MAME 2024 - CyberCriminalité et données de santé

Objectif de notre rencontre

Aujourd'hui, nous allons explorer:

1. l'importance cruciale de protéger les données médicales numériques,
2. comprendre les risques associés,
3. et découvrir des pratiques essentielles pour garantir leur sécurité.

Préambule

Quelle est la première faille de sécurité ?

Quelle est la première faille de sécurité ?

L’humain est la première faille de sécurité:

- Social Engineering
- Erreurs
- ….

Le Social Engineering

“On dit d’une personne qu’elle a recours à la manipulation lorsqu’elle utilise l’influence et la persuasion pour duper les gens en se faisant passer pour quelqu’un qu’elle n’est pas. In fine, le manipulateur sait exploiter autrui afin d’obtenir des renseignements, en s’aidant ou non de moyens technologiques.”

Kevin Mitnick - L’art de la supercherie

Le Facteur Humain

Le maillon le plus faible de la sécurité c’est le facteur humain

En témoignant devant le Congrès Américain, K. Mitnick a expliqué qu’il aurait souvent pu obtenir des mots de passe et d’autres informations sensibles d'entreprises en prétendant être quelqu’un d’autre et **en les demandant tout simplement**.

Rien n’est jamais sécurisé

Adaptez votre niveau de sécurité à ce que vous avez à protéger


Données de santé

Qu'est-ce qu'une donnée de santé?

Qu'est-ce qu'une donnée de santé ?

Article 4 du RGPD « *données relatives à la* ***santé physique ou mentale****, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne* »

Par nature | **Par combinaison** | **Par destination**

3 catégories de données de santé

CNIL. Véronique CABANES et Manon de FALLOIS

https://esante.gouv.fr/sites/default/files/media_entity/documents/la-protection-des-donnees-de-sante.pdf

Qu'est-ce qu'une donnée de santé?

Exemples de traitements de données de santé

- Base de données PMSI de l'établissement de santé
- Tenue d'un dossier patient (papier et informatisé)
- Utilisation d'un dispositif de téléexpertise
- PACS d'imagerie médicale
- Collecte d'échantillons pour réaliser des recherches
- Etc.

CNIL.

Véronique CABANES et Manon de FALLOIS

https://esante.gouv.fr/sites/default/files/media_entity/documents/la-protection-des-donnees-de-sante.pdf

Spécificités des données de santé

1. Sensibilité et Confidentialité

- **Description** : Les données médicales numériques contiennent des informations très personnelles et sensibles, telles que les antécédents médicaux, les résultats de tests, et les traitements de patients.

- **Implication** : La divulgation non autorisée de ces informations peut avoir des conséquences graves, y compris des atteintes à la vie privée, des discriminations et des risques pour la sécurité des patients.

Spécificités des données de santé

2. Exigences Réglementaires Strictes

- **Description** : Les données médicales numériques sont régies par des réglementations strictes, telles que le Règlement Général sur la Protection des Données (RGPD) dans l'Union européenne, la Health Insurance Portability and Accountability Act (HIPAA) aux États-Unis, et d'autres cadres légaux spécifiques à chaque pays.

- **Implication** : Les institutions de santé et les professionnels médicaux doivent respecter des exigences strictes en matière de protection des données, de consentement des patients, et de rapports en cas de violation de données.

Spécificités des données de santé

3. Nécessité de l'Intégrité et de l'Exactitude

- **Description** : L'exactitude des données médicales numériques est cruciale pour le diagnostic, le traitement et le suivi des patients.
- **Implication** : Toute erreur ou manipulation des données peut entraîner des conséquences médicales sérieuses, rendant essentielles l'intégrité et la fiabilité des systèmes de gestion des données médicales.

Spécificités des données de santé

4. Interopérabilité

- **Description** : Les données médicales numériques proviennent souvent de sources diverses (hôpitaux, cliniques, laboratoires) et doivent être compatibles entre différents systèmes et technologies.

- **Implication** : Il est crucial de maintenir des normes élevées d'interopérabilité pour assurer une communication efficace et sécurisée des données entre diverses entités de santé.

Spécificités des données de santé

5. Conservation à Long Terme

- **Description** : Les données médicales numériques doivent souvent être conservées pendant de longues périodes, conformément aux exigences légales et pour le suivi à long terme des patients.

- **Implication** : Les systèmes de stockage doivent être sécurisés, fiables et capables de conserver les données sans perte ou corruption sur de longues périodes.

Spécificités des données de santé

6. Accès Autorisé et Traçabilité

- **Description** : L'accès aux données médicales numériques doit être strictement contrôlé et surveillé.
- **Implication** : Il est essentiel de mettre en place des systèmes de contrôle d'accès robustes et des mécanismes de traçabilité pour enregistrer qui accède aux données, quand et pourquoi, afin de prévenir les accès non autorisés et de détecter les anomalies.

Spécificités des données de santé

7. Risques Élevés de Cyberattaques

- **Description** : En raison de leur valeur, les données médicales numériques sont souvent la cible de cyberattaques, y compris le vol de données, les ransomwares et les attaques de phishing.

- **Implication** : Les organisations de santé doivent investir dans des solutions de cybersécurité avancées et des programmes de formation continue pour protéger les données contre les menaces numériques.


Les risques

Risques (non-exhaustif)

1. Violations de Données et Fuites d'Informations

- **Description** : Des attaquants peuvent accéder illégalement à des données médicales sensibles, souvent pour les vendre ou les utiliser de manière malveillante.

- **Conséquences** : Perte de confidentialité pour les patients, risques de chantage, atteinte à la réputation des établissements de santé, et potentielles sanctions légales et financières pour non-conformité avec les réglementations de protection des données.

Risques (non-exhaustif)

2. Attaques de Ransomware

- **Description** : Des logiciels malveillants chiffrant les données de l'utilisateur et exigeant une rançon pour leur déchiffrement.

- **Conséquences** : Perte d'accès aux données médicales critiques, perturbation des services de santé, coûts financiers pour le paiement de la rançon (non recommandé) ou pour la restauration des systèmes, et dommages à la réputation.

Risques (non-exhaustif)

3. Phishing et Ingénierie Sociale

- **Description** : Techniques utilisées pour tromper les individus afin qu'ils divulguent des informations sensibles ou qu'ils effectuent des actions qui compromettent la sécurité des données.

- **Conséquences** : Accès non autorisé aux systèmes d'information de santé, vol d'identité, et propagation d'autres malwares.

Risques (non-exhaustif)

4. Perte ou Vol d'Appareils

- **Description** : Perte ou vol d'appareils contenant des données médicales, tels que des ordinateurs portables, des smartphones, ou des supports de stockage externes.

- **Conséquences** : Accès non autorisé aux données médicales, risques de violation de la confidentialité des patients, et risques de non-conformité réglementaire.

Risques (non-exhaustif)

5. Erreurs Humaines

- **Description** : Erreurs commises par le personnel, comme l'envoi d'informations sensibles à la mauvaise personne, le mauvais configuration des permissions, ou l'échec de la mise à jour des logiciels.

- **Conséquences** : Exposition accidentelle de données sensibles, vulnérabilités de sécurité non corrigées, et potentielles violations de données.

Risques (non-exhaustif)

6. Manque de Formation et de Sensibilisation

- **Description** : Personnel non formé ou insuffisamment informé sur les meilleures pratiques de sécurité et les politiques de protection des données.

- **Conséquences** : Prise de décisions inappropriées en matière de sécurité, risque accru de violations de données, et non-conformité avec les réglementations de protection des données

Risques (non-exhaustif)

7. Insuffisance des Mesures de Sécurité

- **Description** : Systèmes de sécurité défaillants ou obsolètes, absence de cryptage des données, ou manque de sauvegardes régulières.
- **Conséquences** : Vulnérabilités exploitées par des attaquants, perte de données en cas de panne de système, et incapacité à restaurer les systèmes après une attaque.

Risques (non-exhaustif)

8. Non-conformité avec les Réglementations

- **Description** : Non-respect des réglementations nationales et internationales en matière de protection des données, telles que le RGPD, la HIPAA, ou d'autres cadres législatifs.

- **Conséquences** : Sanctions financières importantes, actions en justice, perte de confiance des patients et des partenaires, et atteinte à la réputation.


Cas d’exemples

Violation de Données chez Dedalus Biologie

- Description : Fuite massive de données impliquant des informations médicales sensibles de près de 500 000 personnes.
- Conséquences : Sanction de 1,5 million d’euros infligée par la CNIL pour manquements à la sécurité des données personnelles.
- Catégories : Violations de Données et Fuites d'Informations, Insuffisance des Mesures de Sécurité.

https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie

Fuite de Données de Santé de l’AP-HP

- Description : Fuite de données de l'AP-HP concernant 1,4 million de personnes testées pour la COVID-19.
- Conséquences : Risques potentiels de phishing et d'usurpation d'identité à la suite de cette fuite de données.
- Catégories : Violations de Données et Fuites d'Informations, Phishing et Ingénierie Sociale.

https://www.cnil.fr/fr/fuite-de-donnees-de-sante-ap-hp-que-pouvez-vous-faire-si-vous-etes-concerne


Comment mieux s’en prémunir?

Phishing (Hameçonnage)

Comment Reconnaître le Phishing :

- **Adresses Email Suspectes** : Vérifiez l'adresse de l'expéditeur. Les emails de phishing proviennent souvent d'adresses qui semblent légitimes mais présentent de petites erreurs ou des modifications subtiles.
- **Demandes Inhabituelles** : Soyez méfiant si l'email vous demande d'effectuer des actions urgentes, comme fournir des informations sensibles ou cliquer sur des liens pour "vérifier" vos informations.
- **Fautes de Grammaire et d'Orthographe** : Les emails de phishing contiennent souvent des erreurs grammaticales ou des fautes de frappe.
- **Liens et Pièces Jointes Suspects** : Évitez de cliquer sur des liens ou de télécharger des pièces jointes provenant d'emails non sollicités ou suspects. Survolez les liens avec votre curseur pour vérifier l'URL avant de cliquer.
- **Mise en Page et Design** : Les emails de phishing peuvent avoir une mise en page inhabituelle, des images de qualité médiocre, ou un design qui ne correspond pas à celui des communications officielles de l'organisation qu'ils prétendent représenter.

Attention: ce n’est pas parceque un email est envoyé qu’il est envoyé par la personne!

Phishing (Hameçonnage)

Comment Se Protéger du Phishing :

- **Vérifier l'Authenticité** : Si vous avez des doutes sur la légitimité d'un email, contactez directement l'organisation en utilisant des informations de contact officielles, et non celles fournies dans l'email suspect.
- **Utiliser des Solutions de Sécurité** : Installez des logiciels antivirus et des filtres anti-spam pour aider à détecter et à bloquer les emails de phishing.
- **Formation et Sensibilisation** : Éduquez-vous et formez votre personnel sur les signes de phishing et les meilleures pratiques pour l'éviter.
- **Mises à Jour Régulières** : Gardez votre système d'exploitation, vos logiciels et vos applications à jour pour vous protéger contre les dernières menaces de sécurité.
- **Utiliser la Vérification en Deux Étapes** : Activez la vérification en deux étapes pour vos comptes en ligne pour ajouter une couche de sécurité supplémentaire.
- **Sauvegardes Régulières** : Effectuez régulièrement des sauvegardes de vos données importantes pour minimiser les dommages en cas de réussite d'une attaque de phishing.

Restez vigilant!

Ransomwares

Les ransomwares sont un type de malware qui chiffre les fichiers de la victime, exigeant un paiement (généralement en cryptomonnaie) pour leur déchiffrement.

1. Mises à jour régulières :

- Systèmes et logiciels : Assurez-vous que tous vos systèmes d'exploitation et logiciels sont à jour avec les derniers correctifs de sécurité.
- Antivirus et anti-malware : Utilisez des solutions de sécurité fiables et assurez-vous qu'elles sont constamment mises à jour.

2. Formation et Sensibilisation :

- Programmes de formation continue : Éduquez-vous et sensibilisez votre personnel aux dernières tactiques utilisées par les acteurs malveillants, notamment les techniques de phishing qui sont souvent l'entrée principale des ransomwares.
- Exercices de simulation : Organisez des simulations d'attaque pour tester la réactivité de votre équipe.

3. Sauvegardes régulières :

- Sauvegarde des données importantes : Effectuez régulièrement des sauvegardes de vos données et systèmes. Stockez ces sauvegardes sur des supports externes ou dans le cloud, isolés de votre réseau principal.
- Tests de restauration : Vérifiez régulièrement que vos sauvegardes peuvent être restaurées.

4. Principe de moindre privilège :

- Restriction des accès : Limitez les droits d'accès aux fichiers, serveurs et autres ressources numériques selon les besoins spécifiques des utilisateurs.
- Contrôles d'accès : Utilisez des méthodes d'authentification forte et des mots de passe robustes.

Ransomwares

Les ransomwares sont un type de malware qui chiffre les fichiers de la victime, exigeant un paiement (généralement en cryptomonnaie) pour leur déchiffrement.

5. Sécurité du courrier électronique :

- Filtrage des emails : Utilisez des solutions de filtrage des emails pour bloquer les pièces jointes et les liens suspects.
- Sécurisation des passerelles email : Assurez-vous que vos passerelles email sont sécurisées et capables de détecter des emails de phishing et des pièces jointes malveillantes.

6. Isolation et segmentation du réseau :

- Segmentation du réseau : Divisez votre réseau en segments pour limiter la propagation des ransomwares en cas d'infection.
- Isolation des systèmes sensibles : Isolez les systèmes et les données sensibles des autres parties de votre réseau.

7. Surveillance et détection :

- Surveillance du réseau : Mettez en place une surveillance constante de votre réseau pour détecter et répondre rapidement à toute activité suspecte.
- Systèmes de détection d'intrusion : Utilisez des systèmes de détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS) pour surveiller et bloquer les activités malveillantes.

8. Planification et réponse aux incidents :

- Plans de réponse aux incidents : Établissez et pratiquez un plan de réponse aux incidents de cybersécurité pour réagir efficacement en cas d'attaque par ransomware.
- Communication et collaboration : Collaborez avec d'autres organisations et autorités pour partager des informations sur les menaces et les meilleures pratiques de réponse.

Que faire en cas de Ransomware ?

Important: **Rappelez-vous, payer la rançon ne garantit pas que vous récupérerez vos données et peut vous exposer à des risques supplémentaires. Il est généralement recommandé de travailler avec des professionnels de la cybersécurité et les autorités compétentes pour gérer l'incident.**

Que faire en cas de Ransomware ?

Immédiatement:

1. Isoler le Système

- ❏ Déconnectez immédiatement les appareils infectés du réseau pour empêcher la propagation du ransomware.
- ❏ Éteignez les appareils affectés mais ne les redémarrez pas, car cela pourrait entraîner la perte de données potentiellement récupérables.

2. Communiquer

- ❏ Informez votre équipe de sécurité informatique et votre direction. La communication interne rapide est essentielle.
- ❏ Contactez les autorités compétentes (ex. la police, la gendarmerie et l'ANSSI).
- ❏ Informez les parties prenantes concernées (clients, partenaires, employés) si leurs données sont compromises ou si le service est perturbé.

3. Identifier et Analyser

- ❏ Identifiez le ransomware (si possible). Certains outils et ressources en ligne peuvent vous aider à déterminer de quel type de ransomware il s'agit.
- ❏ Analysez la situation : quelles données ont été chiffrées, quelles sont les demandes des attaquants, y a-t-il un message de rançon?

Que faire en cas de Ransomware ?

Ensuite:

4. Évaluer et Décider

- ❏ Évaluez les options de récupération :
  - ❏ Avez-vous des sauvegardes récentes et non affectées que vous pouvez utiliser pour restaurer vos fichiers?
  - ❏ Y a-t-il des outils de déchiffrement disponibles pour votre cas spécifique de ransomware?
- ❏ Décidez si vous envisagez de payer la rançon (généralement **déconseillé car cela ne garantit pas la récupération des données et peut encourager les criminels**).

5. Répondre et Récupérer

- ❏ Nettoyez et restaurez :
  - ❏ Utilisez des logiciels antivirus et antimalware pour nettoyer les appareils infectés.;
  - ❏ Restaurez les données à partir de sauvegardes si possible.
- ❏ Renforcez votre sécurité pour prévenir de futures attaques. Cela peut inclure la mise à jour de vos logiciels, la formation de vos employés aux risques de cybersécurité et la révision de vos politiques de sécurité.

6. Enquêter et Apprendre

- ❏ Conduisez une enquête pour comprendre comment la sécurité a été compromise et comment éviter de telles situations à l'avenir.
- ❏ Documentez l'incident et les mesures prises en réponse. Cela peut être précieux pour la prévention des incidents futurs et peut être nécessaire pour les rapports réglementaires.

Perte ou Vol d’Appareils

La perte ou le vol d'appareils peut exposer les données sensibles à des risques de sécurité significatifs.

1. Précautions Physiques :

- Verrouillage sécurisé : Utilisez des câbles de verrouillage et des armoires sécurisées pour les appareils lorsqu'ils ne sont pas utilisés, en particulier dans les lieux publics ou partagés.
- Surveillance : Veillez à ne jamais laisser les appareils sans surveillance, même pour une courte période.

2. Mesures Technologiques :

- Chiffrement des données : Assurez-vous que toutes les données sensibles stockées sur les appareils sont chiffrées. Ainsi, même si l'appareil est perdu ou volé, les données resteront inaccessibles sans la clé de chiffrement.
- Authentification forte : Utilisez des mots de passe robustes, le chiffrement et, si possible, la biométrie (reconnaissance d'empreintes digitales ou reconnaissance faciale) pour sécuriser l'accès à vos appareils.
- Contrôle à distance : Installez des logiciels qui permettent de localiser, de verrouiller ou d'effacer à distance les données de l'appareil en cas de perte ou de vol.
- Mises à jour régulières : Maintenez le système d'exploitation et les logiciels de l'appareil à jour pour protéger contre les vulnérabilités de sécurité.

3. Formation et Politiques Internes :

- Politiques de sécurité : Élaborez des politiques claires concernant la responsabilité et les bonnes pratiques en matière de manipulation des appareils.
- Formation du personnel : Formez les employés aux risques associés à la perte ou au vol d'appareils et aux procédures à suivre en cas d'incident.
- Gestion des incidents : Mettez en place un protocole clair pour la réponse en cas de perte ou de vol d'appareil, y compris la notification aux autorités compétentes et aux parties affectées.


Recommandations

Conseil National de l'Ordre des Médecins

- ❏ Limiter les informations collectées au nécessaire et utiliser les dossiers patients conformément aux finalités définies.
- ❏ Mettre en place des mesures de sécurité appropriées pour les dossiers patients.
- ❏ Utiliser des services de messagerie sécurisée pour les échanges avec d'autres professionnels de santé.
- ❏ Sécuriser l'accès aux appareils mobiles et ne pas stocker d'informations médicales sur ces dispositifs.
- ❏ Réaliser une analyse d'impact avant la réalisation d'études internes sur les données des patients

https://www.conseil-national.medecin.fr/medecin/devoirs-droits/proteger-donnees-sante

Commission Nationale de l'Informatique et des Libertés (CNIL)

- ❏ Protéger l’accès à l’ordinateur, au système d’exploitation et aux applications par des mots de passe.
- ❏ Utiliser des antivirus régulièrement mis à jour et installer un pare-feu logiciel.
- ❏ Effectuer régulièrement des sauvegardes sur des supports amovibles.
- ❏ Vérifier que le contrat d’assistance et de maintenance comporte une clause de confidentialité

(https://www.cnil.fr/fr/donnees-de-sante-un-imperatif-la-securite)

La CNIL :

- ❏ Publie des référentiels pour aider les professionnels de santé libéraux dans la gestion des traitements courants des cabinets médicaux et paramédicaux.
- ❏ Fournit un cadre de référence pour la mise en conformité des traitements de données personnelles utilisés pour la gestion de cabinets médicaux et paramédicaux

(https://www.cnil.fr/fr/la-cnil-publie-trois-referentiels-pour-le-secteur-de-la-sante)

Conseils généraux (pour tous)

- **Consulter la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)** : https://esante.gouv.fr/produits-services/pgssi-s https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
- **Pensez à vérifier que vos hébergeurs soient certifiés HDS (Hébergeurs de Données de Santé)**
- **Mises à jour régulières des systèmes** : Garantissez que tous les systèmes et logiciels sont régulièrement mis à jour pour se protéger contre les vulnérabilités connues.
- **Sauvegardes régulières** : Effectuez des sauvegardes régulières des données importantes et stockez-les de manière sécurisée.
- **Évaluation des risques et audits de sécurité** : Réalisez des évaluations régulières des risques et des audits de sécurité pour identifier et atténuer les vulnérabilités potentielles.
- **Formation continue** : Restez informé des dernières menaces et tendances en matière de cybersécurité. La sensibilisation est la première étape pour se protéger contre les menaces numériques.

Pour les Magistrats

- **Compréhension des lois sur la protection des données** : Restez informé des dernières réglementations en matière de protection des données, telles que le RGPD en Europe, la loi HIPAA aux États-Unis et les lois locales pertinentes.

- **Évaluation des preuves numériques** : Développez une compréhension de la manière dont les données médicales numériques peuvent être manipulées ou compromises, et comment cela peut affecter les affaires judiciaires.

- **Sensibilisation à la cybersécurité** : Soyez conscient des risques de cybersécurité lors de l'examen des preuves numériques et de la communication avec les parties impliquées dans un cas.

Pour les Avocats

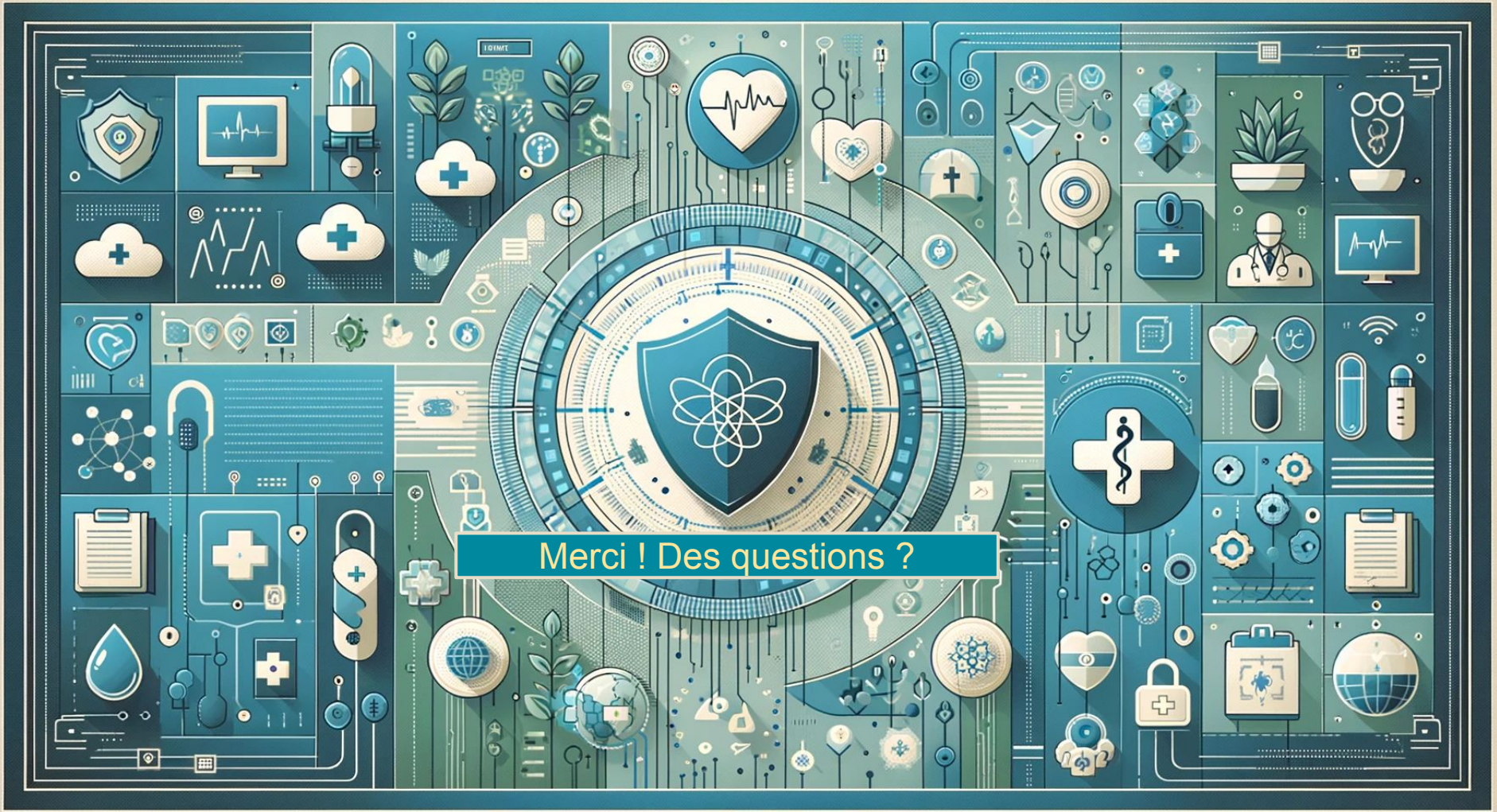
- **Confidentialité et intégrité des données** : Assurez la confidentialité des données médicales numériques de vos clients. Utilisez des méthodes de communication sécurisées et chiffrées pour échanger des informations sensibles.

- **Formation continue** : Restez informé sur les dernières menaces en matière de cybersécurité, les méthodes de phishing et les meilleures pratiques pour protéger les données sensibles.

- **Contrats et conformité** : Assurez-vous que les accords avec les fournisseurs de services tiers (comme les services de stockage en nuage) comprennent des clauses solides sur la protection des données et la conformité avec les réglementations pertinentes.

Pour les Médecins

- **Accès sécurisé aux données** : Utilisez des méthodes d'authentification fortes pour accéder aux dossiers médicaux numériques. Ne partagez jamais vos identifiants et changez régulièrement vos mots de passe.
- **Prudence avec les échanges numériques** : Soyez prudent lors de l'envoi d'informations médicales par voie numérique. Utilisez des services de messagerie sécurisés spécialement conçus pour le secteur de la santé.
- **Formation et sensibilisation du personnel** : Assurez-vous que tous les membres de votre équipe sont formés sur les meilleures pratiques en matière de cybersécurité et comprennent l'importance de la protection des données des patients.
- **Plans de réponse aux incidents** : Ayez un plan clair en place pour répondre aux violations de données, comprenant la notification des parties concernées et des autorités de régulation, le cas échéant.


Merci ! Des questions ?