Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique OFSP

Chancellerie fédérale ChF
Préposé fédéral à la protection des données et à la transparence PFPDT

Enquête sur la situation en matière de droit de la protection des données chez les assureurs-maladie sociaux reconnus

1. Contexte

Dans le cadre de leur activité de surveillance, l'Office fédéral de la santé publique (OFSP) et le préposé fédéral à la protection des données et à la transparence (PFPDT, Hanspeter Thür) ont maintes fois incité les assureurs-maladie à faire preuve d'un comportement conforme à la protection des données. Plusieurs interventions parlementaires ont aussi été déposées en ce sens. Des enquêtes menées sur mandat de l'OFSP et du PFPDT, chez certains assureurs-maladie, ont révélé qu'il existe en partie des lacunes dans ce domaine. Partant, le Conseil fédéral a chargé l'OFSP d'examiner plus scrupuleusement les fichiers de données des assureurs et d'associer à dessein le PFPDT à ces démarches.

En décembre 2007, dans le cadre d'un groupe de travail, les deux organes de surveillance ont envoyé à l'ensemble des assureurs un questionnaire détaillé, comportant 70 questions. Cette enquête étendue devait fournir des conclusions sur l'organisation du droit de la protection des données et sur son application dans le domaine de l'assurance-maladie. Elle se fonde sur les dispositions relevant du droit de la surveillance, soit l'art. 27 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[1] et l'art. 21 de la loi fédérale sur l'assurance-maladie (LAMal)[2]. En raison de points tant qualitatifs que quantitatifs, les assureurs-maladie ont dû répondre à des questions relatives à leur organisation et à la protection des données interne et retourner les documents et preuves nécessaires dans les délais fixés.

Dans un premier temps, les organes de surveillance ont pu se faire une impression détaillée de la situation en matière de droit de la protection des données chez les assureurs. Désormais, une seconde étape vise à aider ces derniers à améliorer leur structure organisationnelle en vue de se conformer à la protection des données. Par ailleurs, sur la base de l'enquête, il est prévu d'inciter les assureurs à effectuer un audit sur la protection des données et à procéder à une certification en la matière à titre volontaire en se fondant sur la révision de la LPD. Afin d'améliorer la protection et la sécurité des données, les assureurs peuvent soumettre, sur une base volontaire, leur système, procédure et organisation en la matière à une évaluation effectuée par des organes de certification indépendants reconnus. La loi ne les y contraint toutefois pas.

L'évaluation et l'analyse des réponses et des preuves détaillées ont pris du temps. Les 93 assureurs-maladie (état à la fin 2007) ont majoritairement déposé des réponses et des preuves pertinentes et complètes, et dans les délais. L'OFSP et le PFPDT les remercient pour leur coopération. Cette dernière montre que les assureurs sont conscients de la question de la protection des données. L'évaluation est disponible sous la forme d'un rapport d'une cinquantaine de pages. Avec les données générales nécessaires à la surveillance de l'OFSP, elle constitue une bonne base en vue d'optimiser la protection des données chez les assureurs. Ce faisant, il est nécessaire de souligner que ceux-ci portent seuls la responsabilité de traiter leurs données sensibles en conformité avec la protection des données afin d'éviter tout problème de sécurité. Les deux autorités de surveillance sont disposées à aider les assureurs en l'espèce.

[1] RS 235.1
[2] RS 832.10

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

2. Questions

Le questionnaire portait sur les domaines d'activité suivants des assureurs:

- activités d'assureur hors LAMal (gestion et placement des assurances complémentaires selon la LCA[3] et de l'assurance-accidents selon la LAA[4] ; groupes d'assurance : différences dans la palette de produits);
- contrôle de l'économicité (contrôle des factures avant et pendant la saisie informatique ainsi que contrôle subséquent, quantité de factures et de contrôles de celles-ci par année, directives et centres de contrôle);
- service du médecin-conseil (composition, intégration organisationnelle, subordination personnelle et technique des médecins-conseils et de leur personnel, infrastructure du service, classement des dossiers et droits d'accès);
- case management (noms, fractions de postes, intégration organisationnelle et subordination personnelle et technique, activité pour quels secteurs d'assurance ou autres assureurs ou entreprises, déroulement des processus, collaboration avec le service du médecin-conseil et les fournisseurs de prestations, déclaration de consentement, classement des dossiers et droits d'accès, primes au succès);
- outsourcing: domaines d'activité et d'affaires externalisées (travaux effectués par des tiers, synergies avec d'autres entreprises ou assurances, flux des données personnelles et à quelle fin, informations sur l'externalisation, concept d'information, garantie de la protection des données);
- gestion et organisation de la protection des données (organigramme, compétences, organisation, concept, règlements concernant le traitement des données, flux des données, formation, gestion de la protection des données en tant qu'assureur LAA, indications concernant les responsables de la protection des données, manipulation des fichiers, attitude à l'égard de l'audit et de la certification en matière de protection des données).

3. Principaux aspects de l'analyse

Il faut mentionner au préalable que la plupart des assureurs-maladie collaborent aujourd'hui au sein d'un même groupe d'assurance ou d'une association de caisses-maladie. Il était nécessaire d'en tenir compte pour les résultats de l'évaluation. **Il en ressort clairement que les assureurs ne disposent actuellement pas de concepts et d'instruments uniformes en vue de respecter la protection des données.**

L'analyse notamment de la partie principale de l'enquête - l'étude approfondie de la gestion et de l'organisation de la protection des données chez les assureurs-maladie - a livré les résultats suivants :

- **Concept de protection des données :** 59 % des assureurs, qui affilient 90 % des assurés, disposent d'un concept de protection des données. Un tel concept donne des renseignements sur la stratégie à moyen et long terme qui permet d'assurer la protection des données au sein de l'entreprise ainsi que sa mise en œuvre. Il décrit l'organisation de la protection des données, dont découlent les tâches concrètes des personnes qui sont responsables de cette protection et des fichiers. Par ailleurs, il faut rappeler qu'un tel concept ne figure pas dans la loi.
- **Règlements concernant le traitement des données :** Seuls 26 % des assureurs, représentant toutefois 62 % des assurés, disposent de règlements concernant le traitement des données pour les fichiers sensibles. En d'autres termes, pour 38 % des assurés, il n'existe aucune exigence relative à la manipulation des données sensibles. Ni la protection, ni la sécurité des données ne peuvent être garanties dans ce cas. La législation prévoit l'élaboration et l'actualisation d'un règlement concernant le traitement des données pour tout fichier soumis à déclaration. Il incombe au responsable de la protection des données auprès de l'assureur de ga-

[3] Loi fédérale sur le contrat d'assurance ; RS 221.229.1

[4] Loi fédérale sur l'assurance-accidents ; RS 832.20

rantir que les règlements concernant le traitement des données soient complets et actualisés, prémisse à la conformité légale du fonctionnement et de l'utilisation de fichiers comportant des données personnelles sensibles.

- **Formation des personnes compétentes en matière de protection des données** et attribution du **rôle de responsable en la matière** : Les responsables de la protection des données auprès de 62 % des assureurs-maladie, comptant 91 % des assurés, disposent d'une formation satisfaisante. Cette dernière dépend de leurs obligations. Dans les autres cas, le titulaire de la fonction n'est pas autonome et se trouve dans un conflit d'intérêts. 40 assureurs n'ont pas établi de cahier des charges pour le responsable de la protection des données, dans lequel serait défini son rôle.
- 80 % des assureurs-maladie avec 91 % des assurés ont un responsable de la protection des données. Ce résultat doit être salué. Les entreprises sans un tel responsable sont tenues de déclarer tous leurs fichiers au PFPDT et d'actualiser leurs règlements concernant le traitement des données.

L'évaluation montre que la qualité des résultats de chaque assureur ne dépend pas de sa taille ou de son appartenance à un groupe. Au contraire, les petites caisses, p. ex., ont présenté de bons, voire d'excellents règlements concernant le traitement des données.

Malgré les lacunes révélées par cette analyse, on peut constater que les assureurs-maladie sont conscients de la problématique de la protection des données et ont plusieurs fois manifesté leur disposition à s'améliorer en l'espèce. Ainsi, une nette majorité des assureurs s'est déclarée prête à se soumettre régulièrement, à titre volontaire, à un audit. En outre, d'aucuns ont déjà indiqué, tout en connaissant la charge de travail escomptée, qu'ils désirent se soumettre, à titre volontaire et au moment opportun, à une certification. Celle-ci recueille toutefois une acceptation moins large qu'un audit. Là aussi, la volonté de se soumettre à un audit ou à une certification ne dépend pas de la taille de la caisse-maladie.

Les problèmes mis en évidence en matière de gestion et d'organisation de la protection des données chez les assureurs se reflètent également dans les autres domaines ayant fait l'objet de la présente analyse :

- contrôles d'économicité
- service du médecin-conseil
- case management
- outsourcing

Ces domaines sont brièvement commentés ci-après :

Contrôles d'économicité

Dans le cadre de l'enquête, une première analyse synthétique du contrôle des factures ayant lieu avant, pendant et après la saisie informatique a été faite. Selon les données des assureurs, env. 62 millions de factures ont été traitées en 2006, près de la moitié d'entre elles de façon automatisée. Il s'agit avant tout des factures TARMED, qui sont contrôlées par les collaborateurs avant leur règlement ou suivent un processus entièrement automatisé, sans intervention humaine, jusqu'au paiement. Pour le traitement des factures non automatisé, le caractère économique de l'ensemble ou d'une partie de celles-ci est contrôlé, par exemple pour toutes les factures supérieures à 1000 francs.

Il a été constaté qu'il existe une multitude de systèmes informatiques. Les programmes usuels standards peuvent être adaptés aux besoins des utilisateurs, des assureurs-maladie en l'occurrence. Il en va de même pour les programmes de contrôle des assureurs, pour lesquels il est possible de définir des critères de vérification personnalisés. La majorité des assureurs (en particulier ceux de grande taille et les groupes d'assurance) disposent de manuels relatifs aux prestations et spécifiques à la caisse, ou de directives internes. Les compétences des collaborateurs sont largement définies.

Les informations obtenues ne permettent pas de savoir si les collaborateurs responsables ont aussi accès aux données sensibles des assurés, outre les données relatives aux prestations et aux factures. Pour ce qui est de la garantie de la protection des données, une réponse qui revient souvent se révèle problématique : toutes les données nécessaires sur le plan médical et administratif sont généralement enregistrées (indépendamment du fait que la facturation se fasse par voie électronique ou sur papier).

En matière de contrôle de l'économicité, il faut ainsi veiller à ce que les assureurs tiennent toujours compte du principe de proportionnalité lors de l'enregistrement ou de l'acquisition de données. Il faut attendre des assureurs qu'ils consignent par écrit les processus relatifs aux données personnelles, et notamment sensibles, par le biais d'un règlement concernant le traitement des données. Il serait aussi judicieux de procéder régulièrement à des examens internes sur le respect des dispositions en matière de droit de protection des données.

Service du médecin-conseil

L'indépendance du médecin-conseil et du service de médecins-conseils (pour les grandes caisses-maladie et les groupes d'assurance) est généralement reconnue à l'heure actuelle. Toutefois, la notion d'indépendance n'a pas la même portée partout. Ainsi, il existe encore des médecins-conseils qui ne peuvent pas eux-mêmes choisir leurs collaborateurs. D'aucuns continuent aussi de travailler dans le domaine des assurances complémentaires. Ce qui manque dans l'ensemble à certains assureurs en matière de gestion et d'organisation de la protection des données s'avère également lacunaire dans le cadre des médecins-conseils. L'indépendance sur le plan structurel nécessite, ici aussi, des règlements concernant le traitement des données qui esquissent clairement les compétences et les tâches des médecins-conseils et de leurs assistants.

Des questions spécifiques se posent pour les médecins-conseils qui travaillent sous mandat. Comment les dossiers des patients sont-ils conservés en conformité avec la protection des données lorsque le médecin-conseil travaille parallèlement pour plusieurs assureurs ? La délocalisation du service du médecin-conseil par des petits groupes d'assurance en un service externe à l'entreprise est-elle légale ? De quelle manière les dossiers des patients des petits assureurs y sont-ils conservés séparément ?

Toute la problématique de la protection des données dans le secteur du médecin-conseil prendra de nouvelles dimensions avec la cybersanté et l'introduction du dossier électronique du patient. Aussi faut-il prendre la bonne voie aujourd'hui déjà en prévision de ces changements.

Case management

En guise d'introduction, il est indispensable de rappeler que le case management n'est pas explicitement réglementé dans la LAMal. Le case management comme mesure d'optimisation des prestations, de contrôle et de réduction des coûts, invite les assureurs à remplir entièrement les exigences de prise en charge sur la base des critères visés à l'art. 32 LAMal, selon lequel les prestations remboursées doivent être efficaces, appropriées et économiques. Cette façon de procéder, notamment pour le contrôle de l'adéquation du traitement, qui intègre la conscience des coûts, se heurte aux dispositions correspondantes en matière de protection des données, qui s'appliquent aussi en l'espèce.

Tout le monde ne comprend pas la notion de case management de la même façon. Chez les assureurs, la plupart des gestionnaires de cas (case manager) sont affiliés à la gestion des prestations, ce qui comporte un risque d'influence. Les divers types de case management impliquent souvent un archivage spécifique, qui n'est pas intégré au service du médecin-conseil. En outre, ces case manager travaillent aussi pour d'autres branches d'assurance dans la majorité des cas. La plupart des assureurs ont eu des difficultés à représenter le déroulement des processus de façon détaillée en matière de case management et à décrire la collaboration nécessaire avec le médecin-conseil et le fournisseur de prestations. Les déclarations de consentement des assurés sont très diverses, partiellement incompréhensibles, et ne suffisent pas pour constituer une « procuration » pour l'échange de données sanitaires. Par ailleurs, la clause standard ne comporte souvent pas de clause de rupture. Le consen-

tement de l'assuré, obtenu en bonne et due forme, est cependant indispensable pour que le case manager puisse avoir accès aux données concernant la santé, et à d'autres indications et documents le cas échéant.

Partant, il est nécessaire d'optimiser les processus de contrôle des prestations en matière de droit de protection des données dans le domaine du case management. Sur le plan structurel, il faut vérifier la subordination personnelle et technique de ces gestionnaires et la corriger le cas échéant.

Outsourcing

Dans les grands groupes d'assureurs notamment, les tâches confiées à des tiers couvrent toute la gamme d'activités afférentes. Une part importante des travaux externalisés concerne le traitement électronique des données, la numérisation et le remaniement correspondant de tous les domaines de données. La digitalisation du dossier du patient, y compris l'ensemble de la comptabilité, a imposé une nouvelle organisation très complexe. Celle-ci a évidemment des conséquences pour la protection des données. Les droits d'accès internes nécessitent une réglementation détaillée, tenant pleinement compte des structures internes des caisses-maladie. Les questions de sécurité sont au centre des préoccupations, et à prendre très au sérieux à la suite d'incidents (vol et perte de données, transmission à des personnes non autorisées, etc.) dans plusieurs pays (Allemagne, Royaume-Uni, Norvège). Il faut souligner que les assureurs-maladie, en tant que propriétaires des fichiers, portent l'entière responsabilité de la sécurité de ces données très sensibles.

Chez les plus petits assureurs, la protection des données reste relativement gérable. L'externalisation de tâches spécifiques y est nettement moins importante. Toutefois, le regroupement des petites caisses et la mise en action d'un pool de partenaires entraîne finalement des problèmes similaires.

Dans le cadre de l'outsourcing, il était aussi intéressant de savoir si les assurés étaient suffisamment informés à ce propos. Il est rare que les assureurs donnent un aperçu détaillé de la liste de leurs partenaires externes. L'information est transmise en majorité par le biais de lettres d'information, de revues, de brochures et de rapports annuels.

Enfin, l'analyse a porté sur la question de savoir si les assureurs remplissent les exigences en matière de protection des données en confiant des tâches à des tiers. La qualité des contrats qui régissent l'étendue de l'externalisation, les exigences en matière de protection des données, les conséquences en cas de non-respect et la procédure de contrôle sont variables. De nombreux assureurs ne disposent pas d'une procédure de contrôle appropriée leur permettant de vérifier le respect des exigences posées à la protection des données.

4. Prochaines étapes

Ces prochains mois, l'OFSP et le PFPDT continueront de traiter les diverses questions encore ouvertes. Ils émettent les recommandations suivantes à l'intention des assureurs-maladie :

- Chaque assureur devrait élaborer un concept (stratégie) en matière de protection des données.
- Chaque assureur doit tenir une liste des fichiers, qui nécessitent tous, s'ils comportent des données personnelles particulièrement sensibles, un règlement concernant le traitement des données (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 responsable de la protection des données et un titulaire pour chaque fichier. Leurs tâches sont consignées dans un cahier des charges.
- Les responsables de la protection des données doivent disposer des connaissances techniques nécessaires.
- Les assureurs doivent procéder régulièrement à des audits sur la protection des données réalisés en dehors du cadre de la surveillance de l'administration et soumettre les résultats aux autorités de surveillance.