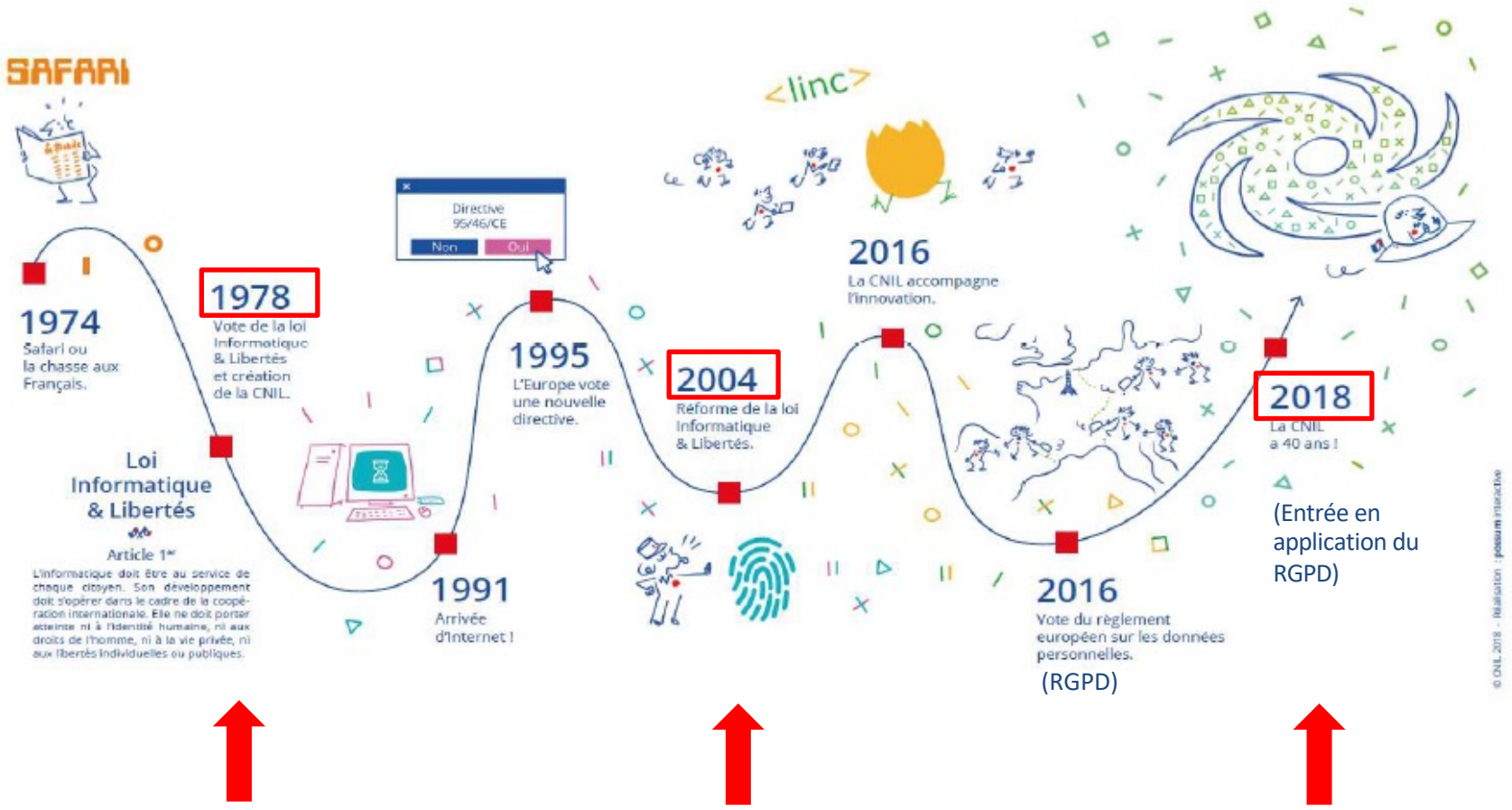
Santé Numérique
Cadre juridique de la Protection des données

Séverine Lair-Préterre
DPO du CHU de Rouen
05/04/2024

CHU ROUEN NORMANDIE

CADRE JURIDIQUE SUR LA PROTECTION DES DONNÉES PERSONNELLES : UN PEU D'HISTOIRE



Les **principes de la protection** des données
sont presque identiques à ceux qui existent en France depuis 1978 :

- **Licéité, loyauté et transparence** dans l'utilisation des données;
- **Limitation des finalités** (finalités déterminées, explicites et légitimes);
- **Minimisation des données** (données adéquates, pertinentes et limitées à ce qui est nécessaire);
- **Exactitude des données** (données exactes, et tenues à jour);
- **Limitation de la conservation** (données conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées);

Le RGPD ajoute deux **nouveaux** principes, qui concernent la **sécurité des données** et la **responsabilisation des acteurs**, et un **renforcement des sanctions**

PROTECTION DES DONNÉES PERSONNELLES : LES ACTEURS

- Le **responsable du traitement** (RT) est un organisme qui détermine les finalités et les modalités du traitement : Etablissement de santé

- Le **sous-traitant** (ST) est celui qui traite des données à caractère personnel pour le compte du responsable de traitement : Prestataires de service, fournisseurs de logiciel, établissements de santé partenaires

- Le **Délégué à la protection des données** (DPD/DPO) désigné auprès de la CNIL : informer et conseiller l'établissement et son personnel, travailler avec le Responsable de la Sécurité du Système d'Information (RSSI : définir et intervenir sur tous les aspects de la sécurité du système d'information), être l'interlocuteur des usagers et de l'autorité de contrôle

- L'**autorité de contrôle,** en France : CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

PROTECTION DES DONNÉES : LES RESPONSABILITÉS DE L'ÉTABLISSEMENT

- Prendre conseil auprès du Délégué à la Protection des Données
  - CHU de Rouen : dpd@chu-rouen.fr ou http://intranet4/infossi/protection-des-donnees/
- Fournir les éléments nécessaires à **l'enregistrement** des **traitements** dans le registre (liste de tous les traitements en place)
- Vérifier avec les **experts métiers** que les données sont sécurisées
- Encadrer les **relations avec les prestataires/fournisseurs**
- Mener une **analyse d'impact sur la vie privée des personnes**
- **Notifier des violations de données,** si atteinte sur la vie privée des personnes
- **Répondre** aux demandes des **usagers** (délai d'un mois)

Renforcement des droit existants

- **Obligation générale de faciliter l'exercice des droits : information concise, transparente, compréhensible et aisément accessible**

- **Information renforcée :**
  - coordonnées du délégué à la protection des données,
  - clarté de l'information apportée à la personne sur les finalités du traitement,
  - les durées de conservation…

- **Droit à être informé d'une violation des données en cas de risques élevés pour les intéressés**

QU'EST CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL (DONNÉE PERSONNELLE) ?

Notion large (article 4 du RGPD) :

Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

- ✓ Données directement identifiantes : nom et prénom, photo, e-mail nominatif, etc.

- ✓ Données indirectement identifiantes : NIR, numéro de patient (IPP) ou encore l'identité nationale de santé, etc.

- ✓ Recoupements d'informations anonymes : le fils aîné du notaire habitant au 5 rue de la gare à Niort

par principe, interdiction

- ✓ Données sensibles : santé, religion ou convictions philosophiques, appartenance syndicale, orientation sexuelle, données biométriques, données de génétiques
- ✓ Numéro d'identification nationale (NIR en France)

- ✓ Exceptions : prise en charge sanitaire, recherche scientifique

PROTECTION DES DONNÉES : DONNÉES DE SANTÉ

Dans le cadre de sa prise en charge médicale, outre les informations relatives à l'identité d'une personne, des donnés de santé sont traitées au quotidien.

Données de santé :

un **régime juridique particulier** justifié par la sensibilité des données s'applique avec différentes législations susceptibles de s'appliquer (liste non exhaustive) :

- loi Informatique et Libertés (chapitre III - section 3) ;
- dispositions sur le secret (art. L. 1110-4 du CSP) ;
- dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du CSP) ;
- dispositions sur l'hébergement des données de santé (art. L. 1111-8 et R. 1111-8-8 et s. du CSP) ;
- dispositions sur la mise à disposition des données de santé (art. L. 1460-1 et s. du CSP) pour des projets « d'intérêt public » (possible d'utiliser ces données pour conduire des projets de recherche) ;
- interdiction de procéder à une cession ou à une exploitation commerciale des données de santé (art. L. 1111-8 du CSP, art. L 4113-7 du CSP)…

PROTECTION DES DONNÉES : EXEMPLE D'UN PATIENT PRIS EN CHARGE À L'HÔPITAL

1ère étape : la collecte des données de santé

Collecte

Un « traitement médical » génère un « traitement de données de santé »

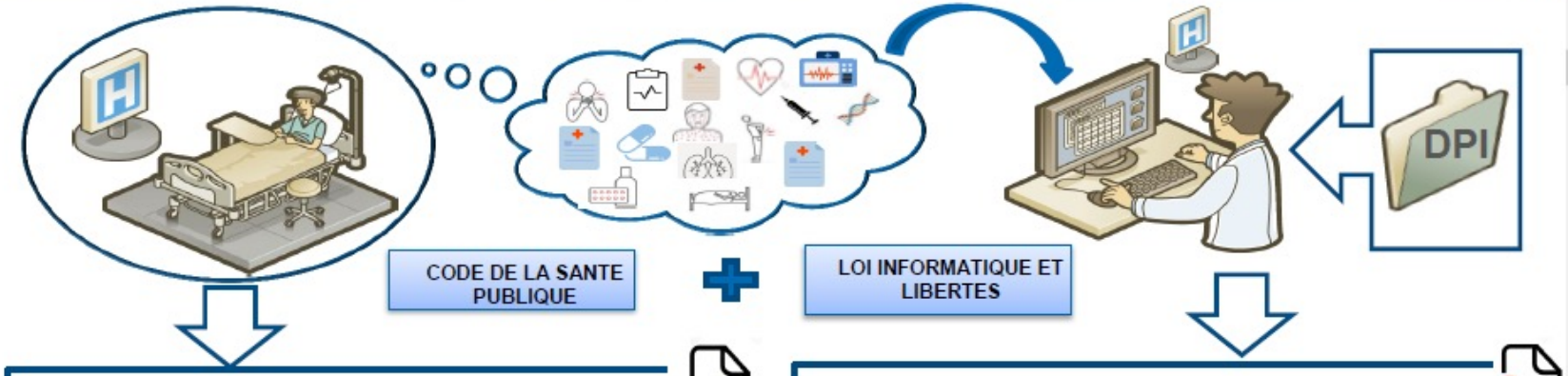
Trois catégories de données de santé

- Données de santé par nature
- Croisement de données devenant des données de santé
- Données de santé en raison de leur utilisation

PROTECTION DES DONNÉES : EXEMPLE D'UN PATIENT PRIS EN CHARGE À L'HÔPITAL

1ère étape : la collecte des données de santé

Collecte



CODE DE LA SANTE PUBLIQUE

LOI INFORMATIQUE ET LIBERTES

Droits du patient

*« Je vais être **informé** sur ma prise en charge et **sur l'utilisation de mes données de santé**. J'ai le droit **au respect de ma vie privée** et les professionnels qui interviennent sont tenus au **secret** ».*

Devoirs et obligations de l'hôpital, responsable du traitement Dossier Patient Informatisé (DPI)

*« L'hôpital met à ma disposition un DPI qui me permet de tracer les soins effectués tout en assurant, **dès la conception du traitement** la protection des données personnelles collectées*

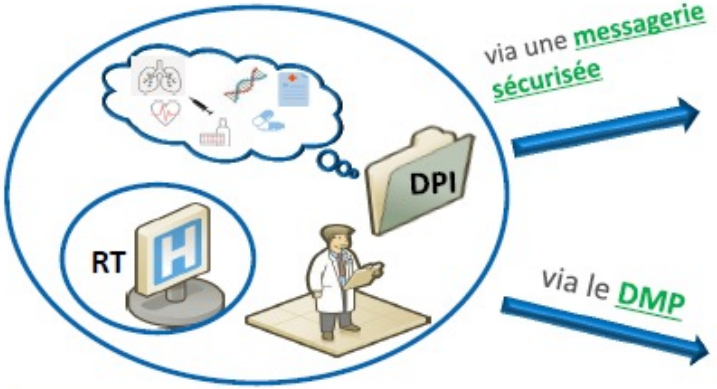
*Je m'engage à traiter uniquement les données à caractère personnel qui sont **adéquates**, **pertinentes** et **nécessaires** pour prendre en charge le patient. »*

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Présentation HIT_ASIP Santé - CNIL

2ème étape : l'échange et le partage des données de santé

Échange et partage



LOI INFORMATIQUE ET LIBERTES + CODE DE LA SANTE PUBLIQUE

ECHANGE D'INFORMATION

Professionnels identifiés participant à la coordination, la continuité des soins et le suivi social et médico-social d'un même patient

Information préalable + droit d'opposition

PARTAGE D'INFORMATION

Professionnels participant à la coordination, la continuité des soins et le suivi social et médico-social d'un même patient

Au sein de la même équipe de soins — **Information préalable + droit d'opposition**

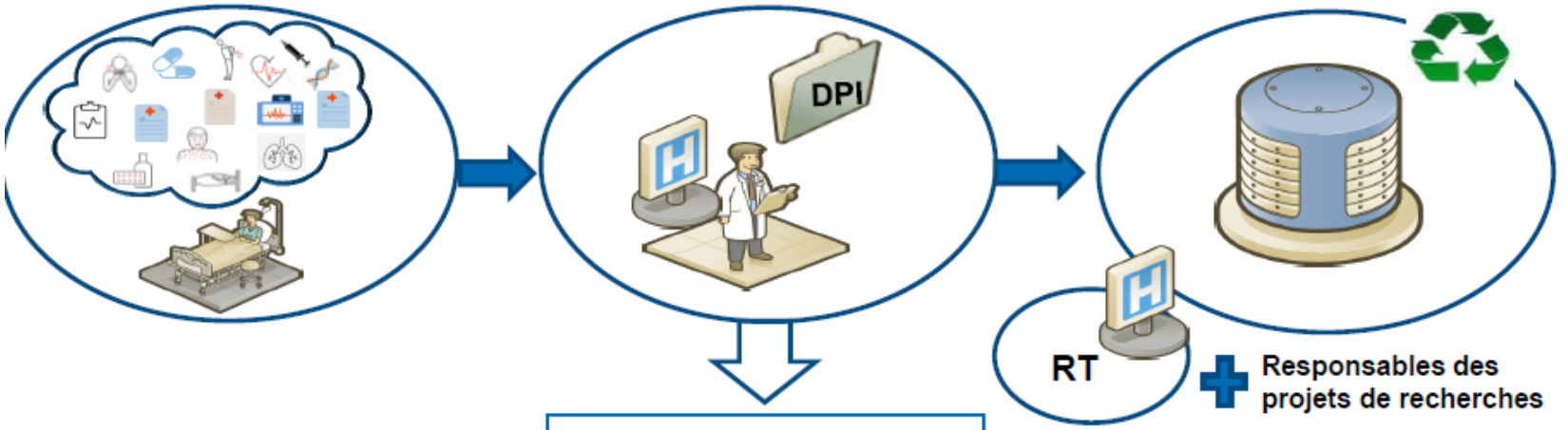
En dehors de l'équipe de soins — **Consentement exprès**

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Présentation HIT_ASIP Santé - CNIL

3ème étape : réutilisation des données de santé à des fins de recherche

réutilisation



J'ai l'idée d'un projet de recherche sur le cas de mon patient: Peux-je utiliser les données de son dossier patient informatisé?

Entrepôt de données de santé

PROTECTION DES DONNÉES : PROJET DE RECHERCHE SUR DONNÉES EXISTANTES

En cas d'étude interne :

Conditions cumulatives :

- à partir de données recueillies dans le cadre de la prise en charge individuelle des patients concernés ;
- par les personnels assurant ce suivi ;
- pour l'usage exclusif de ces derniers.

-> traçabilité du projet de recherche à avoir

⇒ référencement auprès de la Dir. de la Recherche

⇒ Respect des principes du protection données (cf diapo 3)

-> pas soumises à formalités auprès de la CNIL.

Tous les autres cas :

À l'exception des études « internes », tous les projets de recherche, étude ou évaluation en santé doit se faire au regard des référentiels existants de la CNIL

-> traçabilité du projet recherche à avoir

⇒ référencement auprès de la Dir. de la Recherche

⇒ vérification des points de conformité à la MR004 de la CNIL

-> si en conformité avec la MR004 (sous couvert de l'engagement de conformité faite par le CHU), pas de formalité complémentaire auprès de la CNIL

-> à défaut de conformité en tous points à la MR004 : autorisation préalable de la CNIL (délai de 4 mois)

Vous ne devez pas, en tant que interne, doctorant ou étudiant, réaliser une formalité auprès de la CNIL en votre nom propre, c'est le CHU en sa qualité de responsable de traitement (engagement de conformité à une MR ou demande d'autorisation « recherche »).

CHU de Rouen : DRCI_DPO_Fiche Réflexe – Projet de Recherche en santé sur données existantes (GEDI 40197) et http://intranet4/maisondelarecherche/les-textes-de-loi/

PROTECTION DES DONNÉES : DONNÉES PSEUDONYMISÉES # DONNÉES ANONYMISÉES

pas confondre l'anonymisation et la pseudonymisation

- la pseudonymisation = remplacement des données directement nominatives (nom, prénom, numéro de sécu, numéro CPAGE) par un numéro d'anonymat
  - Une donnée non directement identifiante peut être une donnée à caractère personnel : donnée pseudonymisée codée (la plupart du temps, en recherche)
  - Permet le chaînage et l'appariement des données personnelles d'un individu

- l'anonymisation = ensemble de techniques qui rend impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible
  - Une donnée « anonyme » n'est plus/pas une donnée à caractère personnel
  - Appauvrissement des données brutes et une restriction du champ des exploitations possibles

PROTECTION DES DONNÉES :
LES RISQUES LIÉS AUX DONNÉES PERSONNELLES

- **Accès illégitime** aux données :
  - *Exploitation des données (vol, revente, diffusion, profilage…)*
- **Modification** non désirée :
  - *Dysfonctionnement (mauvaises consignes de soin, mesures erronées, attaque sur une pompe à insuline…)*
- **Disparition** :
  - *Dysfonctionnement (dossier médical ne signalant plus les allergies…)*
  - *Blocage (impossibilité de dispenser des soins, impossibilité d'exercer ses droits, démarches administratives interrompues…)*

Cybersécurité :

2022 : 592 incidents de cybersécurité ont ciblé des établissements de santé et ont été déclarés sur le portail des signalements

432 structures ont déclaré au moins 1 incident pendant l'année

Violations de données personnelles :

2023 : > 4500 violations de données personnelles déclarées à la CNIL

571 violations déclarées dans le secteur « Santé humaine et sociale »

PROTECTION DES DONNÉES : SÉCURITÉ DES DONNÉES – LES BONS RÉFLEXES À AVOIR

Le partage de données sécurisé de données de santé dans le cadre du soin

- Sécurité des transferts de données, de leur stockage : messagerie sécurisé de santé, mon espace santé.
- Recours aux outils mis à disposition par l'établissement : outil de capture d'images, dossier patient informatisé
- Partage entre professionnels : demande d'avis médicaux, télé médecine : si nécessaire, via des outils professionnels sous condition d'organisation préalable par l'établissement.

L'accès au dossier médical et la saisie d'informations dans le cadre du soin

- Strictes habilitations des professionnels intervenant dans la prise en charge et notion d'équipe de soins

  Reco : Ne consultez pas votre dossier médical, celui de vos proches ou de vos collègues.

  Ne communiquez aucune information relative aux patients ou à leurs proches en dehors de l'équipe de soins et a fortiori à tout tiers.
- Traçabilité des accès et tentatives d'accès

  Reco : Utilisation de la carte pro afin de se connecter, celles-ci sont personnelles. Ne pas laisser vos sessions ouvertes : possible engagement de responsabilité
- Droit d'accès à ses données : au titre du Code de la santé publique, les patients peuvent en faire la demande

  Reco : Ne mentionnez que des éléments objectifs et nécessaires à la prise en charge

Charte Utilisateur du bon usage des technologies numériques (GEDI 27681), annexée au Règlement Intérieur

L'usage des données de santé dans le cadre de projets de recherche

- Utiliser les données strictement nécessaires à votre projet de recherche
- Réaliser les traitements de données sur les serveurs, outils, répertoires partagés ou postes de travail inventoriés par le CHU de Rouen
- Pseudonymiser les données de votre base (pas de date de naissance complète (se limiter au mois/année), pas d'adresse ...) par le biais d'un code
- Ne pas croiser ces données avec des données d'autres sources (fichiers, bases de données) en dehors des besoins de la recherche ayant obtenu un avis du Comité de Qualification
- Ne pas transférer ces données sur des supports mobiles (clefs USB, disques durs, etc.). Si cela s'avère nécessaire, cela ne peut se faire que temporairement au travers d'une plateforme sécurisée validée par l'établissement pour les échanges professionnels vers l'extérieur (*https://sirrus.chu-rouen.fr/*). Vous devez vous assurer de la suppression effective de ces données une fois le transfert effectué.
- Ne pas communiquer par quelque moyen que soit la base de données constituée dans le cadre de votre projet de Recherche à des professionnels n'intervenant pas dans le projet

Charte Utilisateur du bon usage des technologies numériques (GEDI 27681), annexée au Règlement Intérieur

Protection des données : Fuites et/ou sanctions en santé

- Dedalus Biologie (avril 2022)
  - Fuite de données concernant 500 000 personnes et sanction de la CNIL de 1,5 Md€ pour défaut de respect des instructions de sécurisation des données de santé sur l'encadrement contractuel

- SI-DEP (septembre 2021)
  - Fuite de données concernant 1,4 million de personnes testées contre la COVID-19 mi-2020 : la CNIL et les personnes concernées ont été informées
- Francetest (octobre 2021)
  - Mise en demeure par la CNIL de la société pour défaut de sécurisation des données de santé collectées pour le compte des pharmacies à l'occasion de tests de dépistage à la COVID19
- 2 Médecins généralistes (décembre 2020)
  - Sanctions de la CNIL de 3 000 € et 6 000 € à l'encontre de deux médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL

Protection des données : Fuites et/ou sanctions en santé

- Médecin généraliste (février 2023)
  - Non respect du droit d'accès
  - Défaut de coopération avec la CNIL
  - Amende de 3 000 euros et injonction
- Chirurgien dentiste (mai 2023)
  - Non respect du droit d'accès
  - Défaut de coopération avec la CNIL
  - Amende de 4 500 euros et injonction
- doctissimo.fr, société éditant un site internet proposant des articles, tests, quiz et forums de discussion en lien avec la sante et le bien-être (mai 2023)
  - Durée de conservation
  - Consentement des personnes (données de santé)
  - Encadrement des relations entre le responsable de traitement et le sous-traitant
  - Défaut de sécurité des données
  - Consentement des personnes (cookies et traceurs)
  - Amende de 380 000 euros

PROTECTION DES DONNÉES : RAPPEL / MISE DEMEURE DE LA CNIL EN 2023

- **Rappel aux obligations légales à 2 organismes de recherche** https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-deux-organismes-de-recherche-medicale-leurs-obligations-legales
  - Réaliser une analyse d'impact sur la protection des données pour les recherches médicales (hors études internes)
  - Donner une information complète aux personnes concernées avec notamment la nature de données collectées, la durée de conservation (attention sur la terminologie de données anonymes)

- **Mise en demeure de plusieurs établissements de santé de prendre les mesures permettant d'assurer la sécurité du dossier patient informatisé, rappelant que les données des patients ne doivent être accessibles qu'aux personnes justifiant du besoin d'en connaître**

  https://cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au
  - Sécuriser les accès au système grâce à une politique d'authentification robuste (notamment des mots de passe suffisamment complexes ou des cartes professionnelles)
  - Prévoir des habilitations spécifiques pour que chaque professionnel de santé ou agent de l'établissement n'accède qu'aux dossiers dont il a à connaître.
  - Tracer les accès au DPI (journalisation) : cette traçabilité doit non seulement permettre d'indiquer qui s'est connecté à la base de données à quel moment, mais, plus précisément, qui a accédé à quoi et réaliser des contrôles réguliers de ces accès afin d'identifier ceux susceptibles d'être frauduleux ou illégitimes

SANTÉ NUMÉRIQUE
CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES

Merci de votre attention

Contenus autour de la cybersécurité
et la protection des données sur
l'intranet du CHU :
http://intranet4/infossi/

CHU ROUEN NORMANDIE