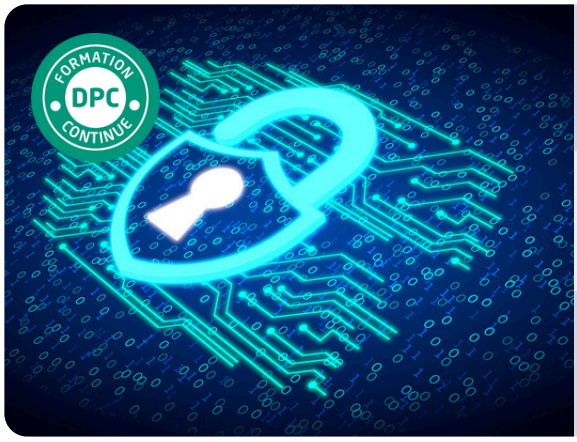
webdental formation

odpc

Référence DPC : 74852325022

DENTISTERIE NUMÉRIQUE

BONNES PRATIQUES POUR LA CYBERSÉCURITÉ EN SANTÉ



FORMAT	**100% e-learning - Formation continue** Votre formation intégralement en ligne : connectez-vous quand vous voulez et d'où vous voulez pendant 1 mois. Formation asynchrone.
DURÉE	**10 heures**
TARIF	450€ Formation éligible aux financements **DPC** (sous réserve de la disponibilité de vos droits)

OBJECTIFS PÉDAGOGIQUES

- Concevoir et maintenir sécurisé son environnement numérique de travail
- Appréhender les bases de l'hygiènenumérique (gestes et protection)
- Se prémunir et réagir face aux incidents
- Être tous cybervigilants

INTERVENANT

Damien PESCHET

INTERVENANTE

Maître Débora COHEN

Résumé de la formation

Les établissements de soins sont la cible de nombreuses attaques de leurs systèmes d'informations (SI) et celles-ci peuvent paralyser en tout ou partie leur activité et être à l'origine de fuites de données sensibles.

En effet, dans le cadre de leur exercice quotidien, les professionnels de santé s'appuient désormais sur des outils informatiques (ordinateurs, messageries, tablettes, smartphones, etc.) devenus essentiels pour assurer la qualité des soins. Ces usages les exposent à des incidents de sécurité qui peuvent impacter leur activité de façon sévère, voire irréversible notamment car ils se trouvent confrontés à une menace cybercriminelle croissante.

En outre, afin d'assurer la protection des données de leurs patients, ils sont par ailleurs tenus de mettre en œuvre des mesures garantissant la sécurité des données sensibles qu'ils manipulent et ils ne disposent parfois pour cela que de moyens techniques limités et de peu de temps disponible.

Cette formation concrète vous permettra de prendre connaissance des règles d'hygiène informatique essentielles ne nécessitant pas de connaissance technique approfondie pour les appliquer de façon stricte et régulière, afin de vous permettre de vous prémunir contre la majorité des attaques informatiques, ou à défaut d'en limiter les impacts.

PUBLIC CONCERNÉ ET PRÉREQUIS

Formation à destination des chirurgiens-dentistes :

- Chirurgie dentaire
- Chirurgie dentaire (specialiste Orthopédie Dento-Faciale)
- Chirurgie dentiste spécialisé en chirurgie orale
- Chirurgie dentiste spécialisé en médecine bucco dentaire

Formation à destination des médecins spécialistes en médecine générale et autres

- Allergologie
- Chirurgie maxillo-faciale
- Chirurgie orale
- Oncologie
- Médecine générale

Modalités pratiques

Plateforme de formation accessible 24/24
Pour une utilisation optimale de la plateforme, nous vous recommandons de vous y connecter depuis le navigateur Google Chrome ou Mozilla Firefox (à jour). Nous préconisons également une connexion internet adéquate au suivi d'une formation en ligne.

Inscriptions en ligne
www.webdental-formation.com ➡ S'inscrire

Contact
- Tél. : 01 84 80 34 80 (du lundi au dimanche)
- Mail : formation@webdental.fr
- Formulaire en ligne : www.webdental-formation.com/contact

Nous sommes à votre écoute, si vous êtes en situation de handicap, contactez notre référent handicap

01 76 31 10 80 referenthandicap@webdental.fr

Prise en charge

Formation éligible à la prise en charge par l'ANDPC sous réserve que le praticien :

- soit libéral et / ou salarié d'un centre de santé conventionné exerçant en France métropolitaine ou dans les DROM,
- dispose du nombre d'heures nécessaire dans son crédit DPC (18 heures par an, à consulter sur agencedpc.fr),
- soit inscrit à la formation auprès de Webdental Formation,
- soit inscrit à la formation auprès de l'ANDPC,
- suive l'intégralité du parcours de formation durant la session choisie

Modalités d'évaluation

Tout au long de la formation :
Les participants sont invités à répondre à des tests de connaissances. Les résultats sont communiqués immédiatement.

SUPPORTS PÉDAGOGIQUES

- Diaporama de formation sous format vidéo
- Articles bibliographiques à lire et télécharger
- Activités pédagogiques sous forme de quizz

Méthode et déroulé pédagogique

Questionnaire de connaissances AMONT

MODULE 1

Introduction à la sécurité numérique en santé

- Les enjeux de la sécurité numérique, déontologique et de la télésanté dans le secteur médical o la confidentialité des données médicales

1. La protection des informations personnelles de santé : définition d'un traitement de données personnelles
2. La conformité aux réglementations et lois en vigueur (Règlement général sur la protection des données – RGPD, régime spécifique de traitement des données à des fins de recherche)
3. Les enjeux liés à l'IA, aux algorithmes, aux biais et aux systèmes d'aide à la décision ainsi que les principes éthiques
4. Les référentiels de référence en cybersécurité
5. Les conséquences potentielles des violations de sécurité

- Les conséquences des incidents de sécurité informatique dans le contexte médical et notamment au cabinet, pour le praticien et pour le patient

6. Perte de données médicales sensibles o compromission de la confidentialité des patients
7. Perturbations du fonctionnement des services de soins de santé o
8. Conséquences légales et financières
9. Impacts sur la réputation du cabinet.

- L'importance d'adopter une mentalité « sécurité numérique » pour soi-même et les équipes pour concevoir et maintenir un environnement numérique de travail sécurisé quotidien au cabinet

MODULE 2

Base de l'hygiène numérique

- Gestes et mesures de protection de base pour assurer la sécurité de son environnement numérique de travail.

1. Verrouillage des écrans o déconnexion des sessions non utilisées
2. Protection des dispositifs avec des mots de passe forts
3. Mise en place de pare-feu et d'antivirus
4. Règles concernant les durées de conservation et d'hébergement
5. Attitude à tenir en déplacement
6. E-réputation o utiliser une messagerie sécurisée
7. Avoir un registre des traitements

- Sensibilisation à la protection des données sensibles, notamment les données de santé.

8. Réglementation et lois en vigueur relatives à la protection des données de santé
9. LiL
10. 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)
11. Informer les personnes concernées par le traitement
12. RGPD
13. Bonnes pratiques de protections, de stockages, de partage des données

- Bonnes pratiques pour la gestion des mots de passe, les mises à jour, les sauvegardes et la navigation sécurisée sur Internet et les outils d'accès aux données de l'usager

14. Conseils pratiques sur la gestion des mots de passe forts, o la mise à jour régulière des logiciels et des systèmes d'exploitation,
15. Sauvegarde régulière des données o navigation sécurisée sur Internet pour éviter les menaces
16. Utilisation d'outils de gestion de mots de passe o bonnes pratiques pour la navigation sécurisée (évitation de sites web douteux et vérification des certificats de sécurité des sites web.)
17. Bonnes pratiques pour les outils d'accès aux données de l'usager (Identifiant National de Santé (INS), Carte de Professionnel de Santé numérique (CPS), identifiant e-CPS, Carte de Professionnel en Formation (CPF), Pro santé Connect] + IoT

MODULE 3

Prévention et réaction face aux incidents de sécurité informatique

- Les différentes menaces et les types d'incidents de sécurité informatique pouvant survenir au cabinet
  1. Attaques de logiciels malveillants
  2. Attaques par hameçonnage
  3. Violations de données
  4. Ransomwares
  5. Attaques DDoS, etc.
- Les mesures de prévention pour se prémunir contre les incidents de sécurité informatique o la charte informatique
  6. Les contrats avec les tiers
  7. Les points d'attention lors de recours à des fournisseurs
  8. Mise en place de politiques de sécurité
  9. Gestion des autorisations d'accès
  10. Sécurisation des réseaux
  11. Sécurisation des dispositifs et des applications o formation du personnel
  12. Mise en place de sauvegardes régulières des données.
- L'importance de la vigilance et de la proactivité dans la protection contre les incidents de sécurité informatique.
- Procédures de réaction en cas d'incident, y compris la détection, la notification, la gestion des incidents de sécurité et la notification à la Cnil et aux personnes concernées
  13. Les signes d'alerte d'un incident de sécurité o
  14. Etapes pour signaler un incident à la personne appropriée
  15. Gestion de la communication interne et externe en cas d'incident
  16. Tenir un registre des violations de données
  17. Mise en œuvre des mesures correctives appropriées pour minimiser les dommages potentiels

MODULE 4

Etude de cas de cybersécurité / Mises en situation

- Attaque par hameçonnage (phishing) :

Scénario : Les employés du cabinet pourraient être confrontés à des e-mails suspects ou à des messages de texte qui tentent de les inciter à divulguer des informations confidentielles, telles que des identifiants de connexion ou des données de patients.
Attendus : L'apprenant est encouragé(e) à reconnaître les signes d'un hameçonnage et à réagir de manière appropriée, en signalant les e-mails suspects et en ne divulguant pas d'informations sensibles.

- Attaque par ransomware :

Scénario : Le système informatique du cabinet est infecté par un ransomware, bloquant ainsi l'accès aux données vitales du cabinet.
Attendus : Identifier les étapes à suivre pour répondre à cette situation, notamment en signalant l'incident à l'équipe de sécurité, en isolant les systèmes infectés et en prenant des mesures pour éviter la propagation du ransomware.

- Attaque physique :

Scénario : Un individu non autorisé tente de pénétrer physiquement dans les locaux du cabinet pour accéder aux informations sensibles ou voler du matériel informatique.
Attendus : Appliquer les procédures de sécurité appropriées, telles que l'identification des visiteurs, la communication avec les autorités compétentes…

- Gestion des mots de passe :

Scénario et attendus : L'apprenant pourrait être évalué sur sa capacité à créer et à gérer des mots de passe forts pour les comptes informatiques du cabinet, ainsi que sur sa connaissance des meilleures pratiques en matière de sécurité des mots de passe, telles que la mise en œuvre de l'authentification à deux facteurs et la modification régulière des mots de passe

- Sensibilisation à la sécurité :

Scénario : L'apprenant pourrait être soumis à des exercices de sensibilisation à la sécurité, tels que l'identification de comportements risqués, tels que l'utilisation de dispositifs USB non autorisés, l'accès à des sites web douteux ou la divulgation d'informations confidentielles par téléphone.
Attendus : Il devra alors prendre des mesures appropriées pour éviter ces risques et protéger les données du cabinet.

Questionnaire de connaissances AVAL

Questionnaire de satisfaction de fin de formation

Modalités de validation

La formation est validée lorsque le participant l'a suivie dans sa totalité durant sa session.

Les certificats de fin de formation seront automatiquement envoyés puis stockés dans l'espace personnel Webdental Formation des participants ayant terminé leur formation.