Cannes, le mardi 7 mai 2024

COURRIER CIRCULAIRE A L'ADRESSE DES PATIENTS PRIS EN CHARGE AU CENTRE HOSPITALIER DE CANNES SIMONE VEIL

Le centre hospitalier de Cannes Simone Veil a subi un acte de malveillance informatique volontaire susceptible de concerner des informations personnelles vous appartenant.

- **QUE S'EST-IL PASSE ?**

Dans la nuit du 15 au 16 avril 2024, le centre hospitalier de Cannes Simone Veil a fait l'objet d'une cyberattaque.

Le 30 avril, l'établissement a pris connaissance d'une revendication de la cyberattaque assortie d'une demande de rançon. Suite à cette revendication et au non-paiement de la rançon, une publication des données exfiltrées a eu lieu dans la nuit du 1er au 2 mai sur le "darkweb".

Cette cyberattaque est caractérisée comme une violation de données personnelles.

- **COMMENT AVONS-NOUS REAGI ?**

En réponse à cette attaque, dès le 16 avril, le centre hospitalier a isolé son réseau et supprimé ses connexions internet. L'établissement a déclenché son plan de gestion des situations sanitaires exceptionnelles en lien avec l'Agence Régionale de Santé et les partenaires publics et privés.

Grâce à la mobilisation de ses équipes médicales et soignantes, l'établissement s'est organisé pour assurer la continuité et la sécurité des prises en charge des patients pour les activités urgentes et programmées.

Depuis le début de l'attaque, les équipes informatiques de l'établissement travaillent avec les experts du groupement hospitalier de territoire, de l'ANSSI[1], du CERT Santé[2] et de différents prestataires spécialisés.

Dès le début de la cyberattaque, l'établissement a déposé plainte auprès de la gendarmerie et procédé aux signalements de violation de données à la CNIL[3]. **Il est rappelé que le fait d'extraire, détenir, reproduire, transmettre, supprimer ou modifier frauduleusement les données d'un traitement automatisé constitue un délit pénal**.

- **QUELLES SONT LES DONNEES CONCERNEES ?**

Les premiers résultats des investigations confirment la fuite de données à caractère personnel concernant des patients et personnels de l'établissement. Les investigations sont toujours en cours. Il n'est pas possible à ce jour d'identifier avec précision la nature exacte et le contenu détaillé des données qui ont fait l'objet de cette exfiltration illégale. Néanmoins, les premières constatations des experts informatiques ont identifié que cette violation pouvait porter sur des données de santé associées ou non à une identité (à titre indicatif : compte rendu médical, suivi médical d'une pathologie, résultats de bilans, résultats d'examen, ordonnances, courriers).

- **QUELLES SONT NOS RECOMMANDATIONS ?**

Il existe un risque que ces informations soient utilisées par des personnes malveillantes. **L'établissement vous invite à la plus grande vigilance** face aux risques d'escroquerie,

[1] Agence nationale de la sécurité des systèmes d'information
[2] Dispositif de traitement des signalements des incidents de sécurité des systèmes d'information des établissements de santé et des établissements et services médico-sociaux
[3] Commission nationale de l'informatique et des libertés

d'hameçonnage, d'usurpation d'identité ou d'extorsion qui pourraient survenir dans les prochaines semaines. A ce titre, nous vous invitons à :

- ✓ Redoubler de prudence quand vous recevez des SMS/mails y compris avec notion d'urgence ;
- ✓ Faire preuve de vigilance si vous recevez des mails ou SMS vous demandant de fournir des informations personnelles et/ou procéder à des paiements ;
- ✓ Ne jamais fournir d'informations confidentielles (bancaires, mots de passe, etc.) ;
- ✓ Contacter vos organismes (financiers, sécurité sociale, mutuelles, etc.) au moindre doute ;
- ✓ Vérifier l'adresse du site qui s'affiche derrière un lien dans un message reçu ;
- ✓ Vérifier l'adresse du site dans le navigateur lors de votre navigation sur internet ;
- ✓ Ne pas cliquer sur un lien douteux et ne pas télécharger les documents joints dans des messages douteux ;
- ✓ Ne pas communiquer d'information sensible par téléphone ou par messagerie : en cas de sollicitations douteuses recontactez l'organisme sur sa ligne officielle ou sur son site officiel ;
- ✓ Utiliser des mots de passe différents et complexes pour chaque site et application ;
- ✓ Activer la double authentification pour sécuriser vos accès lorsque cela est possible.

D'une manière générale et si besoin nous vous recommandons de consulter les ressources présentes sur le site de la CNIL (https://www.cnil.fr/fr/mon-quotidien/ma-securite-numerique) et sur le site https://www.cybermalveillance.gouv.fr/cybermenaces.

En cas de constatation d'une utilisation frauduleuse de vos données personnelles, il est recommandé de porter plainte sans délai et d'informer la direction de l'établissement selon les instructions indiquées ci-dessous. La gendarmerie est en charge de l'enquête suite au dépôt de plainte effectué par l'hôpital pour violation de certaines de ses données.

- **QUELLES SONT LES PROCHAINES ETAPES ?**

L'établissement continue de travailler sur le rétablissement informatique de l'ensemble de ses logiciels. L'établissement poursuivra sa communication régulière.

- **QUI CONTACTER SI VOUS AVEZ DES QUESTIONS ?**

Pour toute question relative à la violation des données de santé, vous pouvez nous contacter l'adresse e-mail suivante : dpo-cannes@ght-alpesmaritimes.fr

Toutes les questions seront instruites en lien avec le délégué à la protection des données (DPO) du Groupement Hospitalier de Territoire des Alpes Maritimes.

Des permanences seront mises en place dans les jours à venir en lien avec les représentants des usagers de l'établissement. Les informations seront indiquées sur le site internet de l'hôpital.

L'établissement condamne cette cyberattaque et est conscient des conséquences qui peuvent en résulter. Nous tenons à vous informer que nous mettons tout en œuvre pour faire face à cette situation inédite, vous informer et vous accompagner.

Yves SERVANT, Le directeur du centre hospitalier	Christophe GARD, Le président de la commission médicale d'établissement	Michel COULOMB Le président de la commission des usagers