Rennes, le 11 juillet 2023

CYBERATTAQUE

Information à l'attention des patients et des usagers du CHU de Rennes

Mesdames et Messieurs les patients et usagers du CHU de Rennes,

Le CHU de Rennes a subi une cyberattaque le 21 juin dernier. Comme indiqué par voie de presse le 22 juin, malgré la détection précoce de l'attaque et l'arrêt rapide de sa propagation, les investigations immédiatement mises en œuvre ont révélé un accès illégitime, par des personnes non autorisées, à des données à caractère personnel relatives aux patients et aux usagers du CHU de Rennes.

Nous ne sommes pas en mesure d'identifier avec précision la nature exacte et le contenu des données qui ont fait l'objet de cet accès illégitime.

Il ressort cependant des investigations complémentaires menées, que pourraient potentiellement être concernées des données de santé, associées ou non à une identité, sur un périmètre restreint des systèmes informatiques du CHU de Rennes.
Les données potentiellement accédées par l'attaquant, identifiées à ce jour, concernent le Centre de Soins Dentaires (CSD), les salles techniques de cardiologie et des laboratoires du CHU.

Ces données n'ont, à notre connaissance, fait l'objet d'aucune diffusion ni exploitation à l'heure actuelle, mais cette possibilité ne peut être totalement exclue. Une veille continue a été mise en place sur Internet, avec l'aide du Centre gouvernemental de veille, d'alerte et de réponse aux incidents de sécurité, afin d'en assurer la surveillance. En parallèle, des mesures de sécurité complémentaires sont en cours de déploiement afin de réduire davantage le risque de fuite de données similaires à l'avenir.

En outre, une notification a été effectuée auprès de la commission nationale de l'informatique et des libertés (CNIL) dès le 21 juin 2023 comme prévu par l'article 33 du règlement européen sur la protection des données (RGPD). Une plainte a également été déposée par le CHU de Rennes le 22 juin 2023. Une enquête est en cours, sous l'égide du Parquet de Paris, spécialisé dans le traitement judiciaire des cyberattaques.

Dans ce contexte, nous vous recommandons la plus grande vigilance dans les prochaines semaines. Si vous constatez une utilisation frauduleuse de vos données personnelles, il est recommandé de porter plainte rapidement. Nous vous invitons également à en informer le CHU via l'adresse cyberattaque@chu-rennes.fr, en prenant soin de décliner votre identité.

Nous joignons par ailleurs au présent courrier les recommandations nationales applicables.

Nous sommes conscients des conséquences qui peuvent résulter de cette attaque et nous mettons tout en œuvre pour en limiter les effets.

Soyez assurés de la totale mobilisation des équipes du CHU pour vous assurer de la qualité de votre prise en charge comme de l'accompagnement nécessaire dans le cadre de cette cyberattaque.

La Directrice Générale

Véronique ANATOLE-TOUZET

Annexe : Recommandations

Si vous pensez être victime d'une utilisation frauduleuse de vos données personnelles :

- Conservez ou faites conserver les preuves ;
- Vous pouvez porter plainte au plus vite au commissariat de police ou à la brigade de gendarmerie, ou encore par écrit au Procureur de la République du tribunal judiciaire dont vous dépendez.
  Le cas échéant, vous pouvez vous faire accompagner gratuitement par une association de France Victimes au 116 006 (appel et service gratuits)
- Si une demande de rançon vous est adressée, ne la payez pas.
- Pour plus d'information, vous pouvez vous rendre sur le site www.cybermalveillance.gouv.fr

Attention : certains sites web indiquent détenir les données et pouvoir vous dire si vous êtes ou non concerné(e). Il est fortement déconseillé de recourir à ces sites.

Dans un contexte où vos données personnelles ont pu être mises en ligne, les principaux risques sont :

- L'hameçonnage (phishing) ou l'usurpation d'identité

L'hameçonnage consiste à vous envoyer un courriel ou SMS frauduleux qui vous paraîtra plus réaliste du fait de l'utilisation des données récupérées grâce à la fuite de données (un soi-disant courriel de votre médecin ou de la sécurité sociale par exemple).

- N'ouvrez surtout pas les pièces jointes, n'y répondez pas, ne consultez pas les liens et supprimez le message immédiatement. Pour repérer une tentative d'hameçonnage dans votre messagerie, et pour vous prémunir contre l'usurpation d'identité en ligne, soyez vigilants :
- Vérifiez que le message/courriel vous est réellement destiné ;
- Faites attention aux expéditeurs inconnus ;
- Soyez attentif au niveau de langage du courriel ;
- Vérifiez les liens dans le courriel ;
- Méfiez-vous des demandes étranges et ne transmettez rien de confidentiel ;
- Portez une attention particulière sur l'adresse de messagerie source.

Si vous pensez être victime d'une usurpation d'identité , vous pouvez :

- Vous rendre sur le site **cybermalveillance.gouv.fr** pour obtenir des conseils ;
- Déposer **plainte** au plus vite ;
- Consulter les recommandations CNIL « Comment réagir face à une usurpation d'identité ? ».

D'une manière générale, soyez vigilant lorsque vous saisissez des données sur le web ou lorsque vous recevez des courriels vous demandant de fournir ou de mettre à jour des données vous concernant.

Vous pouvez également adopter quelques gestes simples :

Changez vos mots de passe des services web que vous utilisez :

- En privilégiant des mots de passe forts ;
- En priorisant les services les plus importants (courriel, impôts, banques, sites de commerce en ligne, etc.) ;
- **Évitez l'utilisation d'un même mot de passe pour différents services** ;
- **Utilisez** les authentifications multifacteurs quand elles vous sont proposées par des services de confiance, par exemple l'envoi d'un SMS à usage unique sur votre téléphone pour valider une connexion ;

Veillez en particulier à ne pas utiliser les mêmes mots de passe pour des usages professionnels et personnels.

Nous recommandons la consultation des pages suivantes :

- https://www.cnil.fr/comment-reagir-face-une-usurpation-didentite,
- https://www.cnil.fr/spam-phishing-arnaques-signaler-pour-agir
- https://cybermalveillance.gouv.fr