Webinaire cybersécurité & RGPD à destination des libéraux – 6 février 2023

Questions – réponses

1. **Comment envoyer une ordonnance de manière sécurisée à un patient? (hors téléconsultation Doctolib ?)**

Il est possible d'envoyer l'ordonnance à votre patient depuis votre adresse de messagerie sécurisée MSSanté, vers la messagerie sécurisée du patient intégrée à son Espace Santé.
Les adresses des patients sont toutes construites autour de leur INS (Identité Nationale de Santé) : **INS**@patient.mssante.fr

2. **Mémoriser le mot de passe sur l'ordinateur est-il dangereux ?**

Oui, il est préconisé de ne pas enregistrer son mot de passe sur le navigateur.

3. **Utiliser MSSanté, bien sûr mais pouvez-vous nous indiquer quand les autres messageries (Apicrypt et autres), seront enfin interconnectées ? Car on ne peut envoyer qu'entre MSSanté…**

L'ensemble des opérateurs fournissant une adresse de MSSanté sont intégrés dans l'espace de confiance MSSanté et permettent d'échanger avec les autres adresses MSSanté, qui sont également intégrés à cet espace.
A titre d'exemple, la V2 d'Apicrypt est bien intégrée à l'espace de confiance et permet d'échanger avec les autres opérateurs MSSanté (ex : Mailiz, offre de MSSanté fournie par votre éditeur de logiciel de gestion de cabinet...). Dans certains cas, il est nécessaire d'activer cette interopérabilité.

4. **Avez-vous déjà eu connaissance de cyber-attaque vers des pharmacies ?**

Récemment, un groupement de pharmacies a été victime d'une attaque, 150 000 patients ont été concernés par une fuite de données.

5. **Force est de constater que peu utilisent une messagerie sécurisée et aucune messagerie de ce type non plus pour communiquer avec des hospitaliers**

La plupart des établissements de santé sont désormais équipés en messagerie sécurisée et ils sont actuellement en train d'équiper leurs professionnels d'adresse personnelle ou d'adresse par service hospitalier.

6. **Est-ce correct d'utiliser un disque dur externe SSD ?**

Cela dépend de son usage : s'il reste connecté en permanence, en cas d'attaque, il sera chiffré

comme le reste.

7. **Est-ce que l'on pourra avoir le PDF ? Avez-vous la répartition du nombre de participants par profession ?**

Bonjour, oui le support et l'enregistrement seront partagés d'ici quelques jours et le lien sera fourni à tous les inscrits ainsi qu'à l'AIUF. Sur les participants, nous lancerons tout à l'heure un sondage pour connaitre les professions et départements des professionnels connectés.

8. **Que pensez-vous des gestionnaires de mots de passe?**

Un gestionnaire de mot de passe est une bonne pratique. Attention toutefois à le sauvegarder régulièrement sur un support distinct.

9. **Un EDR ? Où est-ce que cela se trouve ?**

Les EDR (EndPoint Detection and Response) sont des solutions qui permettent de détecter un comportement anormal sur un poste de travail. Contrairement aux antivirus qui s'appuient sur une base de signatures connues, l'EDR regarde le comportement d'un programme et le bloque en cas de suspicion. Quelques exemples : Harfanglab, SentinelOne, Cybereason, Cortex, ... Une démarche coordonnée pour les professionnels de santé pourrait être intéressante à étudier.

10. **Des patients utilisent des clés USB pour des radiographies. Quelle est votre préconisation pour se protéger contre les virus ?**

Disposer d'un poste déconnecté du réseau pour insérer la clé USB et la vérifier.

11. **Pour les gestionnaires hébergés sur les cloud type Dashlane ou LastPass, vous conseillez de faire des sauvegardes malgré tout? Ils ont l'avantage de pouvoir partager les ID et mots de passe en équipe.**

Sur les gestionnaires hébergés, il faut vérifier le contrat de service. Normalement, ils sont sauvegardés dans le cadre du service souscrit. Néanmoins, un export régulier peut être pertinent (aucun service web n'est sûr à 100%).

12. **Qu'est-ce-que le RGPD ?**

Le RGPD ou Règlement General Protection des Données est le règlement européen du 27/04/2016 applicable à la l'ensemble des états membres, qui a été décliné dans la loi n° 2018-493 du 20 juin 2018 relative à la protection des données, qui se substitue et renforce la loi informatique et libertés de 1978.

13. **Ne serait-il pas pertinent de faire apparaitre sur les ordonnanciers et feuilles de soins l'adresse de la messagerie sécurisée des praticiens ?**

Effectivement, c'est une bonne pratique que nous suggérons notamment aux établissements de santé mais qui auraient vocation à être appliquée également par les professionnels de santé de ville.

14. **Est-ce qu'il y a des cyberattaques chez les opticiens?**

Aucune profession n'est à l'abri, pas même les informaticiens.

15. **Pouvez-vous réexpliquer quand éteindre ou ne pas éteindre l'ordinateur?**

Si vous êtes victime d'une attaque, il est recommandé de ne pas éteindre le PC. Il faut toutefois le déconnecter du réseau.

16. **Préconisez-vous l'utilisation d'un navigateur web plus particulièrement? En déconseillez-vous certains?**

Non, nous ne préconisons pas l'utilisation d'un navigateur web en particulier. L'important est d'utiliser un navigateur maintenu et à jour.

17. **Quid de l'utilisation de messageries instantanées type WhatsApp Ou Doctolib Teams ?**

WhatsApp est une messagerie grand public. Elle n'est pas prévue pour échanger des données de santé. Pour Doctolib, il faut se référer aux CGU. Les données échangées sur ces solutions le sont aux risques de leurs utilisateurs.

18. **Pour les échanges par mail avec les patients que conseillez-vous ? Par ailleurs, de plus en plus de patients souhaitent transmettre leurs ordonnances via WhatsApp ou autre service de messagerie. Qu'en pensez-vous ?**

Les professionnels de santé équipés d'une messagerie sécurisée peuvent échanger avec leurs patients via la messagerie citoyenne (MSS-C) de Mon Espace Santé, à condition que l'usager ait bien activé son compte.
Si un patient vous contacte et souhaite vous envoyer son ordonnance, vous pouvez lui recommander de vous adresser son ordonnance via la messagerie citoyenne de Mon Espace Santé. L'initiation d'un échange avec l'usager doit être faite par le professionnel de santé, il convient que vous lui écriviez pour qu'il puisse vous répondre et joindre l'ordonnance. Celle-ci permet d'échanger des messages mais également des documents avec les professionnels de santé.
WhatsApp est une messagerie grand public, elle n'est pas prévue pour échanger des données de santé.

19. **Au décès d'un patient, que deviennent ses données de santé?**

L'accès aux informations concernant une personne décédée est encadré :

- Cet accès ne peut d'abord s'exercer que si la personne décédée ne s'y était pas opposée de son vivant. Cette opposition peut ne pas prendre la forme d'un document écrit de sa main et peut être constatée en la présence d'éléments concrets et précis (ex : refus exprimé auprès du médecin traitant) ;
- Seuls certains proches de la personne décédée peuvent accéder aux informations la concernant : les ayants droit (héritiers légaux ou testamentaires) dont le conjoint, le concubin ou concubine, le partenaire lié par un pacte civil de solidarité.
- La demande doit être expressément fondée sur un ou plusieurs des trois motifs prévus par l'article L. 1110-4 du code de la santé publique :
    - Connaître les causes de la mort ;
    - Défendre la mémoire du défunt ;
    - Faire valoir ses droits.

Concernant la durée de conservation, pour les dossiers constitués en établissement de santé : la durée de conservation est de 20 ans à compter de la date du dernier séjour ou de la dernière consultation externe du patient (article R. 1112-7 du code de la santé publique). Si la durée de conservation s'achève avant le 28e anniversaire du patient, la conservation du dossier doit être

prorogée jusqu'à cette date.
Si le patient décède moins de 10 ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de 10 ans à compter de la date du décès.
En l'absence de texte fixant le délai de conservation de ces dossiers, à titre d'exemple, le CNOM recommande aux médecins d'appliquer les délais de conservation prévus pour les établissements de santé.

20. En cas de cessation d'activité du médecin (retraite) que faire des données?

Si le médecin a trouvé un successeur, le contrat de cession prévoit la présentation de la patientèle au nouveau venu. Sauf opposition des patients, le médecin va lui transmettre les dossiers médicaux et tout document ou renseignement utile à leur prise en charge. Les notes personnelles et informations qui ne sont pas indispensables doivent être écartées.

Si le médecin n'a pas de successeur, il va devoir remettre en main propre à chaque patient une copie de son dossier médical contre récépissé, ou l'adresser à un médecin nommément désigné par le patient. Les dossiers médicaux et documents originaux doivent alors être conservés par le médecin, ou à défaut, par ses héritiers. Si, pour les établissements de santé, le délai de conservation du dossier médical est de 20 ans à compter du séjour ou de la consultation du patient, aucun texte ne fixe de durée de conservation des dossiers des patients pour les médecins libéraux. Dans ces conditions, l'Ordre des médecins préconise de s'aligner sur le délai minimal de 20 ans appliqué par les établissements de santé. Cependant, pour les patients atteints de pathologies génétiques, neurologiques, de maladies orphelines, etc., la durée de conservation est illimitée, dans la mesure où les descendants des patients peuvent avoir besoin d'accéder à certaines informations dans le cadre de leur propre prise en charge. Quel que soit le support des dossiers (papier ou informatique), ils doivent être conservés dans des conditions qui garantissent leur confidentialité et leur intégrité.

Pour les autres professions, les recommandations peuvent varier mais généraliser il est ^préconisé de conserver les données patients au minimum 20 ans pour s'aligner sur la responsabilité hospitalière. L'information des patients est également fortement recommandée.

21. Y a-t'il plus de risque via un serveur sur hébergeur externalisé agréé par ANS, si on s'équipe d'un EDR type Bitdefender que sur un serveur local ?

Chaque système d'information porte ses propres risques. Sur un serveur externalisé, il faut vérifier les clauses contractuelles et ne pas hésiter à en vérifier le respect : par exemple, le serveur doit être maintenu à jour, les sauvegardes régulières doivent être effectuées, testées, et stockées dans un Datacenter différent suffisamment éloigné, …
Sur un serveur local, il faut également veiller à la mise à jour régulière, veiller à la sécurité physique, faire des sauvegardes, …
L'analyse de risque est une bonne approche pour disposer d'une vue d'ensemble. Le fait d'utiliser un service externalisé n'est pas une garantie de sécurité.

22. Pourriez-vous nous redire les 2 façons d'hacker nos données?

Par phishing, via une clé USB infectée, un prestataire lui-même infecté…