AFTER WORK BY URPS MLB

Je suis Médecin Libéral & je soigne (aussi) les données

Doctolib

Notre webinaire va commencer d'ici quelques minutes !

Au programme :

- Pourquoi protéger les données de santé? *M.DESGENS-PASANAU, magistrat détaché à l'Agence du Numérique en Santé spécialisé dans la protection des données*
- Le voyage de la donnée chez Doctolib – *M. Cédric Voisin, Responsable de la sécurité de l'informaiton chez Doctolib*
- Je suis médecin et je soigne (aussi) les données - *témoignages de médecins*

Animation :

- Dr Loïc KERDILES
- Dr Eric VAN MELKEBEKE

urps mlb Médecins Libéraux Bretagne

Quelques règles d'usage pour le bon déroulement du webinaire

- Vous pouvez poser vos questions par écrit dans le module Q/R

- Vous pouvez utiliser le module de discussion pour publier vos commentaires ou échanger entre vous, si vous le souhaitez.

Merci !

Pourquoi protéger les données de santé?

M.DESGENS-PASANAU,
Magistrat détaché à la direction générale de l'Agence du Numérique en Santé –
Directeur de programme et délégué à la protection des données

L’Agence du numérique en santé (ANS)

Quelles sont les missions principales de l’ANS ?

Objectif général de l’ANS

Accompagner la transformation numérique du système de santé aux côtés de tous les acteurs concernés dans l’écosystème

Un panel de missions

L’ANS est à la fois un régulateur, un opérateur et un facilitateur

Son action se résume en trois mots-clés

Interopérabilité, sécurité, éthique

Plus d’infos sur : https://esante.gouv.fr/

La protection des données de santé

- **2018** : adoption du RGPD et de la nouvelle loi « informatique et libertés » : quelles conséquences pour les professionnels de santé ?

- Un régime de **protection renforcée** pour les données de santé

- Le professionnel de santé est astreint à **plusieurs obligations** :
  - Obligations de fond (sécurité informatique mais pas seulement….)
  - Obligation de documenter sa conformité
  - Obligation de respecter les droits que les patients tiennent de la réglementation

- Le professionnel de santé engage sa **responsabilité**…
  - Pénale, financiere, réputationnelle, disciplinaire
  - Laquelle peut être partagée avec d'autres acteurs de son système d'information

- Au delà de la conformité juridique, un sujet **éthique** et déontologique

Les acteurs de la régulation de protection des données

- **La CNIL (et son au niveau européen le CEPD)** – quelques liens utiles pour approfondir
  - https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_cabinet.pdf
  - https://www.cnil.fr/fr/lespace-numerique-de-sante-ens-ou-mon-espace-sante-et-le-dossier-medical-partage-dmp-questions
  - https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins
  - https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie
- **L'autorité judiciaire**
- **L'ANS et la délégation du numérique en santé (DNS)** – quelques liens utiles pour approfondir
  - https://esante.gouv.fr/esante.gouv.fr/virage-numerique/ethique-et-numerique-en-sante/pourquoi-ethique-et-numerique
  - https://esante.gouv.fr/espace-presse/la-dns-place-lethique-au-coeur-de-sa-feuille-de-route-pour-que-le-citoyen-garde-le-controle-de-la-numerisation-de-son-parcours-de-soin

Le voyage de la donnée chez Doctolib

M.VOISIN,
Responsable de la sécurité de l'information chez Doctolib

Votre équipe locale !

Pierre Georgeault - France Manager

07 76 02 33 20

Kévin Léonec - Regional Manager

07 71 43 58 54

Doctolib

Cédric Voisin

Directeur de la sécurité de l'information

Doctolib

Le chiffrement des données

4 techniques pour 4 utilisations

Au repos

Se prémunir d'un vol matériel.
L'ensemble des données est chiffrée au repos afin de prévenir le risque le vol de matériel contenant des données sensibles qui permettrait un accès en clair

Côté Serveur

Se protéger d'un employé indélicat.
Le chiffrement côté serveur permet d'empêcher un employé ou prestataire de lire les données en clair même si ce dernier dispose d'accès sur les serveurs

En transit

Prévenir les écoutes.
Le chiffrement en transit permet de prévenir le risque qu'un attaquant positionné entre vous et Doctolib puisse intercepter le trafic (Man In The Middle).

Côté Client

Chiffrement de bout en bout.
Le chiffrement de bout en bout est la protection ultime permettant qu'aucune personne hormis l'émetteur et le destinataire d'une information puisse accéder aux données.

Doctolib

L’hébergement des données

Vos données sont en lieu sûr

- Vos données sont stockées en **France et en Allemagne** chez un **hébergeur certifié HDS** (Hébergeur de Données de Santé) conformément à la loi et aux référentiels établis par **l’ANS** (Agence du numérique en santé), en concertation avec la **CNIL** (Commission nationale de l’informatique et des libertés).
- Les centres de données disposent d’une **sécurité physique renforcée 24h/24 et 7j/7** et de mesures de protection technologique parmi les plus avancées au monde.
- **Depuis Novembre 2021,** Doctolib est **certifié ISO 27001** pour l’ensemble de ses activités et **certifié HDS** sur l’ensemble de son périmètre France.
- En 2022, nous visons la certification **ISO 27701** (norme internationale régissant la protection des données personnelles) ainsi que le BSI C5 pour nos opérations en allemagne

Une vigilance continue

Les méthodes de détection d’actes malveillants

DoctoSOC

Détection et réponse à incident.
Une surveillance 24h sur 24 et 7 jours sur 7 déclenchant des alertes à la moindre suspicion d’attaques ciblant Doctolib.

Bug Bounty

Des hackers éthiques.
Analysent constamment nos applications à la recherche de vulnérabilités nous permettant ainsi d’offrir un niveau de sécurité robuste.

CTI

Cyber Threat Intelligence.
Des équipes dédiées analysent le dark et le deep web a la recherche de mots clés ciblant doctolib ou ses employés.

Je suis médecin et je soigne (aussi) les données

Témoignages de médecins