Numérique en Santé : focus sur la cybersécurité

Informations générales :

Durée : 6 h	**Nb de stagiaires par session :** 30	Formateur : **Arnaud BARBIER**	Formation déposée dans le cadre de la **fiche n°11**

Attendus pédagogiques selon la fiche de cadrage :

S'appuyer sur le référentiel socle et transversal de compétences en vigueur : La formation a été conçue en s'appuyant sur les compétences définies par ce document.	*Se déployer autour d'un ou plusieurs grands domaines :* Dans cette formation, seul le domaine de **la cybersécurité en santé** est traité

Numérique en Santé : focus sur la cybersécurité

Présentation globale

6 h distanciel asynchrone

Contexte :

La santé numérique est « l'application des technologies de l'information et de la communication (TIC) à l'ensemble des activités en rapport avec la santé » (Fondation de l'Avenir). Ceci regroupe principalement un ensemble de solutions à destination des usagers, mais aussi des solutions à destination des professionnels (aide au diagnostic, outils de gestion, télésanté, communication et partage, information et formation, sécurité et traçabilité...).

À l'heure du Ségur numérique, et des évolutions attendues dans la pratique quotidienne des professionnels de santé, une transformation du système de santé s'est engagée dans le virage numérique.

La cybersécurité est devenue un sujet que les professionnels de santé ne peuvent plus négliger. La maîtrise de l'environnement numérique (réglementaire, fonctionnel,...) est indispensable afin de pouvoir adopter les bons comportements et respecter la législation.

Objectif général :

A travers cette formation, les professionnels de santé pourront acquérir les savoirs et compétences nécessaires à la maitrise de la cybersécurité dans leur pratique quotidienne

Objectifs spécifiques :

- Concevoir et maintenir sécurisé son environnement numérique de travail,
- Appréhender les bases de l'hygiène numérique (gestes et protection),
- Etre en capacité de se prémunir et de réagir face aux incidents.

Numérique en Santé : focus sur la cybersécurité			
Formation Continue (1/2)			
Module	*Contenu*	*durée*	*obj/compétence visée*
0 - Présentation / Introduction (60min)	*Présentation formation et formateur*	60 min	x Présenter l'expertise du formateur et le déroulement pratique de la formation x Evaluer initialement les connaissances théoriques et les compétences en raisonnement clinique du stagiaire x Présenter les notions clés liées au Numérique en Santé
	QCM de positionnement		
	Cas cliniques		
	Les bases du numérique en Santé		
1 - Concevoir et maintenir sécurisé son environnement numérique de travail (120 min)	*Les enjeux et objectifs de la cybersécurité*	30 min	x Connaitre les référentiels de référence en cybersécurité [notamment la Politique Générale de sécurité des systèmes d'information (PGSSI) et le Guide d'hygiène informatique de l'ANSSI] x Sécuriser le lieu d'accès physique (verrouillage des sessions) x Configurer son poste de travail et son téléphone portable (gestion de l'antivirus et des mises à jour, chiffrement et sauvegarde des données, utilisation de logiciels conformes aux règles de sécurité et de confidentialité) x Gérer des périphériques amovibles et l'utilisation nomade de son matériel - Connaitre les différents principes d'authentification, l'intérêt de l'authentification forte et à double facteurs et la gestion de mots de passe robustes - Sécuriser sa messagerie et respecter les bonnes pratiques pour l'envoi et la réception de courriel et de messages - Comprendre les enjeux de l'identification électronique appliquée au secteur de la santé - Mettre en place les bonnes pratiques pour sécuriser son environnementx identifier une violation de données personnelles au sens du RGPD x Réagir en cas d'incident de cybersécurité en santé
	Les moyens de protéger son environnement numérique de travail	30 min	
	Les mesures de prévention et règles à respecter	30 min	
	A retenir + quiz	30 min	

Numérique en Santé : focus sur la cybersécurité			
Formation Continue (2/2)			
Module	*Contenu*	*durée*	*obj/compétence visée*
2 -Se prémunir et réagir face aux incidents (120 min)	*Usagers et cybersécurité en santé*	15 min	x Connaitre les différents types d'action malveillantes x Sécuriser sa navigation sur internet, savoir reconnaitre les sites de confiance x Savoir se prémunir contre les virus et actes malveillants x Identifier une violation de données personnelles au sens du RGPD x Réagir en cas d'incident de cybersécurité en santé
	Les principales failles de sécurité et les risques de cyberattaques	15 min	
	Présentation de cyberattaques	20 min	
	La stratégie nationale (Programme CARE) face aux risques de	20 min	
	Comment réagir en cas de cyberattaque ?	20 min	
	A retenir + quiz	30 min	
5 - Conclusion (60 min)	*Synthèse*	60 min	x Présentation de la synthèse de la partie formation continue avec les notions clés x Evaluer les connaissances théoriques du stagiaire pour quantifier l'évolution au cours de la partie formation continue
	Quiz post-formation		
	Cas cliniques		