Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Berne, le 23 février 2022

Protection des données des patients et protection des assurés

Rapport complémentaire donnant suite au postulat 08.3493 Heim du 18 septembre 2008

Protection des données des patients et protection des assurés

Condensé

En 2008, le postulat Heim (08.3493 – Protection des données des patients et protection des assurés) a chargé le Conseil fédéral de présenter dans un rapport les mesures prévues pour lutter contre la discrimination dont auraient été victimes certains groupes de patients du fait des formes particulières d'assurance (cf. art. 93 ss OAMal) alors nouvellement mises en place et garantir la protection des données relatives aux patients chez les assureurs-maladie.

Du 4 décembre 2007 au 16 juin 2009, l'Office fédéral de la santé publique (OFSP) et le Préposé fédéral à la protection des données et à la transparence (PFPDT) ont mené la première enquête à l'échelle nationale sur la protection des données. Il en est ressorti que la protection des données des patients était en principe assurée. L'enquête a cependant mis en évidence que certains aspects devaient encore être améliorés. Les résultats ont été publiés le 16 juin 2009 et des recommandations ont été formulées.

La deuxième enquête exhaustive sur la protection des données, qui portait sur la conformité de l'organisation et des processus des assureurs LAMal au droit relatif à la protection des données, a été réalisée entre 2011 et 2012. De plus, les assureurs-maladie ont fait l'objet d'une surveillance continue, aussi bien de la part du PFPDT que de l'OFSP, dans les domaines mentionnés dans le rapport joint.

Les résultats de la deuxième enquête (2011-2012) ont démontré que les assureurs LAMal avaient remédié à la majorité des lacunes constatées et qu'ils faisaient preuve de davantage de professionnalisme à l'égard de la protection des données que lors de la première enquête.

Se fondant sur cette deuxième enquête et sur l'activité de contrôle des autorités de surveillance, à savoir le PFPDT et l'OFSP, le Conseil fédéral a constaté dans son rapport du 18 décembre 2013 (EXE-BRC 2012.2443) que les assureurs LAMal avaient majoritairement pris les mesures nécessaires pour garantir la protection et la sécurité des données. Le rapport relevait cependant que certains points n'étaient pas encore totalement remplis.

Aussi le Conseil fédéral a-t-il chargé l'OFSP et le PFPDT de veiller, dans le cadre de leur activité de surveillance, à ce que les manquements constatés soient corrigés et à ce que les prescriptions en matière de protection des données soient mises en œuvre. Par la suite, le PFPDT et l'OFSP ont procédé à de nombreux contrôles entre 2013 et 2019. Ils ont mené des vérifications assidues et constantes concernant les prescriptions relatives à la protection et à la sécurité des données et fait respecter les piliers de la protection des données.

Comme le rapport du Conseil fédéral du 18 décembre 2013 annonçait une nouvelle enquête sur la protection des données et l'établissement d'un rapport complémentaire du Conseil fédéral, le postulat Heim n'a pas été classé en 2014. Du fait de la surveillance intensive assurée par le PFPDT et l'OFSP depuis 2013, la troisième enquête contenait uniquement des questions sur le thème central du postulat, à savoir la protection des données dans les formes particulières d'assurance.

Trois questions ont ainsi été posées : la première visait à déterminer quelles données sont échangées, et dans quel but, entre les services impliqués (à savoir médecins de premier recours / fournisseurs de prestations assurant la coordination, tiers mandatés et services internes de l'assureur) dans les formes particulières d'assurance. Les participants étaient de plus interrogés sur les canaux (portails / plates-formes, en particulier) utilisés pour ces échanges de données et sur les flux de données qui sont notamment déclenchés lorsque les médecins de premier recours adressent des patients à des confrères (transfert).

La deuxième question portait sur les mesures techniques et organisationnelles prises par les assureurs pour sécuriser les données personnelles sensibles dans les formes particulières d'assurance.

Protection des données des patients et protection des assurés

La troisième question demandait si l'assureur avait la possibilité d'accéder aux systèmes informatiques (par ex. aux systèmes d'information des cabinets) des médecins de premier recours pour consulter les dossiers médicaux des patients.

Les réponses à la question 1 montrent que les données relatives aux effectifs, les transferts (fenêtres temporelles) et les données relatives aux prestations sont échangés entre les assureurs-maladie, les éventuels prestataires externes et les médecins de premier recours. Ces échanges de données ont pour but le contrôle et l'application des règles en matière de transferts stipulées dans les conditions des modèles particuliers d'assurance ainsi que la gestion par les fournisseurs de prestations, lorsque le modèle le prévoit. La transmission se fait par des canaux entièrement sécurisés, c.-à-d. chiffrés (HIN, SFTP, etc.). Une transmission des données sous forme papier n'a lieu que dans de rares cas exceptionnels (du médecin à l'assureur).

Les réponses à la question 2 mettent en évidence que les mesures techniques mises en œuvre (chiffrements, infrastructures dans des zones protégées, connexions sécurisées par certificat, etc.) sont systématiquement conformes à l'état actuel de la technique. Le cercle des personnes disposant d'un droit d'accès et la mise en œuvre des mesures par les prestataires externes sont contrôlés par les assureurs-maladie.

On peut conclure, au vu des réponses obtenues à la question 3, que l'assureur ne peut en aucun cas accéder aux systèmes des médecins de premier recours.

Lorsque le postulat a été déposé, en 2008, la protection des données en était encore au stade de la mise en place. Les première et deuxième enquêtes sur la protection des données, le rapport du Conseil fédéral du 18 décembre 2013 ainsi que la surveillance constante assurée par le PFPDT et l'OFSP ont permis de corriger en continu les manquements qui pouvaient encore être constatés. L'application des prescriptions du droit relatif à la protection des données s'est ainsi généralisée. Elles sont aujourd'hui largement respectées. La troisième enquête sur la protection des données est venue combler la lacune qui concernait notamment le thème central du postulat.

Les résultats de l'enquête de 2019 montrent que les mesures nécessaires ont été prises pour garantir en principe la protection des données dans le domaine des formes particulières d'assurance. La surveillance des assureurs LAMal effectuée par le PFPDT et l'OFSP est suffisante pour garantir que toute lacune dans la protection est identifiée et que les mesures nécessaires peuvent être engagées dans le cadre des compétences de surveillance qui leur sont conférées.

Abréviations

LPGA	Loi fédérale sur la partie générale du droit des assurances sociales
OFSP	Office fédéral de la santé publique
FF	Feuille fédérale
SRD	Service de réception des données
DRG	Diagnosis Related Groups (groupes de cas par diagnostic)
LPD	Loi fédérale sur la protection des données
DFI	Département fédéral de l'intérieur
PFPDT	Préposé fédéral à la protection des données et à la transparence
MF	Médecin de famille
HMO	Health Maintenance Organization (organisation pour le maintien en bonne santé)
HIN	Health Info Net (chiffrement)
MMF	Modèle du médecin de famille
ISO	Organisation internationale de normalisation
LSAMal	Loi fédérale sur la surveillance de l'assurance-maladie sociale
OSAMal	Ordonnance sur la surveillance de l'assurance-maladie sociale
LAMal	Loi fédérale sur l'assurance-maladie
OAMal	Ordonnance sur l'assurance-maladie
RP	Réduction des primes
RVK	Prestataire de services sur le marché suisse de la santé
SFTP	Secure File Transfer Protocol (chiffrement)
SR	Recueil systématique du droit fédéral
SSL	Secure Sockets Layer (chiffrement)
Telmed	Service de conseil médical par téléphone
OCPD	Ordonnance sur les certifications en matière de protection des données

Table des matières

Protection des données des patients et protection des assurés

1 Contexte

Le postulat Heim (08.3493 – Protection des données des patients et protection des assurés) a chargé en 2008 le Conseil fédéral de présenter dans un rapport les mesures prévues pour lutter contre la discrimination dont auraient été victimes certains groupes de patients du fait des formes particulières d'assurance AOS (cf. art. 93 ss OAMal) alors nouvellement mises en place et garantir la protection des données relatives aux patients chez les assureurs-maladie. De 2007 à 2009, une première enquête sur la protection des données a été menée auprès des assureurs LAMal par l'Office fédéral de la santé publique (OFSP) et le Préposé fédéral à la protection des données et à la transparence (PFPDT).

Une deuxième enquête a été menée entre 2011 et 2012 après la publication, le 25 août 2011, de la circulaire 7.1 « Assureurs-maladie : organisation et processus conformes à la protection des données ». Si les résultats étaient fondés pour l'essentiel sur les indications fournies par les assureurs LAMal, il est à noter, par exemple, que la section Audit de l'OFSP avait aussi effectué des contrôles réguliers (par échantillonnages) sur place auprès de ces derniers.

Le rapport du Conseil fédéral en réponse au postulat Heim du 18 décembre 2013 a permis de donner une information complète sur la façon dont les assureurs garantissaient alors la protection des données des patients. Les résultats de la deuxième enquête ont démontré que les assureurs LAMal avaient remédié à la majorité des lacunes constatées et qu'ils faisaient preuve de davantage de professionnalisme à l'égard de la protection des données que lors de la première enquête. De nombreux points avaient été améliorés par rapport à la première enquête de l'OFSP et du PFPDT (2007-2009). D'autres points n'étaient pas encore totalement remplis.

C'est pourquoi le rapport du Conseil fédéral du 18 décembre 2013 a chargé l'OFSP de veiller, dans le cadre de son activité de surveillance, à ce que les manquements constatés soient corrigés. Le rapport indiquait en outre que l'OFSP devrait établir, puis porter à la connaissance du Conseil fédéral et du Parlement, un nouveau rapport sur le sujet dans un délai de trois à cinq ans, raison pour laquelle le postulat Heim n'a pas encore été classé par le Parlement.

Depuis le rapport du Conseil fédéral du 18 décembre 2013, l'OFSP et le PFPDT ont régulièrement surveillé les assureurs LAMal dans les domaines mentionnés dans le rapport joint ; ils ont pu constater que les mesures nécessaires pour garantir la protection des données ont été prises. S'agissant du thème central du postulat, les formes particulières d'assurance, aucune surveillance supplémentaire spécifique n'a été effectuée par l'OFSP et le PFPDT depuis le rapport du Conseil fédéral de 2013.

Mandatées pour mener une troisième enquête et établir un nouveau rapport, les deux autorités ont préparé des questions axées sur les lacunes dans les formes particulières d'assurance, qu'ils ont soumises aux assureurs-maladie. Compte tenu du rapport du Conseil fédéral du 18 décembre 2013 et de la surveillance intensive assurée depuis lors par le PFPDT et l'OFSP, seules des questions relevant du thème central du postulat (la protection des données dans les formes particulières d'assurance) ont été posées pour le rapport complémentaire (cf. ch. 6.1.).

L'analyse des réponses obtenues doit permettre de déterminer s'il reste des points en suspens ou si le postulat Heim peut à présent être classé.

2 Première enquête sur la protection des données (2007-2009)

La première enquête à l'échelle nationale sur la protection des données a été menée du 4 décembre 2007 au 16 juin 2009 par l'OFSP et le PFPDT. Il en est ressorti que les assureurs-maladie étaient sensibilisés à cette question. Les réponses ont permis de constater que la protection des données des patients était en principe assurée malgré des structures organisationnelles très disparates. Cette première enquête a cependant mis en évidence que des améliorations étaient nécessaires dans certains domaines sensibles. L'OFSP et le PFPDT ont également formulé des recommandations lors de la publication des résultats de l'enquête, le 16 juin 2009.

3 Mesures engagées par l'OFSP depuis la première enquête de 2007- 2009

3.1 Circulaire 7.1 du 25 août 2011

L'OFSP a édicté le 25 août 2011 la circulaire « Assureurs-maladie : organisation et processus conformes à la protection des données », qui a été actualisée le 17 juin 2013. Cette circulaire dicte aux assureurs LAMal 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).

Par la même occasion, l'OFSP a annoncé aux assureurs LAMal qu'il leur demanderait quelques mois plus tard, en se référant à la circulaire, quelles démarches ils auraient entreprises et lesquelles ils comptaient encore entreprendre pour mettre en œuvre les recommandations et les prescriptions. Ils ont également été informés que les prescriptions de la circulaire feraient l'objet de contrôles réguliers et d'audits par échantillonnages effectués par la section Audit de l'OFSP.

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

Dans un courrier daté du 13 décembre 2011, 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 concernaient les échanges 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.

3.3 Contrôles des assureurs-maladie effectués sur place par la section Audit de l'OFSP entre 2009 et 2013

Dans le cadre de sa fonction de surveillance, l'OFSP procède régulièrement à des audits. Ces contrôles et échantillonnages auprès des assureurs-maladie ont pour but de contrôler l'application de la loi fédérale sur l'assurance-maladie (LAMal ; *RS 832.10*) et de ses ordonnances ainsi que des instructions données par l'OFSP. Le programme de contrôle porte également sur la protection des données, qui constitue depuis 2012 l'un des thèmes prioritaires des audits. La base de ce contrôle se trouve dans la version en vigueur de la circulaire 7.1.

L'auditeur examine si l'assureur LAMal dispose d'une organisation conforme au droit relatif à 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 loi fédérale sur la partie générale du droit des assurances sociales (LPGA ; *RS 830.1*), de la LAMal et de la loi fédérale sur la protection des données (LPD ; *RS 235.1*) en la matière. Ces audits réalisés sur place par l'OFSP ne sauraient toutefois remplacer une certification au sens de l'art. 11 LPD et ne constituent en aucune manière la base d'une telle certification.

4 Résultats de la deuxième enquête sur la protection des données (2011- 2012) et rapport du Conseil fédéral du 18 décembre 2013

Les résultats de la deuxième enquête sur la protection des données (2011- 2012) se rapportaient aux thèmes suivants : 1. Concepts des assureurs LAMal en matière de protection et de sécurité des données, 2. Règlements de traitement des données et concepts pour les droits d'accès, 3. Registre des fichiers, 4. Externalisation, 5. Médecin-conseil et service du médecin-conseil, 6. Conseiller à la protection des données, 7. Protection des données : systèmes de gestion et certifications, 8. Échange 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]), 9. Gestion des cas, 10. Procurations et déclarations de consentement.

Le rapport faisait état des résultats de l'enquête pour chacun de ces dix thèmes.

Pour synthétiser, il a été constaté que les assureurs LAMal avaient remédié à la majorité des lacunes constatées et qu'ils faisaient preuve de davantage de professionnalisme à l'égard de la protection des données que lors de la première enquête. En ce qui concerne les modèles particuliers d'assurance (question principale du postulat Heim [08.3493]), l'enquête n'a révélé aucun indice concret de traitement des données médicales qui n'aurait pas été en adéquation avec le but visé. De nombreux points avaient été améliorés par rapport à la première enquête, menée aussi conjointement par l'OFSP et le PFPDT entre 2007 et 2009, tandis que d'autres points n'étaient pas encore totalement remplis.

4.1 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 dispose que les fournisseurs de prestations doivent faire figurer dans la facture les diagnostics et les procédures sous forme codée, conformément aux classifications actuelles. Il prévoit en outre que le Conseil fédéral édicte des dispositions détaillées sur la

collecte, le traitement et la transmission des données, dans le respect du principe de la proportionnalité. En vertu de l'al. 4, l'assureur peut exiger des renseignements supplémentaires d'ordre médical.

Le 4 juillet 2012, le Conseil fédéral a ensuite défini à l'art. 59*a* OAMal les modalités de la transmission des données pour les DRG afin que le principe de proportionnalité soit respecté. À partir de 2014 au plus tard, les hôpitaux devraient 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 avaient jusqu'à fin 2013 pour mettre en place ce service et le faire certifier conformément à l'art. 11 LPD. Il a été décidé que la certification serait surveillée par le PFPDT, qui publierait une liste des services de réception des données certifiés.

Le DFI a en outre défini, le 20 novembre 2012, une structure uniforme à l'échelle suisse pour les fichiers de données contenant les indications administratives et médicales 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 ; *RS 832.102.14*). 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 ont suivi et contrôlé la mise en œuvre de ces dispositions par les assureurs LAMal au cours des dernières années.

4.2 Conclusions du rapport du Conseil fédéral du 18 décembre 2013

Se fondant sur cette deuxième enquête et les mesures de contrôle prises par les autorités de surveillance, à savoir l'OFSP et le PFPDT, le Conseil fédéral a constaté que les assureurs LAMal avaient pour l'essentiel pris les mesures nécessaires pour garantir la protection et la sécurité des données et remédié à la majorité des lacunes identifiées. Ils faisaient preuve de davantage de professionnalisme à l'égard de la protection des données que lors de la première enquête.

Le rapport du Conseil fédéral du 18 décembre 2013 a ainsi établi que de nombreux points avaient été améliorés par rapport à la première enquête menée par l'OFSP et le PFPDT entre 2007 et 2009, tout en relevant que certains points n'étaient pas encore totalement remplis.

Aussi l'OFSP et le PFPDT ont-ils été chargés, dans le cadre de leur activité de surveillance, de veiller à ce que les manquements constatés soient corrigés et à ce que les prescriptions en matière de protection des données soient mises en œuvre. Un nouveau rapport sur le sujet devait être établi, puis porté à la connaissance du Conseil fédéral et du Parlement dans un délai de trois à cinq ans. Il a également été constaté que 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.

Le présent rapport complémentaire du Conseil fédéral découle de ce mandat portant sur la réalisation d'une troisième enquête et l'établissement d'un nouveau rapport.

5 Surveillance assurée par le PFPDT et l'OFSP depuis le rapport du Conseil fédéral du 18 décembre 2013

Comme indiqué dans les rapports d'activité du PFPDT à partir de 2013, le préposé a assuré ces dernières années une surveillance de la protection des données chez les assureurs-maladie dans de nombreux domaines : services de réception des données (y c. leur certification), règlements de traitement, facturation dans le domaine SwissDRG, externalisation de la facturation dans le domaine médical, externalisation de tâches des assurances-maladie à des prestataires de services externes à la branche, communication des données de l'assurance-maladie dans le cadre de la réduction des primes, procurations dans le domaine de l'assurance-maladie, guides relatifs aux mesures techniques et organisationnelles de la protection des données ou encore format d'échange de données pour les factures DRG.

Entre 2013 et 2018, la section Audit de l'OFSP a procédé à 42 contrôles en matière de protection des données, qui visaient principalement à vérifier le respect des prescriptions relatives à la protection et à la sécurité des données figurant dans la circulaire 7.1. De 2017 à début 2018, les contrôles ont porté avant tout sur quatre aspects : le système de gestion de la protection des données, le traitement des données personnelles sensibles, l'organisation du service du médecin-conseil et le processus de contrôle SwissDRG hors certification du SRD. Enfin, la thématique de l'externalisation est venue s'y ajouter en 2018. Les auditeurs ont toutefois continué à vérifier le respect des prescriptions de la circulaire 7.1. Conformément à l'art. 84*b* LAMal, les règlements de traitement établis sont évalués par le PFPDT, à qui incombe également la surveillance en matière de certification des services de réception des données (art. 59*a*, al. 7, OAMal). De ce fait, la section Audit de l'OFSP n'a pas effectué de contrôles détaillés dans ces domaines.

Alors que l'OFSP avait réalisé la première enquête conjointement avec le PFPDT entre 2007 et 2009, la collaboration s'est par la suite limitée, pour l'essentiel, à des séances de coordination, par exemple dans le cadre de consultations des offices. Comme on peut le lire dans le rapport d'activités 2016/2017 du PFPDT (cf. point 1.6.2., p. 26), l'objectif de ces séances était de coordonner les activités de surveillance, partiellement redondantes, des deux autorités, et d'aborder des questions en suspens. Au cours de ces années, le PFPDT et l'OFSP sont donc partis du principe qu'il existait un chevauchement des compétences.

Le principe applicable aux contrôles de l'audit de l'OFSP figure actuellement dans la circulaire en vigueur 7.1 de l'OFSP (voir circ. 7.1 du 25 août 2011; circ. 7.1 du 17 juin 2013; circ. 7.1 du 1er novembre 2014 et circ. 7.1 du 17 décembre 2015).

La circulaire 7.1 du 17 décembre 2015 « Assureurs-maladie : organisation et processus conformes à la protection des données » en vigueur jusqu'à fin 2021 a été révisée en profondeur en 2020 et en 2021 et remplacée par la nouvelle circulaire 7.1 « Surveillance par l'OFSP des domaines soumis aux dispositions de la LSAMal, de l'OSAMal, de la LAMal et de l'OAMal relatives à la protection des données » (entrée en vigueur le 1er janvier 2022). Durant cette période, la finalisation du rapport a été suspendue. La révision de la circ. 7.1 a été réalisée en étroite collaboration avec le PFPDT. Les deux autorités ont ainsi également saisi l'occasion pour s'accorder sur leurs compétences. La révision de la circulaire 7.1 a permis de clarifier et de trancher la délimitation de la compétence de la surveillance en matière de protection des données entre le PFPDT et l'OFSP.

6 Troisième enquête sur la protection des données (2019)

6.1 Questions

6.1.1 Question 1

Quelles sont les données échangées, et dans quel but, entre les services impliqués dans les formes particulières d'assurance (LAMal) ?

Par quels canaux (portails / plates-formes, en particulier) ces échanges de données ont-ils lieu ?

Quels sont les flux de données que déclenchent notamment les transferts par les médecins de premier recours ?

Veuillez vous référer notamment aux échanges de données entre les services impliqués (à savoir médecins de premier recours / fournisseurs de prestations assurant la coordination, tiers mandatés [prestataires] et services internes de l'assureur). Merci de joindre, le cas échéant, un schéma représentant les flux de données.

Autrement, nous vous prions de faire apparaître séparément dans votre réponse les éléments suivants : 1. Modèles HMO, 2. Modèles du médecin de famille, 3. Modèles d'assurance avec conseil médical par téléphone, 4. Autres modèles d'assurance et 5. Cabinets de groupe dans lesquels vous seriez éventuellement impliqués.

6.1.2 Question 2

Quelles sont les mesures techniques et organisationnelles que vous avez prises pour sécuriser les données personnelles sensibles dans les formes particulières d'assurance ?

6.1.3 Question 3

L'assureur a-t-il la possibilité d'accéder aux systèmes informatiques (par ex. aux systèmes d'information des cabinets) des médecins de premier recours pour consulter les dossiers médicaux des patients ? Si oui, dans quels cas (suivant l'énumération de la question 2.1) ?

6.2 Résultats de la troisième enquête sur la protection des données (2019)

6.2.1 Généralités

Tous les assureurs qui proposent des formes particulières d'assurance ont répondu aux trois questions. Les groupes d'assurance ont en principe remis une seule réponse pour tous les assureurs impliqués. Ainsi, nous avons reçu des réponses pour 50 assureurs. Sept d'entre eux sont purement des assureurs d'indemnités journalières ou ne proposent pas de formes particulières d'assurance.

Les réponses sont surtout techniques et ne sont pas intégralement restituées dans le rapport, car elles varient en fonction des conditions particulières d'assurance et des produits des différents assureurs. Vous trouverez ci-après un résumé des résultats ainsi que trois exemples qui illustrent des réponses aux questions 1 et 2 et présentent les procédures chez de petits et moyens assureurs qui ont externalisé les contrôles relatifs au respect des formes particulières d'assurance à des prestataires externes et chez des assureurs moyens ou grands qui procèdent eux-mêmes à ces contrôles. Tous les assureurs ont répondu de la même manière à la question 3.

Protection des données des patients et protection des assurés

6.2.2 Réponses à la question 1

De manière générale, on peut constater en résumé que les données relatives aux effectifs, les transferts (fenêtres temporelles) et les données relatives aux prestations sont échangées entre les assureurs-maladie, les éventuels prestataires externes et les médecins de premier recours lorsque le modèle le prévoit. La transmission se fait par des canaux entièrement sécurisés, c.-à-d. chiffrés. Une transmission des données sous forme papier n'a lieu que dans de rares cas exceptionnels (du médecin à l'assureur).

Dans chacune des catégories mentionnées (exemples 1 à 3), un assureur a répondu à la première question de la manière suivante :

1er exemple (externalisation)

L'assureur-maladie transmet au prestataire (partenaire d'externalisation : RVK) des données relatives aux effectifs et aux prestations. Ce dernier traite les données dans son système informatique et les envoie, regroupées par réseau de médecins ou prestataires téléphoniques, au fournisseur informatique désigné par les réseaux, qui importe les données dans ses systèmes et les met à la disposition des médecins ou des prestataires téléphoniques.

Les sociétés d'exploitation (fournisseurs informatiques des réseaux de médecins / prestataires téléphoniques) transmettent mensuellement les transferts saisis dans le système par les médecins au prestataire, qui les entre à son tour sous forme regroupée dans son système informatique et met les données à la disposition de l'assureur-maladie. Des données relatives aux prestations sont également traitées dans les systèmes utilisés par les médecins. Pour les évaluer, le médecin de famille a la possibilité de commander une copie de facture via le prestataire. Celui-ci transmet la commande à la caisse. Dès que le prestataire obtient la copie de facture, il la met à la disposition du médecin via la société d'exploitation.

Les données sur les infractions sont mises à la disposition du prestataire mensuellement par les sociétés d'exploitation. Le prestataire les importe sous forme regroupée dans son système et les communique à la caisse. L'assureur-maladie déclare les infractions sanctionnées aux sociétés d'exploitation, qui en informent les médecins qui leur sont rattachés.

Les prestataires téléphoniques saisissent leurs transferts (fenêtres temporelles), qui sont transmis au prestataire selon la périodicité souhaitée par la caisse-maladie (quotidienne, hebdomadaire, bimensuelle ou mensuelle). Les fenêtres temporelles sont mises en relation avec les données relatives aux prestations et passés dans un système de filtre. Cette procédure permet ainsi aux assureurs de sanctionner toute infraction et de garantir le respect des conditions d'assurance.

2e exemple (surveillance réalisée en interne, assureur de taille moyenne)

L'assureur-maladie transmet aux médecins de premiers recours / fournisseurs de prestations des données administratives (noms des assurés, adresses, indications sur la couverture d'assurance). Des données relatives aux transferts sont également échangées entre les fournisseurs de prestations et les assureurs pour autant que le traitement et la gestion des infractions l'exigent. Les échanges de données décrits concernent le modèle des pharmaciens, le produit Telmed, le modèle HMO, le modèle combiné (Telmed + HMO) ainsi que le modèle HMO avec un cabinet de groupe.

Il n'y a pas d'échange de données dans le modèle du médecin de famille à l'heure actuelle. Les avis de transferts transmis par les médecins de premier recours dans des cas particuliers, qui font toutefois l'objet d'une protection particulière dans le système central, ne déclenchent pas de flux de données spécifiquement définis et ne sont pas traités.

Protection des données des patients et protection des assurés

3e exemple (surveillance réalisée en interne, grand assureur)

Les assureurs-maladie transmettent aux prestataires téléphoniques des données administratives pour la réalisation du produit d'assurance, en particulier l'identification du preneur d'assurance, la vérification de l'assureur et la couverture. Les cabinets HMO et les médecins de famille reçoivent des données relatives aux diagnostics, aux traitements et à la facturation pour contrôler le respect des conditions spécifiques aux produits (un traitement non ordonné a-t-il été réalisé, absence d'obligation de prise en charge ?).

Les échanges de données administratives avec les prestataires téléphoniques se font par des canaux certifiés. Dans les modèles HMO ou du médecin de famille, la transmission des données passe par un canal e-mail sécurisé, et n'intervient sous forme papier qu'à titre exceptionnel. Les transferts effectués par les médecins de premier recours déclenchent les flux de données suivants : le médecin de famille, le médecin HMO ou le prestataire téléphonique évalue les mesures nécessaires du point de vue médical sur la base des indications fournies par la personne assurée et ordonne des traitements médicaux supplémentaires, le cas échéant. En règle générale, dans le modèle par téléphone, aucune donnée médicale n'est communiquée au fournisseur de prestations qui s'occupe de la suite de la prise en charge. S'agissant des fournisseurs HMO ou des médecins de famille, la transmission des données relève de leur responsabilité, elle n'incombe donc pas à l'assureur.

6.2.3 Réponses à la question 2

De manière générale, on peut constater en résumé que les droits et les obligations en matière d'échange et de protection des données sont réglés contractuellement avec les fournisseurs de prestations et les prestataires externes. Seuls des collaborateurs spécifiques ont accès aux données sensibles, comme établi dans les plans relatifs aux rôles et aux autorisations. Les mesures techniques mises en œuvre (chiffrements, infrastructures dans des zones protégées, connexions sécurisées par certificat, etc.) sont systématiquement conformes à l'état actuel de la technique. Le cercle des personnes disposant d'un droit d'accès et la mise en œuvre des mesures chez les prestataires externes sont contrôlés par les assureurs-maladie.

Dans certains cas, tant les prestataires externes que les assureurs eux-mêmes disposent des certifications correspondantes, à savoir OCPD:2014 ou le label de qualité de protection des données GoodPriv@cy. Certains sont de plus dotés d'infrastructures informatiques certifiées conformes à la norme ISO 27001/2013.

Dans chacune des catégories mentionnées (exemples 1 à 3), un assureur a répondu à la deuxième question de la manière suivante :

1er exemple (externalisation)

Les échanges de données personnelles sensibles entre les assureurs et le fournisseur du modèle du médecin de famille se font uniquement par un canal sécurisé du prestataire. Les connexions protégées par des certificats client sont installées exclusivement sur les ordinateurs et dans les profils informatiques des personnes qui échangent des données avec le prestataire. Il n'y a pas d'échange direct de données avec les médecins de premier recours.

Le prestataire (partenaire d'externalisation : RVK) utilise les systèmes exclusivement pour le modèle HMO / du médecin de famille et pour les modèles d'assurance avec conseil médical par téléphone. Un accès est possible uniquement via des connexions chiffrées, lesquelles sont protégées par des certificats utilisateur ou des mots de passe complexes. Seuls disposent de droits d'accès les collaborateurs du prestataire chargés du traitement des données pour les modèles d'assurance mentionnés ainsi que les collaborateurs du support et les développeurs

de la plate-forme logicielle (accès sur autorisation du prestataire). Tous sont soumis au règlement du prestataire en matière de protection des données.

Des systèmes séparés sont prévus pour la préparation et le transport des données à partir et à destination des assureurs. Les données des assureurs relatives aux prestations et aux effectifs sont obtenues par le prestataire via une connexion chiffrée. Les comptes utilisés pour ce faire sont dédiés exclusivement aux données HMO et MF.

Les échanges de données avec les médecins de premier recours via leur société d'exploitation se font exclusivement par l'intermédiaire de la plate-forme de communication sécurisée HIN. Les transmissions se font à chaque société séparément, si bien que ces sociétés ne reçoivent que les données des médecins qui leur sont rattachés.

2e exemple (surveillance réalisée en interne, assureur de taille moyenne)

Une infrastructure dotée d'un firewall multi-niveaux avec système de zones permet d'assurer la protection des données sensibles. Les accès sont contrôlés au moyen d'un plan des rôles et des autorisations et seuls peuvent accéder aux données les collaborateurs qui ont besoin de ces informations pour effectuer leurs tâches quotidiennes. Le cercle des personnes disposant d'un droit d'accès est vérifié régulièrement.

Les échanges de données se font par des canaux et des interfaces sécurisés.

3e exemple (surveillance réalisée en interne, grand assureur)

Des prescriptions en matière de sécurité, de protection des données, de sécurité de l'information et de sécurité informatique permettent de garantir la protection de toutes les données des assurés qui sont traitées (règles de comportement et directives de traitement complètes). Grâce aux plans d'accès, l'accès aux données est strictement réservé aux collaborateurs qui en ont besoin. Le respect de ces prescriptions fait l'objet d'audits annuels effectués par des contrôleurs externes certifiés. Dans une démarche de développement continu, un audit de maintien a lieu tous les ans, et un audit de recertification tous les trois ans.

6.2.4 Réponses à la question 3

Tous les assureurs confirment n'avoir aucun accès aux systèmes des médecins de premier recours.

7 Conclusion

Lorsque le postulat Heim a été déposé, en 2008, la protection des données en était encore au stade de la mise en place. Les assureurs LAMal ont été tenus d'établir une organisation et des processus conformes au droit relatif à la protection des données. La première enquête a été menée à l'échelle nationale et des recommandations ont été formulées lors de la publication des résultats.

Suite à cela, une circulaire a également été édictée et une deuxième enquête exhaustive sur la conformité de l'organisation et des processus des assureurs LAMal au droit relatif à la protection des données a été menée entre 2011 et 2012. Les résultats de la deuxième enquête ont démontré que de nombreux points avaient été améliorés par rapport à la première enquête, mais que d'autres points n'étaient pas encore totalement remplis. Tirant dans son rapport du 18 décembre 2013 des conclusions allant dans ce sens, le Conseil fédéral a chargé l'OFSP et le PFPDT de veiller, dans le cadre de leur activité de surveillance, à ce que les manquements constatés soient corrigés et à ce que les prescriptions en matière de protection des données soient mises en œuvre. Un nouveau rapport sur le sujet devait être établi, puis porté à la

connaissance du Conseil fédéral et du Parlement, dans un délai de trois à cinq ans. Cependant, il a également été constaté dans le rapport du 18 décembre 2013 que les autorités de surveillance – l'OFSP et le 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.

Consécutivement au rapport du Conseil fédéral de 2013, les deux autorités ont effectivement exercé une activité de surveillance soutenue au cours des années qui ont suivi.

Les lacunes identifiées dans les formes particulières d'assurance ont été comblées grâce à la troisième enquête. Les résultats de l'édition 2019, présentés au point 6.2, montrent que tous les assureurs LAMal disposent pour les formes particulières d'assurance d'une organisation conforme au droit relatif à la protection des données et que les mesures nécessaires ont été prises pour assurer la protection dans ce domaine également.

La surveillance des assureurs LAMal effectuée par le PFPDT et l'OFSP est suffisante pour garantir que toute lacune dans la protection des données est identifiée et que les mesures nécessaires peuvent être engagées dans le cadre des compétences de surveillance qui leur sont conférées.

Les deux autorités se sont en outre coordonnées – ainsi que cela est indiqué au chiffre 5 susmentionné – en ce qui concerne leurs compétences respectives et l'OFSP a adapté en conséquence sa circulaire 7.1 en étroite collaboration avec le PFPDT.

Par conséquent, aucune action supplémentaire n'est requise.