

PROTECTION DES DONNÉES

RÈGLEMENT SUR LE TRAITEMENT DES DONNÉES DE SWICA.

SOMMAIRE.

1. Généralités	3	5. Traitement des données	9
1.1 Fondements juridiques	3	5.1 But du traitement des données	9
1.2 But du règlement de traitement	3	5.2 Provenance des données	9
1.3 Champ d'application du règlement de traitement ..	3	5.3 Catégories de données	9
1.4 Organe responsable	3	5.4 Communication de données	9
1.5 But des fichiers	3	5.5 Obligation de garder le secret et devoir de discrétion des personnes concernées	9
1.6 Déclaration des fichiers au PFPDT	3	5.6 Documentation des processus de traitement	9
2. Structures informatiques de SWICA	4	6. Conservation et suppression des données ...	9
2.1 Aperçu	4	7. Droit d'accès des personnes concernées	10
2.2 Responsabilités	5	8. Projets, exploitation et management de la qualité	10
2.3 Interfaces	6	8.1 Projets	10
3. Mesures de contrôle des points de vue technique et organisationnel	7	8.2 Exploitation	10
3.1 Contrôle de l'accès aux locaux	7	8.3 Management de la qualité	10
3.2 Contrôle des supports de données	7	9. Dispositions finales	10
3.3 Contrôle du transport	7	9.1 Autres documents	10
3.4 Contrôle d'identité	7	9.2 Modification du règlement	10
3.5 Contrôle du stockage	7	9.3 Entrée en vigueur	10
3.6 Contrôle des utilisatrices et utilisateurs	7	Liste des abréviations	11
3.7 Contrôle de l'accès aux données	7		
3.8 Contrôle des saisies (consignation/fichiers journaux)	7		
4. Personnes participant aux fichiers	8		
4.1 Participants SWICA internes	8		
4.2 Participants extérieurs/outsourcing	8		

RÈGLEMENT SUR LE TRAITEMENT DES DONNÉES DE SWICA.

1. GÉNÉRALITÉS

1.1 FONDEMENTS JURIDIQUES

SWICA Organisation de santé (Groupe SWICA, appelé ci-après SWICA) est appelée à traiter des données personnelles au sens où l'entend la loi sur la protection des données (LPD). Elle le fait, d'un côté, en tant qu'organe fédéral dans les domaines de la loi fédérale sur l'assurance-maladie (LAMal) et de la loi fédérale sur l'assurance-accidents (LAA) et, de l'autre, en qualité de personne morale de droit privé, dans le domaine de la loi fédérale sur le contrat d'assurance (LCA).

Sur la base des art. 11 et 21 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD), SWICA est tenue d'élaborer un règlement sur le traitement des données de ses fichiers automatisés.

1.2 BUT DU RÈGLEMENT DE TRAITEMENT

Le présent règlement de traitement a pour but d'assurer que le système d'information de SWICA et le traitement des données par cette dernière aient la transparence voulue. Il fournit en particulier des indications sur:

- › les structures informatiques et les fichiers qui y sont contenus,
- › les procédures de traitement des données,
- › les tiers participant aux fichiers,
- › la provenance des données personnelles traitées dans les fichiers, l'accès à celles-ci ainsi que leur transmission,
- › la procédure d'exercice du droit d'accès aux données.

1.3 CHAMP D'APPLICATION DU RÈGLEMENT DE TRAITEMENT

Le présent règlement est applicable aux fichiers automatisés contenus dans les structures informatiques de SWICA et dont se servent l'ensemble des entreprises rattachées à SWICA Organisation de santé:

- › SWICA Assurance-maladie SA
- › SWICA Assurances SA
- › PROVITA Gesundheitsversicherung AG

Les processus de traitement des données sont identiques dans toutes les entreprises mentionnées.

1.4 ORGANE RESPONSABLE

La direction de SWICA répond des dossiers d'assurance qu'elle gère. En cette qualité, elle est également le maître des fichiers.

1.5 BUT DES FICHIERS

SWICA gère des fichiers pour accomplir ses tâches en tant qu'assureur-maladie et accidents, et qu'assureur de l'assurance indemnité journalière et de l'assurance complémentaire, cela dans le cadre fixé par la loi et les clauses contractuelles.

1.6 DÉCLARATION DES FICHIERS AU PFPDT

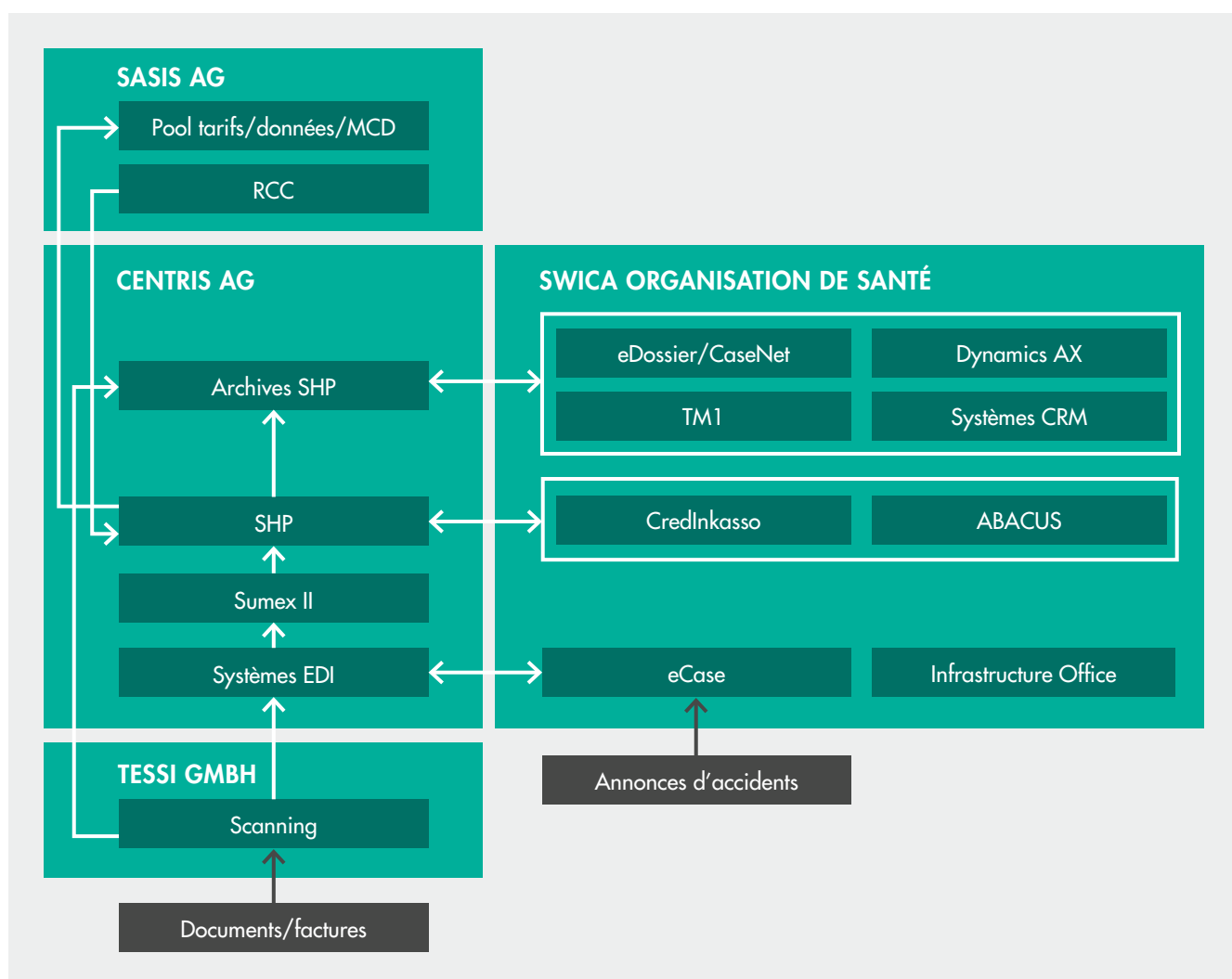
SWICA dispose d'une ou d'un responsable de la protection des données de l'entreprise au sens de l'art. 11a al. 5 lit. e LPD et de l'art. 12a OLPD. Dès lors, SWICA est libérée de l'obligation de déclarer son fichier au Préposé fédéral à la protection des données et à la transparence (PFPDT).

2. STRUCTURES INFORMATIQUES DE SWICA

2.1 APERÇU

Les systèmes d'information centraux et périphériques de SWICA servent à l'accomplissement de ses tâches dans les domaines de l'assurance-maladie obligatoire (LAMal) et de l'assurance complémentaire (LCA). SWICA recourt aux services de Centris SA qui, au travers de la Swiss Health Platform (SHP), met à disposition une solution IT intégrée. SWICA complète cette dernière par des applications supplémentaires propres pour affiner ses services.

Aperçu des applications clés:



COMPOSANTS	DESCRIPTION
SHP	Système central de traitement des dossiers d'assurance dans les domaines des assurances pour particuliers et des assurances pour entreprises
Archives SHP	Mémoires pour l'archivage sûr et de longue durée des données client(e)s ainsi que des valeurs d'assurance
Systèmes EDI	Réception électronique des factures
Sumex II	Contrôle automatisé des factures
Scanning	Numérisation automatisée des factures et des documents
eDossier/CaseNet	Gestion électronique des cas
Dynamics AX	Système de comptabilité de SWICA
TM1	Évaluation des données
Systèmes CRM	Systèmes de vente pour les nouvelles clientes et nouveaux clients, systèmes d'information pour les conseils santé (Achilles)
CredInkasso	Gestion des cas de poursuites
ABACUS	Système de gestion des ressources humaines
eCase	Annonce de cas par voie électronique via un site Internet sûr
Infrastructure Office	Technologies utilisées pour les postes de travail, les e-mails, les mémoires et la sécurité des données
Pool tarifs/données/MCD	Analyses de données
RCC	Données sur les fournisseurs de prestations

2.2 RESPONSABILITÉS

Les collaboratrices et collaborateurs du service informatique de SWICA assument la responsabilité technique des diverses applications clés.

Une liste des fichiers gérés par SWICA (y compris des applications et banques de données contenues dans le système d'information de SWICA) est tenue à l'interne par la ou le responsable de la protection des données de l'entreprise. Cette liste renseigne en particulier sur le service interne compétent, le flux des informations (interfaces), la finalité, la conformité au but indiqué, la proportionnalité ainsi que la durée de conservation des fichiers concernés.

2.3 INTERFACES

Sauf indications contraires, les interfaces ci-dessous constituent des flux permanents et automatisés de données traitées électroniquement.

DE	À	BUT	DONNÉES
Facture	Scanning	Traitement des factures de fournisseurs de prestations	Données des factures
Scanning	Systèmes EDI	Traitement automatisé des factures	Factures électroniques
Systèmes EDI	Sumex II	Contrôle des factures	Données électroniques des factures
Sumex II	SHP	Traitement des factures	Données électroniques des factures
SHP	Archives SHP	Archivage légal des données de client(e)s	Décompte des prestations, transactions
Systèmes EDI	eCase	Possibilité d'annonce d'accidents pour les entreprises	Données contractuelles de la clientèle entreprises
eCase	Systèmes EDI	Annonces de cas d'indemnité journalière et d'accidents	Annonces d'accidents par voie électronique
SHP	CredInkasso	Cas de poursuites	Informations sur les poursuites
CredInkasso	SHP	Contrôles des décomptes	Données de paiement et état des encaissements
SHP	ABACUS	Décomptes des partenaires de vente	Données relatives aux commissions des partenaires de vente
ABACUS	SHP	Décomptes des partenaires de vente	Données de base du personnel et des courtiers
Archives SHP	eDossier/CaseNet	Traitement de patient(e)s faisant l'objet d'un Managed Care après autorisation des client(e)s	Données de base et d'assurance des cas autorisés
Archives SHP	eDossier/CaseNet	Traitement des actions récursoires, oppositions et plaintes	Données relatives à ces cas
Archives SHP	TM1	Évaluations des calculs de primes et de rentabilité	Paiements effectués par région
Archives SHP	Dynamics AX	Tenue de la comptabilité financière et calcul des coûts	Primes, prestations, provisions, capitaux de couverture
Archives SHP	Systèmes CRM	Information sur le suivi des client(e)s existant(e)s	Données de base et couvertures d'assurance à jour
SHP	Pool tarifs/données/MCD	Analyses de données, notamment pour les contrôles de l'économicité et la fixation des tarifs	Données d'assuré(e)s anonymisées selon les définitions ISAK

3. MESURES DE CONTRÔLE DES POINTS DE VUE TECHNIQUE ET ORGANISATIONNEL

3.1 CONTRÔLE DE L'ACCÈS AUX LOCAUX

L'accès aux locaux de SWICA par des personnes non autorisées est empêché électroniquement (accès possible uniquement avec une clé ou un badge).

Les locaux dans lesquels se trouvent des données sensibles ou y sont traitées (service du médecin-conseil [SMC], locaux des serveurs), l'accès est en outre limité au cercle des collaboratrices et collaborateurs indispensables.

De plus, les postes de travail particulièrement sensibles font l'objet de mesures telles que le blocage automatique de l'écran lorsque la collaboratrice ou le collaborateur quitte son poste de travail ou l'utilisation de films de protection anti-regards.

3.2 CONTRÔLE DES SUPPORTS DE DONNÉES

La lecture, la copie, la modification et la suppression de données par des personnes non autorisées sont rendues techniquement impossibles via la procédure de légitimation appliquée. Cette dernière garantit que les collaboratrices et collaborateurs ne reçoivent que les droits d'accès aux données indispensables à l'accomplissement de leur travail.

3.3 CONTRÔLE DU TRANSPORT

Les données transportées via le réseau sont protégées. À cette fin, SWICA utilise des canaux de communication privés cryptés. Les données ne sont pas transférées via Internet. La communication par email entre partenaires a lieu sous une forme codée. Dans ce but, un réseau crypté est utilisé dans l'ensemble de la Suisse. Les périphériques de stockage externes sont équipés systématiquement d'un mécanisme d'encodage.

3.4 CONTRÔLE D'IDENTITÉ

Les partenaires reliés au réseau crypté sont connus et identifiés clairement. Il est garanti techniquement qu'aucune institution ni personne inconnue ait accès à ces réseaux.

3.5 CONTRÔLE DU STOCKAGE

La lecture, la copie, la modification et la suppression de données par des personnes non autorisées sont rendues techniquement impossibles via la procédure de légitimation appliquée. Cette dernière garantit que les collaboratrices et collaborateurs ne reçoivent que les droits d'accès aux supports de stockage indispensables à l'accomplissement de leur travail.

3.6 CONTRÔLE DES UTILISATRICES ET UTILISATEURS

Le processus EMA (entrée, mutation, sortie) est garant de ce contrôle. De nouvelles légitimations ne sont accordées que lorsque les droits de consultation font l'objet d'une double confirmation. Les droits existants sont contrôlés régulièrement et adaptés au besoin. Les collaboratrices et collaborateurs quittant l'entreprise se voient interdire l'accès aux données de clientes et clients et aux données de SWICA dès le dernier jour de travail (ou avant, selon les circonstances).

3.7 CONTRÔLE DE L'ACCÈS AUX DONNÉES

Les collaboratrices et collaborateurs reçoivent uniquement les droits d'accès aux données dont ils ont besoin pour l'accomplissement de leur travail. Les entrées et sorties de collaboratrices et collaborateurs de même que les mutations les concernant sont soumises à une procédure dûment réglée (processus EMA). Lors de mutations, les autorisations d'accès aux systèmes ne répondant plus à une nécessité sont supprimées. Elles le sont dans leur intégralité en cas de sortie.

Un nom d'utilisatrice ou d'utilisateur et des mots de passe sont requis pour accéder au système d'information de SWICA. Les applications portant sur des données personnelles sensibles sont en outre protégées par des mots de passe supplémentaires. Au sein même des applications, les autorisations d'accès sont limitées à des groupes définis de collaboratrices et collaborateurs. Au niveau de ces derniers, l'attribution des autorisations d'accès a lieu conformément au concept des rôles selon le principe du «need to know».

3.8 CONTRÔLE DES SAISIES (CONSIGNATION/FICHIERS JOURNAUX)

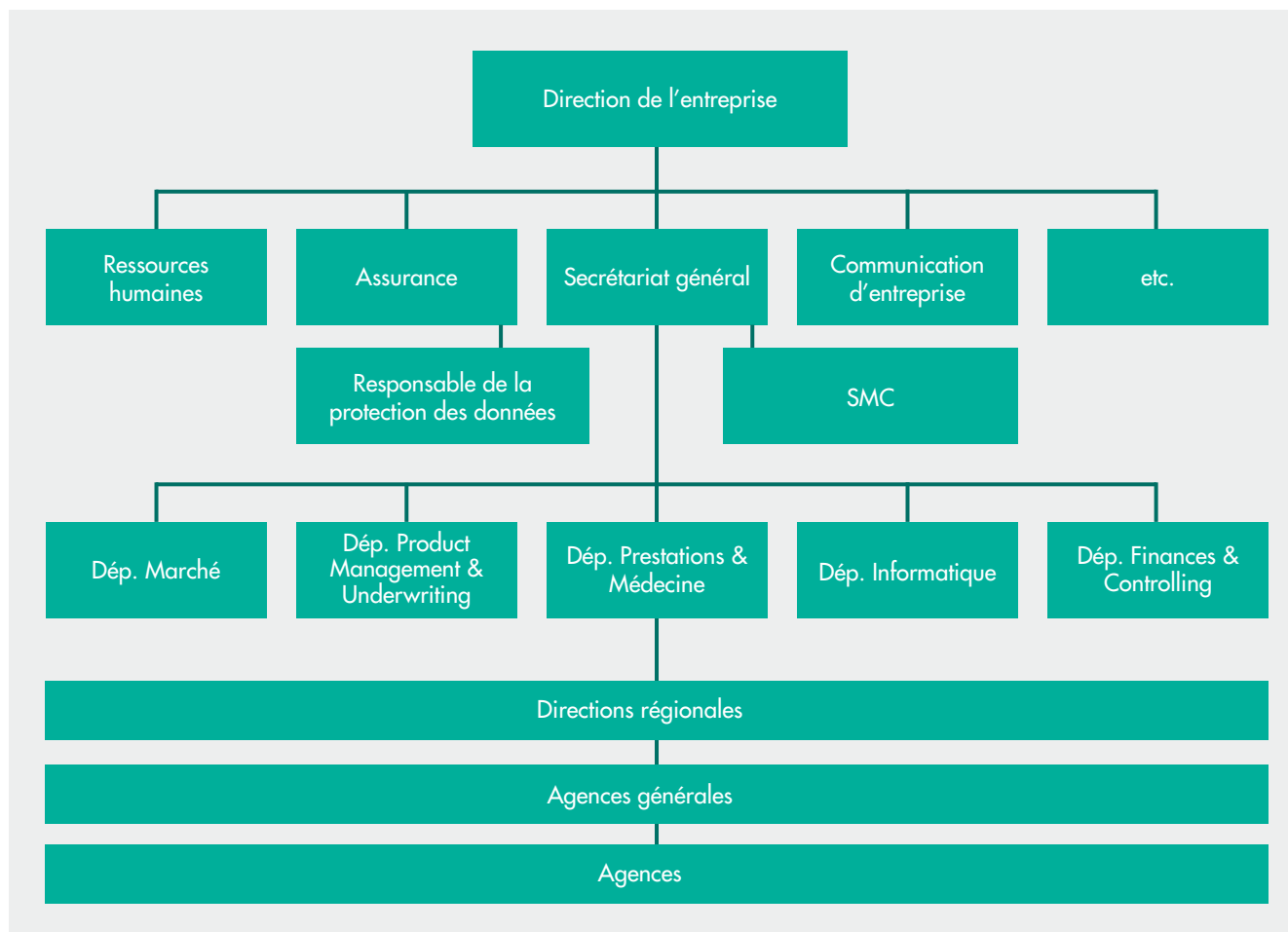
Le système central SHP et les principaux systèmes périphériques consignent toutes les modifications apportées aux données de clientes et clients. Celles-ci sont mémorisées et «historisées» afin de permettre de retrouver en tout temps quelles collaboratrices et quels collaborateurs ont procédé à la modification de données et, si oui, lesquelles.

D'autres fichiers journaux sont disponibles au niveau du réseau et des accès au système de manière à permettre de déceler d'éventuelles irrégularités.

4. PERSONNES PARTICIPANT AUX FICHIERS

4.1 PARTICIPANTS SWICA INTERNES

Le traitement des dossiers d'assurance est effectué par les collaboratrices et collaborateurs, en particulier par ceux de la direction générale et des unités organisationnelles décentralisées (directions régionales, agences générales et agences).



4.2 PARTICIPANTS EXTÉRIEURS/OUTSOURCING

ENTREPRISE	CONTRAT	APPLICATIONS CLÉS
Centris AG, Soleure	Contrat de service avec SLA	SHP, archives SHP, Sumex II, systèmes EDI
Tessi GmbH, Urdorf	Contrat de service avec SLA	Scanning
Aspectra AG, Zurich	Contrat de service avec SLA	CaseNet
SASIS AG	Contrat de fourniture de données	SHP, pool tarifs/données/MCD, RCC

5. TRAITEMENT DES DONNÉES

5.1 BUT DU TRAITEMENT DES DONNÉES

SWICA ne traite des données qu'à des fins de gestion du dossier d'assurance dont elle s'occupe. Il s'agit en particulier de l'établissement des documents relatifs aux rapports d'assurance, au contrôle de la proposition d'assurance, aux prestations et aux paiements ainsi qu'à la tenue de statistiques et à la fourniture de renseignements.

5.2 PROVENANCE DES DONNÉES

Les données émanent des personnes assurées eux-mêmes. Elles peuvent également provenir de personnes et instances (fournisseurs de prestations, assurances, autorités) habilitées à transmettre des données à SWICA, que ce soit en vertu de la loi (assistance administrative) ou sur la base d'une autorisation donnée par les personnes assurées eux-mêmes.

5.3 CATÉGORIES DE DONNÉES

Les catégories de données suivantes sont traitées dans les applications concernées. Elles doivent être protégées par les mesures mentionnées plus haut contre toute consultation non autorisée:

- › nom, prénom, adresse, numéros de téléphone
- › date de naissance
- › nationalité, langue
- › situation familiale
- › représentation légale, proches parents
- › données relatives à la maladie/à l'accident
- › état de santé
- › mesures d'aide sociale
- › numéro d'assuré(e)
- › numéro d'assurance sociale
- › données relatives aux prestations
- › données relatives aux primes
- › coordonnées bancaires
- › données de rappel

5.4 COMMUNICATION DE DONNÉES

Les données sont communiquées dans les limites fixées par la loi (art. 84a LAMal, art. 97 LAA). Les cas dans lesquels SWICA n'est pas autorisée ni obligée par la loi à divulguer des données, la transmission de ces dernières à des tiers n'a lieu qu'avec l'accord écrit de la personne concernée.

5.5 OBLIGATION DE GARDER LE SECRET ET DEVOIR DE DISCRÉTION DES PERSONNES CONCERNÉES

5.5.1 Collaboratrices et collaborateurs SWICA

Pour l'accomplissement de leur tâche, les collaboratrices et collaborateurs SWICA sont appelés à traiter des données personnelles, y compris des données sensibles, dans le système d'information de SWICA.

SWICA accorde une grande importance à la protection des données. Elle se tient à la législation applicable régissant ce domaine et fixe les détails y relatifs dans un règlement accessible à toutes les collaboratrices et tous les collaborateurs. Les collaboratrices et collaborateurs SWICA s'engagent, en signant leur contrat de travail, à faire montre de discrétion, à garder le secret et à respecter la législation sur la protection des données.

Afin de tenir compte du caractère particulièrement sensible de certaines données médicales, les collaboratrices et collaborateurs placés sous l'autorité du SMC sont tenus de signer une déclaration complémentaire de protection des données et d'engagement à garder le secret.

5.5.2 Participants extérieurs

Des contrats de collaboration lient SWICA et ses partenaires extérieurs. Ces derniers s'engagent contractuellement à veiller à ce que les dispositions relatives à la protection des données soient observées par leurs collaboratrices et collaborateurs et leurs auxiliaires à l'instar des obligations imposées aux collaboratrices et collaborateurs SWICA à cet égard.

5.6 DOCUMENTATION DES PROCESSUS DE TRAITEMENT

Les fichiers de SWICA sont intégrés dans diverses procédures de travail. Les processus concernés sont consignés par écrit par les départements compétents en la matière. Des documents exhaustifs existent en particulier pour les procédures dans le cadre desquelles des données personnelles sensibles et des profils de personnalité sont traités (service de réception de données DRG, traitement de données médicales au sein du SMC, etc.).

6. CONSERVATION ET SUPPRESSION DES DONNÉES

Les données soumises à l'obligation d'archivage sont conservées pendant toute la durée requise par les dispositions spécifiques du droit suisse et sont protégées contre toute modification ou tout accès non autorisé.

À l'expiration du délai de conservation légal, les données contenues dans le système d'information de SWICA sont effacées ou détruites.

7. DROIT D'ACCÈS DES PERSONNES CONCERNÉES

Toute personne peut demander à SWICA si des données la concernant sont traitées. Pour exercer ce droit à être renseigné, les intéressés doivent faire parvenir une demande écrite à l'adresse suivante:

SWICA Organisation de santé

Responsable de la protection des données de l'entreprise
Römerstrasse 38

8401 Winterthour

datenschutz@swica.ch

SWICA examine si des données au sens des art. 8 ss. LPD existent et, si oui, lesquelles. Dans ce cas, elle envoie dans les 30 jours une copie de ces dernières à l'auteur de la demande.

8. PROJETS, EXPLOITATION ET MANAGEMENT DE LA QUALITÉ

8.1 PROJETS

Le lancement des projets de systèmes d'information de base et de périphériques ainsi que leur réalisation au sein des structures informatiques de SWICA se sont déroulés dans le cadre de directives données par l'entreprise. Les documents relatifs au projet sont conservés centralement.

8.2 EXPLOITATION

L'exploitation des systèmes de base et des périphériques fait l'objet de manuels mis au point par les secteurs compétents.

8.3 MANAGEMENT DE LA QUALITÉ

La garantie et le développement de la qualité des divers systèmes de base et périphériques des structures informatiques de SWICA sont assurés via le système de contrôle interne (SCI), lequel est soumis à une réglementation à part. Le processus responsable tant du traitement efficient et efficace des données que du respect de leur protection contrôle régulièrement l'impact des processus et détermine les critères à appliquer en la matière. La ou le responsable de la protection des données de l'entreprise participe à la définition des indicateurs dans le domaine de la protection des données.

Des audits internes ont lieu régulièrement. Les rapports d'audit font partie des Corporate Governance Reportings qui sont présentés à la direction générale et au conseil d'administration de SWICA dans le cadre de son concept de Corporate Governance.

9. DISPOSITIONS FINALES

9.1 AUTRES DOCUMENTS

Le règlement de traitement renvoie à divers autres documents complémentaires. Ces derniers ne sont toutefois pas publiés pour des raisons de sécurité des systèmes, processus et données, de sauvegarde de la confidentialité des personnes assurées ainsi que de protection des secrets d'affaires de SWICA et de ses partenaires commerciaux.

9.2 MODIFICATION DU RÈGLEMENT

Le règlement de traitement est revu régulièrement afin de le tenir à jour. Il peut être modifié en tout temps avec l'accord de la direction générale.

9.3 ENTRÉE EN VIGUEUR

Le présent règlement remplace le règlement du 1^{er} septembre 2014 et entre en vigueur le 15 avril 2016.

Winterthour, le 15 avril 2016



Reto Dahinden, docteur ès sc. éco.
Directeur général/CEO



Jérôme Egli
Responsable de la protection
des données de l'entreprise

LISTE DES ABRÉVIATIONS.

CEO	Chief Executive Officer
Dépt	Département
DRG	Diagnosis-Related Groups
IT	Technologie de l'information, terme générique désignant le traitement d'informations et de données
LAA	Loi fédérale du 20 mars 1981 sur l'assurance-accidents
LAMal	Loi fédérale du 18 mars 1994 sur l'assurance-maladie
LCA	Loi fédérale du 2 avril 1908 sur le contrat d'assurance
LPD	Loi fédérale du 19 juin 1992 sur la protection des données
OLPD	Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données
PPDPT	Préposé fédéral à la protection des données et à la transparence
Processus EMA	Processus entrée/mutation/sortie
SCI	Système de contrôle interne
SHP	Swiss Health Platform
SMC	Service du médecin-conseil

À VOTRE SERVICE 365 JOURS PAR AN, 24 HEURES SUR 24.

Téléphone 0800 80 90 80 / swica.ch

