SANTE NUMERIQUE – DFGSM2-2 (LES P2)

I. Connaissance des définitions et du vocabulaire liés aux données personnelles

Définitions Clés :	- Données à caractère personnel : Informations se rapportant à une personne physique identifiée ou identifiable directement ou indirectement (via un identifiant, numéro de téléphone, mail etc…) (données biométriques, génétiques etc sont des données personnelles)
	- Données sensibles : Catégorie spéciale de données personnelles révélant l'origine raciale, opinions politiques, convictions religieuses, santé, etc. Leur utilisation ou leur recueil est interdit par le RGPD (sauf :
	  ○ si consentement
	  ○ si les infos sont rendues publiques par la personne,
	  ○ si elles sont nécessaires à la sauvegarde de la vie humaine,
	  ○ si l'utilisation est d'intérêt public et autorisé par le CNIL,
	  ○ si elles concernent les membres ou adhérents d'une orga politique, religieuse etc…
	- Données de santé : Informations relatives à la santé physique ou mentale d'une personne, incluant les services de soins de santé.

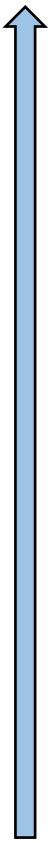
Points Importants :	- Les données de santé sont considérées sensibles et nécessitent une protection particulière. - La distinction entre données anonymes, pseudonymisées et directement identifiantes est essentielle pour comprendre leur niveau de confidentialité et de protection.

II. Qualification d'une donnée de santé

Types de Données de Santé :	- Par Nature : Informations directement liées à l'état de santé (diagnostics, traitements, etc.). - Par Combinaison : Données qui deviennent de santé à travers leur association (poids et nombre de pas). - Par Destination : Informations utilisées dans un contexte médical pour évaluer la santé (photos utilisées pour le diagnostic).

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

Critères de Qualification :	- Une donnée est qualifiée de santé si elle a un lien direct ou indirect avec l'état de santé d'un individu - Les données collectées pour des usages personnels sans partage extérieur ne sont pas considérées comme des données de santé par la réglementation

III. Connaissance des différents niveaux de données identifiantes	
Niveaux d'Identification :	 - Données Directement Identifiantes : Informations permettant l'identification immédiate d'une personne (nom, prénom) - Données Indirectement Identifiantes : Informations qui peuvent mener à l'identification en combinaison avec d'autres données (dates, localisation). - Données Pseudonymisées (ce n'est pas un niveau d'identification) : Informations personnelles transformées de telle manière qu'elles ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires. *Pseudonymisation : remplacer les données directement identifiantes par des données indirectement identifiantes* - Données Anonymes : Informations traitées pour rendre l'identification de l'individu impossible en pratique, même avec des données supplémentaires, et de manière irréversible. Ne sont plus des données personnelles ! - Données Agrégées : sont celles ayant le niveau d'identification le plus faible.
Applications et Implications :	- La pseudonymisation réduit les risques liés au traitement de données personnelles mais ne les rend pas anonymes - L'anonymisation retire toutes les caractéristiques identifiantes d'une donnée, la rendant non-soumise à la réglementation sur la protection des données.

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

IV. Anonymisation des données	
Définition	Processus transformant les données personnelles pour empêcher toute identification des individus. Il s'articule autour de deux techniques principales : - . Randomisation : Modifie les données pour réduire leur précision tout en préservant l'intégrité statistique, empêchant l'identification directe des sujets. - Généralisation : Augmente le niveau de généralité des données (par exemple, en regroupant les âges par tranches) pour éviter l'identification individuelle.
Évaluation de l'anonymisation	3 critères : 1. Individualisation : impossibilité d'isoler un individu 2. Corrélation : incapacité de lier des ensembles de données pour identifier une personne 3. Interférence : impossibilité de déduire des informations sur un individu - Un jeu de données est considéré comme anonyme si ces critères sont respectés, réduisant ainsi les risques de ré-identification.

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

Partie II : Cadre Réglementaire de la Protection des Données

I. Principes de la LIL et du RGPD

Loi Informatique et Libertés (LIL)	Adoptée en France en 1978 (dernier décret en 2019), la LIL réglemente le traitement des données à caractère personnel et établit les droits des individus ainsi que les obligations des entités qui traitent ces données. Elle a créé la CNIL, autorité de régulation en matière de protection des données en France.
Règlement Général sur la Protection des Données (RGPD)	En vigueur depuis mai 2018, le RGPD est une législation européenne qui vise à renforcer et unifier la protection des données pour tous les individus au sein de l'Union Européenne. Il s'applique à toute organisation, publique ou privée, qui traite les données personnelles des résidents européens.
Principes généraux sur la protection des données	***Transparence*** : Les individus doivent être informés de la collecte et de l'utilisation de leurs données. ***Limitation de la finalité*** : Les données ne doivent être collectées que pour des objectifs explicites et légitimes. ***Minimisation des données*** : Seules les données nécessaires pour les objectifs spécifiés sont collectées. ***Exactitude*** : Les données doivent être exactes et à jour. ***Limitation de conservation*** : Les données ne doivent pas être conservées plus longtemps que nécessaire. ***Intégrité et confidentialité*** : Les données doivent être traitées de manière à assurer leur sécurité.
Utilisation des données personnelles : (et donc les données personnelles de santé)	**LEUR TRAITEMENT EST INTERDIT PAR LA LIL ET PAR LE RGPD** [dans ce contexte traitement signifie toute opération appliquées à des données ou des ensembles de données à caractère personnel] Est-ce qu'il y a des exceptions ? bien sûr mais va falloir aller les voir tous seul sur les diapos mon loulou

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

II. À qui s'applique ce cadre réglementaire	
	Le RGPD s'applique <u>si le responsable du traitement est dans l'UE</u> OU si les données concernent des personnes sur le territoire de l'UE (ex : un habitant du pays des burgers vient en vacances en Italie, ses données seront soumises au RGPD parce que vivent l'UE) La LIL s'applique à tout traitement de données personnelles effectué par des entités situées sur le territoire français. (ex : vous vous connectez à moodle, vos données perso sont ainsi soumises à la LIL (on suppose ok je suis pas cadre chez moodle pour savoir ok ??) et en même temps au RGPD)
Point régulation, La CNIL :	"La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle est l'autorité de contrôle nationale au sens et pour l'application du RGPD" (chap.2 de la LIL) Elle a quatre missions : 1. **Informer, protéger les droits** **2. Accompagner la conformité / conseiller** **3. Anticiper et innover** **4. Contrôler et sanctionner**

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.

III. Droits des patients	
Bases légales RGPD	Les “bases légales” proposées par le RGPD donnent le droit à un organisme de traiter des données personnelles, voici la liste : 1. **Le consentement [C’EST IMPORTANT]** **2. Le contrat** **3. L’obligation légale** **4. La mission d'intérêt public** **5. L'intérêt légitime** **6. La sauvegarde des intérêts vitaux**
Droits des individus en vertu du RGPD et de la LIL	● **Droit d'accès** : Les patients ont le droit de savoir quelles données à caractère personnel sont traitées et d'en obtenir une copie. ● **Droit de rectification** : Les patients peuvent demander la correction de données inexactes. ● **Droit à l'effacement** : (Également connu sous le nom de droit à l'oubli), permettant aux patients de demander la suppression de leurs données. ● **Droit à la limitation du traitement** : Les patients peuvent demander que le traitement de leurs données soit limité. ● **Droit à la portabilité des données** : Les patients ont le droit de recevoir leurs données personnelles dans un format structuré et de les transmettre à un autre responsable du traitement. ● **Droit d'opposition** : Les patients peuvent s'opposer au traitement de leurs données dans certaines circonstances
Les droits des patients dépendent de la “base légale” du traitement des données !	

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

Partie III : Traitement des Données de Santé

I. Définition du Traitement de Données

Définition :	▪ Le traitement de données inclut toute opération (ou ensemble d'opérations) effectuées sur des données (ou ensembles de données) personnelles, telles que : La collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion, ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, et l'effacement ou la destruction. ***Importance*** *: Chaque action effectuée sur des données personnelles de santé* ***constitue un traitement et doit respecter la réglementation en vigueur****, notamment le* ***RGPD*** *(Règlement Général sur la Protection des Données).*

II. Recueil du Consentement

Objectif pédagogique : Savoir comment recueillir correctement le consentement conformément au RGPD.

Définition	▪ Le consentement doit être une manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte le traitement de ses données personnelles.
Conditions du consentement	▪ **Libre** : ni contraint, ni influencé ▪ **Spécifique** : un consentement doit correspondre à un seul traitement pour une finalité déterminée. (Lorsqu'il y a plusieurs finalités, les personnes doivent pouvoir consentir indépendamment pour l'une ou l'autre de ces finalités) ▪ **Éclairé** : il doit être accompagné d'informations ▪ **Univoque** : doit être donné par une déclaration ou tout autre acte positif clairs (pas ambiguë en gros…) (les cases pré-cochées, les consentements groupés, et l'inaction ne sont pas considérées comme univoques!) ▪ **Base légale** : le consentement est une des 6 bases légales prévues par le RGPD autorisant la mise en œuvre de traitements de données à caractère personnel.

III. Acteurs du Traitement des Données

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)

Principaux acteurs :	- Le Responsable du Traitement (RT) détermine les finalités et les moyens du traitement de données. (Personne morale ou physique) - Le Sous-traitant : effectue le traitement des données pour le compte du RT. (Personne morale ou physique) - Le Délégué à la Protection des Données (DPO) veille à la conformité des traitements avec le RGPD, conseille et informe l'organisme et ses employés, et est le point de contact avec la CNIL.
Responsabilités :	- Le RT est principalement responsable de la conformité du traitement (aux exigences du RGPD). Il doit être en mesure de la démontrer (principe d'accountability). - Le DPO, bien que non obligatoire pour tous, joue un rôle crucial dans la mise en conformité et la sensibilisation au sein de l'organisation.
Principe d'Accountability (Responsabilité) : Définition et Implications :	- Le principe d'accountability, ou de **responsabilité**, oblige le responsable du traitement (RT) à être en mesure de **démontrer à tout moment sa conformité avec les exigences du RGPD.** Cela signifie que le RT doit **documenter et tracer** toutes les actions et démarches entreprises en relation avec le traitement des données personnelles.
Mesures clés :	- Registre des Activités de traitements : Créer et maintenir à jour un registre détaillant toutes les activités de traitement des données, pour avoir une vision claire et complète des traitements effectués - Analyses d'Impact sur la Protection des Données (AIPD): Effectuer ces analyses pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées. Cela aide à identifier et minimiser les risques liés au traitement des données personnelles. (Le logiciel PIA est dédié à l'AIPD) - Information et Droits des Personnes Concernées: Assurer une communication claire et transparente avec les personnes dont les données sont traitées, en leur fournissant toutes les informations nécessaires et en facilitant l'exercice de leurs droits (accès, rectification, opposition, etc.). - Rôles et responsabilités: Définir clairement et formellement les rôles et responsabilités du RT et des sous-traitants pour assurer une gestion efficace et conforme des données.

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.

	➢ Sécurité des Données : Mettre en place et documenter les mesures de sécurité adéquates pour protéger les données personnelles contre les accès non autorisés, les pertes ou les destructions. ➢ Désignation éventuelle d'un délégué à la protection des données (DPO): Désigner un DPO pour superviser la conformité avec le RGPD. Petite liste de ses rôles : ● conseiller ● informer ● contrôle ● coopérer avec le CNIL (interlocuteur entre l'organisme et le CNIL)
V. Mise en œuvre d'un traitement de données personnelles de santé *Objectif pédagogique : Identifier les étapes clés et les questions essentielles à considérer avant de lancer un traitement de données de santé pour garantir la conformité et la protection des données.*	
	1. Finalité et légitimité : ○ Définir clairement l'objectif du traitement. ○ Assurer que la finalité est légitime, explicite et déterminée. **2. Base légale et dérogations :** ○ Identifier la base légale justifiant le traitement (consentement, intérêt légitime, etc.). ○ Comprendre les conditions de dérogation pour la collecte de données de santé. **3. Minimisation de la collecte, adéquation, pertinence et exactitude :** ○ S'assurer que les données collectées sont adéquates, pertinentes et limitées à ce qui est nécessaire. ○ Vérifier que les données sont exactes et à jour. **4. Droits des patients :** ○ Informer les patients au moment de la collecte des données. (Consentement ? etc.) ○ Offrir la possibilité d'exercer leurs droits (accès, rectification, opposition, etc.). **5. Mesures de sécurité (cybersécurité):** ○ Mettre en place des mesures techniques et organisationnelles pour protéger les données. ○ Assurer l'intégrité et la confidentialité des données. **6. Conservation et qualité :** ○ Adapter la durée de conservation à la finalité du traitement (ex : 20 ans pour le soin.) ○ Maintenir la qualité des données. **7. Conformité et documentation :** ○ Vérifier la conformité du traitement avec les référentiels approuvés par la CNIL. ○ Documenter tous les aspects du traitement pour assurer une traçabilité complète.
Recherche dans le domaine de la santé :	Objectif : Alléger les formalités pour les traitements de données en recherche de santé.

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.

	● Méthodologies de référence : ○ RIPH (MR-001 & MR-003) : nécessite seulement l'avis d'un CPP ○ RNIPH (MR-004): n'exige pas l'avis du CESREES, mais l'inscription dans le répertoire public de l'INDS est requise. ○ MR-005 & MR-006 : Accès aux données du PMSI, nécessite un enregistrement auprès de l'INDS et présente un intérêt public. ● Conformité : Si conforme à une méthodologie, l'autorisation de la CNIL n'est pas nécessaire. ● Non-conformité : Nécessite une demande d'autorisation ou un dépôt de dossier selon le type de recherche.
Problème de sécurité des données → obligation d'information du CNIL	Risque de sanction : - Thune : si défaut de sécurisation et d'information - Disciplinaires + pénales : si copies des données

Take Home Messages	- Toute opération effectuée et appliquée à des données à caractère personnel **constitue un traitement de données.** - Les intervenants dans un traitement de données sont le **RT** (± sous- traitant), le plus souvent aidé d'un **DPO.** - Le **consentement d'un patient**, pour être **valide**, doit être **libre, spécifique, éclairée et univoque**. Le consentement s'accompagne d'un **droit de retrait.** - Tout traitement de donnée à caractère personnel doit être inscrit au **registre des activités de traitement de l'institution par le RT**

© 2024, Ludovic Rousseau. Tous droits réservés. CC BY-NC-SA 4.0.
Document mis en page par Hermes(id discord : heermeess)