CLUB visio

“Tous Cybervigilants”

La FAQ

Aura t’on les coordonnées des intervenants ?

GRADeS : Christel PINTO, Hubert FABRIS, Eric ANDRIAHAMISON :

- ssi@esante-centre.fr

Mais dans un dossier médical on stocke par définition des données de santé ?

Le traitement des données de santé dans les dossiers médicaux fait partie des exceptions du RGPD et de la Loi informatique et libertés dans le cadre de la prise en charge des patients.

Suppression des données... on a une obligation légale de conserver les dossiers médicaux (10 ans il me semble) au décès des patients…

La durée de conservation des dossiers médicaux est de 20 ans à l'issue de la dernière visite du patient ou effectivement de 10ans à la suite du décès.

- Voir le référentiel de la CNIL

Pour les mineurs le délai ne part pas de la majorité ?

Pour les mineurs : "Lorsque la durée de conservation du dossier s'achève avant le 28e anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date…"

Durée de conservation :

- 20 ans après la dernière consultation pour un dossier patient (40% des répondants ont donné la bonne réponse)
- 10 ans en cas de décès du patient (plus de 50% des répondants ont donné la bonne réponse)
- 2 ans pour les feuilles de soins, correspondant à la durée légale de prescription de l’assurance maladie (réponses partagées entre 1 et 2 ans)

Sanctions possibles

Le non-respect du RGPD peut entraîner différents niveaux de sanctions :

- Rappel à l'ordre : sanction légère nécessitant une mise en conformité
- Injonction de mise en conformité : plus sérieuse, avec obligation de se mettre en règle et contrôle ultérieur
- Limitation ou interdiction de traitement : impact majeur sur l'activité du professionnel
- Amendes : variables selon la gravité de l'infraction

Responsabilité des éditeurs ?

Les éditeurs qui hébergent des données de santé doivent être certifiés HDS (Hébergeur de données de santé). Il est également nécessaire de vérifier auprès de vos éditeurs la conservation des données et si les sauvegardes sont ou non cryptés.

Existe-t-il une liste de service externe de DPO fiable ?

Il n'y a pas de liste établie, certains prestataires en protection des données sont spécialisés sur le secteur de la santé, nous pouvons citer par exemple : DrData, RGPD Santé, Les DPO de la santé, Lexagone…

Données sur téléphone ? contacts des patients ?

Sécurisé par verrouillage du téléphone : code PIN ou biométrie (empreinte, reconnaissance faciale…).

Y a-t-il des alternatives sécurisées au Google Form ?

Il faut se doter de logiciel utilisant le protocole HTTPS et du chiffrement SSL/TLS pour sécuriser les données en transit.

Avez-vous connaissance de CPTS qui utilisent des logiciels sécurisés pour les données patients (SNP, accès au médecin traitant ? Si oui, quel logiciel est utilisé ?

Pour le transfert de données médicales, la solution BlueFiles est certifiée HDS.

Que pensez-vous du drive d'Infomaniak (version gratuite) ? Si on prend la version payante, est-ce mieux ou cela ne change rien ?

Infomaniak a bonne réputation. Néanmoins il faut vérifier la certification HDS (hébergement de données de santé) et vérifier leurs process opérationnels.
La Suite WIMI à comparer.

Valeur des données sur le Darknet :

Un sondage a révélé que les participants surestimaient généralement la valeur marchande des données d'identification directe mais sous-estimaient celle des données personnelles :

- Scan de carte vitale : 8 euros (la plupart des participants avaient estimé 100€)
- Numéro de carte bancaire : 25 euros (estimation majoritaire : 550€)

- Données personnelles sur les réseaux sociaux : 550 euros (estimation majoritaire : 25€)
- 90% des cyberattaques sont liées à une faille humaine (résultat confirmé par un sondage auprès des participants)

Ex : En 2024, identifiants de comptes bancaires en ligne : 55€ / Paypal : environ 22€ à 900€ selon les fonds / compte de messagerie : 140€ / comptes de réseaux sociaux : 9 à 45 € / scan ou photocopie d'une carte identité : environ 130€ / carte d'identité physique authentique : environ 3500€ / dossier médical complet : à partir de 350 € / cependant ces prix sont variables comme sur le Le Bon Coin

Quel est le niveau de sécurité des coffres forts pour mots de passe ?

Les coffres-forts pour mots de passe (ou gestionnaires de mots de passe) offrent généralement un niveau de sécurité élevé, mais cela dépend du service ou de l'outil utilisé. Il faut vérifier cela en amont auprès de l'éditeur. Pour exemple, nous utilisons KeePass (certifié par l'ANSSI) au GRADeS CVL.

- En savoir plus

Pouvez-vous indiquer aux hôpitaux de fonctionner avec la MSS pour les échanges avec des données de santé ?

Oui, c'est tout l'enjeu du Ségur Numérique. Les professionnels de santé émetteur/récepteur se doivent d'utiliser la messagerie sécurisée de santé - MSS.

Si on a un compte partagé par plusieurs personnes, alors seul le pass phrase est possible ?

Le partage de compte n'est pas conseillé, il vaut mieux que ce soit, nominatif avec un mot de passe robuste associé, par exemple "passphrase".

Un conseil pour une application de gestionnaire de mot de passe ?

KeePass est un bon outil en soi. En installation locale KeePass sinon Bitwarden, solution en ligne.

Je fais une sauvegarde sur disque dur crypté tous les soirs... Quelle est la fréquence de sauvegarde idéale ?

C'est largement acceptable en journalier. Tous les soirs, c'est très bien. Il est conseillé, de manière générale, de le faire une fois par semaine. Il faut également prendre en compte qu'en cas de panne de votre poste, vous pouvez perdre une semaine de travail.

Est-ce qu'un antivirus a une utilité ?

Oui ! c'est même vital... Les antivirus sont effectivement utiles, car ils permettent de détecter et de mettre en quarantaine de nombreuses menaces connues.