

[LOGO DE LA CPTS]

Charte informatique de la [NOM DE LA CPTS ...]

Préambule :

Cette chartre définit les règles d'utilisation des systèmes d'information de la CPTS.

Elle vise à garantir la sécurité des outils, la protection des données et le bon usage des ressources numériques par l'ensemble des utilisateurs (salariés, adhérents, professionnels de santé).

Chaque utilisateur est acteur de la sécurité du système d'information et s'engage à respecter les règles ci-après.

1. Utilisation des équipements informatiques

Principe général :

Les équipements informatiques sont destinés à un usage professionnel. Un usage personnel raisonnable est toléré, sous réserve qu'il ne porte pas atteinte à la sécurité, au fonctionnement du service ou à l'image de la CPTS.

Directives spécifiques :

Séparation des usages : Utilisez des appareils et des comptes distincts pour vos activités professionnelles et personnelles afin d'éviter toute interférence ou compromission de données.

Accès autorisé : Ne permettez à personne d'utiliser votre équipement dans le cadre de votre activité professionnelle sans autorisation préalable

2. Sécuriser l'accès au compte

Chaque utilisateur est responsable de la sécurité de ses identifiants d'accès et ne doit pas les divulguer à des tiers. Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) est unique à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Mesures à suivre :

Changez régulièrement votre mot de passe conformément à notre politique (à déterminer) et après la déclaration d'un incident malveillant.

Créez des mots de passe forts, qui ne doivent pas être facilement devinables (évités les noms, dates de naissance, etc.).

3. Sécurité des données

La sécurité des données est une responsabilité partagée. Chaque utilisateur doit prendre des mesures pour protéger les informations auxquelles il a accès.

Tout salarié et tout adhérent est responsable de la sécurité des données auxquelles il accède ou qu'il traite.

Directives importantes :

Confidentialité : Ne divulguez jamais les données de santé des patients sans autorisation explicite. Toute transmission de données de santé doit se faire exclusivement via des outils sécurisés (ex : MSSanté, outils métiers sécurisés). L'utilisation d'une messagerie classique est interdite pour ces échanges.

Les utilisateurs s'engagent à protéger les informations, notamment les données de santé, et à respecter les principes du RGPD : licéité, loyauté, transparence, minimisation, limitation de la

conservation, intégrité et confidentialité.

Stockage sécurisé : Conformez-vous aux principes du RGPD, en veillant à ce que les données soient stockées et traitées de manière sécurisée.

Les données des patients ne doivent être accessibles qu'aux membres de la CPTS autorisés à les consulter dans le cadre de leur travail. Il est interdit de partager des données sensibles avec des tiers non autorisés.

[Les dispositifs de stockage amovibles (clés USB, disques durs externes, etc.) ne doivent être utilisés que conformément aux politiques de sécurité de la CPTS, et leur utilisation pour stocker des données sensibles est strictement interdite sauf autorisation expresse]

4. Utilisation d'Internet et des e-mails

L'accès à Internet et l'usage des e-mails doivent être réalisés avec prudence et dans le respect total de la confidentialité et de la sécurité des données de la CPTS.

Les utilisateurs doivent faire preuve de vigilance dans l'usage d'Internet et des outils de communication en ligne, notamment lors de :

- la consultation de sites externes,
- l'utilisation de forums ou réseaux professionnels,
- l'ouverture de liens ou pièces jointes.

Les e-mails professionnels doivent être utilisés de manière responsable et respecter les politiques de confidentialité. Il ne doit pas être envoyé de mails contenant des informations confidentielles à des destinataires non autorisés, et, des destinataires autorisés sur une messagerie non sécurisée [Exemple : ...]

Il est interdit de partager des données de santé ou données sensibles en dehors des canaux sécurisés. En conséquence, toute donnée sensible doit être échangée de manière sécurisée. [Précisez les outils collaboratifs sécurisés. Exemple : Medimail, SPICO discussions, MSS]

5. Sécurité informatique

Tous les utilisateurs sont tenus de prendre des mesures raisonnables pour protéger les systèmes informatiques de la CPTS contre les menaces de sécurité, y compris les virus, les logiciels malveillants et les tentatives d'accès non autorisées.

Il est interdit d'installer des logiciels ou applications sans validation préalable de la CPTS ou du prestataire informatique.

La mise à jour régulière des systèmes et applications ainsi que de l'antivirus sont à faire dès que possible.

[Il est recommandé d'activer l'application des mises à jour automatiques]

Les utilisateurs doivent signaler toute suspicion d'incident de sécurité ou de violation de données à l'administrateur informatique ou au référent RGPD / DPO de la CPTS [Nom et coordonnées] dès que possible.

6. Sauvegardes

La mise en œuvre du système de sécurité [ne] comporte [pas] des dispositifs de sauvegarde des informations destiné à doubler le système en cas de défaillance.
[A définir avec votre prestataire informatique et chaque sous-traitant]

Une sauvegarde est à réaliser sur un support dématérialisé [X fois par mois / trimestre].

7. Utilisation responsable

Tout salarié et membre de la CPTS est responsable de respecter les dispositions de cette charte informatique et d'en diffuser les usages auprès des adhérents de la CPTS.

Les systèmes informatiques de la CPTS ne doivent pas être utilisés pour accéder à du contenu illicite, inapproprié ou offensant, ni pour mener des activités personnelles non liées au travail.

L'utilisation des ressources informatiques de la CPTS pour diffuser des informations confidentielles ou sensibles en dehors de la CPTS est strictement interdite.

[La CPTS s'engage à sensibiliser et former ses adhérents aux bonnes pratiques en matière de sécurité informatique et de protection des données, afin de prévenir les risques de violation de la confidentialité]

8. Utilisation des équipements personnels

L'utilisation d'équipements personnels pour des activités professionnelles doit rester exceptionnelle et respecter les règles de sécurité de la CPTS. Aucune donnée sensible ne doit être stockée sur un équipement personnel non sécurisé

9. Cybersécurité et bonnes pratiques

La sécurité des systèmes d'information repose sur des gestes simples que chacun peut adopter : mots de passe robustes, mises à jour régulières, usage de logiciels sécurisés, verrouillage de session, authentification double facteur lorsque cela est possible, vigilance face aux liens suspects et sauvegarde régulière des données. Ces bonnes pratiques de **cybersécurité** complètent la conformité RGPD et participent à la protection des informations de la CPTS.

10. Référent et mise à jour de la charte

La présente charte est tenue à jour par le référent numérique ou le DPO de la CPTS, en lien avec le prestataire informatique. Elle fait l'objet d'une révision annuelle ou en cas de modification majeure du système d'information.

11. Engagement des utilisateurs

Je reconnais avoir pris connaissance de la présente charte et m'engage à en respecter les règles d'usage et de sécurité des systèmes d'information de la CPTS.

Nom / Prénom : [...]

Le : [...]

Signature de l'utilisateur : [...]

Fait à [...],

Le [...]

Signature du Président de CPTS : [...]