Helsana

Règlement de traitement du Groupe Helsana

1. Finalité du règlement de traitement

Le règlement de traitement doit permettre d'assurer la transparence nécessaire dans le contexte du développement des systèmes et du traitement des données. Il doit être tenu sous une forme aussi concise et compréhensible que possible, de sorte que même des personnes non expertes puissent comprendre ou évaluer l'évolution du système et le traitement des données. Il convient d'appliquer à titre réglementaire le principe du strict nécessaire.

Les principes du traitement des données de toutes les collectes de données des compagnies d'assurance du Groupe Helsana (ci-après également «**Helsana**» ou «**nous**») sont consignés dans ce règlement de traitement. Les compagnies d'assurance du Groupe Helsana incluent Helsana Assurances SA, Helsana Assurances complémentaires SA et Helsana Accidents SA.

2. Traitements des données et procédure

2.1 Structure

Le traitement des données d'Helsana est réparti dans les activités suivantes relatives aux données:

- Développement d'offres pour la clientèle privée (IG)
- Audit, Risk, Legal & Compliance
- Gestion de la sécurité des données
- Facility Management
- Sciences de la santé publique
- Gestion RH
- Encaissement/paiement, finances, actuariat
- Management IT
- Service Clientèle IG
- Service Clientèle entreprises (UG)
- Achat des prestations IG
- Management des prestations IG
- Management des prestations UG
- Nouvelles affaires IG & UG
- Assurance du personnel IG & UG
- Fondation de prévoyance du personnel
- Service du médecin-conseil (SMC)
- Gestion des contrats IG
- Gestion du canal de vente IG
- Gestion du canal de vente UG
- Assistance aux ventes IG

Différentes interfaces permettent de contacter directement des prestataires et fournisseurs de prestations externes, par exemple en cas de décompte direct du fournisseur de prestations avec Helsana. Il existe par ailleurs une interface qui donne la possibilité à certains fournisseurs de prestations de contrôler en ligne la couverture d'assurance d'une personne assurée. La protection des données et la sécurité des données correspondante sont garanties grâce à une authentification forte ainsi qu'à une technologie de cryptage et de transmission moderne.

2.2 Procédure de traitement des données

Dans un règlement interne, Helsana définit comment répertorier les traitements de données et comment en vérifier la conformité en matière de droit (Compliance Checks). Les procédures de stockage, de divulgation à des tiers, de conservation, d'archivage, de pseudonymisation, d'anonymisation, de suppression ou de

destruction des données sont consignées dans les plans de protection des données de chaque traitement de données.

2.3 Utilisation et accès aux données

2.3.1 Personnes détenant un droit d'accès

Les personnes suivantes ont le droit d'accéder aux systèmes informatiques d'Helsana:

- les collaborateurs et collaboratrices d'Helsana, pour autant qu'ils et elles en aient besoin pour exécuter leur mandat de mise en œuvre de l'assurance-maladie;
- les administrateurs et administratrices système d'Helsana;
- les prestataires mandatés par contrat;

(communément dénommé·e·s les personnes détenant un droit d'accès).

2.3.2 Gestion des personnes détenant un droit d'accès

Le service Identity & Access Management d'Helsana gère les droits d'accès de manière centralisée. Les collaborateurs et collaboratrices internes et externes sont signalé·e·s sur l'interface RH. De nouvelles identités, y compris les comptes correspondants, ne sont saisies que s'il existe un contrat de travail ou un contrat de prestations valable et une validation correspondante des droits par le ou la supérieur·e hiérarchique.

2.3.3 Droit d'accès personnel

Lorsqu'elles rejoignent Helsana, toutes les personnes autorisées obtiennent leurs droits d'accès aux informations dans le cadre du modèle de rôle, selon leur fonction et leur appartenance organisationnelle. Tous les autres droits requis doivent être demandés individuellement par le biais du portail d'autorisation. Chaque demande doit être confirmée par le ou la supérieur·e direct·e et, selon le rôle d'autorisation, par la personne approuvant les rôles.

2.3.4 Annulation du droit d'accès

Les personnes ayant accès aux systèmes informatiques d'Helsana n'ont un droit d'accès que tant qu'elles ont besoin des données dans l'exercice de leurs fonctions. En cas de départ ou de changement d'attribution au sein d'Helsana, le droit d'accès est retiré et les droits d'accès requis pour les nouvelles attributions sont réaffectés par le biais du modèle de rôles.

2.3.5 Formation des personnes détenant un droit d'accès

Des cours sont dispensés aux personnes détenant un droit d'accès afin de les former aux différents sous-systèmes et applications.

2.3.6 Manuels et directives de traitement pour les personnes détenant un droit d'accès

Il existe des documents correspondant à chaque sous-système. Le traitement des données est par ailleurs fixé dans des directives, des règlements et des manuels de prestations ainsi que dans des listes. Ces documents sont régulièrement mis à jour par les unités d'organisation compétentes.

Grâce à des instructions spécifiques, celles-ci instaurent un niveau constant d'évaluation des prestations selon la loi fédérale sur l'assurance-maladie (LAMal) pour l'ensemble du territoire d'assurance de la Suisse.

2.3.7 Prestataires informatiques

Si l'exploitation de systèmes informatiques d'Helsana est confiée à des prestataires informatiques externes, ces prestataires doivent respecter des réglementations similaires dans leur domaine.

3. Droit d'accès aux données, droit de rectification et droit à la remise des données

Conformément à l'art. 25 de la loi sur la protection des données (LPD), les personnes concernées peuvent demander au responsable du traitement de leur fournir des renseignements concernant le traitement

éventuel de données personnelles les concernant et exiger que ces données leur soient communiquées. Elles ont également le droit d'exiger qu'Helsana les rectifie, le cas échéant.

4. Mesures techniques et organisationnelles de garantie de la sécurité des données

4.1 Contrôle d'accès

Tous les locaux d'Helsana dans lesquels sont traitées des données personnelles sensibles sont protégés contre les accès de personnes non autorisées, soit manuellement, soit électroniquement. Les responsables journalisent la gestion des clés et le contrôle d'accès électronique. Le ou la mandataire à la sécurité physique peut en tout temps exiger de consulter le journal ou exiger des analyses. Les mesures de sécurité sont déterminées par des zones de protection: les places de travail sont protégées contre l'accès par des tiers non autorisés. Les locaux spéciaux et les pièces sensibles telles que les locaux techniques et les centres de données sont sécurisés comme suit:

- les systèmes informatiques dans les centres de données exploités par le service informatique d'Helsana et les serveurs décentralisés exploités par le service informatique d'Helsana sont sécurisés de sorte à en accorder l'accès exclusivement aux personnes autorisées spécifiques, grâce à des mesures de sécurité physiques renforcées.
- Les systèmes informatiques installés sur des serveurs décentralisés qui ne sont pas exploités par le service informatique d'Helsana sont soumis à des mesures de sécurité comparables à celles qu'il met lui-même en œuvre.

Seules les personnes autorisées peuvent traiter des données grâce à des précautions techniques. Seules les personnes autorisées ont accès à des systèmes informatiques d'Helsana.

4.2 Authentification des personnes détenant un droit d'accès

L'accès à des systèmes informatiques d'Helsana est protégé par l'identifiant de l'utilisateur ou l'utilisatrice associé à une caractéristique d'autorisation individuelle valable pendant une durée déterminée.

4.3 Contrôle de communication

Les personnes auxquelles des données personnelles sont communiquées à l'aide d'équipements de transmission de données sont identifiées par le biais des interfaces (par exemple des consultations de la couverture en ligne par les fournisseurs de prestations en lien avec l'utilisation de la carte d'assurance).

4.4 Transmission des données

La transmission des données est protégée par chiffrement.

4.5 Contrôle de stockage

Les personnes détenant un droit d'accès obtiennent des autorisations spécifiques pour les mutations des champs de données nécessaires à l'accomplissement de leurs tâches (par exemple conformément à la LAMal ou à la loi fédérale sur l'assurance-accidents [LAA]).

4.6 Exigences techniques à l'égard des terminaux

L'accès au réseau interne d'Helsana est restreint, protégé et surveillé grâce à des mesures de contrôle spécifiques. Des précautions similaires existent chez les prestataires informatiques externes pour leurs réseaux.

4.7 Mesures en vue de la protection des données (confidentialité) sur les terminaux

Tous les terminaux de données (clients) sont protégés contre les attaques par diverses mesures techniques de sécurité.

Les données imprimées sont conservées de manière à ce que des tiers (par exemple personnel d'entretien) ne puissent pas les consulter ni les copier. En application d'une directive interne, ces données sont soit conservées dans des conteneurs verrouillables, soit supprimées à l'aide de destructeurs de documents ou de Datarec. Le principe du Clean Desk et du Clear Screen s'applique.

4.8 Journalisation

En plus du contrôle des accès aux systèmes informatiques d'Helsana par le biais de la procédure d'autorisation ainsi que de la protection de l'identifiant personnel de l'utilisateur ou de l'utilisatrice et de son autorisation personnelle, certains systèmes informatiques disposent d'une journalisation du traitement automatisé qui permet de vérifier a posteriori si les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. La journalisation a lieu en vertu de l'art. 4 de l'ordonnance sur la protection des données (OPDo): les procès-verbaux de journalisation sont conservés durant 13 mois et sous une forme répondant aux exigences de la révision. Ils ne sont accessibles qu'aux organes et aux personnes chargés de vérifier l'application de la réglementation relative à la protection des données ou de maintenir ou de rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données. Ils ne peuvent être utilisées qu'à cette fin. Il existe parfois des réglementations similaires mais spécifiques en matière de journalisation chez les prestataires informatiques externes.

4.9 Développement

Les demandes de développement du système sont regroupées et définies, budgétisées et réalisées sous forme de maintenance ou de projet. La procédure et la gouvernance sont régies dans le cadre de la «gestion de projets Helsana».

4.10 Soutien aux personnes détenant un droit d'accès et obligation de déclaration

Sur le plan technique, les personnes détenant un droit d'accès sont soutenues par les services spécialisés de la direction des domaines correspondants. L'assistance technique portant sur les systèmes informatiques et le réseau est assurée par le service informatique d'Helsana ou externalisée.

Les personnes détenant un droit d'accès savent que le système informatique d'Helsana doit être protégé et connaissent les prescriptions en matière de gestion du système informatique et de ses données. Les prescriptions sont décrites dans des directives et dans des notices de sensibilisation à la sécurité de l'information. Les sanctions éventuelles en cas de manquements délibérés ou par négligence à la sécurité de l'information sont connues des personnes détenant un droit d'accès.

Toutes les infractions doivent être immédiatement signalées au supérieur hiérarchique conformément au processus «Incident de sécurité» ou au système d'alerte selon le Code of Conduct.

4.11 Surveillance et responsabilité

Les responsables techniques des systèmes informatiques ou des applications s'assurent du respect des directives et du présent règlement de traitement des données par les personnes détenant un droit d'accès et de leurs prescriptions contractuelles par les prestataires informatiques externes.

5. Version

Ce règlement de traitement ne fait partie intégrante d'aucun contrat conclu avec la personne assurée ou avec d'autres tiers. Nous sommes donc en droit de le modifier à tout moment sans préavis. La version actuelle est celle publiée sur ce site Internet.

Dernière mise à jour: **septembre 2023**