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

Règlement de traitement de la KPT

(Selon les art. 5 et 6 OPDo et l'art. 84b LAMal)

Table des matières

1 Situation initiale 2
2 Contenu 2
3 Documentation du système 2
3.1 Unités d'organisation concernées 2
3.2 Origine des données, buts du traitement, transmission des données 2
3.3 Prestataires externes / Interfaces 2
4 Organigramme de l'organe exploitant le système 3
5 Responsabilités 3
6 Documentation de planification, de réalisation et d'exploitation 3
7 Procédures de contrôle ainsi que mesures techniques et organisationnelles selon l'art. 3 OPDo 3
7.1 Généralités 3
7.2 Contrôles des entrées et des accès 3
7.3 Contrôle des accès 4
7.4 Contrôle de l'introduction (journalisation) 4
7.5 Contrôle des supports de données/mémoires 4
7.6 Contrôle du transport 5
7.7 Contrôle de la communication 5
7.8 Contrôle des utilisateurs 5
8 Journalisation selon art. 4 OPDo 5
9 Formation des utilisateurs 5
10 Version / Modification 5

1 Situation initiale

La KPT Caisse-maladie SA et la KPT Assurances SA traitent des données personnelles (sensibles). Le traitement des données 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 5 et 6 de l'ordonnance sur la protection des données (OPDo), la KPT Caisse-maladie SA, en tant qu'organe fédéral responsable, et la KPT Assurances SA, en tant que responsable privé, doivent rédiger un règlement de traitement pour le traitement automatisé de leurs données personnelles. 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 règlement de traitement contient en particulier des indications sur l'organisation interne, sur la procédure de traitement et de contrôle des données ainsi que sur les mesures visant à garantir la sécurité des données.

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 et la KPT Assurances SA (désignées ci-après par KPT) exploitent ensemble les systèmes informatiques en tant qu'organe responsable.

3.2 Origine des données, buts du traitement, transmission des données

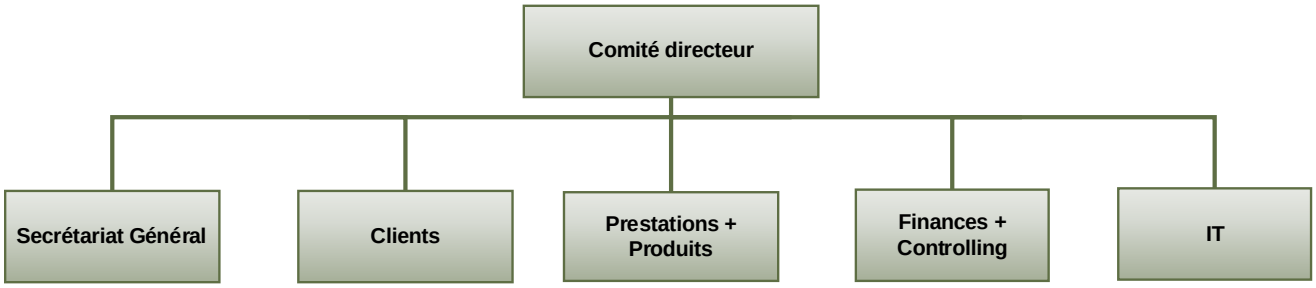
Dans la déclaration de protection des données, la KPT informe de manière transparente comment, à quelles fins et sur quelle base juridique elle collecte et traite des données personnelles et à qui elle communique des données personnelles. En outre, les personnes concernées sont informées de leurs droits (droit d'accès, de rectification et de remise des données).

3.3 Prestataires externes / Interfaces

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 sont 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).

Dans le cadre de la mise en œuvre et de la gestion de l'assurance-maladie et accidents dans le domaine de l'assurance obligatoire des soins selon la LAMal ainsi que de l'assurance-maladie complémentaire selon la LCA, différentes interfaces permettent le contact direct avec les assurés, les prestataires de services externes (p. ex. banques, partenaires de recours, autorités) et les fournisseurs de prestations (p. ex. partenaires HMO, partenaires de services de télémédecine). La protection et la sécurité des données sont garanties par une authentification forte et une technologie moderne de cryptage et de transmission.

4 Organigramme de l'organe exploitant le système



5 Responsabilités

Le Comité directeur de la KPT 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

L'exploitation des systèmes informatiques est décrite de manière appropriée.

Les traitements de données sont définis dans des règlements, des directives et des manuels et sont documentés dans l'outil central de gestion des processus ainsi que dans le registre des activités de traitement. Les documents sont régulièrement mis à jour par les unités organisationnelles compétentes.

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 la gouvernance de projet.

7 Procédures de contrôle ainsi que mesures techniques et organisationnelles selon l'art. 3 OPDo

7.1 Généralités

En matière de mesures techniques et organisationnelles de la sécurité des données, la KPT s'oriente vers des standards établis au niveau international tels que ISO/IEC 27001 et NIST (National Institute of Standards and Technology). En plus de diverses certifications ISO, les partenaires en externalisation informatique disposent d'un rapport ISAE-3402 dans lequel le système de contrôle interne est contrôlé et documenté par des auditeurs indépendants.

7.2 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. Les badges et badges de visiteurs doivent être portés de manière bien visible à l'intérieur du bâtiment. 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.

7.3 Contrôle des accès

La KPT dispose d'une infrastructure de sécurité à plusieurs niveaux pour l'accès aux systèmes informatiques. Tous les collaborateurs disposent d'un login pour leur utilisation.

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.

La définition et la mise en œuvre de concepts d'autorisation adaptés permettent de limiter l'accès aux données personnelles selon le principe «need to know». En particulier, il est également déterminé si les collaborateurs ont uniquement besoin d'une autorisation de consultation ou s'ils ont en outre besoin d'une autorisation de mutation. Ceci permet d'interdire les consultations, modifications ou suppressions non autorisées.

Les autorisations sont accordées ou retirées automatiquement aux collaborateurs en fonction de leur profil (organisation, fonction, niveau de cadre).

Les demandes d'autorisation manuelles supplémentaires sont soumises à une procédure d'autorisation à deux ou trois niveaux. Le retrait des autorisations qui ne sont plus nécessaires s'effectue selon un processus défini.

De plus, des attestations sont régulièrement effectuées pour toutes les autorisations. Les demandes d'autorisation doivent être approuvées par les supérieurs hiérarchiques respectifs et le propriétaire de l'autorisation. Les autorisations sont retirées aux collaborateurs lorsqu'elles ne sont plus nécessaires pour les tâches confiées.

Les collaborateurs de la KPT n'ont pas accès aux données MCD (Minimal Clinical Dataset) qui sont reçues par l'organe indépendant de réception des données de la KPT et qui sont traitées de manière automatisée par celui-ci. Si des factures sont transmises par l'organe de réception des données pour vérification, les collaborateurs chargés de la vérification des cas ont accès aux factures ainsi qu'aux MCD correspondants jusqu'à la clôture du cas. L'accès aux MCD est bloqué à la clôture du cas.

7.4 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.

7.5 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 les systèmes informatiques 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. D'autres développements concernant la limitation d'accès sont exposés au chiffre 7.3 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 documents de référence sur la protection des données.

En outre, il est possible de retracer les modifications effectuées par les collaborateurs dans le système (voir chiffre 7.4).

7.6 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).

7.7 Contrôle de la communication

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

7.8 Contrôle des utilisateurs

Voir le chiffre 7.3

8 Journalisation selon art. 4 OPDo

Outre le contrôle des accès aux systèmes informatiques, il est procédé à une journalisation des traitements automatisés afin de pouvoir constater a posteriori si les données ont été traitées aux fins pour lesquelles elles ont été collectées ou communiquées. La journalisation est effectuée en application de l'article 4 de l'OPDo. Les procès-verbaux sont conservés pendant au moins 12 mois à des fins de révision. Ils ne sont accessibles qu'aux organes et personnes chargés de vérifier l'application des règles de protection des données ou de préserver ou de rétablir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données, et ne peuvent être utilisés qu'à cette fin. Les prestataires de services informatiques externes disposent de leurs propres règles en matière de journalisation.

9 Formation des utilisateurs

Les utilisateurs des systèmes informatiques 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 des systèmes informatiques 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 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 documents de référence sur la protection des données.

10 Version / Modification

Le présent règlement de traitement ne fait pas partie d'un contrat conclu avec les assurés ou d'autres tiers. Il peut être adapté à tout moment. La version publiée sur ce site web est la version actuelle.