'assureur.

Toutes les factures qui ne présentent pas de particularités sont débloquées pour paiement, mais les indications médicales doivent être conservées sous forme cryptée auprès de l'assureur. Si les indications médicales ne sont pas conservées sous forme cryptée, l'identité des assurés doit être pseudonymisée pour la conservation de ces indications. L'assureur doit garantir que le traitement des informations médicales selon l'article 59 alinéa 1 OAMal est conforme à la protection des données (articles 21 et 22 OLPD).

Toutes les factures que le service de réception des données a écartées pour un contrôle renforcé doivent être effectivement vérifiées de façon approfondie par l'assureur. Le triage ne doit pas mener à un stockage des factures.

Après le contrôle approfondi des factures qui présentent des particularités, les indications médicales doivent aussi être archivées sous forme cryptée ou pseudonymisée.

Après l'archivage, le cryptage et la pseudonymisation ne peuvent être levés que par le médecin-conseil (art. **59*a*^{ter}al. 2** OAMal).