HOTELA

HOTELA

L´ASSURANCE SOCIALE

HOTELA Caisse maladie

Règlement de traitement des données

Entrée en vigueur : 05.07.2021

Rue de la Gare 18 • Case Postale 1251 • 1820 Montreux 1 • T. 021 962 49 49 • welcome@hotela.ch • www.hotela.ch

I. Table des matières

II. Historique des modifications

Date	Version	Visa	Modifications
01.04.2013	1.0	CGC/BFA	Rédaction initiale
30.11.2014	1.1	RP/BFA	Revue
28.06.2021	1.2	UHI/CGC	Revue et adaptation

Relecteur	Points / chapitres spécifiques à valider	Date
Direction	Validation du Règlement	05.07.2021

HOTELA

Abréviations

CPD	Conseiller à la Protection des Données
CRM	Customer Relationship Management / Gestion de la Relation Client
GED	Gestion électronique des documents
IDJ	Indemnités journalières
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LPD	Loi fédérale sur la protection des données
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales
OFSP	Office fédéral de la santé publique
OLPD	Ordonnance relative à la loi sur la protection des données
PFPDT	Préposé fédéral à la protection des données et à la transparence
RH	Ressources humaines
RSSI	Responsable de la Sécurité du Système d'Information
SMSI	Système de Management de la Sécurité de l'Information
SOA	Service oriented architecture / Architecture orientée services

1 Introduction

HOTELA Caisse maladie est un assureur maladie social limitant son activité à l'assurance d'indemnités journalières en faveur des membres d'une association professionnelle au sens de l'art. 98, al. 2 de la Loi fédérale sur l'assurance-maladie (LAMal).

HOTELA Caisse maladie est entièrement gérée par HOTELA Caisse de compensation AVS, au siège de cette dernière, selon la délégation de tâches autorisée par l'art. 63, al. 4 de la Loi fédérale sur l'assurance-vieillesse et survivants (LAVS). HOTELA Caisse maladie n'emploie aucun collaborateur.

L'organigramme en annexe 1 représente les unités de HOTELA Caisse de compensation AVS, lesquelles participent presque intégralement à l'activité de HOTELA Caisse maladie.

2 Bases légales et objectifs du document

Au vu des art. 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 chaque fichier automatisé contenant des données personnelles particulièrement sensibles et/ou des profils de la personnalité. 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.

Le règlement de traitement décrit en particulier les processus de traitement et de contrôle des données et la gestion du traitement électronique des données. Il contient les informations sur les organes responsables de la protection et de la sécurité des données, sur la provenance des données et les buts pour lesquels elles sont régulièrement communiquées. Il décrit la procédure relative à l'octroi des autorisations d'accès aux modules des systèmes d'information électroniques.

Le système de données géré par HOTELA Caisse maladie doit permettre à cette dernière l'activité d'assurance précitée (collecte des informations, traitement des dossiers, paiement des prestations, encaissement des primes).

Le système d'information de HOTELA Caisse maladie est conçu sur une architecture SOA. De ce fait, les applications et les données forment un seul et unique système d'information, lequel doit par conséquent être traité comme une application monolithique.

3 Rôles et responsabilités

La Direction de HOTELA assume la responsabilité de la protection des données et de la sécurité de l'information. En ce qui concerne les questions relevant du droit de la protection des données et de la sécurité de l'information, elle est appuyée par le Conseiller à la Protection des données (CPD) et par le Responsable de la Sécurité des Systèmes d'Information (RSSI).

Pour chaque élément composant le système d'information (applications, bases de données, systèmes et réseaux), les responsabilités sont formellement attribuées.

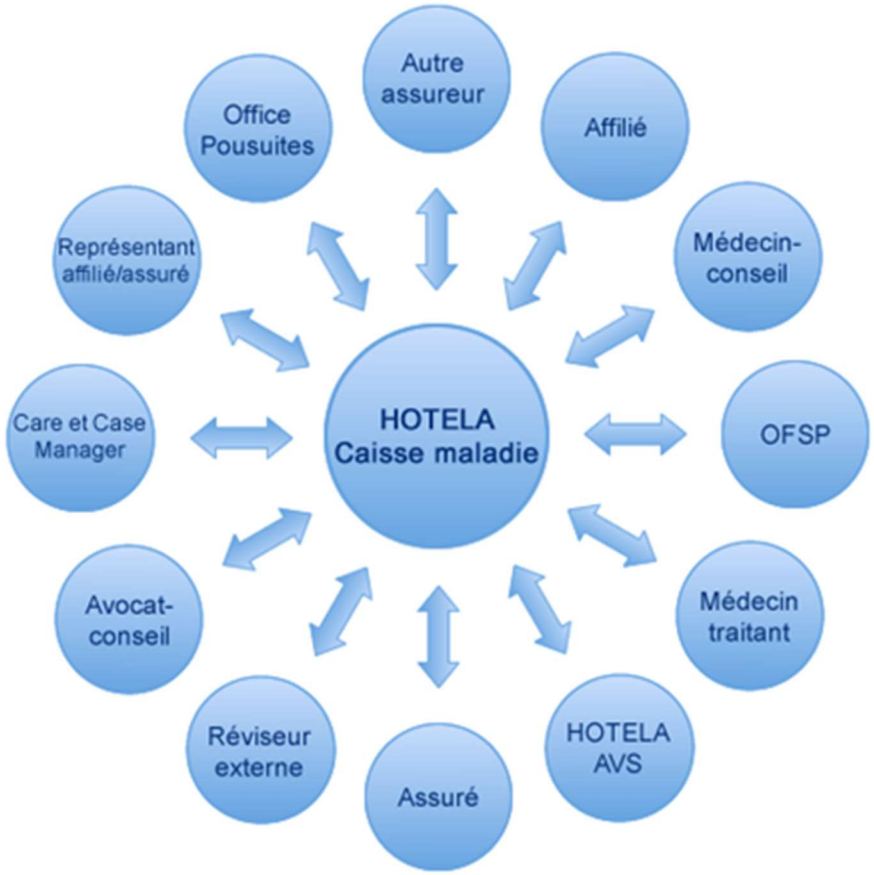
Le tableau ci-dessous décrit la répartition des rôles et responsabilités :

Rôles	**Responsabilités**
Protection des données et sécurité de l'information en général et formations	Conseiller à la Protection des Données (CPD) et Responsable de la Sécurité des Systèmes d'Information (RSSI)
Demandes d'accès et de consultation de dossiers	Conseiller à la Protection des Données (CPD)

Sécurité technique des données	Corporate ICT
Profils d'accès	Ressources humaines et Corporate ICT
Destruction des données électroniques	Corporate ICT
Données clients	Direction Client Services & Processes
Données des sinistres	Management IDJ LAMal
Documents destinés au Médecin- conseil	Médecin-conseil

4 Documentation des unités d'organisation concernées par le système

Le fichier de données fait partie d'un système composé d'unités d'organisation interconnectées.



4.1 Interfaces

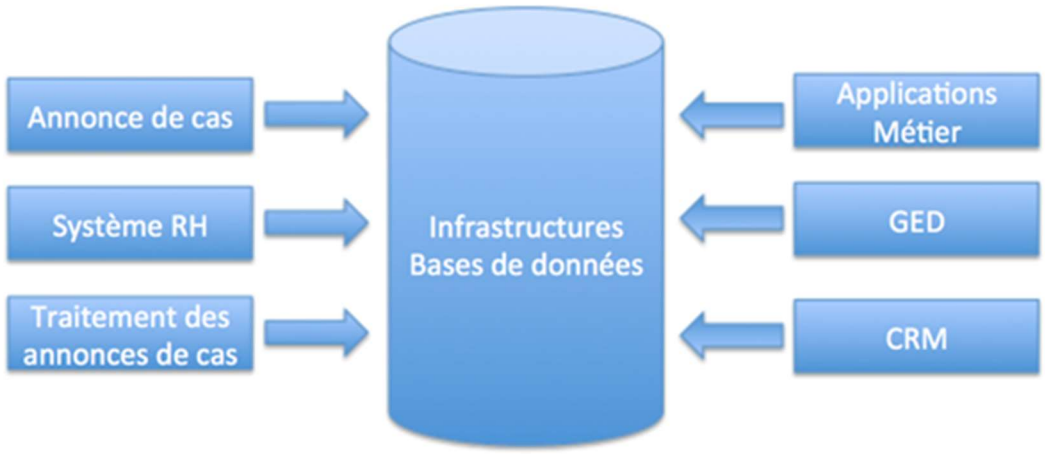
Dans les interfaces grisées, un flux de données identiques s'opère également dans le sens inverse.

De	À	But	Type de données	Périodicité	Initiateur	Média
HOTELA Caisse maladie	HOTELA Caisse de compensation AVS	Délégation de tâches	Administratives, sensibles	Quotidien	HOTELA Caisse maladie	--
HOTELA	Affilié (employeur)	Encaissement des primes	Administratives	Mensuel	HOTELA	Papier
HOTELA	Office des poursuites	Encaissement des primes	Administratives, sensibles	Mensuel	HOTELA	Papier Mail
HOTELA	Réviseur externe	Révision	Administratives, sensibles	Annuel	Réviseur externe	Papier
HOTELA	OFSP	Surveillance et statistiques	Administratives	Annuel	OFSP	Papier
HOTELA	Affilié (employeur)	Paiement des indemnités journalières	Administratives	Quotidien	HOTELA	Papier
HOTELA (Service médical)	Médecin traitant	Justification de l'incapacité de travail	Sensibles	Quotidien	HOTELA	Papier
HOTELA	Assuré	Paiement des indemnités journalières	Administratives	Quotidien	HOTELA	Papier
HOTELA	Care- et Case-Manager	Suivi du cas	Administratives	Quotidien	HOTELA	Papier Mail
HOTELA (Service médical)	Médecin-conseil	Suivi du cas	Administratives, sensibles	Quotidien	HOTELA	Papier Fax
HOTELA	Avocat-conseil	Suivi du cas	Administratives, sensibles	Quotidien	HOTELA	Papier Mail
HOTELA	Inspecteur sinistre	Suivi du cas	Administratives, sensibles	Quotidien	HOTELA	Papier Mail Media
Affilié (employeur)	HOTELA	Etablir le décompte de prime	Administratives	Annuel	Affilié	Papier Web
Affilié (employeur)	HOTELA	Affiliation	Administratives	Quotidien	Affilié ou HOTELA	Papier Mail
Assuré	HOTELA	Affiliation	Administratives, sensibles	Quotidien	Assuré	Papier Web
Représentant de l'affilié/assuré	HOTELA	Affiliation	Administratives	Quotidien	Représentant ou HOTELA	Papier Web
Affilié (employeur)	HOTELA	Annonce des cas	Administratives	Quotidien	Affilié	Papier Web
Affilié	HOTELA	Suivi du cas	Administratives	Quotidien	Affilié	Papier Mail Web

Représentant de l'affilié/assuré	HOTELA	Suivi du cas	Administratives	Quotidien	Tiers	Papier Mail Web
Assuré	HOTELA	Suivi du cas	Administratives	Quotidien	Assuré ou HOTELA	Papier Mail
Autre assureur	HOTELA	Coordination	Administratives, sensibles	Quotidien	HOTELA ou Autre assureur	Papier Mail Media amovibles

4.2 Applications d'exploitation

Les bases de données qui composent la totalité du fichier entretiennent des relations avec des applications métiers tierces, qui accèdent régulièrement au fichier afin de traiter des données relatives à leur besoin métier. Ces applications sont schématisées ci-dessous.



5 Plan de traitement

5.1 Processus de traitement

5.1.1 Réception des données

Les données entrant sous forme de documents papier sont scannées pour être ensuite distribuées au service habilité à les traiter. Les données entrant par le web sont distribuées au service habilité à les traiter.

5.1.2 Traitement des données

Le traitement des données s'opère conformément à la procédure interne de traitement des données en vigueur (« Système de contrôle interne - Prestations IDJ maladie LAMal »).

5.1.3 Archivage des données

Se référer au point 6.1.1.

5.1.4 Destruction des données

Les documents papier sont détruits par une société de service sécurisé de destruction de documents. La destruction des données électroniques s'opère conformément aux directives internes (« Politique de conservation et de mise au rebut des données » et « Politique de gestion de supports électroniques et papier »).

5.2 Organe responsable de la protection et de la sécurité des données

La totalité des activités de HOTELA Caisse maladie est déléguée à HOTELA Caisse de Compensation AVS, raison pour laquelle cette dernière est responsable de la protection et de la sécurité des données conformément au contrat de délégation de tâches.

5.3 Provenance des données

Se référer aux « interfaces » du point 4.1.

5.4 Buts dans lesquels les données sont régulièrement communiquées

Se référer aux « interfaces » du point 4.1.

5.5 Procédure d'exercice du droit d'accès

Toute personne peut demander à HOTELA si des données la concernant sont traitées. Le droit d'accès est basé sur les art. 8 et 9 de la Loi fédérale sur la protection des données (LPD) ainsi que sur les art. 1 et 2 de son Ordonnance d'application (OLPD). Le requérant doit en règle générale présenter une demande écrite et justifier de son identité. Les détails du processus objet de l'annexe 2 au présent Règlement sont traités dans le document interne « Document de gestion IDJ-LAMal ».

6 Gestion des risques

6.1 Mesures techniques et organisationnelles

6.1.1 Contrôle des installations à l'entrée

« les personnes non autorisées n'ont pas accès aux locaux et aux installations utilisées pour le traitement de données personnelles »

- Tous les accès aux différents locaux hébergeant des données sont sécurisés par un contrôle d'accès avec badge.
- L'accès au guichet de la réception est possible durant les heures officielles d'ouverture. Une procédure d'accueil des visiteurs est implémentée afin de sécuriser les accès.
- Les archives sont stockées dans un local distant fermé à clé accessible uniquement à un nombre restreint de personnes autorisées.
- L'accès à la salle serveur est géré par un système électronique de badge. L'accès à cette salle n'est octroyé qu'au personnel strictement autorisé. Le local dispose d'un système d'alarme (effraction et risques naturels).
- L'accès aux applications se fait par l'identification et l'authentification de chaque utilisateur sur son poste de travail, puis sur l'application concernée. La complexité des mots de passe est régie par la politique de mots de passe en vigueur.
- Afin de garantir la sécurité des documents, une politique de bureau propre et d'écran vide est implémentée.

6.1.2 Contrôle des supports de données personnelles

« les personnes non autorisées ne peuvent pas lire, copier, modifier ou éloigner des supports de données »

- Les supports de données (physiques ou logiques) sont protégés contre les accès non autorisés par l'application de la politique de bureau propre et écran vide.

6.1.3 Contrôle du transport

« les personnes non autorisées ne peuvent pas lire, copier, modifier ou effacer des données personnelles lors de leur communication ou lors du transport de supports de données »

- Lors du transport de données sensibles sur supports physiques électroniques (clés USB etc...), les données sont chiffrées.
- Lors du transport de données sensibles sur support papier, les données sont mises sous pli confidentiel fermé.
- Le transport de données sous forme électronique sur la plateforme internet est chiffré par SSL.

6.1.4 Contrôle de communication

« les destinataires auxquels des données personnelles sont communiquées à l'aide d'installations de transmission peuvent être identifiés»

- L'identification des clients sur la plateforme Internet est faite sur la base d'un nom d'utilisateur et d'un mot de passe.

6.1.5 Contrôle de mémoire

« les personnes non autorisées ne peuvent ni introduire de données personnelles dans la mémoire ni prendre connaissance des données mémorisées, les modifier ou les effacer »

- L'introduction de données par l'intermédiaire de supports externes (disques USB, DVD, CD etc.) est limitée au personnel autorisé.
- Pour introduire des données via un support externe, une demande de service doit être faite.
- Aucune introduction ou interrogation de données ne peut être faite sans authentification sur le système d'information et ceci en conformité avec les points « Contrôle d'accès » détaillé ci-dessous.

6.1.6 Contrôle d'utilisation

« les personnes non autorisées ne peuvent pas utiliser les systèmes de traitement automatisé de données personnelles au moyen d'installations de transmission »

- Tous les systèmes sont configurés de manière à demander une authentification.
- Seules les personnes autorisées peuvent se connecter au système d'information.

6.1.7 Contrôle d'accès

« les personnes autorisées ont accès uniquement aux données personnelles dont elles ont besoin pour accomplir leurs tâches »

- Chaque utilisateur HOTELA reçoit un accès lui permettant de consulter les données de base des personnes recensées dans notre système d'information. Cependant des droits d'accès spécifiques sont nécessaires afin d'accéder aux données sensibles (médicales).
- Conformément à la politique de gestion des accès, une revue périodique est effectuée.
- Chaque personne se voit attribuer un identifiant unique ainsi qu'un mot de passe personnel. De plus, chaque utilisateur dispose d'un identifiant et d'un mot de passe spécifique pour les applications de gestion.

6.1.8 Contrôle de l'introduction (journalisation)

« l'identité des personnes introduisant des données personnelles dans le système, ainsi que les données introduites et le moment de leur introduction peuvent être vérifiés a posteriori (des procès-verbaux de journalisation ne doivent être établis qu'en cas de nécessité, après en avoir dûment informé les personnes concernées) »

- L'application CRM journalise toutes les transactions effectuées (ajout, suppression, modification) et ce de manière à pouvoir identifier l'auteur de la transaction.

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

La matrice décrit les accès aux différents champs de données.

Groupes d'utilisateurs	Données liées aux affiliations et contacts clients		Données liées aux prestations		Données médicales physiques		Données médicales électroniques		Données liées aux décomptes de cotisations		Données liées à la comptabilité		Transferts de données	
Actions	Lecture	Saisie, mutation	Lecture	Saisie, mutation	Lecture	Saisie, mutation	Lecture	Saisie, mutation	Lecture	Saisie, mutation	Lecture	Saisie, mutation	Import	Export
Collaborateurs « Assurances » LAMal	x		x	x	x	x	x	x			x	x		
Collaborateurs « Vente », « Gestion des employeurs »	x		x						x	x		x		
Collaborateurs « Gestion des événements »	x	x									x		x	
Collaborateurs « Service interne »	x													
Collaborateurs « Finances »	x										x	x		
Collaborateurs « Transformation & Technology »	x	x	x	x			x	x	x	x	x	x	x	x
Collaborateurs « Marketing »	x													
Collaborateurs « Affaires juridiques »	x		x						x					

Les actions « saisie » et « mutation » comprennent la modification et la suppression.

6.3 Nature et étendue de l'accès des utilisateurs au fichier

Les droits des utilisateurs sont octroyés selon la procédure de création des comptes utilisateurs en vigueur. Chaque demande de droits est faite via un outil de gestion du changement et déclenche une procédure de validation.

6.4 Procédure de traitement des données notamment les procédures de rectification, sauvegarde, conservation, archivage ou destruction des données

Les procédures opérationnelles suivantes sont observées quotidiennement pour le traitement des données personnelles ou sensibles.

Rectification de données : opération manuelle ou scriptée

Sauvegarde de données :	selon politique de sauvegarde SMSi
Conservation des données :	selon concept du SMSi
Archivage des données :	archives physiques (papier) + sauvegardes
Destruction des données :	selon procédure définie dans le SMSi (ITS13)

6.5 Configuration des moyens informatiques

La configuration des moyens informatiques est faite selon les recommandations et procédures opérationnelles décrites dans le système de management de la sécurité de l'information (SMSi).

6.5.1 Application

Les applications sont développées en suivant une méthodologie de développement itérative avec des tests informatiques et métier tout au long du cycle de vie de l'application.
Toute modification des applications est tracée dans l'outil de gestion du changement et fait l'objet d'une mise en production réglementée.

6.5.2 Réseau

- Seuls les équipements HOTELA sont autorisés à se connecter sur le réseau opérationnel de HOTELA.
- Les accès sur les équipements réseau sont restreints au personnel autorisé du service informatique.

6.5.3 Base de données

- Les différentes bases de données sont configurées de manière à n'autoriser aucun accès non identifié et autorisé.
- Les bases de données sont installées dans des zones sécurisées du réseau.

6.5.4 Système d'exploitation

- Les systèmes d'exploitation sont protégés par un antivirus.
- Une gestion du changement permet de tracer toutes les modifications apportées aux différents systèmes d'exploitation.

6.5.5 Hardware

- Tout le hardware est référencé dans un inventaire centralisé.
- Tout le hardware est placé dans des zones surveillées.
- Aucun système n'est laissé en accès ouvert.

7 Entrée en vigueur

Le présent Règlement entre en vigueur le 05.07.2021.

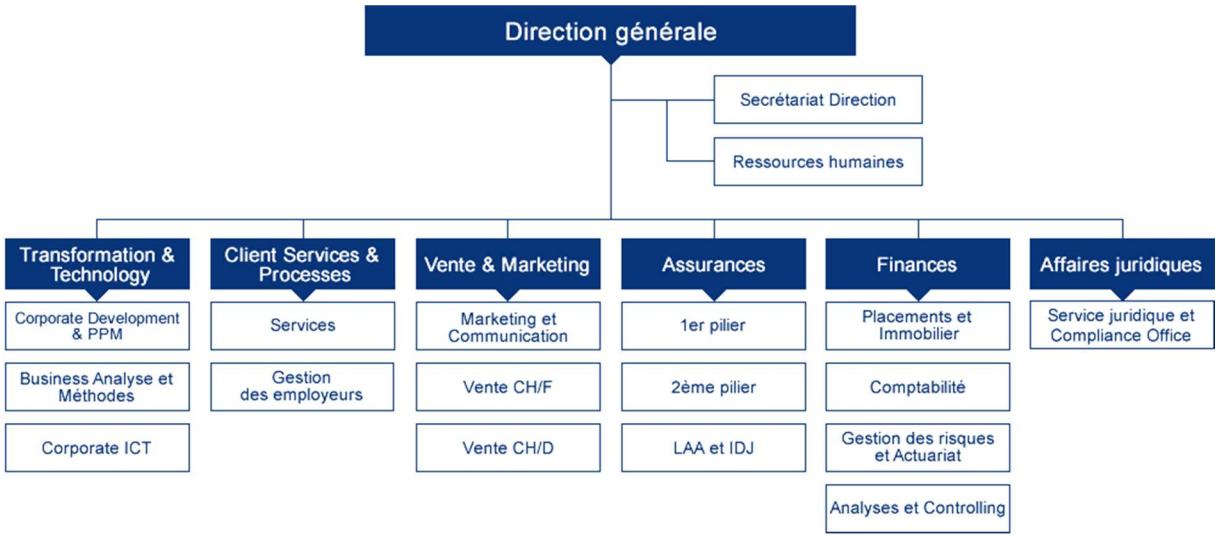
Il remplace le Règlement entré en vigueur le 1er avril 2013.

Il est soumis à l'appréciation du PFPDT et publié sur le site www.hotela.ch (au besoin dans une version succincte).

Approuvé par la Direction lors de sa séance du 05.07.2021.

Annexe 001 au Règlement de traitement des données HOTELA Caisse maladie

Organigramme HOTELA



Annexe 002 au Règlement de traitement des données HOTELA Caisse maladie

Procédure d'exercice du droit d'accès