Politique générale de sécurité de l'information et de protection des données

1. Préambule

La sécurité de l'information et la protection des données figurent parmi les priorités de L'Association CARA dans l'accomplissement de ses missions de santé publique. Le comité de direction accorde à ces thématiques une attention continue et veille au respect de ses principes directeurs en matière de gouvernance des données par l'ensemble des parties prenantes de CARA.

Le présent document présente la politique générale de l'Association CARA en matière de sécurité de l'information et de protection des données. Il détaille les principes directeurs qui chapeautent le dispositif mis en place par CARA pour garantir la sécurité de l'information et la protection des données et qui guident les parties prenantes dans leurs actions.

2. Synthèse

En mettant à disposition de la population des cantons membres, des professionnelles et des professionnels de santé une plateforme de santé numérique, CARA a pour mission de faciliter le partage de l'information sanitaire et d'accroitre la sécurité de la prise en charge sanitaire. Dans ce contexte, CARA place la sécurité de l'information et la protection des données au service de la sécurité des soins.

Champ d'application
Le dispositif de sécurité de l'information et de protection des données englobe la totalité du périmètre de CARA, qui comprend notamment :

- les organes de l'association ;
- la plateforme de santé numérique, incluant le dossier électronique du patient et les services supplémentaires ;
- les institutions affiliées ;
- les patientes et les patients.

Responsabilité
CARA assume la responsabilité de la sécurité de l'information et de la protection des données vis-à-vis de l'ensemble des parties prenantes, en particulier :

- les utilisatrices et les utilisateurs de la plateforme de santé numérique ;
- les cantons membres et leurs autorités ;
- les partenaires publics et privés ;
- la Confédération et les instances de régulation.

Principes directeurs
CARA respecte et applique en tout temps et en toute circonstance les principes de sécurité de l'information, en particulier les principes de confidentialité, d'intégrité et de disponibilité des données.

Engagement
Afin d'exploiter le dispositif de sécurité de l'information et de protection des données mis en place, CARA s'engage à

- se doter des compétences et ressources nécessaires à la conduite et au suivi du dispositif ;
- assurer un suivi et une amélioration continue du dispositif ;
- assurer la conformité du dispositif au cadre légal en vigueur, en particulier la loi fédérale sur le dossier électronique du patient et la loi fédérale sur la protection des données ;
- appliquer le dispositif à la totalité de ses activités, produits ou service sur l'entier de leur cycle de vie ;
- développer une approche proactive et réactive de la sécurité ;
- garantir la transparence sur l'état de la sécurité et la protection des données.

3. Objectifs

L'Association CARA protège ses actifs d'information contre toutes les menaces, qu'elles soient internes ou externes, délibérées ou accidentelles. Ses actifs sont notamment les données stockées sur des supports informatiques, transmises au travers de réseaux de communications, imprimées sur papier, ou discutées lors de conversations et par téléphone.

L'objectif de CARA en matière de protection de ses actifs d'information est de garantir que ses opérations principales et activités liées notamment à la mise à disposition d'une plateforme de santé numérique, incluant le dossier électronique du patient (DEP) et les services supplémentaires, fonctionnent de manière continue avec un minimum de perturbations.

Pour ce faire, CARA met en œuvre la politique générale de sécurité et de protection des données au travers de son système de gestion de la sécurité de l'information et de protection des données (dispositif SIPD, ou SMSI).

4. Politique générale

Les actifs d'information et l'équipement informatique physique, qui permettent aux utilisatrices, utilisateurs, collaboratrices, collaborateurs et tiers de travailler de manière satisfaisante, sont soumis à un contrôle sécurisé pour assurer leur protection contre les accidents ou pertes intentionnelles, manipulations non autorisées, arrêts involontaires ou divulgations non autorisées, tant au sein de CARA qu'à l'extérieur.

Afin de se conformer aux normes et à la technologie d'aujourd'hui, CARA fixe des règles de comportement liées à l'utilisation des ressources informatiques.

CARA protège les actifs d'information appartenant aux utilisatrices, aux utilisateurs et aux tiers qui lui ont été confiés à titre confidentiel, qu'elle traitera de la même manière que tout autre secret lui appartenant, conformément aux contrats et accords applicables. CARA traite de la même manière que ses propres actifs toute information transitant ou résidant sur ses systèmes d'information et qui n'ont pas été spécifiquement identifiées comme étant la propriété d'une des parties prenantes.

CARA prohibe l'accès non autorisé, la divulgation non permise, la duplication et la modification non autorisées, le détournement, la destruction non permise, la perte, la mauvaise utilisation ou le vol de ces informations.

La politique générale de sécurité de l'information et de protection des données s'adosse à trois piliers:

Stratégie globale
CARA contribue à la qualité, à la continuité et à la coordination des soins en stimulant l'interprofessionnalité et en facilitant le partage de l'information sanitaire. À ces fins, CARA met à disposition des professionnelles et professionnels de la santé, des citoyennes et des citoyens, une plateforme de santé numérique commune, conviviale, fiable et sécurisée. La sécurité de l'information est au service de la sécurité des soins.

Conformité aux principes légaux et règlementaires
Les principes légaux et règlementaires sont assurés afin d'être en conformité aux exigences légales fédérales et cantonales, notamment de la loi fédérale sur le DEP et de la loi fédérale sur la protection des données.

Environnement des risques et des menaces
L'environnement des risques et des menaces fait l'objet d'une attention continue. Il est décrit dans le concept de sécurité de l'information et de protection des données (Concept SIPD).

5. Principes directeurs

Les principes directeurs suivants guident l'action de CARA dans la mise en œuvre de son dispositif de sécurité de l'information et de protection des données.

Disponibilité
Les informations sont mises à disposition avec un minimum de perturbation pour les collaboratrices, les collaborateurs et les tiers, afin d'assurer la disponibilité des informations et des services vitaux liés au fonctionnement de la plateforme de santé numérique pour les utilisatrices et les utilisateurs. La plateforme CARA constitue un système secondaire. Les principes fondamentaux en matière de sécurité de l'information et de la disponibilité des systèmes primaires ne font pas partie de la responsabilité de CARA. Parallèlement et indépendamment de la plateforme de santé numérique, les informations des collaborateurs de CARA dans leurs fonctions respectives sont également mises à disposition avec un minimum de perturbation. La disponibilité des informations et des systèmes d'information est assurée au besoin par les opérations et activités de base et de soutien de CARA.

Intégrité
CARA veille à ce que toutes les informations qu'elle collecte, gère ou émet préservent leur intégrité. L'intégrité et la complétude des actifs d'information sont maintenues en protégeant ceux-ci contre toute modification non autorisée.

Confidentialité
La confidentialité de toute information est maintenue afin que la protection des données sensibles soit assurée contre toute divulgation non autorisée. Un contrôle d'accès approprié est maintenu à la fois dans le cadre de la gestion de la plateforme de santé numérique et dans la gestion des systèmes d'information de CARA. Les informations y sont protégées contre tout accès non autorisé.

Continuité
Un plan de continuité des activités est élaboré pour contrer les interruptions des activités opérationnelles et pour protéger les processus critiques contre les effets des défaillances ou des catastrophes majeures. Le plan de continuité des activités est testé périodiquement.

Traçabilité
CARA relève et enregistre les opérations qui sont effectuées dans un but de restitution ultérieure du déroulement des évènements lorsque cela est nécessaire.

Formation
Des programmes de sensibilisation à la sécurité de l'information sont conçus et mis à la disposition des collaboratrices, collaborateurs et des tiers accédant aux systèmes d'information de CARA. Tous les collaborateurs disposant de droits spéciaux leur permettant d'accéder à des données personnelles ou sensibles sont formés aux enjeux de sécurité et aux pratiques à adopter.
Des formations en matière de SIPD sont également dispensées aux institutions affiliées.

Gestion des risques
CARA procède à une analyse des risques et des menaces dans le cadre d'une veille continue de son environnement. Comme les risques et les menaces informatiques sont en constante évolution, et que leurs conséquences sont de plus en plus importantes, les mesures, les contrôles et la stratégie de traitement des risques et des menaces évoluent également. Le suivi de ces changements et l'évolution des mesures seront répertoriés et documentés.

Amélioration continue
Le système de gestion de la sécurité de l'information de protection des données est en constante évolution et bénéficie d'un processus d'amélioration continue. Une revue du dispositif SIPD est effectuée une fois par année par le comité de direction, qui s'assure du respect de sa politique générale, ainsi que de l'adéquation, de l'efficacité et de l'efficience du dispositif SIPD. Son évaluation débouche sur des mesures correctives.

Transparence
La présente politique générale, les directives et procédures qui en découlent sont mises à disposition des différentes parties prenantes concernées.

Signalement et sanctions
Toutes les violations de la sécurité de l'information, réelles ou suspectées, font l'objet d'un signalement au responsable de la sécurité de CARA. CARA dispose d'un processus de gestion des incidents et d'un plan de réponses aux incidents complet et testé régulièrement. En cas de violations et de non-conformité aux politiques et procédures de sécurité, CARA prend des mesures disciplinaires selon une procédure formalisée et émet des sanctions.

6. Responsabilités

Comité de direction
Le comité de direction assume les responsabilités suivantes :

- adopter la politique générale de sécurité de l'information et de protection des données ;
- procéder annuellement à la revue du dispositif SIPD à des fins d'amélioration continue ;
- allouer les ressources organisationnelles et techniques nécessaires à la mise en œuvre, à la gestion et au suivi d'un dispositif SIPD efficace, répondant aux principes directeurs fixés dans sa politique générale.
- contractualiser avec des fournisseurs en tenant des exigences SIPD

Secrétariat général
Le secrétariat général assume les responsabilités suivantes :

- mettre en œuvre la politique générale et le dispositif SIPD ;
- définir les règles et pratiques applicables en matière de sécurité et protection des données ;
- protéger les ressources du système d'information dont il a le contrôle et la gestion, telles que le matériel informatique, les logiciels d'application et de système, les données, la documentation, ainsi que les collaboratrices et les collaborateurs ;
- s'assurer de l'adhésion des collaboratrices et des collaborateurs à la présente politique générale et aux règles et pratiques qui en découlent ;
- s'assurer que les collaboratrices et les collaborateurs comprennent leurs rôles et responsabilités en matière de sécurité et de protection des données, ainsi que dans la gestion des incidents en la matière ;
- contrôler que le dispositif SIPD permette d'atteindre les objectifs définis et escomptés dans la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations reçues, conservées, traitées par CARA ;
- appliquer un processus de gestion des risques et ainsi fournir à toutes les parties prenantes l'assurance que ces risques sont connus et sont gérés de manière appropriée ;
- surveiller le respect des exigences SIPD par les fournisseurs ;
- mandater régulièrement des audits de sécurité ;
- assurer la sécurité de ses locaux.

Collaboratrices et collaborateurs
Les collaboratrices et collaborateurs assument les responsabilités suivantes :

- adhérer à la présente politique générale ;
- respecter et appliquer les règles et pratiques qui en découlent ;
- signaler tout incident en matière de sécurité de l'information et de protection des données.

Institutions affiliées
Les institutions affiliées assument les responsabilités suivantes :

- reconnaitre formellement qu'elles ont lu et compris la politique générale de CARA et adhérer à son dispositif SIPD ;

- mettre en œuvre les exigences de sécurité de l'information et de protection des données édictées par CARA ;
- superviser l'adhésion de ses collaboratrices et collaborateurs à la politique générale de CARA ;
- vérifier périodiquement qu'elles respectent la politique générale de sécurité de l'information et de protection des données de CARA.