Cybersécurité dans le secteur dentaire

RGPD

RGPD

- Le RGPD (Règlement général sur la protection des données) est une réglementation de l'Union européenne qui est entrée en vigueur en mai 2018 et qui vise à protéger la vie privée des citoyens européens en réglementant la collecte, le traitement et la conservation des données personnelles. Une donnée personnelle est selon la CNIL toute information se rapportant à une personne physique identifiée ou identifiable.

La protection et l'hébergement des données personnelles de santé.

- Les établissements et les professionnels de santé sont des cibles particulièrement visées par les cyberattaques, comme l'illustre l'augmentation des attaques par rançongiciel qui les affectent actuellement avec comme conséquences la perturbation du fonctionnement des services médicaux.
  l'application du RGPD favorisent la protection des données.
  En France, les acteurs de santé ont l'obligation de faire stocker les données de santé chez un prestataire agréé HDS (Hébergeur de Données de Santé) pour garantir la
  traçabilité, l'intégrité, la confidentialité et la disponibilité, des données des patients.

Le processus de certification HDS en 6 étapes

Etape 1 : Choisir un organisme certificateur (Celui-ci doit être accrédité par le COFRAC ou une instance équivalente au niveau européen)

Etape 2 : Audit documentaire(L'organisme certificateur vérifie que votre système d'information répond aux exigences du référentiel de certification)

Etape 3 : Audit sur site(Les preuves d'audit sont évaluées, dans les conditions définies par le référentiel de certification)

Etape 4 : Corriger les non-conformités(Vous disposez de 3 mois après l'audit sur site pour apporter des corrections et les faire auditer)

Etape 5 : Recevoir son certificat(Le certificat est délivré par l'organisme certificateur pour une durée de 3 ans)

Etape 6 : Audit de surveillance(Un audit de surveillance est effectué chaque année chez tous les hébergeurs certifiés)

Evolution

Sécurité des données

- **Cryptage avancé** : Utilisation de techniques de cryptage plus robustes pour protéger les données sensibles des patients. Par exemple, le **chiffrement homomorphe** permet de traiter les données chiffrées sans les déchiffrer, réduisant ainsi les risques de fuite de données.
- **Authentification multifacteur** (MFA) : Implémentation de l'authentification multifacteur pour renforcer la sécurité des accès aux RGP et aux serveurs HDS.
- **Interopérabilité**
- Adoption de standards internationaux tels que **HL7 FHIR (Fast Healthcare Interoperability Resources**) pour faciliter l'échange et l'intégration des données entre différents systèmes de santé.
- **Intelligence artificielle et analyse de données**
- Machine Learning : Utilisation de l'apprentissage automatique pour analyser les données des patients, permettant des prédictions plus précises et une personnalisation des traitements.

Evolution

1. Renforcement des amendes : Les autorités de protection des données peuvent augmenter les amendes pour les violations du RGPD afin de dissuader les entreprises de ne pas respecter la réglementation.
2. Expansion du champ d'application : Le RGPD peut être étendu pour inclure des domaines tels que la reconnaissance faciale, l'analyse de données en temps réel et les technologies émergentes qui peuvent potentiellement compromettre la vie privée.
3. Amélioration de la coopération internationale : Les autorités de protection des données peuvent renforcer leur coopération pour garantir une application cohérente du RGPD dans l'ensemble de l'Union européenne et dans les pays tiers.
4. Accent sur les données des enfants : Le RGPD peut être modifié pour renforcer la protection des données des enfants, en particulier en ce qui concerne les activités en ligne et les applications destinées aux enfants.
5. Utilisation accrue de l'IA : Les autorités de protection des données peuvent commencer à utiliser des outils d'intelligence artificielle pour aider à identifier les violations potentielles du RGPD.