Protection des données des patients et protection des assurés

Rapport du Conseil fédéral en réponse au postulat Heim (08.3493)

du 18 décembre 2013

Table des matières

1 Contexte général

1.1 Postulat Heim (08.3493) « Protection des données des patients et protection des assurés »

Le postulat Heim (08.3493 – Protection des données des patients et protection des assurés), transmis par les Chambres, chargeait le Conseil fédéral de présenter dans un rapport les mesures prévues pour lutter contre la discrimination dont seraient victimes certains groupes de patients du fait des nouveaux modèles d'assurance particuliers et pour garantir la protection des données des patients chez les assureurs-maladie. Compte tenu des résultats de la première grande enquête sur la protection des données, qui a été menée auprès des assureurs LAMal du 4 décembre 2007 au 16 juin 2009, ainsi que de l'importance accordée à cette question par une large part des milieux spécialisés et de la population, le Conseil fédéral s'est déclaré disposé à rendre compte des mesures déjà prises ainsi que de celles qui restent à prendre pour garantir la protection des données relatives aux assurés en tant que patients (cf. *Annexe 1* : Texte du Po 08.3493, développement et avis du Conseil fédéral).

Le présent rapport tient compte des travaux préparatoires suivants :

- Première enquête sur la protection des données menée auprès des assureurs LAMal par l'Office fédéral de la santé publique (OFSP) et par le Préposé fédéral à la protection des données et à la transparence (PFPDT) (2007-2009).
  Deuxième enquête sur la protection des données (2011-2012) menée par l'OFSP après la publication, le 25 août 2011, de la circulaire 7.1 « Assureurs-maladie : organisation et processus conformes à la protection des données ».
- Les résultats de ces enquêtes sont fondés pour l'essentiel sur les indications fournies par les assureurs LAMal.
- Echanges avec d'autres instances s'occupant de la protection des données auprès des assureurs LAMal (autres autorités de surveillance [PFPDT, FINMA], associations professionnelles [santésuisse, association de réassurance des petits et moyens assureurs-maladie RVK], service de certification en matière de protection des données [KPMG Suisse]), renseignements auprès de l'ombudsman de l'assurance-maladie.
- Contrôles réguliers effectués par échantillonnages auprès des assureurs LAMal par la section Audit de l'OFSP.
- Contrôle, par le préposé de l'OFSP à la sécurité informatique, des mesures de protection et de sécurité des données que les assureurs LAMal disent avoir prises.

D'autres interventions parlementaires déposées depuis 2008 et relatives à la protection des données des patients sont énumérées à l'*annexe 2*.

1.2 Prescriptions en matière de protection des données et principes de traitement des données applicables aux assureurs LAMal

Les assureurs LAMal doivent respecter de nombreuses dispositions en matière de protection des données, qui se trouvent principalement dans les textes législatifs suivants :

- 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)

- ordonnance du 12 avril 1995 sur la compensation des risques dans l'assurance-maladie (OCoR ; RS 832.112.1)
- ordonnance du 14 février 2007 sur la carte d'assuré pour l'assurance obligatoire des soins (OCA ; RS 832.105)
- ordonnance du 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)

En pratiquant l'assurance-maladie sociale, les assureurs LAMal, tout en étant des entreprises privées, remplissent une tâche publique de la Confédération. Ils sont donc soumis à des règles plus strictes que les entreprises qui ne remplissent pas de tâches de ce type :

- Ils ne sont autorisés à traiter ou à faire traiter des données sensibles[1] ou des profils de la personnalité[2] relatifs aux assurés que dans les limites fixées par les dispositions légales (p. ex., sur la base des art. 42, al. 3 à 5, 42*a*, 56, 57, al. 4, 6 et 7, 58, al. 3, 59, 82 à 84, 84*a* et 84*b* LAMal). Ce faisant, ils sont tenus de respecter les principes du droit de la protection des données, notamment ceux de la *légalité*, de la *proportionnalité*, de l'*adéquation au but visé*, de la *bonne foi*, de la *transparence*, de l'*exactitude des données* et de la *sécurité des données* (art. 4, 5 et 7 LPD).

- Le *principe de la légalité* auquel, en tant qu'entreprises chargées de pratiquer l'assurance-maladie sociale, ils sont soumis en vertu de l'art. 2, al. 1, let. b, et de l'art. 3, let. h, LPD, prévoit qu'une base légale est nécessaire au traitement de données personnelles par les assureurs LAMal. Ils ne peuvent traiter des *données sensibles* et des *profils de la personnalité* au sens de l'art. 3 LPD que si une loi au sens formel le prévoit expressément. Ils le peuvent aussi, dans des cas particuliers et seulement *exceptionnellement*, si la personne concernée y a *consenti* ou a rendu ses données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement (art. 4, al. 1, et art. 17, al. 2, let. c, LPD). Dans la LAMal, c'est plus particulièrement l'art. 84 qui constitue la base légale du traitement des données. Il prévoit que les assureurs ne sont habilités à traiter les données personnelles que pour les tâches que leur assigne la LAMal (la liste des tâches énumérées à l'art. 84 LAMal est exemplative. Les objectifs du traitement sont toutefois réglés de manière exhaustive dans la LAMal).

- Le *traitement des données conformément au principe de la bonne foi* (art. 4, al. 2, LPD) implique que ce traitement soit *transparent* pour la personne concernée, c'est-à-dire que la collecte de données et tout traitement ultérieur soient *reconnaissables* pour elle, autrement dit

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

[2] 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.

qu'elle devait s'y attendre en raison des circonstances ou qu'elle a été dûment informée. La personne concernée doit être informée de toute collecte de données sensibles ou de profils de la personnalité la concernant (art. 14 LPD).

- Le *principe de la proportionnalité* ordonne que seules soient collectées et traitées les données personnelles qui sont *effectivement et objectivement nécessaires et appropriées pour un but précis* (art. 4, al. 2, LPD). Les données ne peuvent être conservées que dans la quantité et pour la durée autorisées par la loi.

- Les 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 l'adéquation au but visé ; art. 4, al. 3, LPD). Toute utilisation dans un autre but est donc exclue.

- Celui qui traite des données personnelles doit s'assurer qu'elles sont correctes (principe de l'exactitude des données ; art. 5, al. 1, LPD), et toute personne concernée est en *droit de requérir la rectification* des données inexactes (art. 5, al. 2, LPD). Elle a en outre le droit de demander des renseignements sur *toutes* ces données (art. 8 LPD). La personne assurée a donc le droit d'obtenir de l'assureur une copie de son dossier complet, sous réserve de la durée de l'obligation de l'assureur de conserver ces données.

- Les assureurs-maladie doivent tenir un *inventaire de tous leurs fichiers* et *les déclarer* au PFPDT (art. 11*a* LPD, art. 16 OLPD). Ils sont libérés de cette obligation 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, ou s'ils ont obtenu un label de qualité dans le cadre d'une *procédure de certification* au sens de l'art. 11 LPD et annoncé le résultat de cette procédure au PFPDT (art. 11*a*, al. 2 et 5, let. e et f, LPD).

- Le personnel des assureurs LAMal est soumis à l'*obligation de garder le secret* en vertu de l'art. 33 LPGA. Une violation de cette obligation constitue un délit et a des conséquences pénales (art. 92, let. c, LAMal). De plus, le personnel autorisé de l'assureur LAMal ne doit avoir accès qu'aux données personnelles dont il a besoin pour accomplir ses tâches clairement définies (art. 9, al. 1, let. g, OLPD). En outre, *le médecin-conseil et ses auxiliaires* sont tenus au secret professionnel en vertu de l'art. 321 du code pénal (CP ; RS 311.0) et ont donc l'obligation de garder le *secret en ce qui concerne le patient*.

- La *transmission* de données personnelles à des services externes n'est admise que dans des *limites très strictes*. On observera à ce propos l'art. 84*a* LAMal (communication de données), en dérogation à l'art. 33 LPGA (obligation de garder le secret), et l'art. 82 LAMal (assistance administrative dans des cas particuliers), également en dérogation à l'art. 33 LPGA, l'art. 120 OAMal (devoir d'information des assureurs sur les données communiquées et l'assistance administrative accordée), l'art. 32, al. 2, LPGA (assistance administrative) et l'art. 47 LPGA (consultation du dossier). L'art. 84*a* LAMal règle dans quelles conditions, énumérées de façon exhaustive, les organes cités dans cette disposition (et eux seuls) peuvent, en dérogation à l'obligation de garder le secret (art. 33 LPGA), communiquer des données personnelles à des tiers précisément définis. Une autre société d'assurance qui propose les assurances visées par la loi fédérale du 2 avril 1908 sur le contrat d'assurance (LCA ; RS 221.229.1) *constitue un tiers* au sens de l'art. 84*a*, al. 5, LAMal. Si l'assureur LAMal propose lui-même des assurances visées par la LCA, les principes cités ci-dessus s'appliquent, notamment celui de la bonne foi et celui de l'adéquation au but visé. Là où l'application des mêmes flux d'informations (automatisés) aux données personnelles issues de l'assurance obligatoire des soins et des assurances LCA recèle un potentiel d'utilisation frauduleuse des données, il importe d'adopter des *processus de traitement séparés*. Les règles de la LPD citées ci-dessus doivent aussi être respectées dans le cadre de l'art. 84*a* LAMal, à moins d'une exception prévue par la LAMal.

1.3 Résultats de la première enquête sur la protection des données (2007-2009)

La première enquête nationale relative à la protection des données menée par l'OFSP en collaboration avec le PFPDT (4 décembre 2007 - 16 juin 2009) a montré que les assureurs-maladie sont sensibilisés à cette problématique et que la protection des données est largement assurée, en dépit de différences considérables dans l'organisation. Mais l'enquête a révélé aussi qu'un potentiel d'amélioration existait encore dans quelques domaines sensibles. L'OFSP et le PFPDT ont donc formulé les recommandations suivantes lors de la publication des résultats de l'enquête le 16 juin 2009 :

- Chaque assureur devrait élaborer un concept en matière de protection des données.
- Chaque assureur doit tenir une liste des fichiers, qui nécessitent tous, s'ils comportent des données personnelles sensibles, un règlement concernant le traitement des données (en particulier description des processus y c. des responsabilités, autorisations, flux des données et mesures techniques visant à garantir la sécurité des données).
- Chaque assureur devrait désigner un conseiller à la protection des données. Ses tâches sont consignées dans un cahier des charges.
- Les conseillers à la protection des données doivent disposer des connaissances techniques nécessaires.
- Un service externe spécialisé devrait effectuer régulièrement un audit en matière de protection des données et soumettre les résultats aux autorités de surveillance.

Les résultats de la première enquête sur la situation en matière de protection des données (rapport et résumé) sont publiés sur Internet à l'adresse suivante :

http://www.edoeb.admin.ch/themen/00794/01154/01236/01237/index.html?lang=fr

2 Mesures prises par l'Office fédéral de la santé publique (OFSP) depuis l'enquête de 2007-2009

2.1 Circulaire 7.1 du 25 août 2011 « Assureurs-maladie : organisation et processus conformes à la protection des données » (actualisée le 17 juin 2013)

Bien qu'il ait constaté que les assureurs LAMal, suite à ces recommandations, ont pris différentes mesures en vue d'améliorer la conformité de leur organisation et de leurs processus au droit relatif à la protection des données, l'OFSP a publié à leur intention, le 25 août 2011, une circulaire détaillée dans le but d'accentuer cette évolution. Entrée en vigueur le 1er septembre 2011, la circulaire 7.1 rappelle aux assureurs les mesures qu'ils doivent prendre pour garantir la protection des données personnelles et notamment des données personnelles sensibles (en particulier celles relatives à la santé des assurés). Mais elle ne comprenait alors encore aucune prescription détaillée sur la manière dont les assureurs devraient garantir la protection et la sécurité des données communiquées par les fournisseurs de prestations après l'introduction du système de forfaits par cas SwissDRG, car la réglementation applicable à la transmission des données médicales pertinentes pour les décomptes n'était pas encore arrêtée à ce moment-là. Entre temps, la circulaire 7.1 a été adaptée à cette nouvelle réglementation (art. 42, al. 3bis et 4 LAMal, art. 59ff OAMal) et envoyée le 17 juin 2013 aux assureurs LAMal (entrée en vigueur le 1 juillet 2013).

La circulaire 7.1 recommande aux assureurs LAMal d'élaborer – s'ils n'en ont pas encore – un concept de protection et de sécurité des données complet et global ; elle leur prescrit de soumettre spontanément au PFPDT à partir du 1er janvier 2012, pour appréciation, un règlement de traitement pour chaque fichier de données, et d'annoncer également au PFPDT, si nécessaire, les fichiers qui manquent encore ou les conseillers à la protection des données désignés par l'assureur. Elle rappelle

aux assureurs LAMal les règles à observer en cas d'externalisation de prestations et consacre un chapitre entier à l'indépendance de leur service de médecin-conseil. En outre, sept (nouvellement huit) annexes à la circulaire 7.1 répondent à des questions techniques touchant la protection des données (bases légales, dispositions déterminantes, contenu du cahier des charges du conseiller à la protection des données, indications relatives aux certifications et systèmes de gestion des données facultatifs, formulaires d'admission et de procuration [libération de l'obligation de garder le secret, déliement du secret médical], nouvellement dans l'annexe 8 des instructions relatives au service certifié de réception des données).

Par la même occasion, l'OFSP annonçait aux assureurs LAMal qu'il allait leur demander quelques mois plus tard, en se référant à la circulaire, quelles démarches ils auraient prises et lesquelles ils allaient encore prendre. Le cas échéant, il ordonnerait les correctifs nécessaires et en contrôlerait la mise en œuvre. Les prescriptions de la circulaire feraient en effet l'objet de contrôles réguliers et d'audits par échantillonnages effectués par la section Audit de l'OFSP. La circulaire rappelait en outre expressément aux assureurs LAMal que toute violation de l'obligation de garder le secret (art. 33 LPGA) de la part de leurs collaborateurs constituait un délit punissable (art. 92, let. c, LAMal) et que le non-respect des prescriptions légales en matière de protection des données pouvait entraîner des sanctions telles que le rétablissement de l'ordre légal aux frais de l'assureur, un avertissement et une amende d'ordre, le retrait de l'autorisation de pratiquer l'assurance-maladie sociale et la communication publique d'informations sur les mesures prises (art. 21, al. 5 et 5^{bis}, LAMal).

La circulaire 7.1 du 25 août 2011 avec ses sept annexes ainsi que la lettre d'accompagnement sont reproduites à l'*annexe 3*.
La circulaire 7.1 du 13 juin 2013 avec ses huit annexes ainsi que la lettre d'accompagnement sont reproduites à l'*annexe 4*.

2.2 Deuxième enquête (2011-2012) concernant la conformité de l'organisation et des processus des assureurs LAMal au droit relatif à la protection des données

Le 13 décembre 2011, tous les assureurs LAMal ont reçu un questionnaire détaillé visant à contrôler la mise en œuvre de la circulaire 7.1 sous les aspects suivants : avancement des concepts de protection et de sécurité des données, avancement des règlements de traitement des données, tenue de registres des fichiers et enregistrement de ces fichiers auprès du PFPDT, externalisation de prestations et conformité au droit de la protection des données du traitement de données effectué par les prestataires, indépendance structurelle du service du médecin-conseil, service responsable de la protection des données au sein de l'entreprise et de la formation interne à la protection des données, systèmes de gestion de la protection des données et certifications, gestion des cas et contenu des procurations et des déclarations de consentement des assurés pour la transmission de données médicales à des tiers. D'autres questions en rapport avec le postulat Heim 08.3493 concernaient l'échange de données entre les services impliqués dans les formes particulières d'assurance. La deuxième enquête n'incluait pas de questions relatives à la garantie de la protection et de la sécurité des données communiquées par les fournisseurs de prestations après la mise en place du système de forfaits par cas SwissDRG, car la réglementation applicable à la transmission des données médicales pertinentes pour les décomptes n'était pas encore arrêtée à ce moment-là.

Tous les assureurs qui pratiquent l'assurance obligatoire des soins ont répondu au questionnaire dans le délai (prolongé) imparti. Sur demande, quelques caisses ne pratiquant que l'assurance d'indemnités journalières ont été exemptées de cette tâche. Mais tous les assureurs LAMal (67, dont six caisses ne pratiquant que l'assurance d'indemnités journalières) ont été pris en considération pour l'analyse des réponses reçues.

Le questionnaire et la lettre d'accompagnement du 13 décembre 2011 sont reproduits à l'*annexe 5*.

2.3 Contrôles sur place (audits/priorité 2012)

Dans le cadre de sa fonction de surveillance, l'OFSP procède à des contrôles ciblés et à des audits par échantillonnages auprès des assureurs LAMal. Ces audits réguliers ont pour but de contrôler l'application de la LAMal et de ses ordonnances ainsi que des instructions données par l'OFSP. Suivant les risques évalués, le programme des audits porte sur les domaines « Organisation et gestion d'entreprise », « Prestations d'assurance » et régulièrement « protection des données » et « Prestations de service et finances ». L'audit prend la forme de contrôles axés sur les processus et les résultats.

L'OFSP contrôle déjà depuis 2009 le respect des dispositions relatives à la protection des données auprès des assureurs. Depuis 2012, ce contrôle constitue l'un des thèmes prioritaires des audits. La base de ce contrôle se trouve dans la circulaire 7.1 publiée par l'OFSP le 25 août 2011, en vigueur depuis le 1er septembre 2011 (actualisée le 17 juin 2013 avec entrée en vigueur le 1er juillet 2013). L'auditeur examine si l'assureur LAMal dispose d'une organisation conforme au droit relatif de la protection des données et si le traitement et la conservation des données et des documents (en particulier au sein du service du médecin-conseil) suivent des processus définis et correspondent aux dispositions légales de la LPGA, de la LAMal et de la LPD en matière de protection des données. Le contrôle effectué sur place par l'OFSP ne saurait remplacer une certification au sens de l'art. 11 LPD et ne constitue en aucune manière la base d'une telle certification.

Depuis le 1er janvier 2009, l'OFSP a donné à 24 reprises à de petits, moyens ou grands assureurs, sur la base de ses 38 audits réguliers, des instructions dans les domaines suivants : conformité de l'organisation au droit de la protection des données, règlements de traitement des données, conservation de dossiers médicaux, de médecine dentaire et du service du médecin-conseil, conservation des données relatives aux diagnostics provenant notamment des factures selon le système DRG. C'est dans les trois derniers domaines cités que les instructions ont été les plus fréquentes. L'OFSP a donné en outre 25 recommandations aux assureurs-maladie concernant l'élaboration d'un concept de protection des données et d'un règlement de traitement des données, l'annonce de fichiers de données personnelles au PFPDT, l'annonce au PFPDT du conseiller à la protection des données au sein de l'entreprise, la réglementation des droits d'accès des collaborateurs aux données personnelles et aux données relatives aux prestations, la conservation des dossiers du service du médecin-conseil, les mesures de contrôle de la protection des données prises au sein de la caisse-maladie, la réglementation écrite des compétences des auxiliaires du médecin-conseil, ainsi que les restrictions d'accès dans la gestion des cas.
Les instructions se fondent sur une base légale et leur mise en œuvre peut être exigée des assureurs, ce qui n'est pas le cas pour les recommandations.

2.4 Contrôle des conditions générales et des conditions spéciales des assureurs LAMal

Bien que les conditions générales d'assurance et les conditions spéciales des assureurs LAMal n'aient pas besoin d'être approuvées par l'autorité de surveillance, l'OFSP les examine. Lorsqu'un assureur LAMal émet de nouvelles conditions d'assurance, il les soumet à l'OFSP. Un contrôle ciblé des conditions générales et des conditions spéciales des assureurs LAMal a montré qu'en particulier les documents relatifs aux formes particulières d'assurance (modèle HMO, modèle du médecin de famille et modèle d'assurance avec conseil médical par téléphone) contiennent les principes essentiels de protection des données, mais formulés de manière très générale, et/ou un renvoi aux dispositions légales en la matière. Les règles spéciales ont trait, par exemple, au but du traitement des données par l'assureur LAMal, au droit de regard du médecin coordinateur – avec l'accord de l'assuré – sur les données relatives au diagnostic, au traitement et à la facturation qui sont nécessaires pour les formes particulières d'assurance, ou, en cas de changement de médecin, à la transmission des données médicales nécessaires au nouveau médecin coordinateur.

3. Résultats de la deuxième enquête sur la protection des données (2011-2012)

3.1 Concepts des assureurs LAMal en matière de protection et de sécurité des données

Le concept de protection et de sécurité des données est un instrument au moyen duquel l'assureur établit les principes fondamentaux qui s'appliquent à la collecte, au traitement, à la conservation, à l'exploitation et à la communication des données. Le concept définit entre autres le type et l'étendue des données dont l'assureur a besoin pour accomplir les tâches que lui confie la loi, les buts dans lesquels les données sont traitées ainsi que les mesures techniques et organisationnelles qu'il doit mettre en œuvre pour garantir le respect des prescriptions en matière de protection des données. Il pose un cadre pour élaborer les règlements de traitement des données (art. 84*b* LAMal ; art. 21 OLPD), les directives à l'attention des collaborateurs et les mesures nécessaires sur le plan informatique. Le concept sert de base pour définir les tâches des personnes chargées du traitement des données, le contenu des fichiers, les droits des personnes dont les données sont traitées (assurés) et les mesures de protection contre l'accès non autorisé à des données personnelles.

En leur qualité d'entités juridiques autonomes, les assureurs sont compétents pour l'élaboration de leur concept de protection et de sécurité des données. Celui-ci définit les principes juridiques de la protection des données que l'assureur doit respecter. La loi n'oblige pas les assureurs à établir un tel concept, mais l'OFSP le leur recommande (cf. circulaire 7.1 du 25 août 2011, p. 2, à l'*annexe 3*).

Il ressort de l'enquête réalisée (question 1.1) que :

- plus de la moitié des assureurs (59 %) ont élaboré un concept de protection et de sécurité des données. Il s'agit du même pourcentage que lors de la première enquête (2007-2009) ;

- la proportion des grands assureurs ayant établi un tel concept est plus importante que celle des petits assureurs (48 % des assureurs comptant jusqu'à 10 000 assurés [petits assureurs], 67 % des assureurs comptant entre 10 001 et 150 000 assurés [moyens assureurs] et 74 % des assureurs comptant plus de 150 000 assurés [grands assureurs] possèdent un concept de protection et de sécurité des données).

La majorité des assureurs a établi ce concept entre 2007 et 2011.

S'agissant des concepts de protection et de sécurité des données, établis pour des domaines particuliers (question 1.2), ils concernent avant tout le secteur informatique et les activités du médecin-conseil.

3.2 Règlements de traitement des données et concepts pour les droits d'accès des collaborateurs

L'art. 21 OLPD prescrit aux assureurs LAMal d'établir un règlement de traitement pour les fichiers automatisés qui contiennent des données sensibles ou des profils de la personnalité, ou qui sont connectés à d'autres fichiers. Ce règlement contient des indications sur l'organisation interne de l'assureur-maladie ainsi que sur la structure dans laquelle le fichier ou le système automatique de traitement sont intégrés. Il décrit les procédures de traitement et de contrôle des données, et y intègre un inventaire de tous les documents relatifs à la planification, à l'élaboration et à la gestion du fichier et des moyens informatiques utilisés. Il règle notamment la nature et l'étendue des droits d'accès des utilisateurs aux données personnelles. Le règlement doit être régulièrement mis à jour et être en tout temps à disposition du PFPDT sous une forme intelligible. La garantie de l'exhaustivité et de l'actualité des règlements de traitement constitue l'une des tâches principales du conseiller de l'assureur LAMal à la protection des données et sert de base effective à un usage des fichiers contenant des données personnelles sensibles qui soit conforme à la loi.

L'art. 84*b* LAMal répète et explicite ces obligations incombant aux assureurs LAMal en vertu de l'OLPD, mais il précise en plus que, depuis le 1er janvier 2012, les règlements de traitement des données doivent être soumis spontanément à l'appréciation du PFPDT et être rendus publics. Mais le règlement de traitement est déjà valable lorsque l'assureur-maladie l'a déclaré contraignant. Un règlement de traitement peut être valable pour plusieurs fichiers, s'il s'applique effectivement pour les fichiers désignés et qu'il remplit pour chaque fichier concerné les exigences de l'art. 21, al. 2, OLPD.

Dans le cadre de la deuxième enquête, près de 2/3 des assureurs (63 %) ont indiqué avoir établi un règlement de traitement conforme à l'art. 21 OLPD pour chaque fichier automatisé connecté à d'autres fichiers ou contenant des données sensibles ou des profils de la personnalité. La proportion des assureurs ayant établi les règlements requis augmente là aussi avec la taille de l'assureur (44 % des petits assureurs, 67 % des moyens assureurs et 95 % des grands assureurs). La majorité des assureurs (66 %) indique l'avoir fait pour tous les fichiers. C'est le cas de presque tous les grands assureurs (95 %) (question 2.1).

Au moment de la première enquête (2007-2009), par contre, seuls 26 % des assureurs LAMal avaient des règlements de traitement relatifs à leurs fichiers de données sensibles. L'OFSP constate donc une évolution positive dans ce domaine.

D'après les indications fournies, 73 % des assureurs LAMal ont élaboré un concept relatif aux droits d'accès de leurs collaborateurs. Là aussi, les grands et moyens assureurs sont en tête (90 % des grands assureurs, 83 % des moyens assureurs et 56 % des petits assureurs) (question 2.2).

Seuls 67 % des assureurs LAMal ont établi un règlement spécifique pour le traitement des données par le médecin-conseil et le service du médecin-conseil (28 % ont rédigé ce règlement de traitement à l'interne, et 39 % ont adopté le règlement élaboré par l'Association de réassurance des petits et moyens assureurs-maladie [RVK], avec laquelle ils collaborent). C'est cette collaboration qui fait qu'ici, le pourcentage est meilleur pour les petits et moyens assureurs (question 2.3).

La majorité des assureurs LAMal (57 %) contrôle une fois par année que les règlements de traitement sont complets et à jour. Le pourcentage est meilleur pour les petits (61 %) et moyens assureurs (67 %) que pour les grands assureurs (55 %), ce qui là aussi est dû à la collaboration des premiers avec la RVK (question 2.4). Le PFPDT examine actuellement les règlements de traitement soumis à son appréciation.

Il faut malheureusement constater qu'un bon tiers seulement des assureurs LAMal (36 %) entend publier ses règlements de traitement, ce que prescrit pourtant l'art. 84*b* LAMal. Les assureurs peuvent soustraire les secrets d'affaires de l'accès au public. La communication sur demande prévue par un petit tiers des assureurs (28 %) ne répond pas à la prescription légale (question 2.5). Pour la majorité des assureurs LAMal (64 %), grands assureurs compris, il faudra donc recourir aux instructions et, au besoin, à la menace de sanctions (avertissement et amende d'ordre) conformément à l'art. 21 al. 2 et 5 LAMal pour obtenir la publication des règlements de traitement. L'OFSP a déjà adressé des instructions sur cet objet.

3.3 Registre des fichiers

La LPD admet l'autorégulation des entreprises en matière de protection des données : il appartient à l'assureur LAMal de veiller à ce que les principes et les prescriptions du droit relatif à la protection des données soient respectés. En tant que maître du fichier, l'assureur-maladie est libéré de l'obligation de déclarer son fichier 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 s'il a annoncé cette personne au PFPDT (art. 11*a*, al. 5, let. e, LPD). Il en va de même s'il a obtenu un label de qualité en matière de protection des données au terme d'une procédure de certification menée conformément à l'art. 11 LPD, et a annoncé au PFPDT le résultat de

cette procédure (art. 11*a*, al. 5, let. f, LPD).

Il est réjouissant de constater que la grande majorité des assureurs LAMal (79 %) tient un registre de tous leurs fichiers à caractère personnel conformément à l'art. 11*a* LPD et à l'art. 16 OLPD. Plus la caisse est importante, plus ces fichiers sont traités avec professionnalisme (95 % des grands assureurs, 89 % des moyens assureurs et 69 % des petits assureurs). Un tel registre est encore en cours d'élaboration pour 6 % des caisses (question 3.1).

Autre point positif, plus de 2/3 des assureurs LAMal (71 %) indiquent que ce registre a été mis à jour pour la dernière fois dans les trois dernières années (65 % des petits assureurs, 89 % des moyens assureurs et 74 % des grands assureurs) (question 3.2).

Plus d'un tiers des assureurs LAMal (36 %) affirme avoir déclaré tous ses fichiers au PFPDT. Presque tous ceux qui ne l'ont pas fait (92 % de ceux-ci) ont désigné un conseiller à la protection des données. C'est le cas de tous les moyens et grands assureurs qui n'ont pas déclaré leurs fichiers au PFPDT (question 3.3).

3.4 Externalisation

L'externalisation désigne la délégation à des prestataires externes de prestations de service que les assureurs-maladie fournissaient jusqu'alors eux-mêmes, mais aussi de prestations qu'ils ne livraient pas eux-mêmes et qu'ils reçoivent nouvellement d'un fournisseur.

Le traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie, à condition que *seuls soient effectués les traitements que l'assureur-maladie serait en droit d'effectuer lui-même et qu'aucune obligation légale ou contractuelle ne l'interdise* (art. 10*a* LPD). L'art. 84 LAMal habilite les assureurs-maladie à faire traiter par des tiers des données personnelles, y compris des données sensibles et des profils de la personnalité. La circulaire 7.1 contient de nombreuses prescriptions que les assureurs LAMal doivent respecter en cas d'externalisation (cf. circulaire 7.1, ch. 5, à l'*annexe 3).*

L'externalisation de tâches est largement pratiquée par les assureurs. Seuls quatre d'entre eux ont déclaré ne pas y recourir. La délégation de tâches permet une rationalisation des ressources, ce qui a un impact positif notamment sur les frais d'administration de la caisse-maladie. De même, les petits et moyens assureurs ont un intérêt à mandater le médecin-conseil du RVK plutôt que de disposer de leur propre médecin-conseil. En fin de compte, les économies réalisées sur les frais d'administration se répercutent sur les primes et sont donc dans l'intérêt des assurés.

Il ressort de la dernière enquête que les caisses-maladie mandatent des tiers dans les proportions suivantes (question 4.1) :

- 46,3 % des assureurs (31) délèguent des tâches dans le domaine informatique ;
- 41,8 % des assureurs (28) délèguent des tâches à la RVK ;
- 28,4 % des assureurs (19) délèguent des tâches à santésuisse (SASIS) et à l'institution commune LAMal ;
- 35,8 % des assureurs (24) délèguent des tâches à Service Sinistres Suisse SA, à SIZ SA et à Avus SA ;
- 31,3 % des assureurs (21) délèguent des tâches à Medgate ;
- 16,4 % des assureurs (11) délèguent des tâches à des sociétés d'encaissement ;
- 55,2 % des assureurs (37) délèguent des tâches à diverses entités ;
- 7,5 % des assureurs (5) délèguent des tâches à des tiers dans le domaine des prestations.

Suivant leur taille, les assureurs recourent à l'externalisation de tâches dans des proportions différentes en fonction des délégataires :

Délégataires	Assureurs comptant jusqu'à 10 000 assurés	Assureurs comptant entre 10 001 et 150 000 assurés	Assureurs comptant plus de 150 000 assurés
IT (sociétés informatiques, notamment Centris, RR Donnelley, BBT Software, Secon SA, MediData, Bambus, AC Services, IT Surplus...)	30,4 % (7 assureurs)	61,1 % (11 assureurs)	65 % (13 assureurs)
RVK	69,6 % (16 assureurs)	55,6 % (10 assureurs)	10 % (2 assureurs)
santésuisse (SASIS) Institution commune	13 % (3 assureurs)	44,4 % (8 assureurs)	35 % (7 assureurs)
Service Sinistres Suisse SA, SIZ SA, Avus SA	26,1 % (6 assureurs)	44,4 % (8 assureurs)	40 % (8 assureurs)
Sociétés d'encaissement	8,7 % (2 assureurs)	16,7 % (3 assureurs)	25 % (5 assureurs)
Tiers mandatés dans le domaine des prestations	4,3 % (1 assureur)	11,1 % (2 assureurs)	10 % (2 assureurs)
Medgate	13 % (3 assureurs)	38,9 % (7 assureurs)	50 % (10 assureurs)
Divers	30,4 % (7 assureurs)	61,1 % (11 assureurs)	85 % (17 assureurs)

24 assureurs mandatent des prestataires étrangers, en Europe, en Afrique du Nord et aux Etats-Unis (question 4.2). Ceux-ci sont principalement chargés des tâches suivantes : assistance à l'étranger, éclaircissements au sujet des prestations fournies à l'étranger, recouvrement de créances, carte d'assuré, sondages téléphoniques de satisfaction auprès des assurés.

La plupart des assureurs utilisent les moyens suivants pour vérifier que le traitement des données par les tiers délégataires est conforme à la législation sur la protection des données (question 4.4) :

- audits ;
- certification de l'entité mandatée ;
- contrôles effectués par le conseiller à la protection des données ;
- contrats de collaboration ;
- instruction des collaborateurs de l'entité mandatée ;
- contrôles sur place, par échantillonnages.

Etant donné le volume des prestations externalisées par les assureurs-maladie à des prestataires externes, certains étrangers qui plus est, c'est par des échantillonnages que le respect des prescriptions spécifiques de la circulaire 7.1, ch. 5, peut être contrôlé.

3.5 Médecin-conseil et service du médecin-conseil

Le médecin-conseil au sens de l'art. 57 LAMal est un organe particulier de l'assurance-maladie sociale. Ses tâches sont définies à l'art. 57, al. 4 et 5, LAMal : il 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 lui incombe en outre une fonction de vérification et de contrôle : il examine si les conditions de prise en charge d'une prestation sont remplies (art. 57, al. 4, LAMal). II lui appartient de contrôler si le traitement est efficace, adéquat et économique au sens des art. 32 et 56 LAMal. Sa compétence se limite à répondre aux questions médicales. L'assureur ne peut rien lui prescrire à cet égard. Indépendant dans son jugement, le médecin-conseil ne peut transmettre 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 pour 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 du médecin-conseil, que la loi exige, doit se refléter aussi dans l'organisation du service du médecin-conseil. Les locaux de ce service doivent être suffisamment séparés et doivent pouvoir être fermés à clé. Le courrier ne peut être ouvert que par le personnel du service et il doit être garanti en tout temps que les données personnelles sensibles ne peuvent sortir du service du médecin-conseil. Un réseau téléphonique indépendant (télécopie incluse) est indispensable. Le système informatique doit être matériellement organisé de telle sorte que les documents établis par le service du médecin-conseil ne puissent être archivés que sur ses propres supports de mémoire, lesquels ne sont accessibles qu'aux collaborateurs du service. Le médecin-conseil doit en outre avoir la compétence d'engager son personnel auxiliaire. Il doit veiller à ce que les postes de ce personnel soient conçus, sous l'angle de leur position hiérarchique et professionnelle et du point de vue de leur taux d'occupation, de manière qu'il n'en résulte pas de conflits d'intérêts pour ces collaborateurs. Le personnel auxiliaire ne doit pas se voir confier des tâches incompatibles entre elles (p. ex., les unes pour le service du médecin-conseil et les autres pour le service « prestations »).

D'après la deuxième enquête, près de la moitié des assureurs LAMal (46 %) dispose d'un médecin-conseil externe ou d'un service du médecin-conseil externalisé. Dans la plupart des cas, cette tâche est confiée à la RVK. 77 % des petits assureurs et 47 % des moyens assureurs l'externalisent. Du côté des grands assureurs, la proportion n'est que de 12 %. Les médecins-conseils actifs à l'intérieur de l'organisation de l'assureur sont en général subordonnés à la direction ou rattachés au service « prestations », quelle que soit la taille de la caisse-maladie (question 5.1).

Chez un peu plus de la moitié des assureurs LAMal (53 %), les auxiliaires du médecin-conseil travaillent exclusivement pour lui. C'est le cas chez 56 % des moyens assureurs et 60 % des grands assureurs. Chez les autres assureurs, les auxiliaires du médecin-conseil remplissent encore d'autres tâches (question 5.2).

Chez 77 % des assureurs LAMal, services du médecin-conseil externalisés inclus (à savoir 82% des petits assureurs, 78% des moyens assureurs et 70% des grands assureurs), les auxiliaires du médecin-conseil ont un cahier des charges écrit. Dans 85 % des cas (à savoir 94% des petits assureurs, 72% des moyens assureurs et 86% des grands assureurs), les cahiers des charges présentés répondent aux exigences de l'OFSP (question 5.3).

Le courrier postal ou électronique adressé au médecin-conseil lui parvient directement chez pratiquement tous les assureurs LAMal (à savoir chez tous les petits et moyens assureurs et chez 95% des grands assureurs) (question 5.4).

Chez plus de 90 % de tous les assureurs LAMal, toutes catégories confondues, le courrier postal n'est ouvert que par le médecin-conseil ou ses auxiliaires (question 5.5).

Chez 96% des petits assureurs, 100% des moyens assureurs et 95% des grands assureurs, seuls le médecin-conseil ou ses auxiliaires ont accès au courrier électronique du médecin-conseil (question 5.6). Chez l'un des autres assureurs, le courrier est ouvert par la direction. Six des autres assureurs n'ont pas répondu à cette question.

Par ailleurs, 85 % des assureurs LAMal indiquent que lorsqu'il est ouvert par inadvertance par un autre service, le courrier destiné au médecin-conseil lui est transmis immédiatement, à lui ou à son service. C'est le cas sans exception chez les grands assureurs, chez 95% des moyens assureurs et 79% des petits assureurs (question 5.7).

Chez 96% des petits, 100% des moyens et 95% des grands assureurs, les locaux du médecin-conseil ou du service du médecin-conseil sont organisés, en termes de protection et de sécurité des données, de manière à correspondre aux prescriptions de la LPD. Le service du médecin-conseil que la majorité des petits et moyens assureurs externalise auprès de la RVK est autonome au niveau de

l'organisation, des locaux et de la structure informatique. Chez les autres assureurs, le service du médecin-conseil a ses propres locaux, ou l'accès est sécurisé (question 5.8).

Dans le service du médecin-conseil, le classement des données sensibles est conforme aux prescriptions de la LPD chez 100% des petits et moyens assureurs et chez 95% des grands assureurs. L'organisation de ce classement diffère selon la taille de l'assureur. Les grands assureurs, par exemple, ont mis en place un service du médecin-conseil qui administre et archive les données sensibles (au format papier et/ou électronique). Le service du médecin-conseil externalisé offert par la RVK dispose de la même organisation. Chez les assureurs qui ont un médecin-conseil externe et/ou qui n'ont pas de service du médecin-conseil à proprement parler, les données sensibles sont conservées dans des armoires fermées à clé, et/ou les documents au format papier sont détruits après avoir été scannés, ou archivés chez le médecin-conseil externe. N'ont accès à ces données que les auxiliaires que le médecin-conseil a expressément désignés à cette fin (question 5.9).

L'accès aux données sensibles (documents papier et documents scannés) traitées par le service du médecin-conseil est réglé de différentes manières : chez 30 % des assureurs LAMal, seul le médecin-conseil y a accès. Chez 26 % des assureurs, cet accès est réservé au médecin-conseil et à ses auxiliaires et chez 5 % des assureurs, au médecin-conseil et à des personnes ayant des fonctions dirigeantes ; chez 5 % des assureurs aussi, ce sont le médecin-conseil, ses auxiliaires et des personnes ayant des fonctions dirigeantes qui ont accès à ces données ; chez 16 % des assureurs, ce sont le médecin-conseil, ses auxiliaires et le service juridique ; chez 12 % des assureurs, ce sont le médecin-conseil, ses auxiliaires et d'autres personnes (question 5.10). Les autres assureurs (trois caisses pratiquant l'assurance d'indemnités journalières et une très petite caisse) n'ont pas répondu à cette question.

91% des petits, 95% des moyens et 95% des grands assureurs indiquent qu'ils concrétisent l'art. 57, al. 7, LAMal en prévoyant que le médecin-conseil et le service du médecin-conseil ne transmettent à l'administration de la caisse que les indications qui sont nécessaires à une prise de décision. Mais seuls 28 % d'entre eux (19% des petits, 30% des moyens et 37% des grands assureurs) affirment le garantir également par des mesures de contrôle (question 5.11).

3.6 Conseiller à la protection des données

Comme indiqué au ch. 3.3, l'assureur-maladie, maître du fichier, est libéré de l'obligation de déclarer son fichier au PFPDT 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 s'il a annoncé cette personne au PFPDT.

Le conseiller à la protection des données (contrairement à sa désignation dans la version allemande de la LPD : *Datenschutzverantwortlicher*) n'est pas responsable de la protection des données dans l'entreprise, mais a un rôle de conseiller ou d'organe de surveillance. La responsabilité du respect de la législation relative à la protection des données incombe dans tous les cas au maître du fichier, donc à l'assureur-maladie, ou à son organe de direction (art. 16, al. 1, LPD).

Le conseiller à la protection des données doit pouvoir exercer sa fonction en toute indépendance, tant sous l'angle organisationnel que professionnel, et sa position dans l'organisation doit être de nature à éviter tout conflit d'intérêts. C'est pourquoi son poste ne doit pas être associé à une responsabilité hiérarchique. L'OFSP recommande un poste dans l'état-major, le service juridique ou le service informatique, ou un poste externe. Le rôle et la fonction du conseiller à la protection des données doivent être définis dans un cahier des charges.

Il ressort de la deuxième enquête qu'à ce jour, 88 % des assureurs LAMal ont désigné au moins un conseiller à la protection des données au sens de l'art. 11*a*, al. 5, let. e, LPD. Chez les grands assureurs, la proportion est de 95 % (question 6.1). Lors de la première enquête (2007-2009) ce

n'était encore le cas que de 80 % des assureurs LAMal. L'OFSP constate donc une évolution positive dans ce domaine.

Dans de nombreux cas, ce poste est rattaché à la direction (40 % des assureurs) et, dans 19 % des cas, au service juridique (la proportion est même de 42 % chez les grands assureurs) (question 6.2).

Seuls 15 % des assureurs LAMal (33% des petits, 19% des moyens, aucun grand assureur) ont confié cette tâche à un service externe, ce qui est également admis en vertu de l'art. 12*a*, al. 2, OLPD. Les grands assureurs ont néanmoins tous désigné pour cela un collaborateur interne (question 6.3).

Les petits et moyens assureurs emploient dans leur majorité (62 %) entre 0 et 1 équivalent plein temps à cette fin, et la majorité des grands assureurs (63 %), entre 0,5 et plus de 1 équivalent plein temps (question 6.4).

Cela dit, dans 93 % des cas, les conseillers à la protection des données exercent encore d'autres tâches. Chez les grands assureurs, c'est toujours le cas. Il s'agit alors fréquemment de tâches au sein de la direction ou du service informatique (question 6.5).

69 % des assureurs LAMal (à savoir 62% des petits, 81% des moyens et 69% des grands assureurs) ont déclaré leurs conseillers à la protection des données au PFPDT (question 6.6).

Dans 75 % des cas (à savoir 57% des petits assureurs, 88% des moyens assureurs et 84% des grands assureurs), les conseillers à la protection des données ont un cahier des charges écrit. Son contenu correspond aux attentes de l'OFSP chez plus de 90% des assureurs-maladie (100% des petits et des grands assureurs, 79% des moyens assureurs), tandis que chez 8 % des assureurs (19% des petits, aucun moyen, 5% des grands assureurs), un tel cahier des charges est en cours d'élaboration (question 6.7).

Lors de l'enquête de 2007-2009, seuls 47 % des conseillers à la protection des données avaient un cahier des charges écrit.

Chez 75 % des assureurs LAMal (67% des petits, 75% des moyens et 79% des grands assureurs) qui ont désigné un conseiller à la protection des données, cette personne a suivi une formation spécifique en protection des données (question 6.8). De plus, les conseillers à la protection des données suivent régulièrement une formation continue chez 95 % de ces assureurs (95% des petits, 94% des moyens et 100% des grands assureurs) (question 6.9). Les conseillers à la protection des données sont mieux qualifiés aujourd'hui que lors de la première enquête (2007-2009).

Chez 80 % des assureurs LAMal (67% des petits, 81% des moyens et 90% des grands assureurs) qui ont désigné un conseiller à la protection des données, ce spécialiste organise des formations en la matière à l'intention des collaborateurs. Chez 37 % des assureurs (52% des petits, 33% des moyens et 30% des grands assureurs), la participation à ces formations est obligatoire pour tous les collaborateurs de l'entreprise, et chez 39 % d'entre eux (18% des petits, 45% des moyens et 65% des grands assureurs), elles ne sont prévues que pour les nouveaux collaborateurs ou pour certains services, p. ex., pour le service « prestations » (question 6.10).

3.7 Protection des données : systèmes de gestion et certifications

Les assureurs ont la possibilité de faire certifier leur système de gestion de la protection des données (SGPD) par un organisme de certification agréé et indépendant au sens de l'art. 11 LPD.

Il ressort de l'enquête réalisée que 10 % seulement des assureurs LAMal ont fait certifier leur organisation dans son ensemble. Il s'agit des petits (9 %) et des moyens (28 %) assureurs. Il faut toutefois relever que la certification au sens de l'art. 11 LPD n'a été effectuée que pour deux assureurs moyens. Pour les autres, il ne s'agit pas d'une certification au sens de l'art. 11 LPD.

Les assureurs n'ayant pas procédé à cette certification invoquent la taille réduite de la caisse (ressources) et/ou les frais d'investissement liés à la procédure de certification (20 % des assureurs LAMal, la proportion étant de 33 % pour les petits assureurs et de 34 % pour les moyens assureurs). 44 % des assureurs LAMal (48 % des petits assureurs, 33 % des moyens assureurs et 8 % des grands assureurs) étudient l'opportunité d'effectuer une procédure de certification au sens de l'art. 11 LPD. Enfin, 20 % des assureurs LAMal, surtout parmi les grands assureurs, indiquent qu'ils se sont organisés eux-mêmes dans le domaine de la protection des données (question 7.1).

Parmi les assureurs qui n'ont pas fait certifier leur organisation dans son ensemble, onze assureurs LAMal, dont huit grands assureurs, n'ont fait certifier qu'une partie de leurs systèmes et/ou procédures. Selon les indications obtenues, seuls les départements informatiques et le service du médecin-conseil ont fait l'objet d'une certification. Les services du médecin-conseil ont été certifiés au sens de l'art. 11 LPD et les départements informatiques ont une certification IQNet. Il en ressort que le service du médecin-conseil de cinq assureurs (deux moyens assureurs et trois grands assureurs) ont fait l'objet d'une certification au sens de l'art. 11 LPD (question 7.2).

La deuxième enquête permet de constater ce fait réjouissant : plus de 3/4 des assureurs LAMal (81 %) contrôlent le respect des exigences en matière de protection des données au sein de leur entreprise (74 % des petits assureurs, 94 % des moyens assureurs et 90 % des grands assureurs) (question 7.3). Parmi les assureurs qui n'ont pas indiqué explicitement qu'ils contrôlaient le respect des exigences en matière de protection des données au sein de leur entreprise, six sur neuf ont toutefois désigné un conseiller à la protection des données qui devrait se charger de cette tâche.

Pour environ 2/3 (63 %) des assureurs LAMal qui contrôlent le respect des exigences en matière de protection des données, ces contrôles sont effectués par la révision interne ou externe et/ou par le conseiller à la protection des données de l'assureur (52 % des petits assureurs, 67 % des moyens assureurs et 85 % des grands assureurs). Pour 18 % des assureurs LAMal, surtout les petits (22 %) ou les moyens assureurs (28 %), ces contrôles sont effectués par la direction ou par les chefs de département. Dans la majorité des cas, ces contrôles prennent la forme d'un audit interne. Il arrive aussi qu'ils soient effectués dans le cadre de programmes de contrôle ou qu'ils soient intégrés dans le système de contrôle interne (SCI). Dans 80 % des cas, ces contrôles sont effectués annuellement. 5 % des assureurs LAMal les effectuent à un intervalle de deux ans ou plus (question 7.4).

Le mandant de ces contrôles du respect des exigences en matière de protection des données est, pour 3/4 des assureurs LAMal, la direction, le conseil d'administration, le comité ou le comité d'audit (70 % des petits et moyens assureurs et 82 % des grands assureurs). Pour 1/4 des assureurs LAMal, ces contrôles sont du ressort du conseiller interne à la protection des données. En principe, les résultats du contrôle sont communiqués au mandant par écrit (question 7.5).

Les résultats de la deuxième enquête (2011-2012) ont donc confirmé ceux de la première (2007-2009), qui indiquaient que la nette majorité des assureurs-maladie était disposée à se soumettre à un audit en matière de protection des données ou que certains assureurs étaient d'accord avec une certification selon goodpriv@cy.

3.8 Echange de données pour la pratique des formes particulières d'assurance (modèle HMO et modèle du médecin de famille [réseaux de médecins], modèle d'assurance avec conseil médical par téléphone [Telmed])

L'auteur du postulat craint que les assureurs LAMal se servent des rapports médicaux exigés pour le contrôle de l'économicité des factures des hôpitaux afin d'établir des profils de risque des assurés concernés et d'empêcher ces assurés d'opter pour une forme particulière d'assurance obligatoire des soins (avec rabais sur les primes). La LAMal prévoit cependant un accès sans discrimination à ces formes particulières d'assurance, et tous les assurés domiciliés en Suisse peuvent choisir une de ces

formes d'assurance pour le début d'une année civile, quel que soit leur âge ou leur état de santé, pour autant que leur assureur-maladie en offre dans leur région. La deuxième enquête de l'OFSP tient néanmoins compte des doutes exprimés dans le postulat.

On a donc cherché à savoir, pour les assureurs qui proposent le modèle HMO, le modèle du médecin de famille ou le modèle d'assurance avec conseil médical par téléphone (Telmed), quelles mesures techniques et organisationnelles de sécurité ils avaient prises pour l'échange de données entre les services impliqués (médecins de premier recours / fournisseurs de prestations assurant la coordination, tiers mandatés [prestataires] et services internes de la caisse-maladie, service du médecin-conseil inclus). Il est apparu que, dans 91 % des cas, les canaux d'information sont sécurisés par des protocoles de cryptage et protégés par des mots de passe (question 8.1).

Certaines données sont échangées entre les services impliqués. Il s'agit surtout de données administratives, en vue de repérer les cas d'inobservation des dispositions relatives aux modèles avec choix limité des fournisseurs de prestations. Les données relatives aux prestations et à l'effectif qui sont saisies dans le système informatique des assureurs sont prises en compte pour contrôler que c'est bien le médecin de premier recours qui a envoyé le patient chez le spécialiste en question (question 8.2). On indique ci-après de façon générale, pour deux modèles, quelles données sont échangées entre les services impliqués.

Dans le cas du *modèle du médecin de famille*, les effectifs d'assurés et le coût brut des prestations fournies sont transmis mensuellement aux réseaux de médecins de famille/HMO. Les réseaux peuvent déléguer à une société externe (p. ex., Bluecare SA ou la RVK) la réception et le traitement des données. Les transmissions se font à chaque société séparément, si bien que ces sociétés ne reçoivent que les données des médecins qui leur sont rattachés. L'échange de données entre les services impliqués se fait par des canaux sécurisés (p. ex., une connexion SFTP [Secure File Transfer Protocol : échange de données crypté, protégé par un mot de passe], ou avec un certificat d'utilisateur [confirme et garantit par une procédure cryptographique l'authenticité et l'intégrité des identités et des objets]). Quant aux données relatives aux prestations, il s'agit de positions de prestations regroupées par types de prestations selon le pool de données SASIS. Ces indications se rapportent uniquement aux décomptes (il n'y a pas de positions TARMED ni de détails relatifs au diagnostic). Les données échangées, outre celles concernant les prestations et les effectifs, comprennent listes de médecins, avis de transfert et copies de factures. Ces éléments sont nécessaires pour contrôler le respect des dispositions relatives aux modèles avec choix limité des fournisseurs de prestations.

Dans le cas du *modèle d'assurance avec conseil médical par téléphone*, p. ex., Medi 24, l'échange de données a lieu par courriel sécurisé (correspond à un transfert SFTP). L'assureur fournit une statistique globale, p. ex. concernant le nombre total d'appels, la répartition entre hommes et femmes, le taux d'utilisation total et le niveau de service atteint (aucune donnée personnelle). Sont également transmises quelques données (personnelles) relatives aux appels, p. ex., n° de partenaire de la personne concernée, date, heure, durée de l'appel, type d'appel, qui a appelé (personne concernée ou autre personne), type de conseil (tri, informations médicales), degré d'urgence du tri, identification de l'appelant. Aucune donnée médicale n'est échangée dans ce modèle. Cela signifie que les collaborateurs de l'assureur ne peuvent pas savoir quelles ont été les questions médicales discutées entre le patient et le centre d'appel médical. L'assureur apprend seulement qui a appelé et quand.

63 % des assureurs LAMal qui proposent le modèle HMO, le modèle du médecin de famille ou le modèle Telmed affirment n'avoir aucun accès aux dossiers des patients ; dans les autres cas, l'accès est limité par des mesures techniques, à de rares exceptions près. De plus, l'accès des médecins de premier recours ou des fournisseurs de prestations assurant la coordination aux dossiers des patients est également, dans plus de 3/4 des cas, limité par des mesures techniques (question 8.3).

L’accès au dossier est par exemple limité comme suit pour le fournisseur de prestations assurant la coordination :

- Authentification au moyen de la carte HPC FMH (hCardManager de H-Net) afin de garantir que le médecin de famille n’ait accès qu’aux données de ses patients.
- Procédure passant par des plates-formes sécurisées, comme AVM-Infonet pour l’échange de données avec les réseaux de médecins.
- Les prestataires de conseil Telmed sont reliés au réseau sécurisé HIN (Health Info Net : met à la disposition de tous les partenaires du système suisse de santé une plate-forme sécurisée pour la messagerie électronique ainsi que des applications).
- Les centres de santé comme Santémed disposent de leur propre logiciel.

Les assureurs n’ont pas accès aux dossiers des patients (données médicales).

Il vaut encore la peine de mentionner ici le cas suivant : en 2010, à la suite d’une plainte, l’OFSP a contrôlé, lors de la résiliation du contrat d’un grand assureur avec des prestataires assurant la coordination, comment les assurés concernés avaient été redirigés vers l’assurance de base ordinaire ou un autre modèle du médecin de famille. Aucune sélection des risques n’a pu être constatée lors du tri. Au contraire, les propositions de répartition ont été faites de manière aléatoire, et les cas de coûts élevés, l’âge moyen et le coût moyen des prestations pour les assurés des deux groupes n’ont permis de déceler aucun indice de sélection des risques.

3.9 Gestion des cas

La gestion des cas n’est pas explicitement réglée dans la LAMal. En mettant en place la gestion des cas comme mesure d’optimisation des prestations, de contrôle et de minimisation des coûts, les assureurs s’efforcent de remplir au mieux les conditions de prise en charge des coûts sur la base des critères de l’art. 32 LAMal, selon lequel les prestations doivent être efficaces, appropriées et économiques. Cette conscience des coûts, notamment s’agissant de l’adéquation d’un traitement, peut se trouver en contradiction avec les prescriptions en matière de protection des données qui sont également applicables dans ce domaine. L’OFSP autorise les assureurs LAMal à pratiquer la gestion des cas, mais il exige d’eux qu’ils observent avec la plus grande attention les principes d’adéquation au but visé et de transparence inscrits dans la loi sur la protection des données.

Il ressort de la deuxième enquête que 60 % des assureurs-maladie pratiquent la gestion des cas. Chez les grands assureurs, la proportion est de 75 %. 45 % des assureurs LAMal qui ont une gestion des cas l'externalisent, et 55 % l'ont rattachée à leur service « prestations » (cela vaut pour tous les grands assureurs) (question 9.1).

Les 40 assureurs LAMal qui ont une gestion des cas ont tous pu – contrairement à ce qui ressortait de la première enquête en 2007-2009 – décrire de façon compréhensible le déroulement d'une telle gestion. Presque tous ont remis un modèle de déclaration de consentement (indispensable) de l’assuré. Dans un peu plus de 2/3 des cas, cette déclaration est correcte du point de vue de l’OFSP ; dans 20 % des cas, elle ne répond qu’en partie aux exigences, p. ex., la clause de retrait manque. Dans 7 % des cas, il s’agit d’une procuration générale, qui n’est pas valable (question 9.2).

Partout où il y a gestion des cas, les accès sont limités. La plupart du temps, seuls le gestionnaire de cas, son suppléant ou sa suppléante ainsi que le médecin-conseil et ses auxiliaires ont accès au dossier du patient (question 9.3).

3.10 Procurations et déclarations de consentement

Aux termes de l'art. 33 LPGA, les assureurs sont tenus de garder le secret à l'égard des tiers. L'art. 84*a* LAMal énumère de façon exhaustive les conditions dans lesquelles les données relatives aux assurés peuvent être communiquées. L'art. 84*a*, al. 5, let. b, LAMal prévoit en particulier que ces données ne peuvent être communiquées à des tiers que si la personne concernée y a, en l'espèce, consenti par écrit. Le traitement de données relatives à la personne assurée n'est donc admis que si celle-ci a donné librement son consentement après avoir été dûment informée, c'est-à-dire si, au moment de le donner, elle est en mesure d'estimer la portée de son consentement et qu'elle peut discerner quelles données peuvent être transmises, quel groupe de personnes peut transmettre ces informations ou à quel groupe de personnes elles peuvent être transmises, et quel est le but de la transmission de ces données. Les données relatives à la santé sont des données personnelles sensibles au sens de l'art. 3, let. c, ch. 2, LPD. Elles ne peuvent par conséquent être traitées qu'avec le consentement explicite de la personne assurée (art. 4, al. 5, LPD).

Quelques assureurs-maladie ont introduit dans leur formulaire d'affiliation une clause par laquelle le preneur d'assurance autorise l'assureur LAMal à communiquer des données et à recueillir des informations auprès d'autres personnes. L'OFSP contrôle régulièrement les formulaires d'affiliation des assureurs et exige d'eux qu'ils corrigent les questions et les clauses qui ne sont pas conformes aux dispositions légales. La personne assurée est parfois aussi invitée à signer une procuration en faveur de l'assureur pour des cas de prestations. L'assureur doit effectivement pouvoir recueillir des informations auprès de tiers (p. ex., des fournisseurs de prestations) afin de vérifier son obligation de prise en charge. Conformément à l'art. 28, al. 3, LPGA, la procuration doit toujours se référer à un cas de prestations concret. Une procuration pour des cas futurs n'est pas valable.

Il ressort de l'enquête réalisée que les clauses de procuration dans les formulaires d'affiliation LAMal et aussi, la plupart du temps, celles en rapport avec des cas de prestations sont conformes à la législation relative à la protection des données. Il en va de même des clauses de consentement établies par la RVK pour la gestion des cas.

La situation est plus complexe s'agissant des clauses de consentement figurant sur les questionnaires pour les assurances complémentaires. Les assureurs pratiquant les assurances complémentaires sont soumis à la LCA et à la surveillance de l'Autorité fédérale de surveillance des marchés financiers (FINMA). Du point de vue de l'OFSP, le contrôle de ces questionnaires est donc du ressort de cette autorité. Mais la clause de consentement que certains de ces formulaires contiennent concerne aussi la LAMal parce qu'elle prévoit que le preneur d'assurance autorise l'assureur LAMal à communiquer à l'assureur LCA des informations sur son état de santé. Il est parfois précisé dans cette clause que la transmission de données sert à apprécier la demande d'affiliation et les futurs cas de prestations. D'autres clauses ne contiennent aucune indication sur le but de la collecte des données. Comme indiqué ci-dessus, les preneurs d'assurance doivent être informés de manière complète et transparente avant de donner leur consentement. On peut donc supposer que sur la base de la plupart des clauses de consentement, les preneurs d'assurance ne sont souvent pas en mesure de saisir toute la portée de leur consentement, ou de discerner quelles données peuvent être transmises et quel est le but de la transmission des données. Du reste, une procuration générale pour des cas de prestations futurs contrevient à l'art. 28, al. 3, LPGA.

Comme il n'a aucune compétence à l'égard des assureurs LCA, l'OFSP s'est entretenu avec la FINMA pour discuter de cette question. Les deux autorités s'emploient à trouver des solutions qui respectent les règles à la fois de l'assurance-maladie sociale et des assurances privées.

4. Transmission de données des hôpitaux aux assureurs LAMal dans le cas d'un modèle de remboursement de type DRG

Le 23 décembre 2011, se fondant sur l'initiative parlementaire 11.429 « Tarmed. Compétence subsidiaire du Conseil fédéral » (FF 2012 51), le Parlement a adopté un nouvel art. 42, al. 3bis, LAMal. Cet alinéa prescrit que les fournisseurs de prestations font figurer dans la facture les diagnostics et les procédures sous forme codée, conformément aux classifications actuelles.

Le Conseil fédéral a ensuite défini, le 4 juillet 2012, les modalités de la transmission des données (art. 59*a* OAMal) afin que le principe de proportionnalité soit respecté. A partir de 2014 au plus tard, les hôpitaux devront transmettre systématiquement, avec la facture, les indications administratives et médicales à un service de réception des données certifié mis en place par l'assureur LAMal. Les assureurs ont jusqu'à fin 2013 pour mettre en place ce service et le faire certifier conformément à l'art. 11 LPD.

La certification est surveillée par le PFPDT, qui publie la liste des services de réception des données certifiés. Pendant la période transitoire, les indications médicales ne peuvent être transmises systématiquement qu'au médecin-conseil.

Le DFI a défini en outre, le 20 novembre 2012, sous la forme d'une ordonnance (ordonnance du DFI sur les fichiers de données pour la transmission des données entre fournisseurs de prestations et assureurs), une structure uniforme à l'échelle suisse pour les fichiers de données contenant les indications administratives et médicales. Cette ordonnance règle ainsi de manière définitive la question de la transmission des données – dans le cadre de la facturation – entre les assureurs LAMal et les hôpitaux.

Les modifications correspondantes de la LAMal (art. 42, al. 3bis et 4) et de l'OAMal (art. 59 ss) ainsi que l'ordonnance du DFI sont entrées en vigueur le 1er janvier 2013.

L'OFSP et le PFPDT suivent la mise en œuvre de ces dispositions par les assureurs LAMal.

5. Conclusions

Le présent rapport constitue un bon "état des lieux" et donne une information complète sur la façon dont les assureurs garantissent actuellement la protection des données des patients. Se fondant sur les enquêtes réalisées et sur les mesures de contrôle prises par les deux autorités de surveillance compétentes, l'OFSP et le PFPDT, le Conseil fédéral constate que dans de nombreux domaines les assureurs LAMal ont pris les mesures nécessaires pour garantir la protection et la sécurité des données.

Les résultats de la deuxième enquête démontrent que les assureurs LAMal ont remédié à la majorité des lacunes constatées et qu'ils font preuve de davantage de professionnalisme à l'égard de la protection des données qu'il y a quelques années encore. En ce qui concerne les modèles particuliers d'assurance, l'enquête n'a révélé aucun indice concret de traitement des données médicales qui ne serait pas en adéquation avec le but visé. De nombreux points ont été améliorés par rapport à la première enquête de l'OFSP et du PFPDT (2007-2009). D'autres points ne sont pas encore totalement remplis.

Dans le cadre de son activité de surveillance, l'OFSP veillera à ce que les manquements constatés soient corrigés et continuera à l'avenir à garantir une mise en oeuvre rigoureuse des prescriptions en

matière de protection des données. Un nouveau rapport sur le sujet sera établi, puis porté à la connaissance du Conseil fédéral et du Parlement dans un délai de trois à cinq ans.

Etant donné les diverses formes d'organisation des assureurs, et notamment la diversité des manières dont la protection et la sécurité des données sont intégrées dans leurs processus de travail, il n'est pas possible de tirer des conclusions générales sur les frais que la protection et la sécurité des données génèrent. Mais il ressort des enquêtes réalisées qu'elles n'influent pas de manière importante sur les frais d'administration.

Les autorités de surveillance (OFSP et PFPDT) disposent de tout un éventail d'instruments pour exiger au besoin des assureurs LAMal des mesures de correction spécifiques en matière de protection des données. En cas de soupçon ou de constatation d'une violation concrète de la protection des données dans la pratique d'un assureur ou en cas de découverte d'une clause contraire à la protection des données dans les dispositions réglementaires d'un assureur, les interventions de l'OFSP auprès de l'assureur concerné ont jusqu'à ce jour permis de rétablir une situation conforme au droit.

L'amélioration de certains éléments de la protection des données des patients est opérée au niveau législatif. Ainsi, les projets de loi du Conseil fédéral mentionnés ci-après apporteront une amélioration dans ce domaine:

1. Le message du Conseil fédéral concernant la modification de la LAMal "Compensation des risques. Séparation de l'assurance de base et des assurances complémentaires" du 20 septembre 2013 (FF 2013 7115) prévoit la séparation institutionnelle de l'assurance-maladie sociale et de l'assurance complémentaire (art. 12 al. 2 P-LAMal). Les groupes d'assureurs au sein desquels une société pratique l'assurance-maladie sociale doivent, au moyen de barrières, empêcher tout échange de données relatives aux assurés entre l'assureur LAMal et les autres sociétés du groupe. (art. 13 al. 2 let. g P-LAMal). Les assureurs doivent par conséquent disposer de banques de données séparées pour les décomptes de prestations de l'assurance de base et pour ceux de l'assurance complémentaire. De plus, le médecin-conseil qui se prononce sur des prestations de l'assurance obligatoire des soins ne doit pas se prononcer sur des prestations de l'assurance complémentaire. La protection des données doit ainsi être améliorée et il s'agit d'éviter que les données personnelles collectées dans un domaine d'assurance ne soient utilisées dans l'autre domaine à des fins de sélection des risques (voir message du Conseil fédéral chiffres 1.2.2 et 5.6).

2. Le projet de loi fédérale sur la surveillance de l'assurance-maladie (P-LSAMal; FF 2012 1779) prévoit que les caisses-maladie mettent en place un système de contrôle interne efficace et adapté à la taille et à la complexité de l'entreprise (art. 22 al. 1 P-LSAMal). En matière de protection des données, l'organe de contrôle interne est chargé d'évaluer la conformité des processus à la loi et établit des rapports. La protection des données au sein des caisses-maladie sera ainsi renforcée avec la LSAMal. La question de la légalité de la transmission de données se pose en particulier au sein des groupes d'assurance. Dans ce domaine également, la LSAMal améliore notablement la protection des données puisqu'elle accorde au Conseil fédéral la compétence d'édicter des dispositions sur le système de contrôle interne (art. 44 al. 2 P-LSAMal).

Fort de ces constats, le Conseil fédéral propose de classer le postulat Heim 08.3493 « Protection des données des patients et protection des assurés ».

6. Liste des annexes

Annexe 1

Texte du postulat Heim 08.3493 « Protection des données des patients et protection des assurés », développement et avis du Conseil fédéral

Annexe 2

Interventions parlementaires relatives à la protection des données des patients (2008 à 2012)

Annexe 3

Circulaire OFSP n° 7.1 du 25 août 2011 « Assureurs-maladie : organisation et processus conformes à la protection des données », avec lettre d'accompagnement et sept annexes

Annexe 4

Circulaire OFSP n° 7.1 du 17 juin 2013 « Assureurs-maladie : organisation et processus conformes à la protection des données », avec lettre d'accompagnement et huit annexes

Annexe 5

Questionnaire à l'attention des assureurs-maladie concernant la conformité de leur organisation et de leurs processus au droit relatif à la protection des données, avec lettre d'accompagnement du 13 décembre 2011

Protection des données des patients et protection des assurés

Rapport du Conseil fédéral en réponse au postulat Heim (08.3493)

du 18 décembre 2013

Liste des annexes

Annexe 1

Texte du postulat Heim 08.3493 « Protection des données des patients et protection des assurés », développement et avis du Conseil fédéral

Annexe 2

Interventions parlementaires relatives à la protection des données des patients (2008 à 2012)

Annexe 3

Circulaire OFSP n° 7.1 du 25 août 2011 « Assureurs-maladie : organisation et processus conformes à la protection des données », avec lettre d'accompagnement et sept annexes

Annexe 4

Circulaire OFSP n° 7.1 du 17 juin 2013 « Assureurs-maladie : organisation et processus conformes à la protection des données », avec lettre d'accompagnement et huit annexes

Annexe 5

Questionnaire à l'attention des assureurs-maladie concernant la conformité de leur organisation et de leurs processus au droit relatif à la protection des données, avec lettre d'accompagnement du 13 décembre 2011

Annexe 1

L'Assemblée fédérale - Le Parlement suisse

Curia Vista - Objets parlementaires

08.3493 – Postulat
Protection des données des patients et protection des assurés

Déposé par	 Heim Bea
Date de dépôt	18.09.2008
Déposé au	Conseil national
Etat des délibérations	Transmis

Texte déposé
Je charge le Conseil fédéral de présenter les mesures prévues pour lutter contre la discrimination dont sont victimes certains groupes de patients du fait des nouveaux modèles d'assurance AOS et garantir la protection des données relatives aux patients chez les assureurs.

Développement
Un avis de droit de H+ et une recherche scientifique (thèse de mastère Y. Prieur) sont venus étayer la critique émise par le préposé du canton de Zurich à la protection des données: de plus en plus souvent, les assureurs exigeraient des hôpitaux les lettres de sorties et les rapports opératoires complets concernant leurs assurés, pour le contrôle des factures. Les assureurs enfreignent ainsi la LAMal aussi bien que le secret médical. Les organisations de défense des patients DVSP et OSP jugent cette pratique illégale. Les risques de discrimination qui en résultent ne peuvent que croître, tout particulièrement avec les nouveaux modèles d'assurance de l'AOS: en exploitant les données des patients ainsi obtenues, les assureurs peuvent établir des profils de risques. Certains modèles d'assurance et certaines remises de primes peuvent être refusés de manière ciblée aux personnes atteintes dans leur santé, ce qui entraîne une désolidarisation insidieuse, même dans le domaine de l'assurance sociale de base. Cette évolution est en totale contradiction avec l'acceptation de la LAMal en votation populaire. Les nouveaux modèles d'assurance assortis de remises peuvent en outre entraîner des hausses de primes dans l'assurance de base. Dans ses réponses à l'interpellation 06.3040 et à la motion 07.3114, le Conseil fédéral a constaté que les assureurs ne garantissent pas suffisamment la protection des données et les droits de la personnalité. Vu la menace qui pèse sur le secret médical et la protection des données, il est incompréhensible que les autorités de surveillance n'épuisent pas toutes les possibilités dont elles disposent pour prendre des mesures concrètes.

Le Conseil fédéral est chargé de présenter les mesures qu'il prend pour garantir que les nouveaux modèles AOS n'entraîneront aucune discrimination à l'encontre de groupes spécifiques de patients.

Afin de protéger les données des patients, la LPD révisée prévoit une certification des systèmes et des procédures de traitement de ces données. Il s'agit maintenant de vérifier dans quelle mesure les assureurs ont donné suite à la certification facultative. La transparence doit en outre être garantie au niveau du traitement ultérieur et de la durée de conservation des données de santé exigées dans le cadre du contrôle des factures. Dernière question enfin: comment garantir l'indépendance des médecins-conseils, sachant qu'ils officient souvent aussi comme médecins d'entreprise?

Avis du Conseil fédéral du 26.11.2008
Le Conseil fédéral est conscient que la situation en matière de protection des données constatée chez certains assureurs nécessite une intervention. C'est pourquoi l'Office fédéral de la santé publique (OFSP), en tant qu'organe de surveillance, a été chargé de procéder à des vérifications et de prendre les mesures qui s'imposent. Un groupe de travail, composé de représentants de l'OFSP ainsi que du Préposé fédéral à la protection des données et à la transparence (PFPDT), a examiné l'ensemble des opérations liées au traitement des données effectué par les assureurs, par le biais d'une enquête menée à l'échelle nationale.

Compte tenu des résultats de cette enquête ainsi que de l'importance accordée à cette question par une large part des milieux spécialisés et de la population, le Conseil fédéral est disposé, dans les deux ans à venir, à rendre compte des mesures déjà prises ainsi que de celles qui restent à prendre pour garantir la protection des données relatives aux assurés en tant que patients.

Au cours de ses travaux, le groupe de travail prendra en considération les inquiétudes exprimées dans le postulat à propos de l'établissement de profils de risque, qui pourrait influencer l'accès à certaines formes d'assurance. Cependant, la LAMal prévoit déjà une possibilité d'accéder sans discrimination aux formes particulières de l'assurance obligatoire des soins. En effet, tous les assurés domiciliés en Suisse, quel que soit leur âge et leur état de santé, ont la possibilité, au début d'une année civile, de conclure une forme particulière d'assurance, pour autant que l'assureur la propose dans la région où ils résident.

Proposition du Conseil fédéral du 26.11.2008
Le Conseil fédéral propose d'accepter le postulat.

Documents

Bulletin officiel - les procès-verbaux

Chronologie / procès-verbaux

Date	Conseil	
19.12.2008	CN	Adoption.

Conseil prioritaire
Conseil national

Cosignataires (28)
Allemann Evi Aubert Josiane Bruderer Wyss Pascale Carobbio Guscetti Marina Daguet André Fehr Hans-Jürg Fehr Jacqueline Graf-Litscher Edith Gross Andreas Jositsch Daniel Kiener Nellen Margret Lumengo Ricardo Marra Ada Nordmann Roger Nussbaumer Eric Pedrina Fabio Rielle Jean-Charles Rossini Stéphane Schenker Silvia Sommaruga Carlo Steiert Jean-François Stöckli Hans Stump Doris Thanei Anita Tschümperlin Andy Voruz Eric Widmer Hans Wyss Ursula

Descripteurs (en allemand): Aide
Patient/in Krankenkasse Datenschutz Versicherungsaufsicht Personendaten medizinische Diagnose Kampf gegen die Diskriminierung

Indexation complémentaire:
2841

Compétence

Département de l'intérieur

Vous êtes ici: Le Parlement suisse > Recherche > Geschaefte

Annexe 2

Interventions parlementaires concernant la protection des données

09.5060 Question Schenker du 9 mars 2009 "Transfert des données entre les hôpitaux et les caisses-maladie"

L'auteur demande s'il existe des bases légales au niveau du droit fédéral autorisant le transfert des données des assurés entre les hôpitaux et les caisses-maladie.

Réponse du Conseil fédéral du 9 mars 2009

Le Conseil fédéral reconnaît que la situation en matière de protection des données chez certains assureurs nécessite une intervention. C'est pour cette raison que l'OFSP et le PFPDT ont été chargés d'examiner l'ensemble des opérations liées au traitement des données par les assureurs au moyen d'une enquête au niveau national. Les personnes mandatées par les assureurs-maladie sont soumises aux mêmes règles que ces derniers en ce qui concerne l'obligation de garder le secret et la protection des données.

09.1025 Question Heim du 18 mars 2009 "Protection des données de santé"

L'auteur demande si la protection des données est suffisamment garantie dans le cadre de l'utilisation des données de santé par les assureurs privés. Dans leurs conditions générales, ces derniers exigent un accès quasi intégral aux données de santé. En concluant le contrat, l'assuré autorise l'assureur à traiter les données nécessaires, à les transmettre, à des fins de traitement, à des coassureurs ou à des tiers. L'assureur peut en outre se procurer toute information utile auprès des fournisseurs de prestations médicales (médecins, psychologues, laboratoires, hôpitaux), auprès des assureurs sociaux (AVS, AI, LAA, LAMal) et privés, des services administratifs, des employeurs et de tiers. L'assureur peut consulter les dossiers de ses assurés et est libéré de son obligation de confidentialité.

Réponse du Conseil fédéral du 20 mai 2009

En matière d'assurances privées, ni la loi sur le contrat d'assurance (LCA; RS 221.229.1), ni la loi sur la surveillance des assurances (LSA; RS 961.01) ne contiennent de dispositions spécifiques sur la protection des données. Ce sont donc les principes de la LPD qui s'appliquent (proportionnalité, opportunité et transparence). Comme les données de santé sont des données personnelles sensibles nécessitant le consentement éclairé de l'assuré, le devoir d'information de l'assureur doit satisfaire à de hautes exigences. La FINMA ne procède pas à un examen systématique des conditions générales des assureurs privés, mais elle le fait sur demande. Si elle constate qu'une clause contrevient à la protection des données, elle intervient.

09.3515 Interpellation Prelicz-Huber du 8 juin 2009 "Gestion par cas. Atteintes illicites au secret du patient et violation de la protection des données"

L'auteur exprime ses inquiétudes au sujet de la protection des données des assurés dans le cadre du Case Management (gestion par cas). Les spécialistes de la gestion par cas des assureurs-maladie peuvent accéder aux données de santé détenues par les hôpitaux. Les conventions conclues entre les assureurs et les hôpitaux contiennent des dispositions insuffisantes en matière de secret médical et de secret du patient. Les assureurs se procurent des données de santé même sans le consentement des assurés.

Réponse du Conseil fédéral du 26 août 2009

Les dispositions en matière de protection des données (LPD, OLPD, art. 33 LPGA, art. 84 - 84b LAMal, art. 59 et 120 OAMal) sont applicables à la gestion des cas. Les assurés dont les examens et les traitements sont suivis par un gestionnaire de cas doivent consentir librement et de façon expresse à ce suivi ainsi qu'à l'accès aux données concernant leur santé. Ce consentement n'est valable que

s'il est éclairé, c'est-à-dire si l'assuré a reçu une information préalable complète de la part de l'assureur. Les assureurs-maladie sont autorisés à traiter - ou à faire traiter - les données dont ils ont besoin pour accomplir les tâches prévues par la loi, notamment lorsqu'il s'agit d'évaluer le droit aux prestations. Ils doivent respecter le principe de la proportionnalité, c'est-à-dire ne pas demander plus de données que ce dont ils ont besoin pour exécuter leurs tâches.

11.429 Initiative de la CSSS-N du 24 mars 2011 "Tarmed. Compétence subsidiaire du Conseil fédéral"

Dans le cadre de cette initiative, le Parlement a adopté l'art. 42 al. 3bis et 4 LAMal.

11.3393 Motion Cassis du 14 avril 2011 "Vérification des calculs effectués par Swiss DRG et rémunération des hôpitaux par un organe collectif neutre"

L'auteur demande l'instauration d'un organe de révision externe, indépendant du débiteur de la rémunération, pour vérifier le calcul de cette dernière et du caractère économique de la prestation lorsqu'il s'agira d'évaluer les forfaits par cas liés au diagnostic (DRG) pour les séjours hospitaliers en soins somatiques aigus.

Réponse du Conseil fédéral du 16 septembre 2011

Le fournisseur de prestations doit remettre au débiteur de la rémunération (soit à l'assureur en cas de traitement hospitalier) une facture détaillée et compréhensible ainsi que toutes les indications nécessaires pour permettre à ce dernier de vérifier le calcul de la rémunération et le caractère économique de la prestation. Dans le cadre de la mise en œuvre de la nouvelle réglementation du financement hospitalier, le Conseil fédéral a introduit l'art. 59d OAMal dont l'alinéa 2 précise que dans le cas d'un modèle de rémunération lié aux prestations basé sur un système de classification des patients de type DRG, la convention tarifaire comprend en outre le manuel de codage et un concept pour la révision du codage. Le Conseil fédéral estime qu'il appartient aux partenaires tarifaires de décider d'attribuer le mandat de procéder à la révision du codage à des réviseurs indépendants ou de confier plutôt cette tâche à un organisme indépendant des fournisseurs de prestations et des assureurs. Après l'échec de la convention entre H+ et santésuisse, le Conseil fédéral a réglé par voie d'ordonnance les principes de la transmission des données. Pour ce faire, il a pris en considération la protection des données et la tâche des assureurs relative au contrôle des factures. La révision de l'OAMal a été adoptée par le Conseil fédéral le 4 juillet 2012 (RO 2012 4089).

11.3622 Interpellation Cassis du 16 juin 2011 "Système des forfaits par cas Swiss DRG. Protection des données et de la personnalité

L'auteur s'inquiète de la transmission systématique de diagnostics et de codes de procédure sous une forme non pseudonymisée dans le cadre de l'introduction de la structure tarifaire Swiss DRG.

Réponse du Conseil fédéral du 16 septembre 2011
La protection des données revêt une importance capitale pour le Conseil fédéral. Dans le cadre des adaptations d'ordonnance relatives au financement hospitalier, il a complété l'art. 59 OAMal qui impose au fournisseur de prestations d'établir deux factures distinctes, l'une pour les prestations à la charge de l'assurance obligatoire des soins, l'autre pour les prestations à la charge de l'assurance complémentaire (art. 59 al. 3 OAMal). Par ailleurs, les données relatives au diagnostic doivent être conservées sous forme pseudonymisée et cette pseudonymisation ne peut être levée que par le médecin-conseil de l'assureur.

11.3646 Motion du Groupe socialiste du 16 juin 2011 "Forfaits par cas. Mettre en place un système adapté au patient, aux besoins du personnel et aux exigences de qualité"

La motion concerne l'introduction des forfaits par cas au 1er janvier 2012. L'auteur demande entre autres que la protection des données soit garantie, que la communication systématique de diagnostics

et de procédures soit interdite et que toutes les autres informations soient évaluées par des médecins-conseils indépendants.

Réponse du Conseil fédéral du 7 septembre 2011

Comme pour l'interpellation Cassis (11.3622), le Conseil fédéral expose que l'art. 59 al. 3 OAMal exige du fournisseur de prestations l'établissement de deux factures séparées, l'une pour les prestations à la charge de l'assurance de base, l'autre pour les prestations à la charge de l'assurance complémentaire. Les données relatives au diagnostic doivent être conservées sous forme pseudonymisée et cette pseudonymisation ne peut être levée que par le médecin-conseil de l'assureur. Pour traiter les données relatives au diagnostic, les assureurs doivent prendre les mesures techniques et organisationnelles nécessaires. *Cette motion a été rejetée le 19 septembre 2011.*

11.3674 Motion du Groupe des Verts du 17 juin 2011 "Assurer la qualité du nouveau financement hospitalier"

Dans le cadre de l'introduction du système Swiss DRG, l'auteur demande entre autres que le transfert systématique des données sensibles du patient à un assureur-maladie ou à toute autre personne ou institution respecte les recommandations du préposé fédéral à la protection des données et à la transparence.

Réponse du Conseil fédéral du 16 septembre 2011

Le Conseil fédéral relève que la condition évoquée dans la motion est déjà applicable de manière générale aux fournisseurs de prestations et aux assureurs.

11.3785 Motion Heim du 14 septembre 2011 "Pour la protection du secret du patient et du secret médical"

L'auteur demande que parallèlement à l'introduction des Swiss DRG, les conventions passées entre les fournisseurs de prestations, les caisses et les cantons règlent la nature et l'étendue de la transmission des données de manière à préserver et à garantir le secret médical, la protection des données et la protection de la personnalité. Il faut renforcer la révision du codage et prévoir un système doté d'un organe indépendant.

Réponse du Conseil fédéral du 9 décembre 2011

Le Conseil fédéral accorde une grande importance à la protection des données dans le cadre de la transmission de données entre hôpitaux et assureurs à la suite de l'introduction de la structure tarifaire Swiss DRG. Différentes mesures de renforcement du contrôle des factures respectant la protection des données sont en cours de préparation. Le Conseil fédéral rappelle qu'il convient de distinguer les deux tâches légales qui consistent, pour l'une, à contrôler les factures (art. 42 LAMal), et pour l'autre, dans le cas d'un modèle de rémunération de type DRG, à réviser le codage (art. 59d al. 2 OAMal). La révision du codage a pour objectif le contrôle et l'évaluation de la qualité du codage dans les hôpitaux. Elle n'a lieu en principe qu'une fois par année et sous la forme d'un contrôle par échantillonnage. Dans le cadre de sa décision d'approbation du 6 juillet 2011 concernant la structure tarifaire Swiss DRG 1.0, le Conseil fédéral a approuvé le manuel de codage ainsi que le concept pour la révision du codage sous la forme d'un contrôle par des réviseurs indépendants.

Après l'échec de la convention entre H+ et santésuisse, le Conseil fédéral a réglé par voie d'ordonnance les principes de la transmission des données. Pour ce faire, il a pris en considération la protection des données et la tâche des assureurs relative au contrôle des factures. La révision de l'OAMal a été adoptée par le Conseil fédéral le 4 juillet 2012 (RO 2012 4089). Le 20 novembre 2012, le DFI a adopté l'ordonnance sur les fichiers de données pour la transmission des données entre fournisseurs de prestations et assureurs (RS 832.102.14).

11.5422 Question Cassis du 21 septembre 2011 "La protection des données vidée de sa substance par une circulaire"

L'auteur demande si la circulaire 7.1 de l'OFSP du 25 août 2011 porte atteinte à la protection des données et à la décision du Parlement de septembre 2007 aux termes de laquelle les diagnostics et les procédures ne doivent pas figurer systématiquement sur les factures DRG.

Réponse du Conseil fédéral du 26 septembre 2011

La circulaire 7.1 de l'OFSP répète ce que prévoit l'art. 42 LAMal et rappelle l'obligation légale des fournisseurs de prestations de livrer aux assureurs toutes les informations dont ces derniers ont besoin. Elle ne prescrit pas le transfert systématique des données du patient. Dans un arrêt de principe du 29 mai 2009, le Tribunal administratif fédéral a statué que les dispositions en vigueur autorisent une réglementation par convention tarifaire prévoyant la transmission systématique de certains renseignements médicaux si les principes généraux (notamment celui de la proportionnalité) sont respectés. La circulaire rappelle que l'assureur peut demander des informations nécessaires au contrôle de la facture et qu'il a le droit de différer le paiement jusqu'à ce qu'il les ait obtenues.

11.5454 Question Glauser-Zufferey du 21 septembre 2011 "Transmission des données dans le domaine médical"

L'auteur demande si la circulaire 7.1 de l'OFSP du 25 août 2011 viole le secret médical.

Réponse de l'OFSP du 26 septembre 2011

La circulaire 7.1 de l'OFSP répète ce que prévoit l'art. 42 LAMal et rappelle l'obligation légale des fournisseurs de prestations de livrer aux assureurs toutes les informations dont ces derniers ont besoin. Elle ne prescrit pas le transfert systématique des données du patient.

12.5107 Question Steiert du 7 mars 2012 "Chantage effectué par certains assureurs pour obtenir des données de patients"

L'auteur demande si la pratique des assureurs, qui consiste à refuser de rembourser les hôpitaux tant que les données des patients ne leur sont pas transmises de manière non cryptée, est légale.

Réponse du Conseil fédéral du 12 mars 2012

Les assureurs ont l'obligation légale de contrôler les factures, c'est-à-dire de vérifier le calcul de la rémunération et le caractère économique de la prestation. Après l'échec de la convention entre les partenaires tarifaires (H+ et santésuisse), le Parlement a adopté le 23 décembre 2011 l'art. 42 al. 3bis et 4 LAMal qui contraint les fournisseurs de prestations à faire figurer dans la facture les diagnostics et les procédures sous forme codée. Cette disposition légale délègue au Conseil fédéral la compétence d'édicter des dispositions détaillées sur la collecte, le traitement et la transmission des données. Le Conseil fédéral a adopté les dispositions correspondantes de l'ordonnance le 4 juillet 2012.

12.5124 Question Kessler du 7 mars 2012 "Diffusion de données sensibles des patients"

Des organisations de patients ont conseillé aux assurés de ne remettre les données sensibles qu'au médecin-conseil. L'auteur demande comment l'OFSP peut garantir que les données non cryptées ne sortiront pas des services du médecin-conseil.

Réponse du Conseil fédéral du 12 mars 2012

L'OFSP examine régulièrement, au moyen d'enquêtes détaillées auprès des assureurs, si le médecin-conseil répond aux exigences légales. Dans le cadre de ses audits, l'OFSP contrôle en particulier que les locaux et les infrastructures des médecins-conseils permettent de garantir leur indépendance vis-

à-vis des assureurs et de traiter les données des patients de manière confidentielle. Il vérifie aussi comment est réglementé l'accès au courrier et comment est organisé le classement des données personnelles.

12.5193 Question Rossini du 30 mai 2012 "Caisses-maladie et protection des données"

L'auteur demande si la pratique des caisses qui utilisent les données de santé de leurs assurés à des fins commerciales est légale.

Réponse du Conseil fédéral du 4 juin 2012

En tant qu'organes exécutant l'assurance-maladie sociale, les assureurs sont soumis à la LPD. Conformément à cette loi, ils ne peuvent traiter les données personnelles des assurés que dans le but pour lequel les données ont été collectées. L'assureur qui utiliserait à des fins commerciales des données dont il a eu connaissance dans le cadre de son obligation légale de contrôler l'efficacité et le caractère approprié et économique d'une prestation médicale contreviendrait aux dispositions applicables en matière de protection des données.

12.441 Initiative parlementaire Neirynck du 13 juin 2012 "Pour la création d'une base nationale d'imagerie médicale"

Cette initiative parlementaire a pour objet la création d'une base nationale informatisée comportant un dossier pour chaque personne soumise à l'obligation de s'assurer. Chaque dossier recueille la totalité des données d'imagerie médicale effectuées pour ce patient. L'accès à cette base de données est réservé au personnel médical moyennant accord du patient. L'initiative a entre autres pour but de garantir le secret médical et les principes de la LPD.

12.3655 Postulat de la CSSS-N du 29 juin 2012 "Transfert des données entre hôpitaux et assureurs. Création d'un organe de triage indépendant"

L'auteur du postulat demande au Conseil fédéral d'exposer dans un rapport le potentiel d'efficacité d'un organe de triage indépendant chargé du transfert des données entre les hôpitaux et les assureurs, les risques inhérents à l'activité de cet organe et la faisabilité du projet. Dans son rapport, le Conseil fédéral doit analyser entre autres les expériences faites dans les autres Etats, le rapport coût/utilité d'un tel organe, la protection des données et le secret médical ainsi que la contribution de cet organe au processus de vérification du caractère économique des prestations. Le Conseil fédéral devra aussi comparer la création d'un tel organe avec celle d'un bureau certifié auprès de chaque assureur.

Réponse du Conseil fédéral du 29 août 2012

Le Conseil fédéral a adopté le 4 juillet 2012 une modification de l'OAMal (RO 2012 4089) qui est entrée en vigueur le 1er janvier 2013. Cette modification spécifie que les assureurs ont jusqu'au 31 décembre 2013 pour disposer d'un service de réception des données et le faire certifier. L'introduction de ces services de réception des données garantira le respect de la protection des données. Il est par conséquent nécessaire d'attendre que ces services aient fonctionné un certain temps avant de pouvoir comparer cette expérience avec la création d'un organe de triage indépendant.

Annexe 3

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 Berne, OFSP

Aux assureurs LAMal

Référence du document :
Votre référence :
Notre référence : Lp
Berne, 25 août 2011

Circulaire 7.1 : Assureurs-maladie : organisation et processus conformes à la protection des données

Madame, Monsieur,

Vous trouverez, jointe au présent courrier, la nouvelle circulaire 7.1, *Assureurs-maladie : organisation et processus conformes à la protection des données*, ainsi que ses annexes 1 à 7. Elle remplace la circulaire 7.1 du 9 mars 2005, *Protection des données et de la personnalité*, et peut être consultée à l'adresse suivante :
http://www.bag.admin.ch/themen/krankenversicherung/02874/02877/06501/index.html?lang=fr

La circulaire 7.1 dresse l'inventaire des principes et des prescriptions en matière de protection des données qui s'appliquent aux assureurs-maladie. Sur la base de ce document, nous vous contacterons **en octobre**, dans le cadre d'une nouvelle enquête, pour savoir quelles mesures vous aurez prises ou compterez encore prendre. Des corrections seront ordonnées si nécessaire et leur mise en œuvre sera contrôlée. Cette façon de procéder est en relation avec l'adoption du postulat Heim (08.3493 Protection des données des patients et protection des assurés, adoption CN 12.12.2008)[1], les résultats de l'enquête sur la protection des données publiée le 16 juin 2009 par

[1] Le postulat demande au Conseil fédéral de présenter les mesures prévues pour lutter contre la discrimination dont sont victimes certains groupes de patients et garantir la protection des données relatives aux patients chez les assureurs.

Office fédéral de la santé publique OFSP
Patricia Leiber
Hessstrasse 27E, CH-3003 Berne
Adresse postale: CH-3003 Berne
tél. +41 31 322 92 23, fax +41 31 323 00 60
Patricia.Leiber@bag.admin.ch
www.bag.admin.ch

l'OFSP/PFPDT[2] ainsi que les nouvelles dispositions relatives à la protection des données, notamment en vue de l'introduction, à partir du 1er janvier 2012, de la compensation des risques affinée et des forfaits par cas en fonction des diagnostics dans le cadre du nouveau financement hospitalier.

Nous vous prions d'agréer, Madame, Monsieur, nos salutations distinguées.

Division Surveillance de l'assurance
La responsable,

Helga Portmann

Annexes : Circulaire 7.1 et annexes 1 à 7

[2] Consultable sur le site de l'OFSP à l'adresse suivante :
http://www.bag.admin.ch/themen/krankenversicherung/00295/index.html?lang=fr

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 Berne, OFSP

Aux assureurs LAMal

Référence du document:
Votre référence:
Notre référence: Lp/AGM/BEJ/TRE
Berne, le 25 août 2011

Circulaire n° :	**7.1**
Entrée en vigueur :	**1er septembre 2011**

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

La présente circulaire remplace la circulaire 7.1 du 9 mars 2005 (*Protection des données et de la personnalité*). Elle s'appuie sur les résultats d'une enquête effectuée le 4 décembre 2007 par l'OFSP/le Préposé fédéral à la protection des données et à la transparence (PFPDT) auprès des assureurs-maladie et publiée le 16 juin 2009[1]. Elle a pour but de rappeler aux assureurs les principes et les prescriptions en vigueur en la matière afin d'optimiser la protection et la sécurité des données dans leurs activités.

1. Contexte

L'enquête réalisée le 4 décembre 2007 par l'OFSP/le PFPDT sur la protection des données montre que les assureurs-maladie sont sensibilisés à cette question et que la protection des données est garantie dans une large mesure malgré des structures organisationnelles très disparates. Il ressort toutefois également que des améliorations sont possibles dans certains domaines sensibles. Parallèlement à la publication des résultats de l'enquête, les présentes recommandations ont été formulées dans le sens suivant :

[1] http://www.bag.admin.ch/themen/krankenversicherung/00295/index.html?lang=fr

Office fédéral de la santé publique
Hessstrasse 27E, CH-3003 Berne
Adresse postale: CH-3003 Berne
Tél. +41 31 323 70 66, fax +41 31 323 00 60
www.bag.admin.ch

- 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).
- 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.

L'OFSP part du principe que les assureurs-maladie ont déjà pris – ou sont sur le point de prendre – 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 7 renvoient les assureurs aux dispositions en vigueur sur la protection des données qui ressortent des différents actes fédéraux2. Les nouvelles dispositions apparaissent en caractères gras. Ces dispositions revêtent une importance d'autant plus grande en vue de l'introduction des forfaits liés au diagnostic dans le cadre du nouveau financement hospitalier.

2. Concept de protection et de sécurité des données

LAMal **84*b*** (nouveau, entrée en vigueur le 1er janvier 2012) / LPD 2, 3, 4, 5, 7 / OLPD 8 à 10, 20 et 21

L'OFSP recommande aux 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 est organisée 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 nouveau LAMal).

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

---

[2] Cf. annexes 1 et 2

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/themen/00794/01154/01236/01237/index.html?lang=fr

3. Règlement de traitement

LAMal **84*b*** (nouveau, entrée en vigueur le 1er janvier 2012) / OLPD 21

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.

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*** (nouveau) 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 nouvelle disposition, les assureurs doivent, à partir du 1er janvier 2012, soumettre *automatiquement pour avis* au PFPDT leur règlement de traitement. Celui-ci est cependant applicable dès que l'assureur le déclare contraignant

En outre, les assureurs doivent publier leur règlement de traitement dès le 1er janvier 2012, 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.

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

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

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, et tout risque de conflit d'intérêts doit être évité de par sa position organisationnelle. 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/themen/00794/01609/01611/index.html?lang=fr

5. Externalisation

LAMal 84 / LPD 10*a*

L'externalisation consiste à confier à un prestataire extérieur des prestations fournies jusque-là par les assureurs eux-mêmes ainsi que des prestations qu'ils ne fournissaient pas jusqu'ici et qu'ils font effectuer par un prestataire.

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). 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. Les personnes de liaison, 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 doivent également être soumis au *secret professionnel* ainsi qu'au droit spécifique à la protection des données de l'assureur. Les collaborateurs du prestataire doivent s'engager contractuellement à respecter le secret, le cas échéant en signant chacun un contrat.

L'assureur doit s'assurer que le prestataire *garantit la sécurité 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 res-

pecte 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'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.

Pour cette raison, il faut renoncer, dans la mesure du possible, à externaliser à l'étranger des domaines comportant des données sensibles. Si, exceptionnellement, tel est le cas, l'assureur doit notamment veiller à respecter l'art. 6 LPD (communication transfrontière de données seulement à certaines conditions et en informant le PFPDT).

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.

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

CP 321 / LAMal 57, 56 et 42, al.5 / OAMal 59

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, entrée en vigueur le 1er janvier 2012). 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).

Avec l'introduction des forfaits par cas liés au diagnostic au 1er janvier 2012, les assureurs auront besoin, pour contrôler les factures et l'économicité, des données relatives au diagnostic afin de pouvoir appliquer les nouveaux forfaits (diagnostics principal et secondaire, procédures). Ils doivent garantir qu'ils utiliseront les données personnelles sensibles exclusivement aux fins prévues par la loi. Les

assureurs appliquent les mesures techniques et organisationnelles nécessaires visées à l'art. 20 OLPD (art. **59, al. 1bis**, OAMal). En outre, pour la conservation des données relatives au diagnostic, l'identité de l'assuré est pseudonymisée. *Seul le médecin-conseil de l'assureur peut décider de la levée de la pseudonymisation* (art. **59, al. 1ter**, OAMal).

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 donnée personnelle sensible 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*. Ceux-ci ne doivent pas assumer des tâches qui ne sont pas compatibles les unes avec les autres (p. ex., une pour le service du médecin-conseil, l'autre pour la division des prestations).

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.

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

LAMal 42, al. 3 – 5 / LAMal 57, al. 4 et 6 / OAMal 59

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. 4, LAMal, prévoit en outre que l'assureur peut exiger un diagnostic précis ou 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. Dans ce dernier 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, 2ème 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. 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'assureur3. Les dispositions imposant aux fournisseurs de prestations l'obligation de transmettre toutes les données pertinentes pour les prestations ont aujourd'hui déjà une grande portée. Leur importance va encore s'accroître dans la perspective du contrôle de la facturation et du caractère économique pour les forfaits par cas liés au diagnostic dans le cadre du nouveau financement hospitalier. 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. Dans l'optique de l'introduction du nouveau financement hospitalier, des audits spéciaux seront réalisés par échantillonnages pour examiner la manière dont les assureurs-maladie traitent les données personnelles liées au diagnostic.

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 (délit) punissable (art. 92, let. c, LAMal) et que le non-respect des prescriptions légales en matière de protection des données entraîne, selon la nature et la gravité des manquements, des sanctions selon l'art. 21, al. 5 et 5bis, LAMal. Les mesures prises pourront également être rendues publiques.

Unité de direction Assurance maladie et accidents
Le responsable

Andreas Faller
Vice-directeur
Membre de la direction

Division Surveillance de l'assurance
La responsable

Helga Portmann

Annexes : Annexes 1 à 7

[3] 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

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)
- Ordonnance du 14 février sur la carte d'assuré pour l'assurance obligatoire des soins (OCA ; RS 832.105)
- 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 29 septembre 1995 sur les prestations de l'assurance des soins (OPAS ; RS 832.112.31)
- 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

LPGA 28, 31, 32, 33, 47 / OPGA 8, 9 / LAMal 42 al. 3 à 5, 42*a*, **57 al.** 6, **7**[4] et 8, 82, **84**[5], **84*a***[6], **84*b***[7], 92 / OAMal 6*a*, **28** et **28*a***[8], **59**[9], 76, 120 / LPD 2, 3, 4, 5, 7, 8, **9**[10], 10*a*, 11, 11*a*, 16, 17, **18*a***[11], **18*b***[12], 19, 20, 22, 25, 27, 35 / OLPD 1, 2, 8, 9, 10, 12*a*, 12*b*, 16, 18, 20, 21, 22, 23, **24**[13], 28, 34, 35 / 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[14] et les profils de la personnalité[15] 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 et uniquement *à titre exceptionnel,* 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 et entrera en vigueur au 1er janvier 2012 (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 acquisition 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. 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).

---

[4] Art. 57, al. 7, LAMal (complété) : entrée en vigueur le 1.1.2012, FF 2008 19

[5] Art. 84, phrase d'introduction et let. i, LAMal (complété) : entrée en vigueur le 1.1.2012, FF 2008 19

[6] Art. 84*a*, al. 1, phrase d'introduction et let. f : en vigueur depuis le 1.1.2009

[7] Art. 84*b* LAMal (nouveau) : entrée en vigueur le 1.1.2012, FF 2008 19

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

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

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

[11] Art. 18*a* LPD (nouveau) : en vigueur depuis le 1.12.2010

[12] Art. 18*b* LPD (nouveau) : en vigueur depuis le 1.12.2010

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

[14] 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.

[15] 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.

- 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 peuvent être conservées uniquement dans les proportions et la durée fixées par la loi.

- 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, DSG). 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 assureurs-maladie doivent *tenir un inventaire de toutes les* ***banques de données*** 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[16], 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)[17].

- Le personnel des assurances-maladie est **tenu de garder le secret**, conformément à l'art. 33 LPGA. Le non-respect de cette obligation peut entraîner des poursuites pénales (art. 92, let. c, LAMal). En outre, les personnes autorisées doivent avoir accès uniquement aux données personnelles dont elles 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. **84*a*** 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. **84*a*** 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 autre compagnie d'assurance 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 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.

---

[16] Cf. annexe 3

[17] Cf. annexe 4

- 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/themen/00794/01609/01610/index.html?lang=fr

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

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

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 ;
- Contrôler et harmoniser en permanence les dispositions internes relatives à la protection des données en fonction de l'évolution du droit ;
- Former et soutenir les collaborateurs dans tous les aspects de la protection des données. Garantir la transmission rapide des informations avec 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 ;
- Garantir la mise à jour régulière des réglementations relatives au traitement et des fichiers comprenant des données personnelles sensibles ;
- Dresser l'inventaire des fichiers utilisés. 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

LPD 11 et 11*a*, al. 5, let. f / 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). Ces organismes indépendants doivent être agréés par le service d'accréditation suisse SAS.

La certification au sens de l'Ordonnance sur les certifications en matière de protection des données (OCPD) se base sur les 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/org/00828/index.html?lang=fr

Les directives tiennent compte des normes internationales relatives aux systèmes de gestion, en particulier d'ISO/CEI 27001:2005.

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 de l'article 59 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.

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 (entre CHF 35'000.00 et CHF 120.000.00 pour l'entreprise dans son ensemble et entre CHF 25'000.00 et CHF 35'000.00 pour des domaines particuliers). 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 (14 à 45 journées-hommes pour une entreprise moyenne).

Pour le maintien de sa validité, les coûts des audits intermédiaires annuels (entre CHF 8'000.00 et CHF 25'000.00 selon la taille de l'entreprise) et les ressources personnelles à prévoir pour l'exécution des audits intermédiaires (entre 1 ½ et 4 ½ journées-homme) 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. – 2 à 5 journées-homme par année)

sont à prendre en considération. Pour l'exécution de ces tâches, l'assureur devrait désigner un conseiller à la protection des données[18] (env. 10 à 25 % journée-homme par année).

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/index.html?lang=fr

[18] Voir annexe 3

Annexe 5 : Gestion des cas

De nombreuses personnes sont assurées auprès de caisses-maladies qui 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-maladie, des conflits d'intérêts peuvent survenir. Il importe donc d'observer scrupuleusement les **principes de la finalité et de la transparence**. Il faut en particulier noter que les assureurs-maladie 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-maladie. *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.

Annexe 6 : Questionnaires relatifs à l'état de santé

Cst. 5 / LAMal 4, al. 2 / OAMal 6*a*, al. 1

Les questions concernant l'état de santé des personnes requérant leur affiliation à l'assurance obligatoire des soins sont contraires à la LAMal 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 4, al. 2, LAMal, 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

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

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 respecter 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 4, al. 2, LAMal, 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. 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 4

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 Berne, OFSP

Aux assureurs LAMal

Référence du document :
Votre référence :
Notre référence : Lp
Berne, le 17 juin 2013

Circulaire 7.1 : Assureurs-maladie : organisation et processus conformes à la protection des données

Madame, Monsieur,

Vous trouverez, jointe au présent courrier, la nouvelle circulaire 7.1, *Assureurs-maladie : organisation et processus conformes à la protection des données*, ainsi que ses annexes 1 à 8. Elle remplace la circulaire 7.1 du 25 août 2011 et tient compte des modifications de la Loi fédérale du 18 mars 1994 sur l'assurance-maladie (art. 42, al. 3bis – 4 LAMal ; RS 832.10) et de l'Ordonnance du 27 juin 1995 sur l'assurance-maladie (art. 59 ss OAMal ; RS 832.102) au 1er janvier 2013. Ces adaptations concernent la protection des données dans le cadre de la facturation dans le cas d'un modèle de rémunération de type DRG. Elles sont expliquées aux pages 2, 5, 6 et 7 de la circulaire et dans ses annexes 4 et 8.

Nous vous prions d'agréer, Madame, Monsieur, nos salutations distinguées.

Division Surveillance de l'assurance
La responsable,

Helga Portmann

Annexes : Circulaire 7.1 et annexes 1 à 8

Office fédéral de la santé publique OFSP
Patricia Leiber
Hessstrasse 27E, CH-3003 Berne
tél. +41 31 322 92 23, fax +41 31 323 00 60
Patricia.Leiber@bag.admin.ch
www.bag.admin.ch

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 Berne, OFSP

Aux assureurs LAMal

Référence du document:
Votre référence:
Notre référence: Lp/NME
Berne, le 17 juin 2013

Circulaire n° :	**7.1**
Entrée en vigueur :	**1er juillet 2013**

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

La présente circulaire remplace la circulaire 7.1 du 25 août 2011 (*Assureurs-maladie : organisation et processus conformes à la protection des données*). Elle tient compte des modifications de la Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal ; RS 832.10) et de l'Ordonnance du 27 juin 1995 sur l'assurance-maladie (OAMal ; RS 832.102) au 1er janvier 2013. Elle a pour but de rappeler aux assureurs-maladie les principes et les prescriptions en vigueur en la matière afin d'optimiser la protection et la sécurité des données dans leurs activités.

1. Contexte

L'enquête réalisée le 4 décembre 2007 par l'OFSP/le PFPDT sur la protection des données montre que les assureurs-maladie sont sensibilisés à cette question et que la protection des données est garantie dans une large mesure malgré des structures organisationnelles très disparates. Il ressort toutefois également que des améliorations sont possibles dans certains domaines sensibles. Parallèlement à la publication des résultats de l'enquête, les présentes recommandations ont été formulées dans le sens suivant :

Office fédéral de la santé publique
Hessstrasse 27E, CH-3003 Berne
Adresse postale: CH-3003 Berne
Tél. +41 31 323 70 66, fax +41 31 323 00 60
www.bag.admin.ch

- 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).
- 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.

L'OFSP part du principe que les assureurs-maladie ont déjà pris – ou sont sur le point de prendre – 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 fédéraux1. Les nouvelles dispositions 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 le 4 juillet 2012 les articles 59 ss OAMal avec effet au 1er janvier 2013. 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

LAMal **84*b*** (nouveau, entrée en vigueur le 1er janvier 2012) / LPD 2, 3, 4, 5, 7 / OLPD 8 à 10, 20 et 21

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 est organisée 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 nouveau LAMal).

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

[1] Cf. annexes 1 et 2

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/themen/00794/01154/01236/01237/index.html?lang=fr

3. Règlement de traitement

LAMal **84*b*** (nouveau, entrée en vigueur le 1er janvier 2012) / OLPD 21

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.

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*** (nouveau) 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 nouvelle disposition, les assureurs doivent, à partir du 1er janvier 2012, soumettre *automatiquement pour avis* au PFPDT leur règlement de traitement. Celui-ci est cependant applicable dès que l'assureur le déclare contraignant

En outre, les assureurs doivent publier leur règlement de traitement dès le 1er janvier 2012, 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.

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

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

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, et tout risque de conflit d'intérêts doit être évité de par sa position organisationnelle. 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/themen/00794/01609/01611/index.html?lang=fr

5. Externalisation

LAMal 84 / LPD 10*a*

L'externalisation consiste à confier à un prestataire externe des prestations fournies jusque-là par les assureurs eux-mêmes ainsi que des prestations qu'ils ne fournissaient pas jusqu'ici et qu'ils font effectuer par un prestataire.

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). 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. Les personnes de liaison, 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 doivent également être soumis au *secret professionnel* ainsi qu'au droit spécifique à la protection des données de l'assureur. Les collaborateurs du prestataire doivent s'engager contractuellement à respecter le secret, le cas échéant en signant chacun un contrat.

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 pres-

tataire 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'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.

Pour cette raison, il faut renoncer, dans la mesure du possible, à externaliser à l'étranger des domaines comportant des données sensibles. Si, exceptionnellement, tel est le cas, l'assureur doit notamment veiller à respecter l'art. 6 LPD (communication transfrontière de données seulement à certaines conditions et en informant le PFPDT).

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, ne sont pas applicables au service de réception des données, car il ne s'agit pas d'une externalisation facultative mais d'une obligation légale de l'assureur pour renforcer la protection des données. L'assureur ne peut pas donner de directives au service de réception des données afin que des données figurant sur des factures lui soient communiquées. Il s'ensuit que l'assureur ne peut ni contrôler, ni avoir accès à des données dont la confidentialité est garantie par le service de réception des données.

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

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

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, entrée en vigueur le 1er janvier 2012). 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 donnée personnelle sensible 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*. Ceux-ci ne doivent pas assumer des tâches qui ne sont pas compatibles les unes avec les autres (p. ex., une pour le service du médecin-conseil, l'autre pour la division des prestations).

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.

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

LAMal 42, **al. 3 – 5** / LAMal 57, al. 4 et 6 / OAMal **59, 59a, 59a bis**

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).

Pour la transmission systématique des diagnostics et des procédures dans d'autres domaines de traitements hospitaliers et dans tout le domaine des traitements ambulatoires, il manque actuellement les 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).

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. 3bis 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. 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. Dans l'optique de l'introduction du nouveau financement hospitalier, des audits spéciaux seront réalisés par échantillonnages pour examiner la manière dont les assureurs-maladie traitent les données personnelles liées au diagnostic.

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 (délit) punissable (art. 92, let. c, LAMal) et que le non-respect des prescriptions légales en matière de protection des données entraîne, selon la nature et la gravité des manquements, des sanctions selon l'art. 21, al. 5 et 5bis, LAMal. Les mesures prises pourront également être rendues publiques.

Unité de direction Assurance maladie et accidents
La responsable a.i.

Sandra Schneider

Division Surveillance de l'assurance
La responsable

Helga Portmann

Annexes : Annexes 1 à 8

[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

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)
- 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

LPGA 28, 31, 32, 33, 47 / OPGA 8, 9 / LAMal 42 **al. 3 à 5**[3], 42*a*, **57 al.** 6, **7**[4] et 8, 82, **84**[5], **84*a***[6], **84*b***[7], 92 / OAMal 6*a*, **28** et **28*a***[8], **59**[9], **59*a ss***[10], 76, 120 / LPD 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 / OLPD 1, 2, 8, 9, 10, 12*a*, 12*b*, 16, 18, 20, 21, 22, 23, **24**[14], 28, 34, 35 / 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 et entrera en vigueur au 1er janvier 2012 (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 acquisition 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

---

[3] Art. 42, al. 3bis 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 et let. i, LAMal (complété) : en vigueur depuis le 1.1.2012

[6] Art. 84*a*, al. 1, phrase d'introduction et let. f : en vigueur depuis le 1.1.2009

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

[8] Art. 28 et 28*a* 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 (nouveau) : en vigueur depuis le 1.12.2010

[13] Art. 18*b* LPD (nouveau) : 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.

informée. 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 peuvent être conservées uniquement dans les proportions et la durée fixées par la loi.

- 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, DSG). 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 assureurs-maladie doivent *tenir un inventaire de toutes les* ***banques de données*** 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].

- Le personnel des assurances-maladie est **tenu de garder le secret**, conformément à l'art. 33 LPGA. Le non-respect de cette obligation peut entraîner des poursuites pénales (art. 92, let. c, LAMal). En outre, les personnes autorisées doivent avoir accès uniquement aux données personnelles dont elles 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 autre compagnie d'assurance 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 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 re-

[17] Cf. annexe 3

[18] Cf. annexe 4

levant 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/themen/00794/01609/01610/index.html?lang=fr

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

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

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 ;
- Contrôler et harmoniser en permanence les dispositions internes relatives à la protection des données en fonction de l'évolution du droit ;
- Former et soutenir les collaborateurs dans tous les aspects de la protection des données. Garantir la transmission rapide des informations avec 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 ;
- Garantir la mise à jour régulière des réglementations relatives au traitement et des fichiers comprenant des données personnelles sensibles ;
- Dresser l'inventaire des fichiers utilisés. 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

OAMal 59a, al. 6 / LPD 11 et 11*a*, al. 5, let. f / 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 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/org/00828/index.html?lang=fr

Les directives s'appuient sur les normes internationales relatives aux systèmes de gestion, en particulier d'ISO/CEI 27001:2005 (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 (2010: entre CHF 35'000.00 et CHF 120.000.00 pour l'entreprise dans son ensemble et entre CHF 25'000.00 et CHF 35'000.00 pour des domaines particuliers). 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 (14 à 45 journées-hommes pour une entreprise moyenne).

Pour le maintien de sa validité, les coûts des audits intermédiaires annuels (2010: entre CHF 8'000.00 et CHF 25'000.00 selon la taille de l'entreprise) et les ressources personnelles à prévoir pour l'exécution des audits intermédiaires (entre 1 ½ et 4 ½ journées-homme) 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. – 2 à 5 journées-homme par année) sont à prendre en considération. Pour l'exécution de ces tâches, l'assureur devrait désigner un conseiller à la protection des données[19] (env. 10 à 25 % journée-homme par année).

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/index.html?lang=fr

[19] Voir annexe 3

Annexe 5 : Gestion des cas

De nombreuses personnes sont assurées auprès d'assureurs-maladie qui 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

Cst. 5 / LAMal 4, al. 2 / OAMal 6*a*, al. 1

Les questions concernant l'état de santé des personnes requérant leur affiliation à l'assurance obligatoire des soins sont contraires à la LAMal 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 4, al. 2, LAMal, 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

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

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 respecter 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 4, al. 2, LAMal, 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. 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

LAMal 42, **al. 3**[bis]/ OAMal **59, 59*a* 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. Les fournisseurs de prestations doivent inscrire sur les factures DRG aussi les diagnostics et les procédures.

Pour qu'un assureur puisse recevoir systématiquement les indications médicales lors d'une facturation dans le cas d'un modèle de rémunération de type DRG, il doit, en date du 31 décembre 2013 au plus tard, disposer d'un service de réception des données certifié selon l'art. **59*a*, al. 6** OAMal (**al. 1 de la disposition transitoire de la modification du 4 juillet 2012**).Tant que l'assureur ne dispose pas d'un service de réception des données certifié, une transmission systématique des indications médicales ne peut se faire qu'au médecin-conseil. Passé ce délai, chaque assureur doit avoir établi un service de réception des données certifié.

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 a une durée de validité de trois ans. Le domaine certifié comprend toutes les procédures de traitement de données (aussi celles effectuées par des prestataires externes) visant la réalisation de l'art. **59a** OAMal. L'organisme de certification peut suspendre ou révoquer une certification lorsque des manquements graves sont constatés qui ne sont pas corrigés dans le délai fixé (art. 9 ss OCPD). Dans un tel cas, les conditions de l'art. **59a, al. 6** OAMal ne seraient plus remplies et les indications médicales (MCD) ne pourraient plus être transmises à l'assureur. Leur transmission systématique au service du médecin-conseil ne sera plus admise dès le 1er janvier 2014. A partir de cette date, les factures de type DRG ne pourront donc plus être reçues que par le service de réception des données, à défaut de quoi les fichiers de données DRG ne pourront plus être transmis à l'assureur ou reçus par ce dernier de manière complète et systématique. Cela vaut également en cas de retrait du certificat de protection des données du service de réception des données. Dans les deux cas, l'assureur ne pourra plus procéder au contrôle systématique des factures selon le système DRG sans le service de réception des données. Sont réservées les mesures du droit de la surveillance que l'OFSP est habilité à prendre en vertu de l'art. 21, al. 5 et 5 [bis] LAMal.

Pendant le délai transitoire de même que lorsque l'assureur a établi un service de réception des données certifié, les fournisseurs de prestations doivent transmettre simultanément les indications administratives et médicales à 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. Une facture dans le cas d'un modèle de rémunération de type DRG contient par conséquent les indications visées à l'art. **59, al.1** OAMal, ainsi que les variables de l'annexe relative à **l'art. 1 de cette ordonnance du DFI**.

3. Service de réception des données

Chaque assureur doit, en date du 31 décembre 2013 au plus tard, disposer d'un service de réception des données certifié (**al. 1 de la disposition transitoire de la modification du 4 juillet 2012**).

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 selon l'art. **59*a*^{ter}, al. 1** OAMal.

Toutes les factures qui ne présentent pas de particularités sont débloquées pour paiement, mais les indications médicales doivent être conservées sous forme cryptée ou pseudonymisée auprès de l'assureur. Ce dernier doit garantir que personne n'ait accès aux indications médicales après le triage et que celles-ci soient 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).

Après le contrôle approfondi des factures qui présentent des particularités, les indications médicales doivent aussi être archivées sous forme cryptée ou pseudonymisée. Le cryptage et la pseudonymisation ne peuvent être levés que par le médecin-conseil (art. **59*a*^{ter}al. 2** OAMal).

Annexe 5

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 Berne,
OFSP

A l'attention des assureurs LAMal

Référence du document:
Votre référence:
Notre référence: AGM/Lp
Berne, 13 décembre 2011

Enquête auprès des assureurs-maladie sur l'organisation et les processus conformes à la protection des données, partie 1

Madame, Monsieur,

Le 25 août 2011, nous vous faisions parvenir la circulaire 7.1 *Assureurs-maladie : organisation et processus conformes à la protection des données* ainsi que ses annexes 1 à 7. Ce document résume les principes et les prescriptions applicables en matière de protection des données. Il est accessible en ligne à l'adresse
http://www.bag.admin.ch/themen/krankenversicherung/02874/02877/06501/index.html?lang=fr.

Partant, et en nous fondant sur l'art. 21, al. 1 et 3, de la loi sur l'assurance-maladie (LAMal), nous souhaitons soumettre à tous les assureurs-maladie le questionnaire ci-joint afin d'évaluer, une nouvelle fois, les mesures que vous avez prises en vue de protéger les données de vos assurés (protection et sécurité des données). Les résultats de cette enquête seront intégrés dans un rapport du Conseil fédéral, rédigé en réponse au postulat Heim (P 08.3493, Protection des données des patients et protection des assurés, adoption par le CN le 12.12.2008)[1]. Une fois le système de forfaits par cas Swiss DRG en place, nous vous proposerons un autre questionnaire pour savoir comment vous garantissez la protection et la sécurité des données dans le cadre des échanges avec les fournisseurs de prestations. Cette enquête interviendra plus tard, car la réglementation relative à la transmission des données déterminantes pour la facturation reste à édicter. Ces dispositions devront ensuite être mises en œuvre par les assureurs-maladie.

[1] Le postulat charge le Conseil fédéral de présenter les mesures prévues pour lutter contre la discrimination de certains groupes de patients et pour garantir la protection des données relatives aux patients chez les assureurs.

Office fédéral de la santé publique OFSP
Patricia Leiber
Hessstrasse 27E, CH-3003 Berne
Adresse postale: CH-3003 Berne
Tel. +41 31 322 92 23, Fax +41 31 323 00 60
Patricia.Leiber@bag.admin.ch
www.bag.admin.ch

Ceci étant, nous vous saurions gré de bien vouloir fournir tous les renseignements exigés dans le présent questionnaire, conformément à l'art. 21, al. 3, LAMal. Nous nous réservons le droit de vous contacter pour toute indication complémentaire et de faire examiner vos informations dans le cadre des contrôles aléatoires menés par la section Audit de notre office.

M[me] Patricia Leiber (031 322 92 23, patricia.leiber@bag.admin.ch) se tient volontiers à votre disposition pour toute question.

Veuillez nous retourner le questionnaire dûment rempli ainsi que les annexes d'ici au 31 janvier 2012 à l'adresse : Office fédéral de la santé publique, section Surveillance juridique AM, à l'attention de M[me] Patricia Leiber, Hessstrasse 27E, 3003, Berne, ou par courriel : patricia.leiber@bag.admin.ch.

Vous remerciant par avance de votre collaboration, nous vous prions d'agréer, Madame, Monsieur, nos salutations distinguées,

Division Surveillance de l'assurance
La responsable,

H Portmann

Helga Portmann

Annexe: Questionnaire

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

Organisation et processus conformes à la protection des données : questionnaire à l'intention des assureurs-maladie
1ère partie

1. Concept de protection des données

1.1. Avez-vous élaboré un concept de protection et de sécurité des données complet au sein de votre organisation ? Si oui, quand a-t-il été établi ou mis à jour ?

1.2. Avez-vous élaboré un concept de protection et de sécurité des données pour certains domaines de votre organisation ?

a) Si oui, pour quels domaines ou activités ? Quand a-t-il été mis à jour ?

b) Quels domaines ou activités ne sont pas encore pris en compte ?

2. Règlements de traitement

2.1. Avez-vous établi un règlement de traitement pour tous les fichiers automatisés qui contiennent des données personnelles sensibles ou des profils de la personnalité, ou qui sont connectés à d'autres fichiers, conformément à l'art. 21 de l'Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11) ?

2.2. Avez-vous élaboré un concept pour les droits d'accès des collaborateurs ?

2.3. Avez-vous établi un règlement pour le traitement des données par le médecin-conseil et le service du médecin-conseil ?

2.4. A quelle fréquence vous assurez-vous que les règlements de traitement sont complets et mis à jour ?

2.5. Avez-vous l'intention de publier les règlements de traitement sur Internet à partir du 1er janvier 2012 ? Si non, quelle autre forme de publication prévoyez-vous ?

3. Fichiers

3.1. Tenez-vous un registre de tous les fichiers à caractère personnel conformément à l'art. 11a de la Loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1) et à l'art. 16 OLPD ?

3.2. Si oui, quand a-t-il été mis à jour pour la dernière fois ?

3.3. Avez-vous fait une demande d'enregistrement pour tous les fichiers à caractère personnel auprès du PFPDT ?

a) Oui

b) Si non, pourquoi ?

3.4. Le PFPDT dispose-t-il des derniers fichiers ?

a) Oui

b) Si non, pourquoi ?

4. Externalisation

4.1. Quels tiers (prestataires) mandatés par vos soins obtiennent les données personnelles de vos assurés ? A quelles fins ?

4.2. Mandatez-vous des prestataires étrangers pour traiter les données personnelles de vos assurés ? Si oui, lesquels et dans quels pays ? A quelles fins ?

4.3. Les prestataires bénéficient-ils d'une certification au sens de l'Ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD ; RS 235.13) ?

4.4. Comment vérifiez-vous que le traitement des données des assurés par les prestataires est conforme à la protection des données ?

4.5. Veuillez joindre au questionnaire un modèle ou une copie d'un tel contrat de collaboration (avec la clause relative à la protection des données).

5. Médecin-conseil et service du médecin-conseil

5.1. A quel service le médecin-conseil au sens de l'art. 57 de la Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal ; RS 832.10) et le service du médecin-conseil sont-ils rattachés au sein de votre entreprise ? Veuillez joindre au questionnaire une copie de l'organigramme correspondant.

5.2. Les auxiliaires du médecin-conseil travaillent-ils exclusivement pour lui ?

a) Oui

b) Si non, quelles autres tâches assument-ils ?

5.3. Les auxiliaires du médecin-conseil ont-ils un cahier des charges écrit (compétences déléguées par le médecin-conseil) ? Si oui, veuillez le joindre au questionnaire.

5.4. Le courrier (électronique également) parvient-il directement au médecin-conseil ?

5.5. Comment l'ouverture de son courrier est-elle réglementée ?

5.6. Comment l'accès à son courrier électronique est-il réglementé ?

5.7. Que se passe-t-il avec le courrier destiné au médecin-conseil en cas d'envoi erroné ou d'ouverture par inadvertance par un autre service ?

5.8. Comment les locaux du médecin-conseil et du service du médecin-conseil sont-ils organisés en termes de protection et de sécurité des données ?

5.9. Comment le classement des données particulièrement sensibles est-il organisé (classement en fonction du caractère sensible des données reçues, au format papier et électronique) ?

5.10. Comment l'accès aux données particulièrement sensibles est-il réglementé ? Qui y a accès (documents papier et documents scannés) ?

5.11. Comment garantissez-vous la concrétisation de l'art. 57, al. 7, LAMal ?

6. Conseiller à la protection des données

6.1. Avez-vous désigné, dans votre entreprise, au moins un conseiller à la protection des données au sens de l'art. 11*a*, al. 5, let. e, LPD ?

6.2. A quel service ce poste est-il rattaché au sein de votre entreprise ? Veuillez joindre au questionnaire une copie de l'organigramme correspondant.

6.3. Avez-vous confié cette tâche à un service externe ? Si oui, lequel ?

6.4. Combien d'équivalent plein-temps employez-vous à cette fin ?

6.5. Les conseillers à la protection des données exercent-ils encore d'autres tâches ? Si oui, lesquelles ?

6.6. Avez-vous déclaré les conseillers à la protection des données auprès du PFPDT ?

6.7. Les conseillers à la protection des données ont-ils un cahier des charges écrit ? Si oui, veuillez le joindre au questionnaire.

6.8. Ces personnes ont-elles suivi une formation spécifique en protection des données ?

6.9. Se perfectionnent-elles dans le domaine de la protection des données ?

6.10. Le conseiller à la protection des données organise-t-il des formations en la matière à l'intention des collaborateurs ? Si oui, à quelle fréquence ? La participation à ces formations est-elle obligatoire pour l'ensemble des collaborateurs de l'entreprise ?

7. Gestion de la protection des données, système d'information et de sécurité des données, certification en matière de protection des données

7.1. Avez-vous soumis vos systèmes et procédures de traitement des données de même que votre organisation dans son ensemble à une procédure de certification en matière de protection des données au sens de l'OCPD ?

a) Oui ; organisme de certification :

b) Non ; raisons :

7.2. N'avez-vous soumis que certains domaines et procédures à une certification en matière de protection des données ?

Si oui, quels domaines et procédures ? Et par quel organisme de certification ?

7.3. Le respect des exigences en matière de protection des données est-il contrôlé au sein de votre entreprise (audits internes) ?

7.4. Par quel service, comment et à quelle fréquence ?

7.5. Qui est le mandant et comment les résultats sont-ils communiqués ?

8. Modèles HMO et du médecin de famille, modèle d’assurance avec conseil médical par téléphone

8.1. Quelles mesures techniques et organisationnelles de sécurité avez-vous prises pour l’échange de données entre les services impliqués (médecins de premier recours / fournisseurs de prestations assurant la coordination, tiers mandatés et services internes de la caisse-maladie, service du médecin-conseil inclus) ?

8.2. Quelles données sont échangées entre les services impliqués ?

8.3. Comment les droits d’accès au dossier de l’assuré sont-ils réglementés ?

9. Gestion des cas par l'assureur-maladie

9.1. A quel service une éventuelle gestion des cas[1] est-elle rattachée au sein de votre entreprise ? Veuillez joindre au questionnaire une copie de l'organigramme correspondant.

9.2. Décrivez le déroulement de la gestion d'un cas, la collaboration avec l'assuré, le médecin-conseil ou le service du médecin-conseil et les fournisseurs de prestations, et joignez en annexe un modèle de déclaration de consentement de l'assuré.

9.3. Comment les droits d'accès à un dossier de gestion des cas sont-ils réglementés ?

[1] Sont entendus tous les types de gestion des cas que l'assureur-maladie propose dans l'assurance obligatoire des soins comme mesure d'optimisation des prestations, de contrôle et de minimisation des coûts.

10. Compensation des risques

10.1. Quelles mesures techniques et organisationnelles de sécurité avez-vous prises, en tant qu'assureur précédent, en lien avec le traitement et la transmission, au service central de transfert, des données des assurés qui changent d'assureur et qui sont pertinentes pour tenir compte du risque de maladie élevé dans la nouvelle compensation des risques en vertu de la modification de la LAMal du 21 décembre 2007 ?

10.2 Quelles mesures techniques et organisationnelles de sécurité avez-vous prises, en tant qu'assureur ultérieur, en lien avec le traitement et la transmission des données que vous avez reçues du service central de transfert, qui concernent les assurés qui changent d'assureur et qui sont pertinentes pour tenir compte du risque de maladie élevé dans la nouvelle compensation des risques en vertu de la modification de la LAMal du 21 décembre 2007 ?

11. Procurations et déclarations de consentement

11.1. Veuillez joindre au questionnaire un modèle de toutes les procurations et déclarations de consentement qui sont soumises aux assurés et autorisent la caisse-maladie à requérir des renseignements auprès de tiers. Il vous faut aussi joindre les modèles concernant les données de l'assurance obligatoire de base si celles-ci sont requises pour les assurances complémentaires.

12. Remarques complémentaires

12.1. Avez-vous des remarques et informations complémentaires ?

13. Coordonnées de la personne responsable en cas de demande de précisions de la part de l'OFSP

Madame/Monsieur .....
Tél. ….....
Courriel ….....
Fonction ….....

Merci de votre participation !