Cannes, le 29 mai 2024

HÔPITAL DE CANNES
SIMONE VEIL

Objet : lettre de notification de potentielle violation de données à caractère personnel consécutive à la cyberattaque du centre hospitalier de Cannes Simone Veil

Vous faites partie du registre des patients du centre hospitalier de Cannes Simone Veil.

Le centre hospitalier a été victime d'une cyberattaque dans la nuit du 15 au 16 avril 2024 du type « rançongiciel ». Autrement dit, les cybercriminels ont volé et chiffré une partie des données de l'établissement.

Dès le début de l'attaque, le personnel de l'hôpital a su se mobiliser pour garantir la continuité et la sécurité des soins dans des conditions inédites avec le plus grand professionnalisme.

L'établissement s'est immédiatement mis en contact avec l'ensemble des autorités compétentes :

- Une plainte a été déposée et l'enquête confiée au Centre de lutte Contre les Criminalités Numériques (C3N), le service compétent de la gendarmerie nationale ;
- Une notification de violation de données à caractère personnel a été effectuée dès le 16 avril auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) conformément à l'article 33 du Règlement européen Général sur la Protection des Données (RGPD) ;
- Les experts informatiques de la CNIL, de l'agence Nationale de Sécurité du Système d'Information (ANSSI), de Cert Santé, de l'Agence Régionale de Santé et du Groupement Hospitalier de Territoire des Alpes Maritimes ont également été impliqués et continuent de l'être en vue de mettre en place les mesures pour limiter les conséquences de cette violation sur les données et la vie privée des patients concernés, stabiliser la situation et contribuer à sécuriser les installations.

Le 30 avril, les rançonneurs ont lancé un ultimatum de diffusion en masse des données volées. L'établissement n'ayant pas cédé aux rançonneurs, ces derniers ont divulgué le 2 mai certaines données qu'ils avaient exfiltrées. L'établissement a aussitôt informé par voie de communiqué de presse et sur les réseaux sociaux ces éléments liés à la revendication et à la diffusion de ces données par les rançonneurs. Un premier document circulaire récapitulatif a été diffusé le 7 mai dans la soirée sur les réseaux sociaux afin de prévenir les personnes susceptibles d'être concernées et sensibiliser sur les risques que pourrait engendrer une éventuelle divulgation de données.

Nous vous écrivons aujourd'hui pour vous informer de manière individuelle que la violation porte potentiellement sur des données vous concernant. Nous en sommes profondément désolés.

Les données en question sont susceptibles de porter sur des éléments relatifs à des informations d'identité (nom, prénom, date et lieu de naissance, sexe), au numéro de sécurité sociale, aux données de contact (adresse postale, téléphone, adresse électronique) lorsque renseignées lors de votre passage dans nos services ainsi que des informations relatives au parcours hospitalier (comptes rendus médicaux, résultats d'examen médicaux, nature de la pathologie, hospitalisation, ordonnance, participation à un essai clinique le cas échéant, etc.) en violation du secret médical et professionnel.

Centre hospitalier Cannes Simone Veil - 15 avenue des Broussailles CS 50008 - 06414 CANNES Cedex

Cannes, le 29 mai 2024

HÔPITAL DE CANNES
SIMONE VEIL

C'est dans ce contexte en lien avec l'Agence Nationale de Sécurité du Système d'information (ANSSI) et la Commission Nationale de l'Informatique et des Libertés (CNIL) que nous vous recommandons la plus grande vigilance notamment s'agissant de tentatives d'escroquerie qui pourraient survenir dans les prochains mois et notamment les tentatives d'hameçonnage[1].

Ainsi, nous vous recommandons :

- D'être particulièrement vigilants face aux emails, SMS et appels qui pourraient chercher à tirer profit de cette fuite de données en particulier :
  - Vérifiez que l'expéditeur est bien légitime et est bien en lien avec le sujet ;
  - Ne fournissez jamais d'informations confidentielles (bancaires, mots de passe, etc.) ;
  - Soyez vigilant si le ton du message est pressant, qu'il vous pousse à l'action d'autant plus si vous n'attendiez pas ce message ;
  - Si le message contient des pièces jointes, elles peuvent être piégées. Ne les ouvrez pas.
- De vérifier les comptes associés à votre numéro de sécurité sociale. Surveillez l'activité de vos comptes en ligne associés, changez les mots de passe de ces accès ;
- De changer vos mots de passe au moindre doute et de choisir des mots de passe suffisamment longs et complexes sur tous les services que vous utilisez en activant si possible une double authentification.

Si vous pensez être victime d'une usurpation d'identité à la suite de la divulgation vous concernant, vous pouvez:

- Vous rendre sur le site www.cybermalveillance.gouv.fr pour obtenir des conseils pour vous protéger contre cette usurpation ;
- Déposer plainte.

De manière générale, vous pouvez signaler aux autorités judiciaires tout élément suspicieux que vous estimeriez être en lien avec cette attaque. Pour en savoir plus nous vous invitons à consulter ces bonnes pratiques d'hygiène informatique : https://www.cybermalveillance.gouv.fr/bonnes-pratiques

Si vous souhaitez avoir de plus amples informations sur la violation, vous pouvez nous contacter soit par mail adressé au délégué en charge de la protection des données (dpo-cannes@ght-alpesmaritimes.fr) soit par le biais de votre encadrement usagers. Une page internet est mise en place : https://www.ch-cannes.fr/informations-cyberattaque. Cette page internet sera actualisée régulièrement avec toutes les informations utiles (recommandations pratiques, réponses aux questions, modalités de dépôt de plainte en cas d'usurpation d'identité ou d'escroquerie, etc.).

Nous collaborons étroitement avec les services chargés des enquêtes, avec le souhait qu'elles permettent d'appréhender le ou les auteurs de cette cyberattaque. Croyez que nous sommes conscients des conséquences, qui peuvent résulter de cette cyberattaque. Nous vous assurons que nous mettons tout en œuvre pour en limiter les effets.

Le directeur
Yves SERVANT

Le Président de la CME
Christophe GARD

[1] L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Centre hospitalier Cannes Simone Veil - 15 avenue des Broussailles CS 50008 - 06414 CANNES Cedex