ENTRE PARANOÏA ET OBLIGATION JURIDIQUE
LE RGPD

1374 RÉPONSES A UNE ENQUÊTE

230 EIAS

VOS DONNÉES NOUS INTÉRESSENT… MAIS elles sont PROTÉGÉES par la loi informatique et libertés (loi 78-17 du 06/01/1978)

LES DONNÉES PERSONNELLES

régime général

Autorisation préalable de l'usage de cookies

- Cliquer sur « j'accepte »
- Les cookies alimentent les bases de données de data brokers (les « partenaires commerciaux ») ; IQVIA
- Jusqu'à 50 cookies intrusifs pour un clic (testez vous-mêmes avec PIA privacy impact assessment)
- Profilage sélectif et vente de fichiers (n° de téléphone, adresses mail…) sur le black market
- Croisements de fichiers

La loi 2018-493 du 20/06/2018 modifie la précédente en transcrivant le règlement UE 2016/679 ou RGPD

LES DONNÉES SENSIBLES

régime particulier

Autorisation explicite

- Toutes les données de santé (article 16 de la loi)
- Anonymisation, cryptage, définition stricte des buts du traitement des données, durées de conservation, recours des particuliers,
- Exemple: Plainte du 01/07/20 déposée auprès de la CNIL par Privacy international contre Doctissimo (vente des résultats de tests gratuits de dépistage de dépression)

DANS LE DOMAINE MÉDICO-SOCIAL LE BUT EST DE PROTÉGER

- LES ÉCHANGES DE DONNÉES
- LE STOCKAGE ET L'ÉVENTUEL TRAITEMENT DES DONNÉES LA OU ELLES SE TROUVENT

LES REBONDS DE LA CHAINE MÉDICO-SOCIALE sont autant de points d'attaques potentiels

- Ma montre connectée: elle est connectée à mon ordinateur personnel
- Micro entreprises: mon ordinateur portable ou celui du cabinet qui communique avec mes clients et mes confrères et l'établissement de santé
- Petites entreprises: ES indépendants, Sofcot, Orthorisq, syndicats médicaux qui communiquent entre eux et avec les précédents
- Grandes entreprises: AP-HP, HCL, AP-HM, caisses de SS, mutuelles) qui communiquent avec le public et les précédents
- Très grandes entreprises nationales ou internationales: Fournisseurs de matériel médical ou de médicaments, Institut Pasteur, chaines d'établissements de santé, Health Data Hub ((mis en service en 2019, géré par IQVIAet dont les données sont dans le cloud de microsoft)…
- Sans oublier les hébergeurs de données parfois situés à l'étranger (Exemple: référé Conseil d'état du 12/03/2021 contre Doctolib et Amazon web services ou le RGPD comme réponse au Patriot act, au Cloud act et à l'exterritorialité de la loi américaine; les privilèges des 16 agences de sécurité US)

LES RISQUES

- Simple malveillance et atteinte à votre réputation
- Cyber attaques (surtout crypto verrouillage)
- Pillages de données (par des data brookers, des concurrents, des « intérêts » économiques voire politiques) ou modification de données
- Plaintes à la CNIL (clients, fournisseurs, correspondants) pour non respect de vos obligations
  - Sanctions contre les acteurs « négligents »: avertissement, injonctions sous astreintes 200 à 3 000 € par **jour**;
  - amendes: au maximum 20 millions d'euros ou 4% du chiffre d'affaires mondial.

CNIL : RAPPORT 2020

- 2825 Notifications de violation de données (+24% par rapport à 2019) dont 1393 malveillantes (+42%) ce qui comprend 500 attaques par crypto verrouillage
- 13 585 plaintes (chiffre stable)
- Le secteur de la santé représente 7% de ces évènements indésirables (4% en 2019)

2 EXEMPLES DE CONDAMNATIONS APRÈS PLAINTES DANS LE DOMAINE MÉDICO SOCIAL

- CNIL juillet 2020
  3 000 et 6 000 € d'amendes (avec publicité mais sans publication des noms) à l'encontre de 2 médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients (art 32 RGPD, obligation de sécurité) et ne pas avoir notifié une violation de données à la CNIL (art 33 RGPD).

- CNIL juillet 2021

1.75 million d'euros d'amendes à l'encontre de AG2R La Mondiale pour non observation de l'obligation de limiter la durée de conservation des données et de l'obligation d'information des personnes

OBLIGATION DÉJÀ EXISTANTE avant le RGPD

Loi Informatique et Libertés n°78-17 du 06/01/1978 .

Faire la preuve de « la mise en place des mesures techniques et opérationnelles sécurisant les données » nous incombe

➢ Le RGPD renforce ce cadre par 4 nouvelles obligations :

- Tenue d'un registre recensant toutes les violations de données personnelles et les documenter
- Notification des violations à la CNIL dans les 72 heures,
- Information des personnes concernées
- Effectuer une analyse d'impact

LA CNIL NOUS AIDE…

- Depuis le 11/03/2019 , 109472 comptes MOOC « ateliers RGPD » ouverts aboutissant à 35 110 attestations de succès et 25 494 DPO désignés
- Référentiel de gestion (établissements médicaux et paramédicaux)
- Référentiels des durées pertinentes dans la santé et la recherche (tenue de dossiers patients, ordonnances, recherches…).
- MOOC de l'ANSII: 42 mesures d'hygiène informatique

ET POUR LE RESTE…

RÉSULTATS ENQUÊTE ET EIAS

mise au point d'une « check-list » RGPD

LE BOF

A-NOUS FAISONS LA PREUVE DE LA DÉLIVRANCE D UNE INFORMATION EXPLICITE

- Par une affichette en salle d'attente destinée aux patients: oui 16.5%
- Mais avez-vous pensé que cette affichette devait être présente aussi sur tous vos logiciels recueillant des données médicales et tout particulièrement les logiciels de prise de rendez-vous?

UNE «BONNE » AFFICHETTE DEVRAIT MENTIONNER QUE:

- Vos dossiers informatisés peuvent être aussi détenus dans une structure de soins sous votre responsabilité
- La finalité du dossier médical est exclusivement de soins(en cas d'utilisation éventuelle à des fins de recherche une affichette spécifique est nécessaire)
- La durée de conservation du dossier est de 20 ans à partir de la majorité (article R 1112-7 CSP); au delà destruction avec traçabilité)
- Les droits du patient sur son dossier sont permanents: accès, rectification, effacement, réclamation auprès de la CNIL
- Il existe un système de sauvegarde: copies chiffrées, éventuel hébergeur extérieur agréé (article L 1111-8 CSP) ce qui est obligatoire si vos copies si vos copies sont dans un « Cloud »
- Tous le personnel du cabinet médical et ses sous traitants ont signés un engagement de confidentialité (oui 30%) et de respect du RGPD

B- NOUS FAISONS LA PREUVE QUE NOUS PROTÉGEONS LES DONNÉES QUE NOUS DÉTENONS

- En conservant les données »papier » qui subsistent dans un local ou une armoire fermée à clef (oui 45%)
- En n'introduisant pas de CD ou clef USB de patient pour lire des documents ou des RX (je le fais parfois ou souvent 30.5%); PACS sécurisé
- En utilisant toujours toujours un compte utilisateur et jamais administrateur sur mon ordinateur personnel (je ne sais pas…)
- En utilisant un mot de passe conforme aux recommandations (oui 43%), renouvelé tous les 6 mois minimum (oui 40.5%) Np5mp1pr,na3
- Avec verrouillage automatique après 15mn d'inactivité (oui 78%)
- En nous assurant , en cas de recours à des hébergeurs qu'ils respectent les exigences du RGPD (oui 42%)
- En nous assurant que nos prestataires de service (notamment informaticiens) respectent les exigences du RGPD (oui 44%)

MAIS AUSSI

- En faisant des sauvegardes au minimum hebdomadaires avec conservation des sauvegardes mensuelles sur 12 mois glissant (oui 75%; je le fais moi-même 28%; je ne sais pas qui le fait 12%)
- En conservant les sauvegardes dans un lieu différent du cabinet (je conserve dans mon cabinet 22%; je ne sais pas ou elles sont conservées 28.5%)
- En disposant d'un antivirus à jour (oui63%), d'un pare feu à jour (oui 61%), (les deux sont présents mais je ne sais pas s'ils sont à jour 20%)
- En appliquant systématiquement les correctifs de sécurité des système d'exploitation informatiques (oui 60%)
- Et comme 29% d'entre nous conservent parfois et 20% souvent des données dans leurs téléphones portables ou leur tablettes, ceux-ci sont protégés selon les recommandations de la CNIL (non 32%; je ne sais pas 53%)

C-NOUS FAISONS LA PREUVE DE PROTÉGER LA TRANSMISSION DES DONNÉES

- En nous étant assuré que le destinataire de nos données respecte les exigences du RGPD (oui 17%)
- En chiffrant les données avec un logiciel adapté (oui 22%, non 27%, je ne sais pas 51%)
- En utilisant une messagerie électronique sécurisée MS santé ou Apicrypt (en fait 56% d'entre nous utilisent une messagerie standard et parmi eux 5% chiffrent)
- En respectant scrupuleusement les recommandations de la CNIL sur la manipulation des liens, des pièces jointes, sur la protection de la box, du wifi y compris celui de votre domicile si vous utilisez un portable (précautions détaillées dans notre fiche de conseils), de notre portable et de notre montre connectée
- En n'utilisant jamais d'applications communautaires (Facebook, Whatsapp…yp) sauf à chiffrer le données
- En utilisant une messagerie dédiée cryptée (type signal ou proton mail; oui 11%) quand nous échangeons des informations médicales avec un établissement de santé à l'aide d'un téléphone portable (38% d'entre nous le font) Nous ne rechargeons JAMAIS notre portable sur notre ordinateur

BIEN ENTENDU

- En cas de prise de rendez vous informatique
- Nous ne mentionnons jamais le motif du rendez vous ou d'éventuelles prescriptions (radiographie de contrôle post opératoires par exemple)
- 64% d'entre nous le mentionne

D- NOUS RESPECTONS SCRUPULEUSEMENT LES NOUVELLES OBLIGATIONS ADMINISTRATIVES DU RGPD

- Nous avons défini une procédure à appliquer en cas de violation des données que nous détenons (non 61%; je ne sais pas 33%)
- Nous tenons un registre des activités de traitement informatique (non 57%; je ne sais pas 22%)
- En fait nous avons OBLIGATION de tenir différents registres dont le contenu est défini par le RGPD (ils sont détaillés dans l'article de conseils mis à votre disposition).

AU TOTAL : LE RGPD

- Ne fait que compléter des obligations déjà existantes depuis longtemps
- Surtout organise leur application par la CNIL
- Entraine l'application de sanctions en cas de non observations, ce qui n'était pas le cas précédemment

Un IDEAL sophistiqué

IDEAL =

Instrument de Défense
Européen Anti Lobby

Lutter pour un idéal est plus valorisant que de se considérer comme une victime d'institutions envahissantes

LA SITUATION EST PROMETTEUSE

- Nous ne pouvons qu'améliorer notre pratique actuelle comme nous l'avons fait pour la check list
- Vous avez librement créé Orthorisq pour vous y aider
- Vous trouverez sur le site, outre un article de fond écrit en coopération avec la Sofcot, le BOF et le CNP-COT, des fiches d'aides pratiques (projet d'affichette pour salle d'attente, check-list RGPD)