URPS KINÉS PAYS DE LA LOIRE

En partenariat avec :

ars Agence Régionale de Santé Pays de la Loire

TOUS CYBER VIGILANTS !

Guide des bonnes pratiques en sécurité informatique pour les kinés

- PROTÉGER VOS DONNÉES SENSIBLES
- APPLIQUER DES MESURES D'HYGIÈNE NUMÉRIQUE
- RÉAGIR EN CAS DE CYBERATTAQUE

KINÉS, TOUS CYBER VIGILANTS !

Le dispositif SEGUR amorce un virage numérique essentiel à l'évolution de notre système de santé actuel. L'identification, l'échange, le partage de l'information sont des points capitaux à une meilleure prise en charge de nos patients.

Les professionnels adoptent de nouveaux outils dans leur exercice au quotidien. Cela implique également un devoir de protection des données personnelles, encadré par des directives européennes (RGPD).

Par ses missions, votre URPS Kinés des Pays de la Loire s'inscrit dans le développement du numérique en santé depuis de nombreuses années. C'est pourquoi nous souhaitons vous accompagner dans le **déploiement des systèmes de partage informatique et leur sécurisation**.

Les cyberattaques se multiplient, votre activité peut en être impactée de façon irréversible... **les bons réflexes sont indispensables** !

Ce livret a été pensé pour vous aider à **prévenir** et à **lutter** contre ces menaces potentielles.

Bonne lecture !

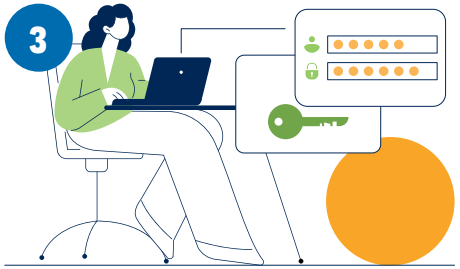
PROTÉGER SON POSTE DE TRAVAIL

Maîtriser l'accès physique au lieu d'exercice

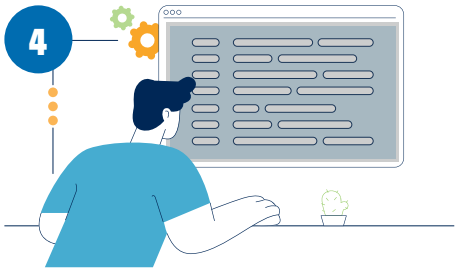
Même si une cyberattaque « physique » est peu probable, il est plus facile d'accéder aux données à proximité de l'ordinateur. **Ne tentons pas les personnes trop curieuses.**

PROTÉGER l'accès au poste de travail **en cas d'absence**.

PROSCRIRE l'écriture de mots de passe sur des supports **non sécurisés**.



SÉCURISER l'accès aux données en **verrouillant** le poste de travail.



CACHER l'écran avec un **filtre confidentialité**.

PROTÉGER SES APPLICATIONS

Respecter les règles de sécurité pour l'usage des cartes CPS et e-CPS

Respecter leur caractère **personnel et strictement incessible** :

- **Garder secrets** le code PIN et le code PUK.
- Maintenir la carte **en lieu sûr** lorsqu'elle n'est pas sous surveillance.
- Pour la e-CPS, appliquer au téléphone les mêmes principes de protection que ceux recommandés en p. 3 pour le poste de travail et être attentif aux notifications de connexions.

e-CPS

Utiliser des mots de passe robustes

Choisir un mot de passe d'au moins **12 caractères** :

- Utiliser une combinaison de **minuscules, de majuscules, de chiffres et de caractères spéciaux** (# » !-...).
- Choisir un mot de passe **non prédictible** *(ex : pas de date de naissance)*.
- S'assurer qu'il est **mémorisable** sans avoir à le noter. Privilégier une approche mnémotechnique pour s'en souvenir. Par exemple utiliser une phrase.
- Utiliser un **mot de passe unique pour chaque compte**.
- Utiliser un **gestionnaire de mots de passe** pour organiser les différents mots de passe *(ex : Bitwarden, KeePassXC, KeePass, Password Safe)*.

⚠ **Au cabinet, chacun son mot de passe.**

Veiller à la mise à niveau du système et des outils logiciels

Veiller à la mise à niveau du système et des outils logiciels est au moins **aussi important que tenir son antivirus à jour**. Maintenir à jour l'antivirus d'un système d'exploitation obsolète n'est pas suffisant.

Séparer les usages professionnels des usages personnels

Par exemple, **ne pas connecter de supports amovibles personnels** sur un équipement professionnel.

SÉCURISER LE WIFI

- **Recommander l'utilisation de protocoles sécurisés** (WPA2 ou WPA3).
- Mettre un **mot de passe complexe, changer le mot de passe par défaut**.
- **Mettre son matériel à jour** (box, routeur wifi, etc.) afin de limiter les risques de failles.
- Ne pas l'afficher sauf si wifi public totalement séparé du réseau wifi auquel sont connectés les terminaux professionnels.

MAÎTRISER LES ACCÈS AUX INFORMATIONS

Utiliser une messagerie sécurisée de santé : MSS

MS Santé

MON ESPACE SANTÉ

C'est nécessaire pour protéger les échanges de messages de manière adéquate entre professionnels de santé.

Des échanges fiables et sécurisés sont possibles entre les professionnels de santé et leurs patients via Mon Espace Santé.

Renforcer la protection des comptes informatiques les plus sensibles

Pour les logiciels métiers, les accès internet aux comptes de gestion de votre activité (CPAM, URSSAF, CAPRIMKO, impôts, etc.) : **limiter l'accès au compte administrateur et le protéger de manière sécurisée par une double authentification** dès lors que celle-ci est disponible via e-CPS, CPS, OTP (mail ou SMS), etc.

CONNAÎTRE LES PRINCIPES DE SÉCURITÉ ET LES DIFFUSER

S'informer régulièrement sur les cybermenaces

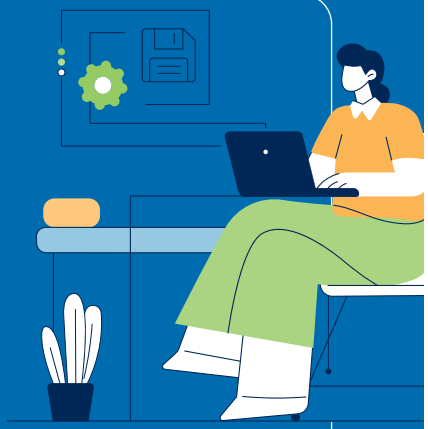
L'État propose sur le site internet **cybermalveillance.gouv.fr** des informations claires, concises et accessibles à tous sur les principales menaces et les mesures préventives associées. Il est fortement recommandé de les consulter.

Documenter et partager les usages de l'informatique au sein du cabinet

Avoir un document qui permet à tous les intervenants sur les postes informatiques d'avoir un pense-bête de cybersécurité.

ANTICIPER LA SURVENUE D'INCIDENTS DE SÉCURITÉ

SAUVEGARDER LES DONNÉES



- Cela permet de **restaurer le système** en cas d'incident.
- **Tester la restauration** pour s'assurer qu'elle fonctionne.
- **Les sauvegardes doivent être déconnectées** dans la mesure du possible afin de les protéger de toute atteinte suite à une cyberattaque (notamment chiffrement par un ransomware).
- Ne pas utiliser une **sauvegarde sur le Cloud** type OneDrive ou Google Drive pour les données de santé.
- En cas d'utilisation **d'un ou plusieurs disques durs externes dédiés aux usages professionnels, veiller à ce qu'ils soient chiffrés**. Idéalement, le support des sauvegardes doit être dupliqué et conservé à deux endroits différents *(ex : un au cabinet, un autre au domicile)*.
  → **Pour aller plus loin :**
  cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

Détruire les données qui doivent être supprimées

Détruire physiquement les équipements intégrant un espace de stockage de données (disque dur, CD / DVD, etc.).

Effacer les données stockées de manière sécurisée. En effet, les données supprimées de façon « basique » restent parfois récupérables avec des outils spécifiques après un effacement « simple ».

→ **Pour aller plus loin :**
cnil.fr/fr/effacer-ses-donnees-dun-ordinateur-dun-telephone-ou-dune-tablette-avant-de-sen-separer

Savoir détecter un incident de sécurité informatique

Considérer un mail suspect, un ordinateur qui ne répond pas, un logiciel installé sans votre accord comme un drapeau rouge. Ne pas remettre à plus tard les alertes des antivirus.

PROTÉGER LES DONNÉES DE SANTÉ

Les données de santé sont des données personnelles considérées comme sensibles. Elles font à ce titre l'objet d'une protection particulière (Règlement Général sur la Protection des Données personnelles ou RGPD, loi Informatique et Libertés, Code de la santé publique, etc.) afin de **garantir le respect de la vie privée des personnes**.

Lors de nos soins, nous collectons des informations relatives à l'état de santé de nos patients.

Qu'il soit papier ou informatique, le dossier patient que nous tenons correspond à un **« traitement de données » dont nous sommes responsables**.

De fait, nous avons l'obligation de respecter les exigences du RGPD.

RGPD, QUÈSACO ?!

Pour s'informer, la CNIL (Commission nationale de l'informatique et des libertés) a créé un **dossier thématique** adapté aux professionnels de santé libéraux.

EN PRATIQUE

Plusieurs obligations sont à respecter. Elles sont résumées ci-dessous :

INFORMER LES PATIENTS
de la collecte et du traitement des données et de leurs droits relatifs à ces données, par exemple avec une **affiche disposée dans la salle d'attente**.

TENIR UN REGISTRE
des activités de traitements de données personnelles.

Pour vous aider, vous pouvez consulter le **modèle de registre proposé par le CNOMK** et adapté à notre activité en cliquant sur le lien ci-dessous :

→ ordremk.fr/je-suis-kinesitherapeute/specification-et-explications/

CONSERVER LES DONNÉES
pendant **20 ans** à compter de leur dernière consultation (durée préconisée par la CNIL). Se référer au paragraphe sur la sauvegarde des données.

VEILLER À LA SÉCURITÉ
de ces données : **c'est l'objet de ce livret** !

S'ASSURER DU RESPECT
des bonnes pratiques par les prestataires de service informatique[1] grâce aux questionnaires proposés par l'ANS[2].

[1] On entend par service informatique l'installation, la maintenance, le stockage de données à distance, la prise de rendez-vous en ligne, la gestion des dossiers patients. [2] esante.gouv.fr

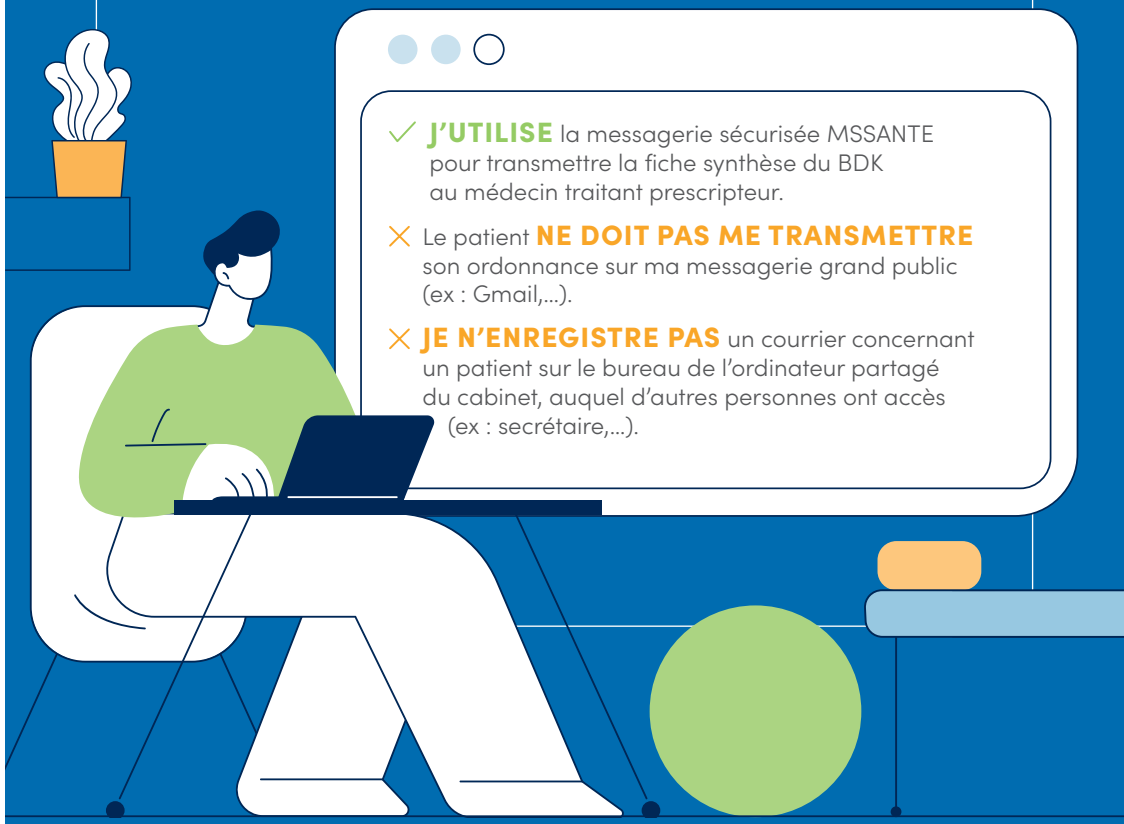
COMMUNIQUER DES DONNÉES DE SANTÉ

Communiquer des informations de santé concernant un patient à d'autres professionnels de santé intervenant dans la prise en charge du patient, c'est possible et c'est défini par l'article L.1110-4 du Code de la Santé Publique.

Les outils numériques facilitent l'échange et le partage d'informations afin de fluidifier le parcours de soin des patients (messagerie sécurisée, DMP, logiciels partagés). Cependant certains principes doivent être respectés.

Nous devons collecter uniquement les **informations pertinentes** et **nécessaires à la prise en charge du patient** et les communiquer en respectant les principes du **secret professionnel** et en veillant à leur confidentialité.

EN PRATIQUE



✓ **J'UTILISE** la messagerie sécurisée MSSANTE pour transmettre la fiche synthèse du BDK au médecin traitant prescripteur.

✗ Le patient **NE DOIT PAS ME TRANSMETTRE** son ordonnance sur ma messagerie grand public (ex : Gmail,...).

✗ **JE N'ENREGISTRE PAS** un courrier concernant un patient sur le bureau de l'ordinateur partagé du cabinet, auquel d'autres personnes ont accès (ex : secrétaire,...).

BONS RÉFLEXES EN CAS D'INCIDENT DE SÉCURITÉ INFORMATIQUE

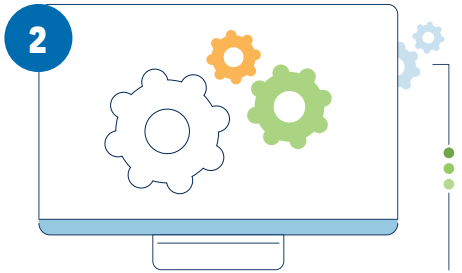
LES ÉTAPES À SUIVRE :

1

DÉCONNECTER DU RÉSEAU la machine sur laquelle l'incident est suspecté (câble réseau ou désactivation du wifi). S'il s'agit d'une intrusion, l'attaquant connecté à distance perdra alors l'accès à la machine compromise, cela permet également de protéger les autres machines du réseau.

MAINTENIR SOUS TENSION la machine. Ne pas l'arrêter ni la redémarrer et ne plus interagir avec elle afin de conserver l'information utile pour l'analyse de l'attaque potentielle et pour constituer des éléments de preuve pour le dépôt de plainte.

2

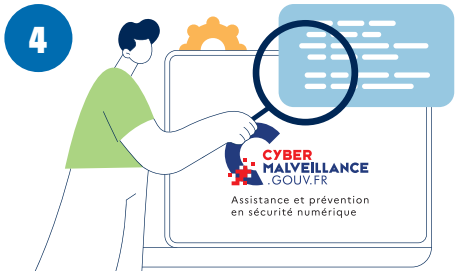


3

ALERTER son fournisseur de service informatique en charge du suivi de la machine et lui demander de l'assistance. À défaut, faire appel à un professionnel de l'informatique.

DÉCRIRE l'incident de sécurité sur le site cybermalveillance.gouv.fr et suivre les conseils proposés.

4



CAS SPÉCIFIQUES :

Si l'incident constitue une violation de données à caractère personnel, susceptible d'engendrer un risque pour les droits et libertés des personnes concernées par les données, une notification auprès de la CNIL ainsi que, dans certains cas, une information des personnes concernées, doivent être réalisées dans les délais impartis (72h) :

→ **cnil.fr/fr/notifier-une-violation-de-donnees-personnelles**

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Si l'incident s'avère être la conséquence d'une malveillance, il est important de le déclarer via un dépôt de plainte auprès des services de police ou de gendarmerie, d'autant plus en cas de vol de matériel informatique ayant hébergé des données de santé à caractère personnel ou d'accès illicite à des données de santé.

Le site **cybermalveillance.gouv.fr** est un outil de diagnostic et d'assistance en ligne qui indique les contacts utiles dans ce cadre :

→ **cybermalveillance.gouv.fr/diagnostic/accueil**

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

La réception de spam (ou courriers indésirables) peut être déclarée sur le site internet suivant :

→ **signal-spam.fr**

signal spam

Face aux cyber menaces, apportons une réponse collective, déterminée et coordonnée.

Ensemble, soyons tous cyber vigilants !

→ Ressource utile : Mémento de l'ANS à retrouver sur le site esante.gouv.fr

URPS KINÉS PAYS DE LA LOIRE

MAISON DES URPS

5 boulevard Vincent Gâche | 44200 Nantes
02 41 24 03 04 | urpskinepdl@gmail.com

urps-mk-paysdelaloire.fr

Abonnez-vous à notre newsletter
et suivez-nous sur les réseaux sociaux :

En partenariat avec :

ars Agence Régionale de Santé Pays de la Loire

TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

e-santé GRADeS Pays de la Loire

Avec le soutien de : AGENCE DU NUMÉRIQUE EN SANTÉ — La transformation commence ici