



Règlement relatif au traitement des données

Sommaire

1. Situation initiale.....	3
2. Description des unités d'organisation concernées par le système.....	3
3. Description des interfaces.....	3
3.1 Interfaces avec des destinataires ou des fournisseurs de données externes.....	3
3.2 Provenance des données.....	4
4. Organigramme de l'organe exploitant le fichier	4
5. Responsabilités.....	5
6. Documents relatifs à la planification, à l'élaboration et à la gestion du fichier.....	5
7. Déclaration du fichier au Préposé fédéral à la protection des données et à la transparence (PF PDT) en accord avec la préposée à la protection des données (DSB)	5
8. Description des processus relatifs au traitement des fichiers	5
9. Provenance des données	5
10. Buts de la communication régulière de données	5
11. Procédures de contrôle et mesures techniques et organisationnelles selon l'art. 20 OLPD..	5
11.1 Contrôle des installations à l'entrée	5
11.2 Contrôle des supports de données.....	6
11.3 Contrôle du transport.....	6
11.4 Contrôle de communication.....	6
11.5 Contrôle de mémoire.....	6
11.6 Contrôle d'utilisation	6
11.7 Contrôle d'accès.....	6
11.8 Contrôle de l'introduction (journalisation).....	6
12. Description des champs de données et des unités d'organisation qui y ont accès	7
13. Nature et étendue de l'accès des utilisateurs au fichier	7
14. Procédures de traitement des données, notamment de rectification, de blocage, d'anonymisation (pseudonymisation), de sauvegarde, de conservation, d'archivage ou de destruction des données	7
15. Configuration des moyens informatiques	7
16. Procédure d'exercice du droit d'accès.....	7

1. Situation initiale

CONCORDIA Assurance suisse de maladie et accidents SA est le maître du fichier de données automatisé constitué dans le cadre de la loi fédérale sur l'assurance-maladie (LAMal). Ce dernier vise à mettre en œuvre et à gérer l'assurance-maladie et accidents dans le domaine de l'assurance obligatoire des soins (AOS) conformément à la LAMal.

Le présent règlement relatif au traitement des données est également valable pour le service indépendant de réception des données (SRD) selon l'art. 59a OAMal, qui, chez CONCORDIA, est géré en interne.

2. Description des unités d'organisation concernées par le système

CONCORDIA Assurance suisse de maladie et accidents SA exploite le système et, en sa qualité de maître du fichier de données automatisé, en est l'organe responsable.

3. Description des interfaces

3.1 Interfaces avec des destinataires ou des fournisseurs de données externes

Sur la base de l'art. 84 LAMal, CONCORDIA a délégué à des partenaires externes certains services en matière de solutions postales et d'élaboration de documents qui comprennent en partie aussi le traitement de données personnelles. Dans ce contexte, différents contrats de collaboration règlent le respect des dispositions relatives à la protection et à la sécurité des données. Certains partenaires informatiques de CONCORDIA sont en outre certifiés selon différentes normes ISO (notamment les normes ISO 9001:2008 «Systèmes de management de la qualité» et ISO/IEC 27001 «Systèmes de management de la sécurité de l'information»).

En sa qualité de maître du fichier automatisé, CONCORDIA demeure responsable de la protection des données pour les domaines externalisés (art. 22 de l'ordonnance relative à la loi sur la protection des données, OLPD).

Dans le cadre de la mise en œuvre et de la gestion de l'assurance-maladie et accidents dans le domaine de l'AOS selon la LAMal, CONCORDIA dispose d'interfaces avec des destinataires et des fournisseurs de données. Ils sont énumérés dans le tableau ci-dessous:

Destinataire/Fournisseur	But	Données particulièrement sensibles	Activation
Banques	Opérations de paiement	Non	Automatique
Autorités/Tribunaux	Art. 82 LAMal, art. 84a LAMal	Oui	Manuelle
Imprimerie externe	Magazine clients	Non	Automatique
Fournisseurs de prestations financières	Fichier des banques	Non	Automatique
Institutions communes LAMal	Compensation des risques, jours d'hospitalisation	Non	Manuelle
Partenaires HMO	Art. 84a LAMal	Oui	Manuelle
Comparateurs en ligne	Offres calculées	Non	Automatique
Cantons	RIP, art. 64 LAMal	Oui	Automatique
Fournisseurs de prestations	Art. 84a LAMal, art. 59 OAMal	Oui	Automatique / Manuelle

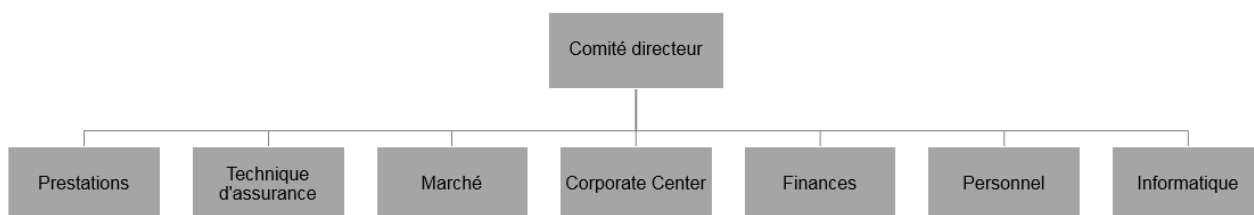
Destinataire/Fournisseur	But	Données particulièrement sensibles	Activation
MediData	Plate-forme d'échange de documents électroniques	Oui	Automatique
Partenaires de services télé médicaux	Prise en charge médicale	Oui	Manuelle
santésuisse	Renseignements, RCCo, banque de données	Non	Automatique
Sedex	RIP	Oui	Automatique
Assureurs sociaux	Art. 84a LAMal	Oui	Manuelle
Swiss Post Solutions	Affichage des justificatifs de paiement	Non	Manuelle
Centre Cada	Carte d'assuré (art. 42a LAMal, OCA)	Oui	Automatique
Assurés	Renseignements, correspondance, décomptes de prestations	Oui	Automatique / Manuelle
RCCo	Renseignements	Non	Manuelle

3.2 Provenance des données

Les données proviennent des fournisseurs de prestations, des assurés, d'autres assureurs sociaux, d'autorités et de fournisseurs de prestations financières.

4. Organigramme de l'organe exploitant le fichier

Organigramme de CONCORDIA Assurance suisse de maladie et accidents SA



5. Responsabilités

En sa qualité de maître du fichier automatisé, le Comité directeur de CONCORDIA Assurance suisse de maladie et accidents SA est responsable du respect des dispositions relatives à la protection et à la sécurité des données.

Pour toutes les questions ayant trait à la protection et à la sécurité des données, CONCORDIA dispose de préposés à la protection des données, à la sécurité des informations et à la sécurité physique. Ils conseillent le Comité directeur, édictent des directives et participent aux processus de contrôle.

6. Documents relatifs à la planification, à l'élaboration et à la gestion du fichier

L'exploitation du fichier est régie par des manuels ad hoc. La planification et l'élaboration techniques figurent dans des documents de projet, tandis que les composants du système sont répertoriés dans des manuels d'exploitation de l'unité d'entreprise Informatique.

7. Déclaration du fichier au Préposé fédéral à la protection des données et à la transparence (PFPDT) en accord avec la préposée à la protection des données (DSB)

Conformément à l'art. 11a al. 5 let. e de la loi fédérale sur la protection des données (LPD), CONCORDIA Assurance suisse de maladie et accidents SA a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers. CONCORDIA est dès lors déliée de l'obligation de déclarer le fichier au PFPDT prévue par l'art. 11a al. 2 LPD.

CONCORDIA satisfait à l'obligation de soumettre le règlement à l'approbation du PFPDT au sens de l'art. 84b LAMal.

8. Description des processus relatifs au traitement des fichiers

Les processus relatifs au traitement des données pour les différents fichiers sont réglés dans des documents internes ad hoc.

9. Provenance des données

Se référer au tableau du chapitre 3 du présent règlement.

10. Buts de la communication régulière de données

Se référer au tableau du chapitre 3 du présent règlement.

11. Procédures de contrôle et mesures techniques et organisationnelles selon l'art. 20 OLPD

Des mesures techniques et organisationnelles adéquates sont mises en œuvre afin de garantir la confidentialité, l'intégrité et la disponibilité des données.

11.1 Contrôle des installations à l'entrée

Dans l'optique d'éviter que des personnes non autorisées aient accès aux immeubles commerciaux de CONCORDIA, seuls les collaborateurs de CONCORDIA disposant d'un badge ou d'une clé peuvent y accéder.

L'accès aux immeubles commerciaux de CONCORDIA est réglé dans les directives «Accès aux biens immobiliers commerciaux de CONCORDIA» et «Zutritts- und Schliessorganisation» (règlement en matière d'accès et de fermeture, disponible en allemand uniquement).

La directive supplémentaire «Zutrittsrechte bei der Informatik» (droits d'accès aux locaux informatiques, disponible en allemand uniquement) concerne l'accès aux locaux informatiques.

11.2 Contrôle des supports de données

Par le biais de mesures techniques et organisationnelles, CONCORDIA veille à ce qu'aucune personne non autorisée ne puisse lire, copier, modifier ou supprimer des données personnelles, introduire des données personnelles dans la mémoire, ni prendre connaissance des données mémorisées, les modifier ou les effacer.

Il est possible de retracer dans les systèmes certaines modifications spécifiques effectuées par les collaborateurs.

Différents règlements et directives rappellent à ces derniers la manière correcte de traiter les données. Dans ce contexte, la directive «Utilisation du matériel informatique, des logiciels et des données électroniques» est essentielle.

L'unité d'entreprise Informatique se charge d'éliminer les supports de données en suivant un processus bien défini.

11.3 Contrôle du transport

CONCORDIA garantit, au moyen de mesures techniques et organisationnelles (par exemple, cryptage des données ou directives relatives à la gestion des e-mails), qu'aucune personne non autorisée ne puisse lire, copier, modifier ou effacer des données personnelles lors de leur communication ou lors du transport de supports de données.

11.4 Contrôle de communication

Les destinataires auxquels des données personnelles sont communiquées font l'objet d'une identification, que ce soit manuellement ou par des moyens techniques.

11.5 Contrôle de mémoire

Se référer au point 11.2 du présent règlement.

11.6 Contrôle d'utilisation

CONCORDIA dispose d'un programme de sécurité à plusieurs échelons adapté au besoin de protection des données. Les utilisateurs doivent s'identifier pour accéder aux systèmes d'informations.

11.7 Contrôle d'accès

Les autorisations d'accès aux données sont attribuées selon le principe du besoin de connaître (*need-to-know principle*), c'est-à-dire que seuls les droits nécessaires à l'exercice d'une fonction sont octroyés. L'attribution se base sur des profils d'autorisation. Des processus bien définis, complétés par des instruments techniques, permettent en outre de gérer les droits et les utilisateurs.

Les autorisations attribuées font l'objet d'un contrôle ponctuel dans le cadre des processus de contrôle internes.

11.8 Contrôle de l'introduction (journalisation)

Les données personnelles saisies sont archivées chronologiquement dans le système d'information central. En cas d'abus ou de soupçon d'abus, elles peuvent être analysées. La

directive «Utilisation du matériel informatique, des logiciels et des données électroniques» en informe les collaborateurs.

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

Dans le cadre de la déclaration du fichier, la description des champs de données et l'illustration du système de gestion des autorisations figurent dans des règlements de traitement distincts.

13. Nature et étendue de l'accès des utilisateurs au fichier

Chaque collaborateur dispose uniquement d'un accès aux données dont il a besoin pour réaliser ses tâches.

Un système de gestion des autorisations règle les modalités d'accès au fichier, définit les différents profils (rôles) et les fonctions autorisées, ainsi que l'étendue de l'accès aux données. Il contient également une liste approuvée des personnes autorisées à demander ces rôles et des responsables chargés d'approuver les attributions.

Les collaborateurs de CONCORDIA n'ont pas accès aux données MCD (Minimal Clinical Dataset) parvenant au service indépendant de réception des données et traitées de manière automatisée par ce dernier. Lorsque des factures sont sélectionnées par le service de réception des données pour vérification, les collaborateurs chargés de vérifier le cas obtiennent un accès aux factures et aux MCD s'y rapportant jusqu'à la clôture du cas.

14. Procédures de traitement des données, notamment de rectification, de blocage, d'anonymisation (pseudonymisation), de sauvegarde, de conservation, d'archivage ou de destruction des données

Les procédures relatives au traitement des données sont réglées dans des directives, règlements et manuels spécifiques (voir aussi les chapitres 13 et 15 du présent règlement).

Les utilisateurs d'un fichier suivent régulièrement des formations sur les processus techniques et les règles applicables en matière de protection des données.

15. Configuration des moyens informatiques

Les outils informatiques utilisés par CONCORDIA (matériel et logiciels) répondent à des normes internationales usuelles dans la branche. Ils sont soumis à un processus bien réglé dans le cadre de la gestion du cycle de vie.

La configuration du matériel informatique figure dans des manuels d'exploitation et fait l'objet d'adaptations ponctuelles.

16. Procédure d'exercice du droit d'accès

Les demandes d'accès au sens de l'art. 8 LPD doivent être adressées à la préposée interne à la protection des données:

CONCORDIA Assurance suisse de maladie
et accidents SA
Préposée à la protection des données
Bundesplatz 15
6002 Lucerne