KPT, Case postale, CH-3001 Berne
kpt.ch

Règlement de traitement Système d'information de la KPT

(Selon l'art. 21 OLPD et l'art. 84b LAMal)

Version 4.0 valable dès le 1. janvier 2022

Table des matières

1 Situation initiale

La KPT Caisse-maladie SA est le maître du fichier automatisé «**Système d'information de la KPT**», déclaré au préposé fédéral à la protection des données et à la transparence (PFPDT) et contenant des données sensibles et des profils de la personnalité Le fichier vise à la pratique et au suivi de l'assurance maladie et accidents dans le domaine de l'assurance obligatoire des soins et de l'assurance-maladie complémentaire selon la LCA.

Vu les articles 11 et 21 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD), un règlement de traitement doit être élaboré pour le fichier. Selon l'art. 84b de la loi fédérale sur l'assurance-maladie (LAMal), le règlement est soumis à l'appréciation du PFPDT et doit être rendu public.

2 Contenu

Le présent règlement de traitement décrit en particulier les procédures de traitement et de contrôle des données ainsi que la gestion du «système d'information de la KPT». Le règlement contient en outre les informations nécessaires à la déclaration des fichiers (art. 16 OLPD) et les indications concernant l'organe responsable de la protection et de la sécurité des données, la provenance des données, les buts dans lesquels des données sont régulièrement communiquées, les procédures de contrôle et en particulier les mesures techniques et organisationnelles visées à l'art. 20 OLPD, la description des champs de données et des unités d'organisation qui y ont accès, l'accès des utilisateurs au fichier ainsi que la nature et l'étendue de cet accès, les procédures de traitement des données, notamment les procédures de rectification, de blocage, d'anonymisation, de sauvegarde, de conservation, d'archivage ou de destruction des données, la configuration des moyens informatiques ainsi que la procédure d'exercice du droit d'accès.

Le présent règlement de traitement est également valable pour le service indépendant de réception des données selon l'art. 59a OAMal, qui est géré en interne à la KPT.

3 Documentation du système

3.1 Unités d'organisation concernées

La KPT Caisse-maladie SA est l'organe exploitant le système et, en qualité de maître du fichier automatisé «Système d'information de la KPT», l'organe qui en est responsable.

3.2 Description des interfaces

Sur la base de l'art. 84 LAMal, la KPT a externalisé quelques prestations de services comprenant en partie aussi le traitement de données personnelles et les a confiées aux partenaires d'externalisation pour l'exploitation IT ainsi qu'aux partenaires en matière de traitement des documents et de solutions postales. Le traitement des données conformément à la protection des données de même que la sécurité des données ont été réglés dans les contrats de collaboration respectifs. De plus, les partenaires IT sont en partie certifiés selon diverses normes ISO (notamment les normes ISO 9001: Système de management de la qualité et ISO/IEC 27001: Système de management de la sécurité de l'information).

Maître du fichier, la KPT demeure responsable du respect de la protection des données pour les secteurs externalisés (art. 22 OLPD).

Dans le cadre de la pratique et du suivi de l'assurance-maladie et accidents dans le domaine de l'assurance obligatoire des soins selon la LAMal, la KPT entretient des interfaces avec les fournisseurs et les utilisateurs de données qui sont décrites ci-après.

Utilisateur/fournisseur	But	Données personnelles sensibles	Déclencheur
Banques/prestataires de services financiers	Trafic de paiements	Non	Automatique/manuel
Autorités/tribunaux	Art. 82 LAMal Art. 84a LAMal	Oui	Manuel
Plaque tournante des données	Traitement de prestations LAMal	Oui	Automatique
Imprimerie externe	Magazine clients	Non	Automatique
Institution commune LAMal	Compensation des risques	Non	Manuel
Partenaire HMO	Gatekeeping, respect du contrat	Oui	Automatique
Cantons	Réduction des primes individuelle	Oui	Manuel
Fournisseur de prestations	Art. 84a LAMal	Oui	Automatique/manuel
Partenaires en matière de services télémédicaux	Suivi santé	Oui	Automatique
Partenaire en matière de recours	Recours	Oui	Automatique
santésuisse	Renseignements, RCC, pool de données	Non	Automatique
Assureurs sociaux	Art. 84a LAMal	Oui	Manuel
Cada	Carte d'assuré (LAMal art. 42a, OCA)	Oui	Automatique
Assurés	Renseignement	Oui	Automatique/manuel
Registre central des conventions (RCCo)	Renseignement	Non	Manuel

3.3 Provenance des données

Les données proviennent de fournisseurs de prestations, d'assurés, d'autres assurances sociales, d'autorités et de prestataires de services financiers.

3.4 Destinataire des données

La KPT Caisse-maladie SA est le destinataire des données. Les documents adressés personnellement (surtout les documents adressés à la direction et au médecin-conseil) sont transmis directement aux collaborateurs concernés de la KPT. Les autres documents (lettres, formulaires et factures) sont numérisés, structurés et transcodés par le partenaire en matière de traitement des documents (partenaire d'externalisation) et sont introduits respectivement dans le «système d'information de la KPT» et le flux de traitement.

Lors de la facturation de type DRG dans le domaine stationnaire, le fournisseur de prestations transmet systématiquement et simultanément avec la facture les fichiers de données avec les indications administratives et médicales visées à l'article 59, alinéa 1, OAMal au service indépendant de réception des données de la KPT selon l'art. 59a OAMal.

Les processus de traitement des données au service de réception des données sont fixés à l'annexe du présent règlement.

3.5 But de la communication régulière des données

Le but de la communication des données est dans tous les cas la pratique de l'assurance obligatoire des soins selon la loi fédérale sur l'assurance-maladie (LAMal). Des indications plus détaillées sont fournies dans la description des interfaces (chiffre 3.2).

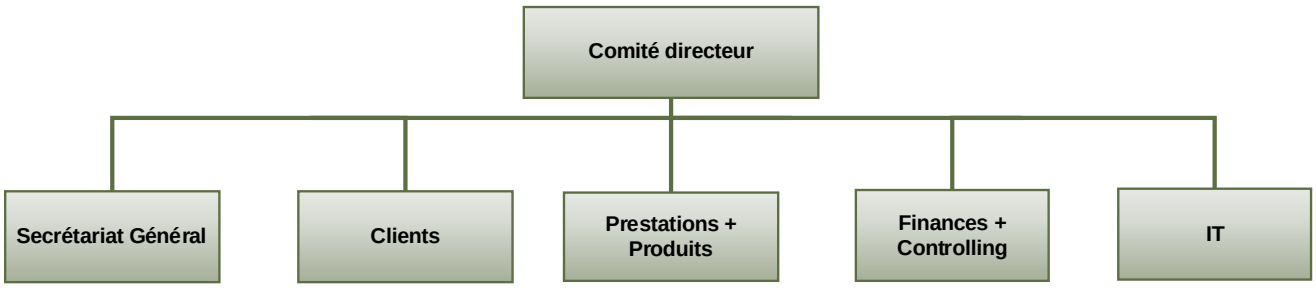
3.6 Étendue de la communication des données

La description des interfaces (chiffre 3.2) mentionne quelles données sont communiquées et quels en sont les destinataires respectifs. Les données sont communiquées exclusivement aux fins

- de l'assistance administrative dans des cas particuliers selon l'art. 32, al. 2, LPGA et l'art. 82 LAMal
- des renseignements et conseils selon l'art. 27 LPGA
- de la consultation du dossier selon l'art. 47 LPGA
- ainsi que dans le cadre de la communication de données au sens de l'art. 84a LAMal.

Toute autre communication des données s'effectue uniquement dans des cas d'espèce et si la personne assurée a donné son consentement. En outre, les données ne sont communiquées que dans la mesure où les principes énoncés à l'art. 4 et les suivants de la loi fédérale sur la protection des données (LPD) sont respectés, en particulier uniquement dans les limites des principes d'adéquation et de proportionnalité.

4 Organigramme de l'organe exploitant le système



5 Responsabilités

En qualité de maître du fichier, le Comité directeur de la KPT Caisse-maladie SA assume la responsabilité de la protection des données et de la sécurité des données. Les affaires relatives à la protection et à la sécurité des données sont couvertes par les fonctions de Governance (protection des données, Corporate Security, Compliance et GIRC). Les fonctions de Governance conseillent le Comité directeur, définissent des prescriptions et sont intégrées aux processus de contrôle.

6 Documentation de planification, de réalisation et d'exploitation du fichier

L'exploitation du fichier est décrite de manière appropriée.

La documentation technique des composantes du système est fournie dans les manuels d'exploitation correspondants.

La planification et la réalisation des actualisations (cycle de vie) et des développements sont gérées et documentées via la gestion de projet selon HERMES.

7 Déclaration du fichier au PFPDT (Art. 16 OLPD)

Conformément à l'art. 11a, al. 5, let. e, LPD, la KPT Caisse-maladie 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. La KPT est ainsi dispensée de l'obligation de déclarer le fichier au PFPDT.

8 Documentation des processus du système d'information de la KPT

Les processus de traitement des données du «système d'information de la KPT» sont documentés dans l'outil central de gestion des processus et peuvent être consultés par l'ensemble des collaboratrices et collaborateurs de la KPT.

9 Procédures de contrôle ainsi que mesures techniques et organisationnelles selon l'art. 20 OLPD

9.1 Contrôles des entrées et des accès

Afin de garantir que des personnes non autorisées n'auront pas accès aux immeubles de la KPT, seuls les collaborateurs de la KPT possédant un badge ou une clé peuvent y accéder.

Il n'est permis de pénétrer dans les bureaux qu'aux fins de service. Aucun accès à l'immeuble n'est accordé aux personnes inconnues. En cas de doute, les personnes doivent décliner leur identité.

Les visiteuses et visiteurs doivent se présenter à la réception et être enregistrés. Un interlocuteur de la KPT vient les chercher à la réception et ils ne peuvent se déplacer dans le bâtiment qu'accompagnés. L'accès aux immeubles de la KPT est régi par des instructions internes.

9.2 Contrôle des accès

La KPT dispose d'une infrastructure de sécurité à plusieurs niveaux pour l'accès au «système d'information de la KPT». Tous les collaborateurs disposent d'un login pour l'utilisation du système.

Les droits d'accès sont régis à l'aide d'un système d'autorisation des accès basé sur des rôles et sont consignés dans des concepts d'autorisations ainsi que des matrices d'accès (art. 21, al. 2, let. e OLPD).

La définition et la mise en œuvre de concepts d'autorisation adaptés permettent de limiter l'accès aux fichiers selon le principe «need to know» (exécution des tâches selon l'art. 84 LAMal). Ceci permet d'interdire les consultations, modifications ou suppressions non autorisées.

Les collaborateurs disposant de droits d'accès afin d'exécuter des tâches sont tenus de traiter correctement les données conformément aux documents prescriptifs.

9.3 Contrôle de l'introduction (journalisation)

Toutes les entrées et tous les accès font l'objet d'une journalisation vérifiable.

La KPT effectue une journalisation des activités les plus importantes déployées. Afin de contrôler le respect du règlement d'utilisation, la KPT analyse les journalisations sous forme anonyme.

Lorsqu'un abus est constaté ou suspecté, les journalisations sont analysées nommément avec la liste de correspondance. En cas d'abus avéré, les sanctions correspondantes sont engagées. Les collaborateurs de la KPT sont informés de ce procédé.

9.4 Contrôle des supports de données/mémoires

La KPT assure en outre à l'aide de mesures appropriées qu'aucune personne non autorisée ne pourra lire, copier, modifier ou supprimer des données dans le «système d'information de la KPT» et qu'il sera impossible d'introduire des données non autorisées dans la mémoire de même que de prendre connaissance des données mémorisées, de les modifier ou de les effacer.

Comme décrit ci-dessus, il est garanti d'une part par le contrôle des installations à l'entrée que des personnes externes non autorisées n'auront pas accès aux immeubles de la KPT de sorte qu'un traitement de données par des externes non autorisés peut être exclu. Afin d'éviter un traitement de données non autorisé par des collaborateurs de la KPT, la KPT limite ou empêche, par des mesures techniques, l'accès aux données dont les collaborateurs n'ont pas besoin pour accomplir les tâches qui leur sont confiées selon la LAMal (art. 84 LAMal). D'autres développements concernant la limitation d'accès sont exposés au chiffre 11 du présent règlement.

Aussi, divers règlements ainsi que des directives exhortent les collaborateurs au traitement correct des données. La manière correcte de traiter des données est transmise aux collaborateurs par le biais de règlements.

En outre, il est possible de retracer les modifications effectuées par les collaborateurs dans le système (voir chiffre 9.3).

9.5 Contrôle du transport

La KPT garantit par des mesures techniques et organisationnelles appropriées que des personnes non autorisées ne pourront pas lire, copier, modifier ou effacer des données personnelles lors de leur communication (e-mail p. ex.) ou lors du transport de supports de données (p. ex. à l'aide de cryptage, de HIN-mail ou d'instructions relatives à la gestion des e-mails).

9.6 Contrôle de la communication

Le destinataire auquel des données personnelles sont communiquées est vérifié manuellement ou à l'aide d'outils techniques.

9.7 Contrôle des utilisateurs

Voir le chiffre 9.2

10 Description des champs de données et des unités d'organisation qui y ont accès (art. 21, al. 2, let. e, OLPD)

Les droits d'accès au «système d'information de la KPT» sont régis par un système d'autorisations d'accès basé sur des rôles. Une matrice de droits précise quels rôles disposent d'un accès au «système d'information de la KPT» et quelle en est la nature.

11 Accès des utilisateurs au fichier, ainsi que nature et étendue de cet accès (art. 21, al. 2, let. f, OLPD)

L'accès au «système d'information de la KPT» n'est accordé qu'aux collaborateurs qui en ont effectivement besoin. Les collaborateurs sont attribués à un profil d'utilisateur (cf. chiffre 9.2 ci-dessus) et reçoivent ensuite une autorisation d'accès personnelle qui ne peut pas être transmise à des tierces personnes. On détermine notamment aussi si les collaborateurs ont uniquement besoin d'une autorisation de consultation ou s'ils ont également besoin d'une autorisation d'effectuer des mutations.

Les collaborateurs de la KPT n'ont pas accès aux données MCD parvenant au service indépendant de réception des données de la KPT et qui sont traitées de manière automatisée par ce dernier. Lorsque des factures sont déviées 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. L'accès aux MCD est bloqué dès la clôture du cas.

Les demandes d'autorisation doivent être approuvées par le supérieur concerné et le propriétaire de l'autorisation. Il faut ensuite retirer les autorisations aux collaborateurs lorsqu'elles ne sont plus nécessaires à l'exécution des missions qui leur sont confiées.

12 Formation des utilisateurs du fichier

Les utilisateurs du «système d'information de la KPT» sont formés par différentes voies en matière de droit de la protection des données ainsi que dans la technique des applications. Tous les nouveaux collaborateurs de la KPT doivent suivre une formation dans le domaine de la protection des données. Une formation relative aux applications du «système d'information de la KPT» doit également être accomplie. En outre, la KPT forme les collaborateurs par un module e-learning dans le domaine de la protection des données.

Les utilisateurs du «système d'information de la KPT» sont soutenus dans tout le système en fonction des champs par divers manuels d'utilisateurs et dans le domaine de la protection des données par des règlements sur la protection des données.

13 Les procédures de traitement des données, notamment les procédures de rectification, de blocage, d'anonymisation (pseudonymisation), de sauvegarde, de conservation, d'archivage ou de destruction des données (art. 21, al. 2, let. g, OLPD)

Chaque mutation effectuée par un collaborateur de la KPT est consignée techniquement (cf. chiffre 9.3 ci-dessus). L'état avant et après la mutation apparaît toujours afin de garantir la traçabilité du traitement des données.

Les procédures de traitement des données sont documentées dans des instructions, des règlements et des manuels spécifiques.

14 La configuration des moyens informatiques (art. 21, al. 2, let. h, OLPD)

Le matériel informatique et les logiciels utilisés par la KPT après concertation avec les partenaires d'externalisation correspondent aux standards internationaux et font l'objet de contrôles réguliers réalisés par des auditeurs indépendants (ISAE-3402; ISO 27001).

Les documentations relatives à la configuration des moyens informatiques utilisés pour le «système d'information de la KPT» sont conservées dans le secteur IT et auprès des partenaires d'externalisation de la KPT et mises à jour le cas échéant.

15 La procédure d'exercice du droit d'accès (art. 21, al. 2, let. i, OLPD)

Les demandes d'accès selon l'art. 8 LPD doivent être soumises au conseiller à la protection des données:

KPT
Protection des données
Wankdorfallee 3
3014 Berne

datenschutz@kpt.ch

16 Publication

Selon l'art. 84b LAMal, le présent règlement est publié sur Internet sous kpt.ch.