CHARTE DE BON USAGE DU SYSTEME D'INFORMATION, PROTECTION DES DONNEES ET CONFIDENTIALITE

Préambule

La CPTS Provence Santé met en œuvre un système d'information (SI) et des ressources informatiques nécessaires à ses activités qui comprend un système informatique et de communication. Ce système d'information est mis à disposition des salariés de l'association, des professionnels de santé membres actifs, des prestataires.

Les règles de bon usage décrites dans cette charte leur sont applicables ; elles sont également applicables aux invités.

Salariés, membres actifs, prestataires et invités sont nommés « utilisateur ».

Le présent document décrit les règles de bons usages de ce SI par l'utilisateur, qui s'engage à les respecter. Ce document, consultable sur le site de la CPTS et dans l'outil numérique de gestion documentaire, comprend également des engagements mutuels en matière de protection et de confidentialité des données.

1 - Rappel des règles de protection des données et engagement de confidentialité

La CPTS Provence Santé est une structure qui, par ses missions d'appui aux professionnels et à la population qui lui ont été confiées par l'Agence Régionale de Santé, est amenée à collecter/enregistrer/ traiter/conserver/partager des données à caractère personnel.
Tout utilisateur du SI s'engage par conséquent, conformément à l'article 32 du règlement général sur la protection des données du 27 avril 2016, à :

- Ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions ;
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de ses fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
-

- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- S'assurer d'anonymiser les données envoyées si elles sont transférées par des moyens de communication autres que par une boite mail sécurisée ;
- En cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité - en vigueur pendant toute la durée des fonctions du salarié ou membre actif, et du partenariat avec les invités ou prestataires - demeurera effectif, sans limitation de durée, après la cessation des fonctions/du contrat/de la rencontre, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
La violation du présent engagement de confidentialité des données à caractère personnel expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-13 et 226-16 à 226-24 du code pénal.

Les données personnelles peuvent être partagées avec des sociétés ou structures tierces exclusivement dans l'Union européenne, dans les cas suivants :

- Quand l'utilisateur autorise le site web d'un tiers à accéder à ses données ;
- Quand la CPTS Provence Santé recourt aux services de prestataires pour fournir l'assistance utilisateurs, la publicité et les services de paiement. Ces prestataires disposent d'un accès limité aux données de l'utilisateur, dans le cadre de l'exécution de ces prestations, et ont une obligation contractuelle de les utiliser en conformité avec les dispositions de la réglementation applicable en matière protection des données à caractère personnel ;
- Si la loi l'exige, la CPTS Provence Santé peut effectuer la transmission de données pour donner suite aux réclamations présentées contre la CPTS et se conformer aux procédures administratives et judiciaires ;
- Dans le cadre du suivi des financements et des actions de la CPTS, par les organismes de tutelles (CPAM, ARS…).

Conformément au Règlement européen concernant la protection des données, chacune des personnes dont les données à caractère personnel ont été collectées dispose également de droits sur les données personnelles le concernant (accès, modification, suppression, limitation de traitement, portabilité des données).

Vous trouverez également des informations concernant ces droits sur le site internet de la Commission Nationale de l'Informatique et des Libertés : https://www.cnil.fr

Vous pouvez faire valoir vos droits en contactant un membre du Bureau de la CPTS Provence Santé : contact@cptsprovencesante.com

Ou par courrier à l'adresse suivante :
CPTS Provence Santé - Pôle Santé les Genêts, 606 Av. Du Général De Gaulle-13109 Simiane-Collongue

Vous disposez également un droit de déposer une réclamation auprès de la CNIL :
CNIL-3, Place de Fontenoy-TSA 80715-75334 PARIS

2 - Les différentes ressources du Système d'Information auquel a accès l'utilisateur :

- Les postes de travail ordinateur de bureau ;
- Les équipements ordinateurs portables ; tablettes, smartphones (utilisés notamment dans le cadre du télétravail et de travail nomade ;
- Les espaces de stockage collectif dans le cloud associé à l'outil numérique de coordination ;
- Les réseaux locaux d'accès à internet (fibre/ADSL, WiFi…) ;
- La messagerie électronique ;
- La téléphonie mobile ;
- Les plateformes donnant un accès « structure » à la CPTS (DOCTOLIB pro, Plateforme SAS, ou autre compte nécessaire à la gestion de l'Association)
- Les plateformes de communication telles WHATSAPP

3 - Utilisation professionnelle du Système d'Information (SI)

L'utilisation du SI, des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder, est destinée à l'activité professionnelle des utilisateurs conformément à la législation en vigueur. Toutefois, leur utilisation à des fins non professionnelles est tolérée de manière exceptionnelle, conformément au droit à une vie privée résiduelle sur le lieu de travail, lorsqu'elle :

- Ne perturbe pas leur bon fonctionnement ;
- S'inscrit dans le cadre des nécessités exceptionnelles et urgentes de la vie familiale ;
- Reste raisonnable et raisonnée ;
- Ne porte pas atteinte ou n'est pas susceptible d'engager la responsabilité de la CPTS Provence Santé, ni de dégrader son image ;
- Ne poursuit pas un but lucratif, ludique ou illicite ;
- Reste conforme aux conditions précisées dans la présente Charte.

Toute information stockée sur le SI est considérée comme professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans un répertoire explicitement prévu à cet effet et intitulé " privé ". Sachant que, dans tous les cas, un utilisateur ne peut pas nommer l'ensemble de son disque dur comme étant « Personnel » ou « Privé ». La présence de tels fichiers doit rester accessoire et très exceptionnelle. Aussi, l'utilisateur s'interdit expressément à ce qu'un tel dossier personnel ne soit pas trop volumineux, et ce, afin de ne pas affecter les Ressources informatiques.

4 - Droit à la déconnexion

Le développement du numérique peut entraîner une certaine « confusion » entre les sphères professionnelles et personnelles. Les outils numériques (messagerie électronique, tablettes, ordinateurs portables, smartphone …) étant tout aussi répandus dans l'entreprise qu'en dehors de l'entreprise.
Les utilisateurs sont invités à un usage efficient et raisonnable des outils numériques afin d'éviter à la fois, les sur-connexions, mais également les sur-sollicitations.

5 - Règles de sécurité élémentaires auxquelles les utilisateurs doivent se conformer

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à la préservation de ces ressources.

Les 10 REGLES de sécurité de l'ANSI pour se prémunir des cyberattaques

1. **Séparez strictement vos usages à caractère personnel de ceux à caractère professionnel.** Vos moyens de communication personnels ne doivent pas être utilisés pour vos échanges professionnels (courriel, compte d'échange de fichiers, clé USB, etc.) et inversement.
2. **Mettez régulièrement à jour vos outils numériques.** Les mises à jour ne sont pas automatiques. Veillez à bien les accepter sur vos outils personnels et professionnels pour garantir leur sécurité.
3. **Protégez vos accès par une authentification double-facteur lorsque c'est possible, ou *a***
4. ***minima* par des mots de passe complexes.** Vos mots de passe doivent être longs, complexes, sans information personnelle, uniques et secrets.
5. **Ne laissez pas vos équipements sans surveillance lors de vos déplacements,** sous peine de les voir manipulés, compromis à votre insu et vos données volées.
6. **Protégez votre espace de travail et vos données.** Verrouillez votre poste de travail lorsque vous n'êtes pas à votre bureau et placez en lieu sûr tout matériel sensible (support de stockage).
7. **Prenez soin de vos informations personnelles en ligne**. Préservez votre identité numérique en vous montrant vigilant sur Internet et les réseaux sociaux.
8. **Protégez votre messagerie professionnelle.** Soyez vigilant avant d'ouvrir les pièces jointes et ne cliquez pas sur les liens présents dans les messages qui vous semblent douteux.
9. **Ne faites pas confiance aux réseaux non maitrisés pour connecter vos équipements en mode nomade.** Par exemple : des réseaux Wi-Fi publics, des bornes de recharge USB…
10. **Faites preuve de vigilance lors de vos échanges téléphoniques ou en visioconférence.** La confidentialité des conversations n'est pas assurée sur les réseaux publics.
11. **Veillez à la sécurité de votre smartphone.** Évitez de prendre votre smartphone pendant les réunions sensibles. Il peut être utilisé pour enregistrer vos conversations, y compris à votre insu.

Notamment et en particulier dans le cadre de ses activités professionnelles, tout utilisateur se doit de :

- Signaler toute violation ou tentative de violation suspectée de son compte informatique, toute perte ou vol de matériel et, de manière générale, tout dysfonctionnement;
- Ne jamais confier son identifiant/mot de passe à un tiers ;
- Ne pas installer, copier, modifier, détruire des logiciels et leur paramétrage sans autorisation ;
- Verrouiller son ordinateur, smartphone dès que l'on quitte son poste de travail ;
- Se déconnecter des logiciels et des sessions de travail en fin de journée ;
- Éteindre les appareillages alimentés par le réseau électrique ;
-

- Ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ;
- Ne pas utiliser et connecter au SI de moyens de stockage externes (clef USB, disque dur, liste non exhaustive) ;
- Ne pas télécharger des fichiers dont l'origine n'est pas connue ;

Les moyens d'authentification utilisés et la politique de mots de passe

Les autorisations d'accès aux SI sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée. L'entité peut en outre prévoir des restrictions d'accès spécifiques lorsqu'ils ne sont pas octroyés directement par l'administrateur du SI ou le fournisseur de logiciel. Les mots de passe doivent respecter les règles suivantes : 8 à 12 caractères minimum, au moins une majuscule, au moins une minuscule, au moins un chiffre et au moins un caractère spécial.
Les mots de passe ne doivent pas être liés à l'identité (composés d'un nom, prénom, date de naissance, etc.) ou à des éléments facilement identifiables (nom des enfants, sport favori, etc.).
Les mots de passe sont confidentiels et personnels, et ne doivent pas être communiqués à une tierce personne ; ils doivent être changés régulièrement.

6- Règles d'utilisation du SI

a) Respect de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

b) Préservation de l'intégrité des ressources informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques...
L'évolution permanente des technologies de l'informatique met à disposition des utilisateurs de nouveaux services qui peuvent être accessibles depuis le réseau de leur entité. Ces nouvelles technologies, qui peuvent présenter un risque de vulnérabilité particulier, ne peuvent être utilisées qu'après accord préalable de l'administrateur du SI et dans le strict respect de la politique de sécurité des systèmes d'information.
Parallèlement, l'utilisateur met à jour régulièrement et utilise les dernières versions des logiciels des systèmes d'exploitation de ces ressources informatiques, selon les recommandations de l'éditeur du logiciel.

c) Usage des services Internet

Internet est un outil de travail dont l'utilisation doit respecter des principes généraux et des règles propres aux divers sites qui les proposent, ainsi que dans le respect de la législation en vigueur. En particulier, l'utilisateur :

- Ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;
- Ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers ;
- Ne doit pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions… ;
- N'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à la CPTS Provence Santé ;
- Doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire. La CPTS Provence Santé ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

d) Messagerie électronique

Tout message sera réputé professionnel sauf s'il comporte une mention particulière et explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

- Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.
- L'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages de masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.
- La transmission de données à caractère personnel doit être effectuée par un dispositif agréé à cet effet (messagerie sécurisée à ce jour : MMSSANTE, AZUREZO, DOCTOLIB TEAM).

7 - Devenir des données au départ de l'utilisateur

Lors du départ d'un salarié, le matériel informatique et de téléphonie sera rendu en ayant pris soin au préalable de supprimer les fichiers personnels. Les fichiers professionnels seront partagés sur le cloud de

l'outil numérique PLEXUS ou envoyé par mail à la personne concernée. Les mails devront être retransmis à la personne remplaçante, à la coordinatrice ou à un membre du Bureau de la CPTS Provence Santé.

8 - Rappel des dispositions réglementaires et légales

En cas de non-respect des règles édictées dans cette charte informatique, et si le caractère délibéré est établi, l'utilisateur s'expose à des sanctions disciplinaires au sein de la CPTS Provence Santé et également à des poursuites judiciaires le cas échéant.

L'observation de ces règles fait partie des obligations inhérentes au contrat de travail.

Rappel des principales dispositions légales :

Il est rappelé que l'ensemble utilisateurs quel que soit leur statut, sont soumis à la législation française en vigueur et notamment :

► la loi du 29 juillet 1881 modifiée sur la liberté de la presse,
► la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,
► la législation relative aux atteintes aux systèmes de traitement automatisé de données (art. L 323-1 et suivants du code pénal),
► la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
► le règlement européen pour la protection des données personnelles (UE) n°2016/679 promulgué, par la loi d'application n°2018-493 du 20 juin 2018,
► les dispositions du code de propriété intellectuelle relative à la propriété littéraire et artistique.