Annexe IV de l'arrêté du 5 juillet 2024 / Nouvelle annexe XIII de l'arrêté du 19 juillet 2019

Attestation de validation de la formation au numérique en santé

Nom et coordonnées complètes

du centre de formation

ATTESTATION DE VALIDATION DE LA FORMATION AU NUMÉRIQUE EN SANTÉ
Formation préparant au diplôme d'assistant de régulation médical
Attestation à délivrer par le directeur du centre de formation en complément du diplôme

Article 9 bis de l'arrêté du 19 juillet 2019 relatif à la formation conduisant au diplôme d'assistant de régulation médicale
et à l'agrément des centres de formation d'assistant de régulation médicale

Je soussigné …… Directeur (trice) du centre de formation

Nom de l'institut de formation
……

Adresse postale de l'institut de formation
……

atteste que
Prénom ……..…….. ***NOM***
……..

Né(e) le …… *A ……*

À validé la formation au numérique en santé prévue par l'article 9 bis de l'arrêté du 19 juillet 2019 relatif à la formation conduisant au diplôme d'assistant de régulation médicale.

La formation au numérique en santé délivrée est conforme au référentiel de compétences et de connaissances socles prévu à l'annexe XII de l'arrêté précité.
Elle s'est déroulée durant l'année scolaire ……. préparant au diplôme d'assistant de régulation médicale.

La formation au numérique en santé est intégrée dans les modules de formation correspondant référentiel de certification comme suit :

À compléter par l'institut de formation

Référentiel socle et transversal de compétences du numérique en santé des assistants de régulation médicale V1.1.2023	Blocs de compétence et modules de formation

N°	Compétences	Capacités	Heures	
1.	Données de santé		4	
1.1	Identifier un usager ou un professionnel de santé	-connaître les enjeux et critères liés à l'identitovigilance vis-à-vis d'un usager [Identité Nationale de Santé (INS), référentiels nationaux d'identité des personnes physiques]		
1.2	Caractériser et traiter la donnée à caractère personnel de santé en appliquant la réglementation	-connaître le Règlement UE 2016/679 général de protection des données du 27 avril 2016 (RGPD) -connaître le régime du traitement de données à caractère personnel de santé -identifier les modalités de traitement de données à caractère personnel, données de santé et les sanctions encourues		
1.3	Accéder aux données de santé en respectant les exigences professionnelles et légales	-**identifier les critères d'accès aux données des usagers : connaître le cadre réglementaire et la notion d'équipe de soins** -**connaître les responsabilités pénale et civile encourues** -respecter le secret professionnel appliqué aux professions médicales et de santé, la protection du professionnel et de l'usager et le secret médical partagé -**respecter le droit des usagers et les obligations liées à l'information des patients : savoir être et savoir-faire** -utiliser les outils d'accès aux données de l'usager [Identité Nationale de Santé (INS), Carte de Professionnel de Santé numérique (CPS), identifiant e-CPS, Carte de Professionnel en Formation (CPF), Pro santé Connect] -faire preuve d'éthique dans l'accès aux données de santé		
1.4	Exploiter les données de santé pour l'évaluation, la recherche et l'innovation	-connaître les grands enjeux liés à l'intelligence artificielle, aux algorithmes, aux biais et aux systèmes d'aide à la décision ainsi que les principes éthiques associés aux traitements des données de santé -connaître le régime spécifique de traitement des données à des fins de recherche (Recherches Impliquant la personne humaine, Loi Jardé, RGPD, LIL)		
2.	Cybersécurité en santé		4	
2.1	Concevoir et maintenir sécurisé son environnement numérique de travail	-**sécuriser le lieu d'accès physique (verrouillage des sessions)** -**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)** -**gérer des périphériques amovibles et l'utilisation nomade de son matériel** -**connaître les différents principes d'authentification, l'intérêt de l'authentification forte et à doubles 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 environnement**		
2.2	Se prémunir et réagir face aux incidents	-connaître les différents types d'actions malveillantes -sécuriser sa navigation sur internet, savoir reconnaître les sites de confiance -savoir se prémunir contre les virus et actes malveillants -**réagir en cas d'incident de cybersécurité en santé**		

3.	Communication en santé		3	
3.1	Utiliser les outils permettant d'interagir avec les usagers pour une transmission efficace de l'information	- **connaître le cadre réglementaire régissant les bonnes pratiques de communication avec l'ensemble des acteurs [Identité Nationale de Santé (INS), secret médical, codes de déontologie…]** - **maîtriser la notion de responsabilité professionnelle**		
3.2	Interagir de manière adaptée entre professionnels, avec l'usager, avec les aidants et accompagnants et avec les institutions et administrations	- **mettre en œuvre les bonnes pratiques de savoir être** - **respecter les principes éthiques** - renseigner les étudiants ou stagiaires - adopter les bonnes pratiques et les bons outils pour interagir et partager des données de santé		
3.3	Interagir sur internet en maîtrisant son identité numérique	- connaître les enjeux liés à la e-réputation (référencement, diffamation …) - connaître les bonnes pratiques en cas de connexion a des plateformes - interagir en tant que professionnel de santé		

Attestation établie à …… le ……..

Prénom NOM ……

Signature

Cachet de l'institut de formation