Groupe Mutuel
Assurances
Versicherungen
Assicurazioni

Assuré. Là. Maintenant.

Règlement de traitement des données du Groupe Mutuel, association d'assureurs

Martigny, le 24 septembre 2013

Groupe Mutuel
Assurances
Versicherungen
Assicurazioni
Assuré. Là. Maintenant.

Table des matières

Afin de faciliter la lecture du présent règlement, le terme « collaborateurs » s'applique indifféremment aux femmes ou aux hommes.

1 Dispositions générales

1.1 Droit applicable

Assurance obligatoire des soins et assurance facultative d'indemnités journalières
- Loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal)
- Ordonnance du 27 juin 1995 sur l'assurance-maladie (OAMal)

Coordination du droit fédéral des assurances sociales
- Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA)
- Ordonnance du 11 septembre 2002 sur la partie générale du droit des assurances sociales (OPGA)

Protection des données
- Loi fédérale du 19 juin 1992 sur la protection des données (LPD)
- Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)

Dans le domaine de l'assurance obligatoire des soins, les dispositions de la LAMal et de la LPGA priment sur celles de la LPD. Les dispositions de la LPD s'appliquent à titre subsidiaire.

1.2 Point de départ du Règlement de traitement

Selon les art. 11 et 21 OLPD, un règlement de traitement doit être élaboré pour le fichier. Selon l'art. 84b LAMal, le règlement est soumis à l'appréciation du Préposé fédéral à la protection des données et à la transparence (PFPDT) et doit être rendu public.

Il a pour objectif de fournir une information transparente quant au traitement des données effectué dans le cadre de la gestion administrative offerte par le Groupe Mutuel, association d'assureurs, à ses assureurs membres.

1.3 Principes du traitement des données

Le but de la récolte des données ressort des dispositions de la LAMal. Selon l'art. 84 LAMal, l'assureur maladie chargé d'appliquer la présente loi ou d'en contrôler ou surveiller l'exécution est habilité à traiter et à faire traiter les données personnelles, y compris les données sensibles et les profils de la personnalité, qui leur sont nécessaires pour accomplir les tâches que leur assigne la présente loi.

Le traitement des données personnelles est assujetti aux principes juridiques suivants en matière de protection des données :

Licéité: le traitement doit être fondé sur une base légale (loi, ordonnance, statuts, règlement ou équivalent) ou effectué avec le consentement des personnes concernées.

Principe de la bonne foi: le traitement doit être réalisé selon le principe de la bonne foi. La collecte des données personnelles ne peut être effectuée sans que la personne concernée en ait connaissance, ni contre son gré.

Proportionnalité: le traitement doit être adéquat, c'est-à-dire proportionnel au but visé et se limiter à ce qui est nécessaire pour atteindre l'objectif fixé.

Finalité: les données personnelles ne peuvent être traitées que dans le but indiqué lors de leur récolte, découlant des circonstances prévues par la loi, les statuts ou les règlements applicables.

Collecte reconnaissable: la collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée; les finalités du traitement doivent être indiquées lors de la collecte des données; elles peuvent aussi découler des circonstances.

Exactitude: les données personnelles doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

Sécurité des données: les données doivent être protégées par des mesures techniques et organisationnelles appropriées contre la perte et les traitements non autorisés.

Droit des personnes concernées: les personnes dont les données sont traitées par le Groupe Mutuel, sur la base du mandat qui lui a été conféré par ses assureurs membres, ont le droit de les connaître et, le cas échéant, d'en obtenir la correction ou leur effacement. L'effacement des données n'est effectué qu'à la condition que cela ne nuise pas à la bonne gestion du contrat.

1.4 Champ d'application

Le présent règlement vaut pour le traitement des données que le Groupe Mutuel, association d'assureurs effectue pour le compte des sociétés qui lui ont confié un mandat de gestion défini dans le cadre des accords conclus entre le Groupe Mutuel et les assureurs affiliés.

1.5 Obligations des collaborateurs du Groupe Mutuel et de ses mandataires

On entend par collaborateurs du Groupe Mutuel aussi bien les personnes bénéficiant d'un contrat de travail à durée indéterminée, que celles bénéficiant d'un contrat à durée déterminée les liant au Groupe Mutuel.

On entend par collaborateurs des mandataires du Groupe Mutuel, les personnes au bénéfice d'un contrat de travail les liant à une société mandatée par le Groupe Mutuel.

Obligation de garder le secret
En application de l'art. 33 LPGA, les personnes qui traitent les données des assurés gérées par le Groupe Mutuel dans le cadre d'un contrat de travail ou sur mandat sont tenues de garder le secret à l'égard des tiers sur tout ce qu'elles apprennent pendant leur activité professionnelle, en particulier en ce qui concerne les données de nature médicale.

L'obligation de garder le secret reste applicable après la fin du contrat de travail ou du mandat spécifique. Cette obligation figure dans les accords contractuels relatifs à l'engagement ou au mandat.

Fait partie intégrante des contrats de travail du Groupe Mutuel, le règlement du personnel fixant les devoirs du collaborateur.

2 Structure du Système d'Information du Groupe Mutuel

2.1 Composition du système d'information du Groupe Mutuel

1. Système de gestion du Core Business
- Sous-système de gestion de l'assurance-maladie et accident
- Sous-système de gestion des assurances entreprise
- Sous-système de gestion des ventes
- Sous-système de gestion des dossiers juridiques

2. Système de gestion du pilotage d'entreprise

3. Système de gestion des Finances
- Sous-système de gestion de la comptabilité et des frais généraux
- Sous-système de la gestion financière client
- Sous-système de gestion du contentieux
- Sous-système de gestion des placements

4. Système de gestion des ressources humaines

5. Système de gestion des infrastructures et des bâtiments

6. Système de gestion de la messagerie et des communications
- Sous-système de gestion des échanges électroniques
- Sous-système de gestion de la messagerie (e-mail)
- Sous-système de gestion de la téléphonie et des fax

7. Système de gestion documentaire

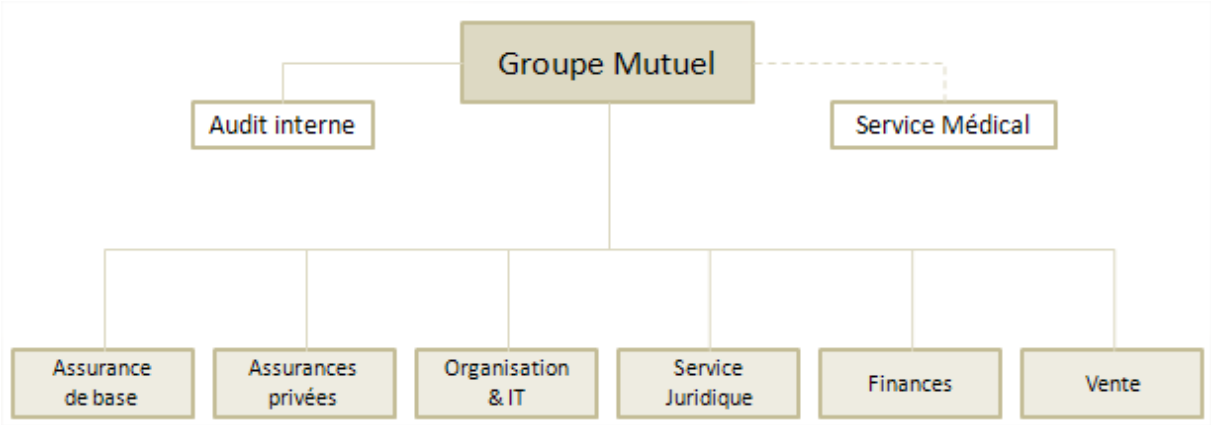
- Sous-système de numérisation documentaire
- Sous-système d'archivage documentaire
- Sous-système d'indexation documentaire

8. Système de gestion Internet / Extranet

9. Système de gestion de l'exploitation informatique

- Sous-Système de développement informatique
- Sous-Système de gestion du MiddleWare
- Sous-Système de gestion de la sécurité

2.2 Organigramme



2.3 Responsabilités

La Direction du Groupe Mutuel assume la responsabilité de la protection et de la sécurité des données. Dans les questions relevant du droit de la protection des données, elle est conseillée par le Conseiller interne à la protection des données.

Le tableau ci-dessous décrit la répartition des rôles et responsabilités :

Rôle	Responsabilité
Protection des données en général, SGPD et formations	Conseiller indépendant à la protection des données et Responsable du système de gestion de protection des données
Demandes d'accès et de consultation de dossiers	Service Juridique
Sécurité technique des données	Service IT
Profils d'accès	Ressources humaines et service IT
Destruction des données électroniques	Service IT
Documents destinés au Médecin-conseil	Médecin-conseil

2.4 Participants au traitement des données

2.4.1 Centres de services régionaux

La gestion de l'assurance-maladie selon la LAMal est assurée par les collaborateurs des Centres de Services Régionaux et des Agences Régionales. Afin d'accomplir cette tâche, ces collaborateurs traitent des données personnelles, y compris des données requérant une protection spécifique à l'aide du Système d'information du Groupe Mutuel décrit au point 2.1.

2.4.2 Secteurs opérationnels

Les collaborateurs des secteurs mentionnés ci-après ont accès au Système d'information du Groupe Mutuel, afin de pouvoir gérer l'assurance-maladie selon la LAMal.

1. Secteur Prestations
2. Secteur Sociétariat
3. Actuariat & Statistiques
4. Comptabilité & Finances
5. Primes, Trafic Paiement & Contentieux
6. Assurances entreprises
7. Service du Médecin-conseil
8. Service juridique & Surveillance légale

2.5 Interfaces

Plusieurs interfaces permettent le contact direct avec des fournisseurs de prestations; notamment dans le cadre de la réception des factures de prestations fournies par les Trust Center, dans le cadre des assurances avec choix limité des prestataires ainsi que les produits d'assurances utilisant des services de télé-médecine.

Il existe également une interface qui permet à certains fournisseurs de prestations, notamment les pharmacies, d'accèder online à la couverture d'assurance des assurés au moyen de la carte d'assurés fournie aux assurés du Groupe Mutuel.

En principe, les données sont transmises électroniquement ou sur support papier. Au moyen d'un système d'authentification fort, du chiffrement et des technologies avancées de transmission des données, la protection et la sécurité des données sont garanties.

3 Traitement des données / Types de données

3.1 Données récoltées

Les données proviennent essentiellement des assurés eux-mêmes, des personnes autorisées par les assurés à les transmettre aux assureurs LAMal du Groupe Mutuel (fournisseurs de prestations selon la LAMal, assurances, administrations, etc.), des décomptes de prestations établis par les fournisseurs de prestations, d'institutions (par ex. réduction de primes).

Les données peuvent aussi être collectées dans le cadre de l'assistance administrative (Art.32 LPGA).

3.2 Catégories de données du contrat d'assurance maladie

L'annexe #1 recense les catégories de données figurant dans l'inventaire des fichiers du Système d'information du Groupe Mutuel.

3.3 Communication des données

Les données sont communiquées sur la base d'une autorisation de l'assuré, reposant sur une base légale ou si la communication répond à un intérêt public prépondérant.

3.3.1 Des données sont régulièrement communiquées pour :

- transmettre des informations concernant des personnes ne payant pas leur prime(Art. 64a al 3 LAMal);
- vérifier la non interruption de la protection d'assurance (Art. 7 al. 5 LAMal : communication de l'ancien assureur au nouvel assureur);
- évaluer les demandes de prise en charge des prestations (par ex. limitations selon l'OPAS);
- coordonner les prestations avec d'autres assurances sociales (Art. 27 LAMal : Coordination avec l'AI en relation avec les infirmités congénitales);
- exercer le droit de recours contre les tiers-responsables;
- établir des statistiques;
- attribuer ou vérifier le numéro d'assuré AVS

3.3.2 Ces données sont communiquées notammant aux:

- assurés et les tiers qui agissent pour le compte des assurés;
- fournisseurs de prestations (par ex. système de vérification online par carte d'assuré);
- autorités (cantons, OFSP, AI, etc.);
- associations suisse des assureurs-maladie santésuisse, tarifsuisse SA et SASIS SA;
- assureurs partenaires;
- tribunaux;
- services sociaux;
- les médecins-conseil et experts médicaux externes.

3.3.3 Autres communications des données selon l'art. 84a LAMal

Les autres communications des données sont réglées selon l'art. 84a LAMal. Des données peuvent ainsi être communiquées dans des cas d'espèces et sur demande écrite et motivée aux autorités compétentes en matière d'aide sociale, aux tribunaux civils, aux tribunaux pénaux et aux organes d'instruction pénale, aux offices des poursuites, au Service de Renseignement de la Confédération (SRC).

3.3.4 Traitement et communication des diagnostics DRG selon l'article 59a OAMal

Conformément à l'art. 59a al. 6 OAMal, le service de réception des données du Groupe Mutuel sélectionne certaines factures qui sont candidates à un contrôle plus approfondi, et conserve dans ce cas le MCD (Minimal Clinical Dataset) contenant les données administratives et médicales (diagnostics) du patient dans un conteneur dont la sécurité est renforcée par une ACL spécifique. Ces données ne sont accessibles qu'aux auxiliaires médicales de manière électronique et aux médecins-conseil sous format papier. Dans ce dernier cas, les données sont détruites après avis.

3.3.5 Traitement des données pour le compte d'assureurs partenaires

Sur la base d'un contrat de mandat, le Groupe Mutuel traite les données des assureurs membres de l'association et des partenaires à l'aide du Système d'information du Groupe Mutuel dans le cadre de l'exécution de l'assurance obligatoire des soins en appliquant les dispositions de l'art. 84 LAMal. Les assureurs du Groupe Mutuel sont responsable du respect des dispositions de l'art. 10a de la LPD dans le cadre du traitement des données personnelles par un tiers.

4 Durée de conservation des données, effacement des données

La durée de conservation des données est basée sur les dispositions spécifiques du droit suisse en la matière. Après l'écoulement de la durée de conservation légale, les données doivent être détruites du Système d'information du Groupe Mutuel.

5 Documentation de planification, de réalisation et d'exploitation du système d'information

Les dossiers de documentation de planification, de réalisation et d'exploitation des systèmes et sous-systèmes d'information du Groupe Mutuel sont conservés dans le secteur IT.

6 Déclaration du fichier au PFPDT (art. 16 OLPD)

Le conseiller interne à la protection des données procède à un inventaire des fichiers de données qu'il tient à disposition du PFPDT.

7 Processus

La collecte, le traitement et la transmission des données du Système d'Information du Groupe Mutuel sont basés sur des processus. Ces derniers sont documentés dans les « descriptions de processus ». Ces documents sont internes au Groupe Mutuel.

8 Procédures de contrôle et mesures techniques et organisationnelles

8.1. Contrôle d'accès

Tous les locaux du Groupe Mutuel dans lesquels des données sensibles personnelles sont traitées sont protégés électroniquement et/ou manuellement contre l'intrusion de tiers non autorisés.

L'accès aux locaux du Groupe Mutuel n'est accordé qu'aux collaborateurs munis d'un badge électromagnétique qui est également utilisé pour l'enregistrement de leur temps de travail. Ce badge est personnel et intransmissible. Les visiteurs sont appelés à s'annoncer à la réception des bâtiments pour être enregistrés et se voir attribuer un badge « visiteur ».

Les droits d'accès sont attribués selon la fonction et le titre du collaborateur. Ils sont plus ou moins étendus. De plus les accès sont gérés par site et par plage horaire. Tous les accès ou tentatives d'accès sont historisés par le logiciel de gestion des accès physiques. Des systèmes de vidéosurveillance et d'alarmes protègent certains locaux.

Certains locaux, en particulier les agences régionales, sont accessibles à l'aide d'une clé fournie au collaborateur après signature d'un document attestant sa bonne remise; chaque clé est identifiée et un registre des clés remises aux collaborateurs est tenu à jour.

Les accès aux centres de calculs sont protégés par un système d'authentification fort. Des journaux d'accès permettent d'identifier les personnes ayant accédé à ces locaux et à quel moment.

8.2. Contrôle des supports de données personnelles

Grâce à des dispositifs techniques implémentés dans le système d'information, seules les personnes autorisées peuvent traiter les données enregistrées sur les supports électroniques.

Seules les personnes dûment autorisées obtiennent les accès au Système d'information du Groupe Mutuel.

8.3. Authentification des utilisateurs

L'accès aux modules du système d'information du Groupe Mutuel n'est possible qu'en disposant des moyens d'authentification nécessaires.

8.4. Contrôle du transport

Les mesures techniques appropriées sont mises en place afin de sécuriser la transmission des données, de sorte à ce que les personnes non autorisées ne puissent pas lire, copier, modifier ou effacer des données lors de leur communication ou lors du transport de supports de données.

8.5. Contrôle de communication

Les destinataires de données qui accèdent aux données personnelles au moyen d'installations de transmission de données sont identifiés, en particulier les fournisseurs de prestations qui accèdent aux données relatives à la couverture d'assurance au moyen de la carte d'assuré.

8.6. Contrôle de mémoire

Les mesures techniques appropriées sont mises en place afin que des personnes non autorisées ne puissent ni introduire de données dans la mémoire ni prendre connaissance des données mémorisées, respectivement les modifier ou les effacer.

8.7. Contrôle d'utilisation

Seuls des terminaux agréés par le Groupe Mutuel peuvent être raccordés au réseau informatique du Groupe Mutuel.

8.8. Contrôle d'accès

Les personnes autorisées ont accès uniquement aux données dont elles ont besoin pour accomplir leurs tâches. La nature et l'étendue de l'accès des utilisateurs du fichier sont décrites dans le chapitre #10.

8.9. Contrôle de l'introduction (journalisation)

En plus du contrôle de l'accès au Système d'information du Groupe Mutuel, les traitements automatisés de données font l'objet d'une journalisation afin qu'il soit possible de vérifier à posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. Les procès-verbaux de journalisation sont conservés sous une forme répondant aux exigences de la révision. Ils sont accessibles aux seuls organes ou personnes chargés de vérifier l'application des dispositions de protection des données personnelles, et ils ne sont utilisés qu'à cette fin.

8.10 Développement d'applications

Les environnements de développement, de test et de production sont strictement séparés.

8.11 Supervision et responsabilité

Le maître de fichier s'assure que les utilisateurs se conforment aux instructions, au présent Règlement de traitement et à ses annexes.

9 Description des champs de données et des unités d'organisation qui y ont accès

Les droits d'accès au système d'information du Groupe Mutuel sont réglés au moyen d'un système d'autorisations d'accès.

10 Nature et étendue de l'accès des utilisateurs au système d'information

10.1 Utilisateurs

Les personnes autorisées à accéder au Système d'information du Groupe Mutuel sont :

1. les collaborateurs, les mandataires du Groupe Mutuel, ainsi que le personnel des sociétés affiliées.

2. Les administrateurs systèmes du Groupe Mutuel.

10.2 Gestion des droits d'accès

La Sécurité du Système d'Information (SSI) a pour but d'assurer la confidentialité, l'intégrité et la disponibilité des informations. Une composante importante de la sécurité repose sur la notion de gestion des accès qui comporte deux pôles principaux, les accès physiques qui permettent à un utilisateur d'accéder aux différents bâtiments et locaux de l'entreprise et les accès logiques qui lui permettent de se connecter aux systèmes et applications pour accéder aux informations dont il a besoin.

10.3 Contrôle des accès aux applications de gestion

Les contrats des assurés sont gérés sur une plate-forme informatique.

Les accès logiques sont gérés, d'une part par le secteur Informatique pour les applications standard, d'autre part par les métiers pour certaines applications spécifiques. Un workflow initial permet d'attribuer une authentification à tout nouveau collaborateur. Des accès supplémentaires peuvent ensuite être demandés. Un workflow de validation permet aux responsables d'accepter ou non les demandes formulées. La gestion des accès se base sur le principe du moindre privilège (least privilege), c'est-à-dire qu'un collaborateur n'aura accès qu'aux éléments pertinents pour la réalisation de ses tâches. Le principe veut qu'initialement tous les accès soient verrouillés et que les droits ne sont accordés que sur demande.

Lorsqu'un collaborateur quitte l'entreprise, les accès sont radiés et il n'est plus possible pour le collaborateur de se connecter aux systèmes logiques, ni d'accéder aux locaux.

10.4 Accès aux documents bureautiques (suite Office de Windows)

Les données gérées au travers des différentes applications de gestion du Groupe Mutuel peuvent être transférées dans des fichiers bureautiques.

Ces documents de travail sont enregistrés dans un répertoire bureautique spécifique à chaque secteur du Groupe Mutuel. Le responsable hiérarchique définit les droits d'accès à ce répertoire sur la base de la fonction du collaborateur. La gestion des droits (attribution, modification, suppression) est assurée par le Service de support informatique du Groupe Mutuel qui attribue chaque collaborateur à un groupe d'utilisateurs autorisés à accéder aux données enregistrées dans chaque répertoire.

Les accès aux documents enregistrés dans les répertoires bureautiques font l'objet d'une journalisation au travers d'un logiciel de gouvernance des données. L'accès aux journaux d'audit générés par ce logiciel est limité aux collaborateurs du secteur informatique chargés de la sécurité du système d'information.

10.5 Accès des collaborateurs travaillant à domicile / télétravail

Le Groupe Mutuel dispose de collaborateurs travaillant depuis leur domicile à des tâches d'indexation de documents. Cette activité consiste à référencer des factures de prestations afin que celles-ci soient transmises aux gestionnaires des prestations dans le processus adéquat. L'accès aux applications depuis le domicile est régi par les mêmes principes que ceux concernant les collaborateurs travaillant sur site. La connexion au système informatique du Groupe Mutuel est effectuée au travers d'une ligne sécurisée.

10.6 Contrôle des accès aux données disponibles sur les plates-formes Extranet

Un nombre restreint de données personnelles sont rendues accessibles sur les plates-formes Extranet du Groupe Mutuel. Leur accès, par des personnes autorisées, est protégé par une méthode d'authentification forte.

11 Droits des personnes concernées

Les demandes d'accès selon l'art. 8 LPD doivent être adressées par écrit au Service juridique du Groupe Mutuel, accompagnées d'une preuve de l'identité du requérant (copie d'une attestation officielle, avec photo), à l'adresse suivante :

Groupe Mutuel
Service juridique
Rue des Cèdres 5
1920 Martigny

La procédure interne de traitement des demandes d'accès est fixée dans le document « Procédure d'exercice du droit d'accès ».

12 Configuration des moyens informatiques

Le matériel informatique et les logiciels utilisés au Groupe Mutuel correspondent aux standards techniques.

Les documentations relatives à la configuration des moyens informatiques utilisés pour le système d'information du Groupe Mutuel sont conservés dans le secteur IT ou auprès des fournisseurs/partenaires externes.

Pour des raisons de sécurité, aucune indication n'est fournie sur la configuration des moyens informatiques.

13 Dispositions finales

13.1 Annexes

Les annexes mentionnées dans le présent règlement de traitement font partie intégrante du présent règlement.

13.2 Elaboration et modifications du règlement

Le règlement de traitement est mis à jour régulièrement par le maître de fichier conformément aux dispositions de l'art. 11 de l'OLPD. Ce règlement peut être modifié en tout temps. Les modifications doivent être apportées sous forme écrite et approuvées par la Direction du Groupe Mutuel.

Le règlement de traitement est élaboré par le Conseiller à la protection des données, le responsable du système de gestion de protection des données et supervisé par le Service juridique du Groupe Mutuel.

La responsabilité pour la modification du règlement incombe au Service juridique du Groupe Mutuel.

13.3 Entrée en vigueur

Ce règlement entre en vigueur immédiatement.

13.4 Publication

Selon l'art. 84b LAMal, le présent règlement et ses annexes sont publiés sur internet, sous www.groupemutuel.ch.

Annexe 1

Catégories des données basées sur l'inventaire des fichiers du Groupe Mutuel

Catégories des données personnelles traitées (Art. 3, alinéa 1, lettre e OLPD)

Nom/Prénom
Sexe
Date de naissance / âge
Numéro AVS
Langues
Nationalité / lieu d'origine
Appartenance cantonale / communale
Numéro d'assuré
Adresse
Adresse bancaire / postale
Genre d'assurance et de couverture
Données sur la santé
Fournisseur de prestations
Date d'entrée / de sortie
Suspension du contrat d'assurance
Suspension des prestations
Prime
Facturation des primes
Franchise
Participation aux coûts
Subventions
Réduction des primes
Réduction des primes par les cantons
Données de rappel

Annexe 2

Catégories des données basées sur l'inventaire des fichiers du Groupe Mutuel

Catégories de destinataires de données (Art. 3, alinéa 1, lettre f OLPD)

Assurés
Fournisseurs de prestations
Autorités
Canton
Autres assureurs maladie et sociaux
Santésuisse, Tarifsuisse, Sasis
Service juridique
Service social
Médecins-conseil