AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

Guide des bonnes pratiques

Statut : validé | Classification : publique | Version : V2.0 – 17/11/2021

Table des matières

1

POURQUOI CE MEMENTO ?

Les enjeux de la cybersécurité pour les professionnels de santé en exercice libéral, et ce que propose ce mémento.

Les incidents de cybersécurité sont évoqués de façon très régulière dans l'actualité. Les attaques portant sur les moyens informatiques sont récurrentes et touchent toutes les catégories de populations : entreprises, administrations, particuliers... Les sources d'information sur les moyens permettant de se prémunir de ces attaques sont nombreuses, mais elles peuvent diverger et il est souvent difficile de se faire une idée précise des bonnes pratiques de sécurité à adopter.

Dans le cadre de l'exercice quotidien de votre activité de professionnel de santé libéral, vous vous appuyez désormais sur les outils informatiques (ordinateurs, messageries, tablettes, smartphones, etc.). Ces usages vous exposent à des incidents de sécurité qui peuvent impacter votre activité de façon sévère, voire irréversible.

Par exemple, le disque dur de votre ordinateur peut tomber en panne, et rendre tout ou partie de vos dossiers patients définitivement inaccessibles. Ou encore, ces mêmes dossiers peuvent être rendus inexploitables en étant chiffrés par des pirates informatiques à l'aide d'un « rançongiciel » qu'ils ont réussi à introduire sur votre poste de travail. Ces pirates vous proposent ensuite de restaurer l'accès à ces données contre une rançon (cette promesse étant tenue après paiement… ou pas).

Afin d'assurer la protection des données de vos patients, vous êtes par ailleurs tenu de mettre en œuvre des mesures garantissant la sécurité des données sensibles que vous manipulez et ne disposez parfois pour cela que de moyens techniques limités et de peu de temps disponible.

Ce mémento rassemble des règles d'hygiène informatique ne nécessitant pas de connaissance technique approfondie. Lorsqu'elles sont appliquées de façon stricte et régulière, elles peuvent vous permettre de vous prémunir contre la majorité des attaques informatiques, ou à défaut d'en limiter les impacts.

En outre, vous pouvez être amené à faire appel à des fournisseurs de services informatiques pour l'installation, la gestion et la maintenance matérielle et logicielle de tout ou partie de votre infrastructure technique et de vos outils informatiques, ou encore pour vous fournir des téléservices, services « en ligne » ou services « cloud » tels que des applications de gestion de cabinet ou d'officine, de prise de rendez-vous, de téléconsultation...

Il est important que tous ces services soient compatibles avec vos obligations de sécurisation des données sensibles. **Ce memento propose un ensemble de questionnaires permettant de vérifier, avec vos fournisseurs de service, différents points d'attention concernant les services informatiques fournis.**

Ce document, qui fait partie du corpus documentaire de la politique générale de sécurité des systèmes d'informations en santé (PGSSI-S), doit être considéré comme un aide-mémoire qui rassemble les points essentiels à suivre par les professionnels de santé libéraux et que nous vous invitons à conserver et à consulter régulièrement.

1.1 Quels sont les enjeux ?

1.1.1 La protection des données de santé

La prise en charge d'un patient nécessite le traitement de données à caractère personnel et tout particulièrement des données de santé. A ce titre, un certain nombre d'obligations législatives et réglementaires sont imposées aux professionnels de santé qui traitent (créent, consultent, utilisent, conservent, communiquent…) ces données.

Par ailleurs, vous devez pouvoir vous appuyer sur une base d'informations disponibles mais aussi vérifiées, à jour, précises et cohérentes. Cela nécessite des moyens informatiques performants dont le bon fonctionnement soit garanti pendant vos périodes de travail.

Pour répondre aux enjeux liés à une bonne prise en charge des patients, il est nécessaire d'assurer :

- La **disponibilité des données de santé des patients** et des **moyens informatiques** pour limiter le risque de perte de chance ;
- La **confidentialité des données de santé** des patients pour préserver le secret médical ;
- L'**exactitude des données de santé** des patients pour un diagnostic rapide et juste ;
- Le **partage maîtrisé des données de santé** des patients pour permettre la coordination des soins ;
- La **traçabilité** des actes médicaux dont les prescriptions médicales, les produits de santé dispensés ou administrés, les produits de santé utilisés ou implantés lors d'un acte chirurgical et la conservation de l'historique des antécédents médicaux, afin de conserver la mémoire des actions réalisées dans le cadre de la prise en charge du patient.

Ce document vise à rassembler les bonnes pratiques qui vous sont nécessaires en tant que professionnel de santé libéral pour répondre à l'ensemble de ces enjeux dans votre utilisation quotidienne des moyens informatiques.

1.1.2 La multiplication des cyberattaques

Les moyens informatiques, devenus essentiels pour assurer la qualité des soins, se trouvent confrontés à une menace cybercriminelle croissante.

Les cyberattaques dites « opportunistes », le plus souvent à but lucratif, sont très courantes. Elles sont le fait de cybercriminels qui les diffusent de façon très large afin de toucher un maximum d'utilisateurs qui n'auraient pas mis en œuvre les bonnes pratiques de sécurité. **Tout professionnel de santé peut un jour être la cible de ce type d'attaque**.

Les vecteurs d'attaque les plus couramment rencontrés sont :

- La **messagerie électronique**, qui reste la porte d'entrée privilégiée de nombreuses attaques car son utilisation est largement répandue ;
- L'**exploitation de failles non corrigées** des outils informatiques : tous les jours, des failles de sécurité sont découvertes, et celles-ci peuvent parfois être exploitées par les cybercriminels.

L'adoption de quelques bons réflexes et l'apprentissage des bonnes pratiques de sécurité permettent de se prémunir de la plupart de ces attaques. L'ambition du présent mémento est de porter ces éléments à votre connaissance pour vous permettre de mieux vous protéger.

1.2 A qui s'adresse ce mémento ?

Ce mémento s'adresse à tout professionnel de santé en exercice libéral. C'est pourquoi il couvre diverses situations d'exercice, diverses formes d'utilisation de solutions informatiques et différentes natures de solutions. Le tableau suivant résume, pour ces trois axes, les différentes situations que couvre le mémento.

Situations couvertes par le mémento			
Votre mode d'exercice	► Individuel	► Avec un(e) assistant(e)	► En collectif
Votre mode d'usage des outils logiciels	► Vous utilisez exclusivement des logiciels individuels	► Au moins certains des logiciels que vous utilisez sont partagés avec d'autres acteurs (assistant(e), autres professionnels de santé du cabinet…)	
Les types de solutions utilisées	► Pour au moins certains usages, les solutions logicielles que vous utilisez sont installées sur des postes de travail et/ou des serveurs localisés au sein de votre lieu d'exercice	► Pour au moins certains usages, les solutions que vous utilisez incluent un hébergement externe (type cloud)	

1.3 Que contient ce mémento ?

Vous trouverez dans ce mémento élaboré à l'attention des professionnels de santé en exercice libéral :

- Une checklist vous permettant de pointer, au fur et à mesure de leur mise en application, les principes et mesures d'hygiène informatique que vous avez effectivement mis en œuvre, et ceux qu'il reste à traiter (chapitre 2.1) ;
- La description de ces principes et mesures d'hygiène informatique de base qui vous sont recommandés (chapitre 2.2 et suivants) ;
- Quatre questionnaires, à faire remplir par vos fournisseurs de prestations de service informatique[1] en fonction de la nature de la prestation qu'ils assurent pour vous, afin de vérifier qu'ils respectent bien les bonnes pratiques essentielles au vu de votre activité (rassemblées dans le document « **Annexe 1 – Questionnaires fournisseurs** ») ;
- Une fiche réflexe précisant les points clés qu'il vous est proposé de suivre en cas d'incident de sécurité informatique sur vos équipements (dans le document « **Annexe 2 – Fiche réflexe en cas d'incident de sécurité informatique** »).

[1] Telles que les activités d'installation, de maintenance ou de télémaintenance de matériel informatique ou de logiciel, ou encore de stockage de données à distance (y compris sauvegardes ou archivage) ou de fourniture d'accès à des téléservices.

2

PRINCIPES DE SECURITE ET MESURES D'HYGIENE INFORMATIQUE A METTRE EN ŒUVRE

Checklist et recommandations de mesures d'hygiène informatique à mettre en œuvre.

Les principes décrits dans ce chapitre ne requièrent aucune connaissance technique pour être mis en œuvre. Ils s'adressent à vous, professionnel de santé, indépendamment du fait que vous ayez établi ou non un contrat avec des fournisseurs de services informatiques pour la prise en charge sécurisée de vos outils informatiques.

L'application de ces principes est donc recommandée à tout professionnel de santé en exercice libéral.

- Une **checklist** vous est proposée ci-après. Elle vous permettra de pointer, au fur et à mesure de leur mise en application, les principes et mesures d'hygiène informatique que vous avez effectivement mis en œuvre, et ceux qu'il reste à traiter. Cette checklist ne se substitue pas aux informations détaillées dans les différents chapitres qui suivent et qu'il vous est fortement recommandé de lire.
- La checklist sera utilement revérifiée de façon régulière, par exemple annuellement, pour vous assurer que les différents principes sont toujours bien appliqués.

2.1 Checklist des mesures d'hygiène informatique à mettre en œuvre

Les colonnes « L » et « C » indiquent, pour chaque action, si l'action mentionnée vous est applicable en fonction du type de solutions que vous utilisez :

- **L** (pour « informatique **L**ocale ») : pour certains usages au moins, les solutions logicielles sont installées sur des postes de travail et/ou des serveurs localisés au sein du lieu d'exercice ;
- **C** (pour « services **C**loud ») : pour certains usages au moins, les solutions incluent un hébergement externe (type cloud).

En fonction de ces critères, il est possible que les colonnes L et C soient toutes deux applicables à votre situation.

Mesure d'hygiène informatique	L	C	Voir chapitre…	OK ? (Oui/Non)
Maîtriser l'accès physique au lieu d'exercice	X		2.2.1	
Maîtriser la sécurité physique des équipements informatiques				
Assurer la protection de l'alimentation électrique des équipements informatiques (*prise parafoudre et parasurtenseur, onduleur*…)	X		2.2.2	
Ne pas laisser accessibles au public les équipements informatiques	X		2.2.2	
Être vigilant sur la protection des supports de stockage de données amovibles *(ne pas les laisser connectés à l'ordinateur ni sur une table entre les utilisations, les ranger*…)	X		2.2.2	
Assurer la protection des équipements informatiques mobiles (*utiliser un câble de sécurité pour les accrocher ou les ranger entre les usages*)	X	X	2.2.2	
Protéger le poste de travail et l'accès aux applications				
Respecter les règles de sécurité pour l'utilisation des cartes de type CPx et e-CPS (*garder le code PIN secret, garder la carte à portée de main ou la ranger entre les usages*)	X	X	2.3.1	
Utiliser des mots de passe robustes (*minimum 12 caractères de types variés, pas de mot du dictionnaire ou en lien avec vous, construit par exemple à partir d'un texte que vous connaissez selon une méthode que vous vous fixez*)	X	X	2.3.2	
Utiliser un gestionnaire de mots de passe (*pour conserver facilement et de façon sécurisée un mot de passe différent, même très complexe, par application*)	X	X	2.3.2	
Ne pas stocker de mot passe dans le navigateur Internet sans mot de passe « maître »	X	X	2.3.2	
Protéger l'accès au poste de travail en cas d'absence (*verrouillage manuel et activer le verrouillage automatique du poste de travail*)	X	X	2.3.3	
Veiller à la mise à niveau du système et des outils logiciels (*activer la mise à jour automatique du système, des applications, de l'antivirus…)*	X		2.3.4	
Séparer les usages professionnels des usages personnels (*n'accéder à des données de patients que depuis un terminal à usage exclusivement professionnel*)	X	X	2.3.5	
Maîtriser les accès aux informations				
Utiliser une messagerie sécurisée de santé	X	X	2.4.1	
Renforcer la protection des comptes d'administrateur informatique	X	X	2.4.2	

Mesure d'hygiène informatique	L	C	Voir chapitre…	OK ? (Oui/Non)
Connaître les principes de sécurité et les diffuser				
Se renseigner sur les cybermenaces (*https://www.cybermalveillance.gouv.fr/cybermenaces*)	X	X	2.5.1	
Documenter les procédures d'exploitation	X		2.5.2	
Rédiger une charte informatique (s'il y a plusieurs utilisateurs de votre informatique)	X		2.5.2	
Anticiper la survenue d'incidents de sécurité				
Sauvegarder les données *(en ligne ou sur supports amovibles stockés dans un rangement sécurisé protégé des vols et sinistres qui affecteraient le cabinet)*	X	X	2.6.1	
Détruire les données qui doivent être supprimées	X	X	2.6.2	
Respecter les règles d'échange et de partage des données de santé à caractère personnel	X	X	2.7	
Respecter les principes du Règlement Général sur la protection des données (RGPD)				
Prendre connaissance du Référentiel relatif aux traitement de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux établi par la Commission nationale de l'informatique et des libertés (CNIL)	X	X	2.8.1	
Elaborer un registre des activités de traitement de données à caractère personnel	X	X	2.8.2	
Informer les personnes concernées par un traitement de données (*Notice d'information affichée ou remise au patient…*)	X	X	2.8.3	
Répondre aux obligations de conservation et de restitution des données				
Appliquer les durées règlementaires ou recommandées de conservation des données	X	X	2.9.1	
S'assurer de la capacité de restitution des données à caractère personnel	X	X	2.9.2	
Intégrer la sécurité dans les contrats avec les tiers				
Définir l'objet des fournitures de service informatique et les engagements et responsabilités des fournisseurs	X	X	2.10.1	
Réunir les conditions pour travailler en toute sécurité au sein d'environnements maîtrisés par un tiers	X		2.10.2	
Respecter les règles relatives à l'hébergement de données de santé à caractère personnel (*s'assurer que tout hébergeur de données de santé est titulaire d'un agrément ou d'un certificat d'hébergement de données de santé (HDS)*)		X	2.10.3	
Vérifier les points d'attention lors de recours à des fournisseurs de service informatique				
Questionnaire 1 : Points généraux applicables à toute fourniture de service informatique	X	X	Annexe 1	
Questionnaire 2 : Installation et/ou de maintenance informatique	X		Annexe 1	
Questionnaire 3 : Maintenance informatique à distance	X	X	Annexe 1	
Questionnaire 4 : Stockage de données à distance ou téléservice		X	Annexe 1	
Prendre connaissance de la Fiche réflexe prévue en cas d'incident de sécurité informatique et en conserver un exemplaire imprimé à un endroit accessible	X		Annexe 2	

2.2 Assurer la sécurité physique

Il est essentiel d'assurer la sécurité « physique » des équipements informatiques, c'est-à-dire les protéger des menaces directes liées à leur environnement. Par exemple : contre les pertes, les vols, les dégradations (inondations, chaleur, surtensions…).

2.2.1 Maîtriser l'accès physique au lieu d'exercice

Les équipements informatiques contenant les données des patients sont le plus souvent hébergés sur le lieu d'exercice. Il convient donc de mettre en place les mesures de sécurité physique adéquates pour protéger ces équipements et de sensibiliser régulièrement les utilisateurs à leurs responsabilités quant au respect des règles associées.
Il est par exemple recommandé de :

- Mettre en œuvre des mesures de protection contre les vols (*par exemple protection renforcée des portes extérieures et des fenêtres, installation d'un système d'alarme*), s'imposer de fermer à clé les pièces qui contiennent des équipements informatiques ou d'autres informations sensibles en cas d'absence ;
- Protéger les clés permettant l'accès aux locaux et les éventuels codes de désactivation d'alarme ;
- Établir les règles et moyens de contrôle d'accès des visiteurs et du personnel.

2.2.2 Maîtriser la sécurité physique des équipements informatiques

Outre les mesures concernant le lieu d'exercice, il est recommandé de :

- Ne pas laisser d'équipement informatique (*ordinateurs, tablettes, smartphone, imprimante, … et même de simples prises du réseau informatique si elles sont actives*) dans des pièces qui sont accessibles au public en dehors de la présence d'une personne de l'établissement[2] ;
- Positionner les équipements informatiques de préférence à un emplacement qui n'est pas facilement accessible par le public (*par exemple de telle sorte que son positionnement empêche l'accès à l'écran et aux ports USB par les patients et les accompagnants*) ;
- Protéger ces équipements de tout vol (*par exemple : attacher son ordinateur portable avec un câble antivol ou le mettre dans un coffre*) aussi bien pendant qu'en dehors des heures de travail ;
- Veiller à relier électriquement les équipements informatiques à un équipement qui les protège des anomalies de tension électrique (*multiprise avec dispositif anti-surtension, onduleur*…).

Pour les supports de stockage de données amovibles (disques durs externes, clés USB, mémoire flash, CD ou DVD), il est recommandé de :

- Les stocker systématiquement dans un coffre ou une armoire qui ferme à clé dès qu'ils ne sont plus utilisés ;
- Ne jamais utiliser de tels support provenant d'une personne en laquelle vous n'avez pas une totale confiance, et a fortiori ne jamais connecter un tel support qui aurait été trouvé ou qui aurait été temporairement égaré ;
- Chiffrer préalablement les données confidentielles avant de les transférer sur un matériel susceptible d'être égaré ou volé (les logiciels d'archivage/de compression permettent notamment d'effectuer ce chiffrement). Seules les personnes disposant du mot de passe utilisé lors du chiffrement seront alors en mesure de lire les données.

[2] « Etablissement » est pris dans un sens large dans ce mémento : cabinet ou toute structure de santé au sein de laquelle le professionnel de santé exerce.

- **7-zip** est un logiciel gratuit d'archivage de données faisant partie du socle interministériel de logiciels libres (SILL). Il permet de chiffrer les données lors de la création d'une archive. Il est important de choisir AES comme méthode de chiffrement et de saisir un mot de passe robuste (voir chapitre 2.3.2). La CNIL propose un tutoriel sur **cette page**.

  Pour en savoir plus…

Enfin il convient d'accorder une attention particulière aux équipements mobiles, tels que smartphones ou ordinateurs portables, qui sont les plus exposés aux pertes, vols et dégradations. Il est notamment recommandé de :

- Toujours conserver les équipements mobiles à portée de vue, ou à défaut les placer dans un rangement sûr ;
- Activer le verrouillage automatique et mettre en œuvre s'il est disponible l'effacement à distance des données de l'équipement -qui pourra être activé en cas de vol ou de perte de l'équipement- (option disponible sur les smartphones notamment) ;
- Activer le chiffrement pour protéger les données sensibles : les smartphones et tablettes comportent une option dédiée, à activer lorsque le chiffrement n'est pas actif par défaut, et certaines solutions antivirus permettent de chiffrer le contenu du disque dur d'un ordinateur portable quand cette fonction n'est pas fournie par le système d'exploitation ;
- Ne jamais connecter d'équipements mobiles à des prises USB publiques.

2.3 Protéger le poste de travail et l'accès aux applications

Les bonnes pratiques de sécurité présentées dans ce chapitre, telles que le bon usage des cartes de type CPx ou d'e-CPS et l'utilisation de mots de passe robustes, lorsqu'elles sont correctement mises en œuvre sur le poste de travail, permettent de se prémunir de nombreuses cyberattaques.

On considère ici les « postes de travail » au sens large : ordinateurs fixes, ordinateurs portables, smartphones, tablettes…

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

La carte CPS et les cartes de type CPx

La carte CPS (Carte de Professionnel de Santé) est une carte d'identité professionnelle électronique dédiée aux secteurs de la santé et du médico-social. Elle permet à son titulaire d'attester de son identité et de ses qualifications professionnelles, et de façon générale, de sécuriser les échanges des données de santé à caractère personnel.

Seuls les professionnels de santé peuvent obtenir une carte CPS. D'autres professionnels peuvent obtenir des cartes correspondant à leur situation :

- Carte de Personnel d'Etablissement (CPE) ;
- Carte de Directeur d'Établissement (CDE) ;
- Carte de Personnel Autorisé (CPA ou CDA) ;
- Carte de Personnel en Formation (CPF).

L'ensemble de ces cartes sont désignées sous l'appellation générique de carte CPx.

Il est important de respecter certaines règles lors de l'utilisation de ces cartes :

- Respecter le caractère personnel et strictement incessible de ces cartes ;
- Garder secret le code PIN (en particulier détruire ou protéger les courriers relatifs au code PIN) et le code PUK.

- Maintenir la carte près de son propriétaire en période d'utilisation et dans un lieu sûr (pour éviter la perte ou le vol) lorsqu'elle n'est pas utilisée.

Ces principes doivent être diffusés à tout utilisateur de carte CPx, et notamment aux éventuels porteurs de Cartes de Professionnels d'Etablissements (CPE) au sein du lieu d'exercice. Ces cartes ne doivent en aucun cas faire l'objet d'un usage en « libre-service ».

e-CPS et Pro Santé Connect

La carte e-CPS est la version dématérialisée de la carte CPS. C'est un nouveau moyen d'authentification fort, sous la forme d'une application pour smartphone. Elle fonctionne en lien avec le service Pro Santé Connect (PSC), un fournisseur d'identité dédié à la santé permettant l'authentification des professionnels des secteurs sanitaire, médico-social et social.

D'un niveau de sécurité équivalent à la CPS, la e-CPS permet au professionnel de santé ou du médico-social de s'authentifier directement auprès d'un service en ligne avec son mobile ou sa tablette, sans passer par un poste configuré et équipé d'un lecteur de carte.

Les exigences de sécurité à respecter lors de son utilisation sont identiques à celles de la carte CPS.

Pour en savoir plus…

- Si vous recevez sur votre téléphone une demande d'authentification e-CPS qui vous parait suspecte, vous devez refuser l'accès ou ignorer la demande.
- Pour vous accompagner dans cette démarche et répondre à vos éventuelles interrogations, il est mis à votre disposition le numéro du service client : 0825 85 2000 (0,06 Euros/min + prix d'un appel local).
- Si vous suspectez une utilisation frauduleuse de votre carte CPS ou e-CPS, nous vous invitons à porter plainte et à vous rapprocher de votre caisse d'assurance maladie au 36 08 (service gratuit + prix appel, du lundi au vendredi de 8 h 30 à 17 h 30) qui vous renseignera sur les démarches à suivre.

2.3.2 Utiliser des mots de passe robustes

Le mot de passe est en général la clé qui permet d'accéder aux données du poste de travail et aux applications, quand la carte CPx ou d'autres moyens d'authentification ne sont pas mis en œuvre. Conditionner l'accès à un ordinateur par un mot de passe est comparable à la mise sous clé des dossiers médicaux papier.

Ce « sésame » est donc recherché lors d'une cyberattaque, que l'attaquant ait gagné un accès physique ou distant au poste de travail. Il peut s'appuyer sur des outils capables de tester un grand nombre de mots de passe différents (donc ceux couramment utilisés, génériques, appartenant à un dictionnaire, basés sur les données personnelles de la victime ou générés aléatoirement) en un temps réduit. Il est donc essentiel, comme le rappelle également la CNIL, de s'appuyer sur un mot de passe suffisamment complexe pour ne pouvoir être découvert dans un temps raisonnable par ces techniques.

Ce principe s'applique bien évidemment aux mots de passe de tout équipement informatique ou application.

Voici quelques recommandations à suivre pour le choix du mot de passe (notamment diffusées par la CNIL) :

- Fixer à au moins 12 caractères la longueur du mot de passe ;
- Utiliser une combinaison de minuscules, de majuscules, de chiffres et de caractères spéciaux (# » !-…) ;
- Choisir un mot de passe non prédictible, c'est-à-dire qui n'a aucun lien avec son propriétaire (Ex : pas de nom ou prénom de proches, de nom de l'animal de compagnie, de date de naissance, de liens avec les centres d'intérêts de la personne, etc.) et qui n'appartient à aucun dictionnaire ;
- S'assurer que le mot de passe est mémorisable sans jamais avoir à le noter. Il est fortement recommandé d'adopter une approche mnémotechnique pour se souvenir des mots de passe sans jamais les inscrire sur un support potentiellement accessible par un tiers. Par exemple, il est possible de penser à une phrase dont on extrait le premier caractère de chaque mot en y intégrant des chiffres et des caractères spéciaux. Exemple : « je suis Isabelle, je vis à Paris et je suis fan de cinéma » = *js1jvaP€jsf2c* (I = 1 ; € = et ; 2 = de).

Afin d'éviter un piratage en cascade, il est recommandé d'utiliser un mot de passe unique pour chaque compte. Toutefois, il est bien entendu fastidieux de mémoriser ces nombreux mots de passe… **L'utilisation d'un gestionnaire de mots de passe est donc recommandée**. Il s'agit d'un logiciel qui permet de stocker l'ensemble de ses mots de passe et de les sécuriser avec un unique mot de passe « maitre » robuste, à la manière d'un coffre-fort. Il suffit alors de retenir cet unique mot de passe pour accéder à tous les autres. Généralement, ce logiciel permet également de générer en un clic des mots de passe robustes qui répondent aux trois premiers critères indiqués précédemment ; comme ces mots de passe seront conservés dans le gestionnaire, il n'est pas nécessaire d'être en mesure de les mémoriser.

- **Keepass** est un exemple de gestionnaire de mots de passe open source faisant partie du socle interministériel de logiciels libres (SILL) et dont la sécurité a été évaluée par l'ANSSI.

  Pour en savoir plus…

Par ailleurs, il est fortement déconseillé de stocker les mots de passe de sites Internet dans votre navigateur, sauf si votre navigateur vous propose de définir un mot de passe maître pour protéger les mots de passe qu'il stocke dans son gestionnaire de mots de passe intégré, et que vous configurez effectivement ce mot de passe. Même dans ce cas, il peut être finalement plus pratique d'utiliser un unique gestionnaire de mots de passe dédié comme conseillé ci-dessus, afin d'y conserver l'ensemble de vos mots de passe -Internet et autres- de manière sécurisée.

2.3.3 Protéger l'accès au poste de travail en cas d'absence

Si vous vous absentez de votre poste de travail en laissant votre session ouverte, il existe un risque d'accès non autorisé à des données de santé à caractère personnel en votre absence.

Pour s'en prémunir :

- Activer le verrouillage automatique du poste de travail après une durée compatible avec l'activité (une durée de 15 à 30 minutes est en général bien adaptée), en vous assurant que votre mot de passe est bien demandé pour le déverrouiller ensuite ;
- Verrouiller manuellement le poste de travail lorsque l'on s'en éloigne (*par exemple, le raccourci clavier à utiliser est généralement touches* ***ctrl + ⌘ + Q*** *sous Mac et touches* ***Windows + L*** *sous Windows)*.

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

Chaque jour, de nouvelles failles de sécurité sont découvertes dans les systèmes d'exploitation et logiciels du marché. Des attaquants exploitent ces vulnérabilités informatiques afin de s'introduire dans des systèmes d'information et d'accéder illégalement à des données. Il est donc essentiel d'installer régulièrement les correctifs de sécurité qui sont proposés par les éditeurs afin de se prémunir de ce type d'attaque.

Les recommandations à suivre sont les suivantes :

- S'assurer régulièrement que les logiciels et le système d'exploitation sont toujours maintenus et mis à jour par leurs éditeurs et anticiper leur fin de vie et leur remplacement ;
- Activer et paramétrer la mise à jour automatique du système d'exploitation et des logiciels pour qu'elle s'active dès que cela est possible (y compris la mise à jour des signatures de l'antivirus) ;
- N'utiliser que des logiciels distribués sur des supports originaux, à l'exclusion de toute copie.

2.3.5 Séparer les usages professionnels des usages personnels

La mutualisation des usages professionnels et personnels sur les mêmes équipements (*ordinateur, tablette, smartphone, etc.*) comporte des risques importants. Cette pratique est donc à éviter autant que possible. En effet, les équipements informatiques professionnels doivent faire l'objet d'une sécurisation la plus stricte possible dès lors qu'ils contiennent des informations sensibles ou qu'ils sont amenés à accéder à des systèmes d'information qui en contiennent.

Il est recommandé d'appliquer les principes de sécurité suivants :

- Ne connecter sur le réseau du lieu d'exercice que des matériels informatiques à usage exclusivement professionnel ;
- Ne pas mutualiser les usages personnels et professionnels sur un seul et même terminal (*par exemple, ne pas synchroniser pour ces différents usages les agendas, la messagerie, les réseaux sociaux*) ;
- Ne pas héberger des données professionnelles sur un équipement personnel ;
- Ne pas connecter de supports amovibles personnels sur un équipement professionnel.

2.4 Maîtriser les accès aux informations

Les équipements informatiques stockent des données dont la confidentialité doit être protégée, d'autant plus s'il s'agit de données de santé à caractère personnel. Pour cela, il est essentiel de s'assurer que seules les personnes autorisées à les consulter disposent des droits d'accès nécessaires.

2.4.1 Utiliser une messagerie sécurisée de santé

Les échanges par messagerie électronique entre professionnels de santé peuvent impliquer des données de santé à caractère personnel dont la confidentialité doit obligatoirement être garantie. Afin de protéger ces messages de toute interception malveillante, il est nécessaire de recourir à un chiffrement des échanges qui garantit que seuls les destinataires souhaités pourront consulter les informations transmises.

- L'utilisation d'une **messagerie sécurisée de santé** est **nécessaire** pour protéger ces échanges de messages de manière adéquate.

2.4.2 Renforcer la protection des comptes informatiques les plus sensibles

Le compte administrateur (du poste de travail ou du groupe de postes et serveurs en réseau) dispose de privilèges lui permettant généralement d'accéder à l'ensemble des informations stockées, dont certaines sensibles, et de lancer des actions pouvant avoir des conséquences irréversibles sur les équipements informatiques. Certains comptes applicatifs peuvent parfois également disposer de privilèges leur permettant d'accéder à de nombreuses données. Il est donc essentiel de protéger l'accès à ces différents comptes de manière renforcée en suivant les principes suivants :

- Limiter l'accès à ces comptes aux seules personnes habilitées à effectuer des actions d'administration telles que des installations et des paramétrages de logiciels, de la gestion de comptes utilisateurs, etc. (en général les équipes en charge de l'informatique) ;
- Conserver le mot de passe administrateur de façon sécurisée. Par exemple :
  - Au format numérique : dans un gestionnaire de mots de passe avec un mot de passe « maitre » robuste (cf. chapitre 2.3.2 - **Utiliser des mots de passe robustes**),
  - Au format papier : dans une enveloppe conservée dans un rangement sécurisé (à clé ou code) ;
- Conserver une copie de ce mot de passe de façon sécurisée dans un endroit externe au lieu d'exercice.

2.5 Connaître les principes de sécurité et les diffuser

2.5.1 Se renseigner sur les cybermenaces

Afin de se prémunir des incidents de sécurité, il est important d'avoir connaissance des principales menaces dont le professionnel de santé peut être victime et de la forme que peuvent prendre les cyberattaques. C'est ce qui va permettre d'identifier rapidement une attaque et d'adopter les bons réflexes.

Exemple : L'hameçonnage (ou phishing) est une technique frauduleuse qui vise à amener la victime à communiquer des données personnelles telles que des mots de passe par exemple. En sachant simplement que ce type d'attaque existe, voire en connaissant la forme que peut prendre un message électronique d'hameçonnage, le professionnel de santé a beaucoup moins de chances de se faire leurrer s'il reçoit ce type de message électronique malveillant.

Cette sensibilisation est essentielle pour vous, professionnel de santé, ainsi que pour toute personne qui exerce au sein de votre cabinet ou établissement de santé (assistant, secrétaire médicale...). Une information régulière sur ce sujet est nécessaire afin d'être au fait des nouvelles menaces.

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

  Pour en savoir plus sur les cybermenaces…

  Pour en savoir plus sur le sujet général des cyber malveillances…

2.5.2 Documenter les usages de l'informatique

Il est également important de bien documenter les procédures d'exploitation dans un manuel d'utilisation, de les tenir à jour et de les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action impliquant des données à caractère personnel, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer. **Votre fournisseur ou installateur de solution informatique devrait vous fournir cette documentation.**

- **Dans le cas d'une structure de santé qui mutualise des ressources informatiques :**

  Il est essentiel que l'ensemble du personnel, et notamment les personnes amenées à accéder à des données sensibles, soit informé de ses obligations afin d'assurer la sécurité du système d'information.

  Il est pour cela recommandé de rédiger une charte informatique (qui pourra être établie avec l'assistance d'un fournisseur de services informatiques) et de la rendre opposable (elle pourra par exemple être annexée au règlement intérieur). Cette charte devrait au moins comporter les éléments suivants :

  - Le rappel des règles en matière de de protection des données ;
  - Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition ;
  - Les responsabilités et sanctions encourues en cas de non-respect de la charte ;
  - La mention des éventuelles traces de l'activité du personnel susceptibles d'être conservées (en précisant la finalité et la durée de conservation de ces traces).

2.6 Anticiper la survenue d'incidents de sécurité

Lorsqu'un incident de sécurité survient, il est compliqué de réagir efficacement en partant de zéro. C'est pourquoi il est essentiel d'anticiper la survenue des incidents afin de disposer des éléments qui permettront de revenir rapidement à un fonctionnement de l'informatique suffisant pour reprendre votre activité.

2.6.1 Sauvegarder les données

La mise en œuvre de sauvegardes régulières des données permet, en cas de sinistre, d'être en mesure de restaurer les données perdues afin de revenir au plus vite à une situation opérationnelle vous permettant d'exercer votre activité malgré l'incident. Cette précaution s'avère crucial lorsque l'on fait l'objet d'attaques malveillantes « destructrices » telles que les attaques par rançongiciel (ou ransomware) qui chiffrent les données sur le poste de travail et les rendent ainsi inutilisables, mais également en cas de dysfonctionnement ou de simple maladresse ayant un impact sur les équipements informatiques ou les données stockées.

Il est fortement recommandé de confier la mise en œuvre du processus de sauvegarde et de restauration des données à un professionnel de l'informatique (en vous assurant qu'il respecte les points d'attention correspondants mentionnés à la section « **Sauvegardes** » du questionnaire n°2 proposé dans le document « Annexe 1 – Questionnaires fournisseurs ».

Toutefois, **c'est vous, en tant que professionnel de santé, qui devez déterminer quelles sont les données essentielles à sauvegarder** pour vous permettre d'assurer la continuité de votre activité **et vous assurer régulièrement que les sauvegardes sont bien réalisées**.

Pour ce faire, il est recommandé de :

- Définir le périmètre métier concerné par les sauvegardes (quelles activités, quelles données associées). Il faut identifier ce que l'on est prêt à perdre ou pas en cas d'incident de sécurité ;
- Définir la fréquence de sauvegarde, ce qui détermine la perte de données informatiques (en nombre de jours d'activité) que l'on est prêt à accepter : toutes les modifications de données informatiques étant intervenues entre la dernière sauvegarde et un incident potentiel sont susceptibles d'être perdues.

Si les sauvegardes sont effectuées exclusivement dans vos locaux, par vous ou par d'autres personnes habilitées, il est important que les supports de stockages utilisés à cette fin :

- Soient amovibles ;
- Soient systématiquement déconnectés physiquement du système informatique entre les sauvegardes ;
- Soient utilisés à tour de rôle afin qu'un problème avec l'un des supports de sauvegarde laisse, dans le pire des cas, la possibilité de restaurer les données avec le support précédent ;
- Soient conservés dans un lieu qui n'est pas susceptible d'être atteint par le même sinistre que celui qui aurait atteint le système sauvegardé, et en respectant les mêmes principes que ceux indiqués au chapitre 2.2.

De manière générale, il est recommandé de favoriser une solution de sauvegarde mixte, locale et en ligne :

- La sauvegarde en ligne, par exemple journalière, permet une mise en œuvre simple et éventuellement automatique, évite la manipulation fréquente de supports de sauvegarde, permet de disposer d'une sauvegarde stockée hors des locaux d'exercice et accessible depuis un éventuel lieu de repli en cas d'indisponibilité des locaux ;
- La sauvegarde locale, réalisée à la fréquence déterminée comme indiqué plus haut, sur des supports de sauvegarde conservés déconnectés du système dans un rangement **sécurisé** du local d'exercice, permet de disposer d'une sauvegarde utilisable en dernier recours, si la sauvegarde en ligne se trouvait indisponible ou corrompue.

2.6.2 Détruire les données qui doivent être supprimées

Quelles que soient les raisons motivant la suppression des données (par exemple dans le cas où celles-ci ne sont plus nécessaires à la pratique médicale, dans le cas où leur durée légale de conservation est dépassée ou dans le cas d'un changement de matériel), il est essentiel que ces données ne puissent pas être récupérées après leur suppression.

Cela suppose de mettre en œuvre l'une des deux mesures suivantes au choix :

- 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 accessibles après leur effacement à des outils de récupération. L'effacement sécurisé nécessite l'utilisation d'outils d'effacement sécurisé qui empêchent toute récupération des données une fois l'opération réalisée.

Dans un cas comme dans l'autre, il est fortement recommandé de confier la destruction des données à un professionnel de l'informatique (en vous assurant qu'il respecte le point d'attention correspondant mentionné à la section « **Maintenance** » du questionnaire n°2 proposé dans le document « Annexe 1 – Questionnaires fournisseurs ».

Pour les équipements mobiles légers (tablette, smartphone…) comme pour les ordinateurs portables ou fixes, le fait d'avoir activé dès leur installation initiale les fonctions de chiffrement du stockage des données (fonction intégrée ou logiciel additionnel, voir chapitre 2.2.2) permet, en utilisant la fonction « réinitialisation usine » de l'équipement ou en effectuant un **formatage avec effacement complet** du disque dur, de rendre les données inaccessibles à toute personne ne disposant pas de capacité technique très avancée.

2.6.3 Savoir réagir en cas d'incident de sécurité informatique

En cas d'incident de sécurité informatique, comme dans tout type d'incident, il est important d'avoir les bons réflexes pour éviter une aggravation de la situation et pour agir efficacement afin de résoudre le problème dans les meilleures conditions.

- Une fiche réflexe vous est proposée dans le document « **Annexe 2 – Fiche réflexe en cas d'incident de sécurité informatique** ». Elle détaille les points clés qu'il vous est recommandé de suivre en cas d'incident de sécurité informatique sur vos équipements.
- Vous êtes invité à prendre connaissance de cette fiche puis d'en conserver un exemplaire imprimé, à un endroit dont vous vous souviendrez facilement, au cas où votre poste de travail ne serait pas accessible du fait de l'incident subit.

2.7 Respecter les règles d'échange et de partage des données de santé à caractère personnel

Dans l'exercice de vos fonctions, vous êtes amenés à collecter et conserver des données de santé qui concernent vos patients. Ces données de santé dites « à caractère personnel » peuvent être échangées ou partagées dans les conditions prévues à l'article L.1110-4 du code de la santé publique.

L'échange ou partage de données de santé, c'est la communication d'informations relatives à une personne prise en charge, par un émetteur à un ou des destinataire(s) **clairement identifié(s)**. L'utilisation d'une messagerie sécurisée en constitue un exemple.

L'échange de données de santé entre professionnels de santé est subordonné aux conditions cumulatives suivantes :

- Les professionnels de santé participent tous à la prise en charge du patient concerné ;
- Les données échangées se limitent aux données strictement nécessaires à la coordination ou à la continuité des soins du patient, à la prévention ou à son suivi médico-social et social.

Les règles suivantes s'appliquent alors :

- Lorsque ces professionnels appartiennent à l'équipe de soins[3] qui prend en charge le patient, les informations nécessaires à cette prise en charge peuvent être partagées sans avoir à recueillir le consentement du patient. Ces informations sont réputées confiées par le patient à l'ensemble de l'équipe de soins ;
- En revanche, pour partager des informations avec des professionnels ne faisant pas partie de l'équipe de soins, le recueil préalable du consentement du patient est requis.

[3] Au sens de l'article L.1110-12 du code de la santé publique

Dans tous les cas, le patient doit être préalablement informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant et pouvoir exercer ce droit à tout moment (voir chapitre 2.8.3).

2.8 Respecter les principes de la protection des données de santé à caractère personnel

Le traitement de données à caractère personnel est encadré par les dispositions du Règlement Général sur la Protection des Données n°2016/679 du 27 avril 2016 (RGPD) et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (Loi informatique et libertés modifiée). Elles définissent notamment les principes à respecter lors du traitement et la conservation des données à caractère personnel.

Pour rappel, les « données concernant la santé » sont définies par le RGPD comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

2.8.1 Connaitre et appliquer les principes du règlement général sur la protection des données (RGPD)

- Afin d'accompagner les cabinets des professions médicales et paramédicales exerçant à titre libéral, la CNIL a établi un **référentiel qui encadre la mise en œuvre des traitements de données à caractère personnel pour ces professionnels dans le cadre de la gestion médicale et administrative de leur patientèle**.
  Pour en savoir plus…

La lecture de ce référentiel adapté aux professionnels de santé en exercice libéral vous est vivement recommandée afin de bien comprendre et connaître les grands principes applicables.

Dans les grandes lignes, on retiendra que :

- Seules les données strictement nécessaires à la prise en charge du patient doivent être collectées et traitées ;
- Ces données ne peuvent être utilisées ultérieurement à d'autres fins[4] ;
- Leur conservation dans le temps doit se limiter à la durée nécessaire à la réalisation de la finalité poursuivie ;
- Elles doivent être protégées de toute modification ou accès non autorisé ;
- Les patients ont des droits vis-à-vis de ces données : droit à l'information, d'opposition à leur collecte, d'accès à leurs données, de rectification ou de suppression des données qui les concernent…

[4] Sauf cas prévus par un texte légal ou règlementaire (*comme par exemple l'utilisation ultérieure de données de santé à fins de recherche selon le cadre et les modalités fixés par la loi*).

- La CNIL a également réalisé avec le Conseil National de l'Ordre des Médecins (CNOM) un « guide pratique sur la protection des données à caractère personnel » qui traite de façon plus large la question de la **protection des données personnelles pour les professionnels de santé qui exercent en cabinet groupé et partagent un système d'information commun**.
  Pour en savoir plus…
- Certains fournisseurs de service informatique peuvent aussi être en mesure de vous accompagner dans la mise en conformité avec le RGPD.

2.8.2 Elaborer un registre des activités de traitement de données à caractère personnel

Avant toute collecte de données de santé à caractère personnel, vous devez, en tant que professionnel de santé, vous assurer du respect des formalités préalables à la mise en œuvre du traitement, notamment en élaborant un registre des activités de traitement de données à caractère personnel.

- Un **modèle de registre des activités de traitement** est proposé en Annexe 2 du « guide pratique sur la protection des données à caractère personnel » que la CNIL a réalisé avec le Conseil National de l'Ordre des Médecins (CNOM).
  Pour en savoir plus…

2.8.3 Informer les patients du traitement de leurs données à caractère personnel

En tant que professionnel de santé, vous êtes soumis à l'obligation d'information préalable des patients sur les traitements de données personnelles effectués. Cette information peut se faire par voie d'affichage, dans la salle d'attente, ou par la remise d'un document spécifique au patient. Certains ordres de professionnels de santé proposent, sur leur site internet, leur propre modèle de note d'information à usage de la profession.

- Un **exemple de notice d'information pour la gestion d'un cabinet médical** est proposé en Annexe 1 du « guide pratique sur la protection des données à caractère personnel » que la CNIL a réalisé avec le Conseil National de l'Ordre des Médecins (CNOM).
  Pour en savoir plus…
- Pour plus d'informations sur ce sujet, vous pouvez consulter la page dédiée du site internet de la CNIL.
  Pour en savoir plus…

2.9 Répondre aux obligations de conservation et de restitution des données

2.9.1 Appliquer les durées règlementaires ou recommandées de conservation des données

Le dossier médical constitué pour chaque patient doit être conservé, en interne ou par un Hébergeur de Données de Santé (HDS), pendant une durée de vingt ans à compter de la date de la dernière prise en charge[5]. Cette durée couvre la durée de conservation des archives dites actives (documents directement accessibles) ainsi que la durée des archives intermédiaires[6] (documents nécessitant parfois une opération spécifique pour les rendre de nouveau accessibles à l'utilisateur, mais restant dans tous les cas sous la responsabilité du professionnel de santé).

- **La CNIL propose sur son site internet un document qui précise les durées de conservation réglementaires ou recommandées (lorsqu'il n'existe pas de règlementation spécifique) de la majorité des documents et données utilisés dans le domaine de la santé.**
  Pour en savoir plus…

2.9.2 S'assurer de la capacité de restitution des données à caractère personnel

Lors de recours à une fourniture de service comprenant de l'hébergement de données de santé à caractère personnel, le contrat doit prévoir que lorsqu'il sera mis fin à l'hébergement, l'hébergeur restituera les données au professionnel de santé auquel il fournit le service, sans en garder de copie. Le support sur lequel seront restituées les données devra permettre au professionnel de santé de poursuivre son activité et, le cas échéant, de recourir à un autre fournisseur de service pour les héberger.

Il faut également veiller à la mise en œuvre de ces mêmes mesures en cas de passation du cabinet à un autre professionnel de santé, et à l'existence d'une solution permettant de les mettre en œuvre en cas d'indisponibilité imprévue et définitive du professionnel de santé[7], afin que les dossiers informatisés des patients ne soient pas perdus et puissent être transmis.

2.10 Intégrer la sécurité dans les contrats avec les tiers

2.10.1 Définir l'objet des fournitures de service informatique et les limites d'engagement

Vous pouvez être amenés à faire appel à des fournisseurs de services informatiques pour la gestion et la maintenance matérielle et logicielle de tout ou partie de votre infrastructure technique et de vos outils informatiques, ou encore pour vous fournir des téléservices, services « en ligne » ou « cloud » tels que des applications de gestion de cabinet ou d'officine, de prise de rendez-vous, de téléconsultation... éventuellement interfacés avec vos autres logiciels.

[5] Article R1112-7 du code de la santé publique (pour les établissements de santé) et référentiel CNIL mentionné en début de chapitre 2.8.1

[6] Au-delà de cette durée, les règles qui s'appliquent sont celles fixées par le code du patrimoine.

[7] Voir commentaire de l'article 45 du code de déontologie médicale, transposable aux codes des autres professionnels de santé

La description précise du contenu des activités confiées au tiers fournisseur de service dans le contrat est alors essentielle. En effet, c'est ce qui va permettre d'apprécier la répartition des responsabilités entre le fournisseur de service et vous. Il reste de votre responsabilité d'obtenir de vos sous-traitant (ces fournisseurs de services) les garanties suffisantes quant à la protection et à l'usage des données à caractère personnel qui vous ont été confiées et dont vous restez de fait le « responsable de traitement ».

Vous pouvez avoir recours à des fournisseurs de services spécialisés qui établissent fréquemment des prestations de service et contrats standards à signer par le client et fixant *de facto* un certain mode de traitement standardisé des données à caractère personnel. Il vous appartient, en tant que responsable des données de santé à caractère personnel de vos patients, de veiller à ne pas accepter de contrat dont les clauses et conditions contractuelles seraient contraires à la législation sur la protection des données à caractère personnel et des données de santé.

Le contrat doit idéalement prévoir que le tiers fournisseur de service s'engage notamment à respecter les éléments du Mémento et les référentiels cités en référence qui le concernent. Les questionnaires proposés dans le document « Annexe 1 – Questionnaires fournisseurs » peuvent notamment être repris dans le contrat. A défaut, il est recommandé que ces questionnaires constituent des attestations remplies et signées par les fournisseurs de services en complément au contrat.

2.10.2 Réunir les conditions pour travailler en toute sécurité au sein d'environnements maîtrisés par un tiers

Il est **important**, en tant que professionnel de santé, **de vous assurer de disposer de conditions de sécurité adaptées** concernant les moyens informatiques mis à votre disposition **lorsque vous exercez dans un environnement maîtrisé par un tiers**. En effet, dans le cas où vous n'êtes pas maître des moyens de travail informatiques qui sont mis à votre disposition par un tiers *(par exemple lorsque exercez en EHPAD, en établissement de santé, au sein de sociétés civiles ou que vous effectuez des remplacements*), vous pouvez **inclure dans le contrat** qui organise vos relations avec ce tiers une clause l'engageant à garantir que **ces moyens informatiques respectent les dispositions législatives et règlementaires** en matière de sécurité des systèmes d'information et de protection des données, **et intègrent les principes du présent Mémento et des référentiels cités en référence**. Les questionnaires proposés dans le document « Annexe 1 – Questionnaires fournisseurs » peuvent également, dans ce cas de figure, être repris dans le contrat.

En cas de manquement aux obligations de sécurité qui apparaîtraient à l'usage des moyens informatiques mis à votre disposition, il est important que vous le signaliez formellement au responsable de ces moyens informatiques, voire aux autorités compétentes en l'absence de correction de ces manquements.

2.10.3 Respecter les règles relatives à l'hébergement de données de santé à caractère personnel

Si vous confiez les données de vos patients à un tiers (*par exemple dans le cadre de l'utilisation d'un service de gestion informatisée des dossiers patients*), **vous devez vous assurer que ce tiers est titulaire d'un agrément ou d'un certificat d'hébergement de données de santé (HDS) conformément à l'article L.1111-8 du code de la santé publique, et ce pendant toute la durée de cet hébergement de données de santé effectué pour votre compte**.

- La CNIL peut être consultée en cas de question sur la contractualisation avec des tiers impliquant des données à caractère personnel.
  Pour en savoir plus…

Annexe 1 : Questionnaires fournisseurs

Voir document « Annexe 1 – Questionnaires fournisseurs »

Annexe 2 : Fiche réflexe en cas d'incident de sécurité informatique

Voir document « Annexe 2 – Fiche réflexe en cas d'incident de sécurité informatique »

Annexe 3 : Abréviations

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANS	Agence du Numérique en Santé
CD	Compact Disc
CDE	Carte de Directeur d'Etablissement
CNIL	Commission Nationale de l'Informatique et des Libertés
CPA	Carte de Personnel Autorisé
CPE	Carte de Personnel d'Etablissement
CPF	Carte de Personnel en Formation
CPS	Carte de Professionnel de Santé
DVD	Digital Versatile Disc
EHPAD	Etablissement d'Hébergement pour Personnes Agées Dépendantes
PAS	Plan d'Assurance Sécurité
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PIN	Personal Identification Number
PSC	Pro Santé Connect
PUK	PIN Unlock Key
RGPD	Règlement Général sur la Protection des Données
USB	Universal Serial Bus