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

Fiche synthétique

Le « Mémento de sécurité informatique pour les professionnels de santé en exercice libéral » rassemble des **règles d'hygiène informatique de base** qui, si elles sont appliquées de façon stricte et régulière, peuvent vous permettre de vous prémunir contre la majorité des attaques informatiques, ou à défaut d'en limiter les impacts.

Il s'agit ici d'une fiche synthétique, la version intégrale du mémento est disponible à cet emplacement.

Quels sont les professionnels de santé libéraux concernés ?

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 informatiques utilisées	► **L** (pour « informatique **L**ocale ») : Pour 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	► **C** (pour « services **C**loud ») : Pour certains usages, les solutions que vous utilisez incluent un hébergement externe (type cloud)	

Checklist des mesures d'hygiène informatique à mettre en œuvre

Les colonnes « **L** » et « **C** » de la checklist font référence aux types de solutions informatiques décrites dans le tableau plus haut. Elles indiquent, pour chaque mesure, si celle-ci vous est applicable en fonction des types de solutions que vous utilisez. 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 (*prises 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	

Mesure d'hygiène informatique	L	C	Voir chapitre…	OK ? (Oui/Non)
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	
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 traitements 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	