SORBONNE UNIVERSITÉ

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS
Centre de la Formation et du Développement des Compétences

ifsi INSTITUT DE FORMATION EN SOINS INFIRMIERS
INSTITUT HOSPITALIER FRANCO-BRITANNIQUE

FONDATION ŒUVRE DE LA CROIX SAINT-SIMON

CROIX-ROUGE FRANÇAISE

HEALTH DATA HUB

sesan
SERVICE NUMÉRIQUE DE SANTÉ

FEIMA
Fédération des Éditeurs d'Informatique Médicale et paramédicale Ambulatoire

ikigai games for citizens

ESIEE PARIS

utc

SFMG
le plaisir de comprendre

Relations Médicales
Raphaël Gassin

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

FRANCE 2030

SN@SU
Santé Numérique
Sorbonne Université

La cybersécurité dans le domaine des données de santé et de la recherche

Plateforme des données de santé

1.2, 1.3, 2.1

Juin 2025

Ce document vise à informer un large public sur la cybersécurité appliquée à la réutilisation secondaire des données de santé.

Ce module a été réalisé en co-construction avec la Commission nationale de l'informatique et des libertés (CNIL), la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES) et France Assos Santé.

Version juin 2025

Résumé du module

Niveau avancé

Ce module explique comment **sécuriser les données de santé** lorsqu'elles sont réutilisées pour la recherche. Il présente les **cadres et référentiels** (RGPD + règles françaises), la démarche d'**homologation** (analyse de risques, audits, mesures de sécurité) et l'**AIPD** pour évaluer/réduire les risques. Il rappelle aussi les rôles clés (RSSI, DPO, CNIL/CPP/CESREES) et des mesures comme la **pseudonymisation** et la **transparence** des projets (répertoire HDH).

PLAN Assurer la cybersécurité des données de santé pour la recherche

1. Qu’est-ce que qu’une donnée de santé ?
2. Les données de santé sont sensibles, leur traitement implique d’assurer leur protection
3. Une démarche de cybersécurité encadrée par l’homologation
4. Qu’en est-il de l’AIPD ?
5. Des ressources pour encadrer la cybersécurité

PLAN Assurer la cybersécurité des données de santé pour la recherche

1. Qu’est-ce que qu’une donnée de santé ?
2. Les données de santé sont sensibles, leur traitement implique d’assurer leur protection
3. Une démarche de cybersécurité encadrée par l’homologation
4. Qu’en est-il de l’AIPD ?
5. Des ressources pour encadrer la cybersécurité

Qu’est-ce qu’une donnée de santé ?

Cette définition s’étend à trois catégories de données :

- Les données de santé “par nature”
- Les données de santé “par croisement” - si un croisement avec d’autres données permet de tirer une conclusion sur l’état de santé ou le risque pour la santé d’une personne
- Les données de santé “par destination”, c’est-à-dire en raison de l’utilisation qui en est faite au plan médical.

Les données de santé sont indispensables pour les acteurs du système de santé, par exemple, pour :

Assurer les soins

Données sur la santé des patients (diagnostics, résultats d’examens, comptes-rendus médicaux, prescriptions…)

Financer les soins

Données sur les actes réalisés. Il faut en particulier savoir : quoi ? où ? quand ? par qui ? à qui ? à quel prix ?

Piloter le système de santé

Données **médico-économiques** (dépenses, activités…) et **épidémiologiques** (prévalence, incidence…)

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

Et si ces données sont réutilisées ? Que se passe-t-il ?

Quelles sont les utilisations possibles des données de santé ?

Lorsqu'un patient se rend à l'hôpital, par exemple pour y réaliser des analyses afin d'identifier un problème de santé, les données qui y sont produites peuvent avoir plusieurs vies…

1

La consultation à l'hôpital, les analyses et l'imagerie qui y sont réalisées **produisent des données de santé** : informations, diagnostics, données biologiques, décisions de l'équipe médicale, prise en charge.

1

Par ailleurs certaines données nécessaires pour assurer le **remboursement des prestations** (consultation, biologie…) sont inscrites dans les **bases de données médico-administratives**.

1

Ces usages constituent des **utilisations primaires** de ces données, autrement dit leur **"première vie"**.

2

Les mêmes données peuvent aussi être **réutilisées pour des usages secondaires** fonctionnement de l'hôpital, recherche : c'est leur **"seconde vie"**

2

Les **données détaillées de l'activité locale** (résultats biologie, comptes-rendus, etc.) peuvent être mobilisées afin de **piloter l'activité de l'hôpital, améliorer les connaissances médicales et la prise en charge des patients** si le recueil et l'utilisation des données respectent la réglementation en vigueur ainsi que des mesures de sécurité.

Les données de la **base principale du SNDS** peuvent servir à faire de la **recherche épidémiologique à l'échelle nationale.**

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

PLAN Assurer la cybersécurité des données de santé pour la recherche

1. Qu’est-ce que qu’une donnée de santé ?
2. **Les données de santé sont sensibles, leur traitement implique d’assurer leur protection**
3. Une démarche de cybersécurité encadrée par l’homologation
4. Qu’en est-il de l’AIPD ?
5. Des ressources pour encadrer la cybersécurité

Qu’est-ce que la protection des données ?

La **“protection des données”** est un ensemble de **droits et d’obligations**…

…qui permet d’atteindre un **équilibre**…

… entre la **protection de la vie privée** des personnes, l’**utilisation des données à caractère personnel** (notamment les données de santé, qui sont des données dites « sensibles ») et la **protection de l’intégrité** morale et physique des individus;

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

Quels enjeux à protéger les données de santé ?

Les **données de santé** constituent une **ressource de grande valeur** qu'il est indispensable de **protéger de façon maximale**.

Ne pas protéger les données de santé ⇨ risques

- ➔ Risque de **causer du tort aux personnes** concernées
- ➔ Risque de **réputation** et d'**image**
- ➔ Risque **financier** en cas de contrôle (CNIL) donnant lieu à une **sanction pour non-conformité** d'un projet de recherche

Protéger les données de santé ⇨ bénéfices

- ➔ **Sérénité** dans la gestion des données au quotidien
- ➔ **Confiance** des citoyens et des partenaires dans les activités de recherche en santé
- ➔ **Sécurisation active** des bases de données
- ➔ **Qualité** des soins et de la prise en charge

Quel cadre juridique pour les données de santé en France ?

Le Règlement Général pour la Protection des Données (RGPD) a défini la notion de **donnée de santé** et a laissé des marges de manœuvre aux Etats membres pour adopter des dispositions qui leur sont propres quant à la mise en oeuvre des traitements impliquant des données de santé

La définition posée par le RGPD (Art. 4. 15) :

« *Les **données à caractère personnel** relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique, y compris la prestation de services de soins de santé, **qui révèlent des informations sur l'état de santé** de cette personne* »

Des modalités d'accès spécifiques à la France, dont les dispositions sont notamment inscrites dans le **Code de la santé publique** (par exemple les recherches impliquant la personne humaine – RIPH – ou l'accès au Système national des données de santé – SNDS), et complétées par **divers textes législatifs et réglementaires,** tels que la loi Informatique et Libertés et ses décrets d'application.

Le RGPD protège-t-il la sécurité des données ?

Limitation de la finalité	Le traitement poursuit une **finalité** (objectif) **déterminée, explicite, légitime**
Licéité	Le traitement a une **base juridique** (ex. consentement, intérêt public, contrat)
Transparence	Les **personnes concernées sont informées** du traitement de leurs données
Minimisation	Seules les données **strictement nécessaires** à la réalisation de l'objectif sont traitées
Exactitude	Les données sont **exactes et tenues à jour**
Limitation de la conservation	La conservation des données est limitée au **temps nécessaire à la réalisation de l'objectif**
Sécurité	Les données sont sécurisées de façon à **prévenir toute atteinte à leur confidentialité, intégrité et disponibilité**
Responsabilité (*"accountability"*)	Le responsable de traitement (RT) **documente sa conformité** à l'ensemble des principes du RGPD (registre, AIPD, procédures internes)

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

Quel cadre pour la mise en oeuvre de la cybersécurité des données de santé ?

La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)*

Élaborée par l'Agence du Numérique en Santé (ANS), elle constitue un corpus documentaire qui **encadre les règles spécifiques de sécurité pour l'e-santé.**

- Elle s'applique dès lors que des données de santé sont utilisées
- Elle s'applique au service public et au privé : les professionnels de santé, les secteurs médico-social et social, les établissements de soins et les offreurs de services
- Elle encadre notamment **l'identification électronique et l'authentification des patients** à travers un **Référentiel des Moyens d'Identification Électronique** (Identité Nationale de Santé, Application Carte Vitale…).

**La PGSSI-S constitue un cadre de référence en matière de sécurité, mais d'autres référentiels s'appliquent également selon les usages.*

Le Guide d'hygiène informatique

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) a élaboré un guide pour fournir un aperçu des bonnes pratiques de cybersécurité. Il concerne tous les acteurs travaillant sur des données sensibles et est conçu comme une **feuille de route** qui accompagne les **responsables de la sécurité des systèmes d'information**, dans tous les types d'entité.

Il présente **42 mesures essentielles pour assurer la sécurité du système d'information** et les moyens de les mettre en œuvre. Elles constituent le socle minimum à respecter pour protéger les informations de la structure.

Projet de recommandation pour la conformité et la sécurité du dossier patient informatisé (DPI)

À la suite de contrôles et de mises en demeure de plusieurs établissements de santé, la CNIL a élaboré **un document consolidant les règles applicables au DPI ainsi que ses recommandations juridiques et techniques.** Il était soumis à consultation publique jusqu'au 16 mai 2025.

Existe-t-il d'autres référentiels pour la cybersécurité des données de santé ?

Des **certifications techniques** et des **référentiels juridiques et technologiques** sont déjà en place depuis plusieurs années pour améliorer le niveau de cybersécurité en santé. Ils peuvent être propres aux données de santé ou plus généraux.

Certification HDS

Hébergement des données de santé, notamment dans le cadre de l'utilisation pour le soin

SecNumCloud

Référentiel édicté par l'ANSSI, fixant les exigences de sécurité et de souveraineté pour la conservation de données dans un cloud

ISO 27001

Norme internationale de référence en matière de cybersécurité et de sûreté des systèmes d'information

ISO 27701

Norme internationale qui décrit la gouvernance et les mesures de sécurité à mettre en place pour les traitements de données personnelles.

Référentiel sécurité SNDS

promulgué par le Ministère de la santé et de l'accès aux soins, il encadre strictement les recherches sur les données de santé issues du SNDS

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

PLAN Assurer la cybersécurité des données de santé pour la recherche

1. Qu’est-ce que qu’une donnée de santé ?
2. Les données de santé sont sensibles, leur traitement implique d’assurer leur protection
3. **Une démarche de cybersécurité encadrée par l’homologation**
4. Qu’en est-il de l’AIPD ?
5. Des ressources pour encadrer la cybersécurité

L’homologation des systèmes, à quoi ça sert ?

L’homologation implique une phase de définition de la stratégie, de maîtrise des risques, et de décision

Définition	Maîtrise des risques	Décision

• **Définir le référentiel réglementaire applicable**
• **Définir le périmètre à homologuer :**
  ○ Fonctionnel et organisationnel (fonctionnalités, utilisateurs, conditions d’emploi, procédures,…)
  ○ Technique (architecture, briques logicielles et matérielles)
  ○ Géographique et physique (localisation, caractéristiques des locaux)
• **Identifier les acteurs et les rôles**
• **Convenir des livrables et du planning**
	• **Conduire une analyse de risque** :
	  ○ Contexte, événements redoutés et scénarios de menace, étude des risques, étude des mesures de sécurité
	• **Mesurer les écarts entre les objectifs de sécurité et le réalisé sur la plateforme :**
	  ○ Audit technique (« test de pénétration »)
	  ○ Audit organisationnel
	• **Définir les mesures de sécurité additionnelles requises et/ou prendre acte des risques résiduels restant dans le cadre de l’homologation**
	• **Prévoir de mettre en place un plan d’action**
		• **Produire les pièces nécessaires à la prise de décision d’homologation :**
		  ○ Définir le périmètre d’homologation, les conditions accompagnant l’homologation, la durée de l’homologation et les conditions de suspension
		  ○ Produire les pièces du rapport d’homologation
		• **Obtenir de l’autorité d’homologation l’autorisation d’emploi :**
		  ○ En particulier, valider les risques résiduels mesurés à l’issue du chantier de maîtrise des risques

SORBONNE UNIVERSITÉ SN@SU Santé Numérique Sorbonne Université

L’homologation des systèmes, à quoi ça sert ?

Cette opération permet de **démontrer :**

- que **les risques cyber** vis-à-vis des **données personnelles de santé** susceptibles d’être exploitées ont été **clairement identifiés**
- que les **risques résiduels** sont pris en compte et **acceptables**.

Quelles mesures peuvent être déployées ?

- Sécuriser les **postes de travail**
- Gérer les **identités** et les **habilitations**
- Contrôler les **imports**, **exports, transferts** de données ou la localisation de leur hébergement
- Prévenir les **risques de réidentification ou de vol de données** et de **traitements illicites** via la sensibilisation, la traçabilité, la gestion des accès ou les audits

Comment savoir quelles mesures déployer dans mon cas ?

C’est justement à cela que servent les **référentiels de sécurité !**

- Par exemple, **le référentiel de sécurité du SNDS prévoit des obligations pesant sur plusieurs acteurs :**
  - **les utilisateurs** des systèmes mettant à disposition les données (signature de convention, ne pas mener une action visant à ré-identifier une personne etc.) ;
  - **les gestionnaires** de système qui mettent à disposition des données, les transmettent ou les reçoivent ;
  - **les administrateurs** de ces systèmes ;
  - **les sous-traitants** de ces gestionnaires
- C’est parfois des centaines d’exigences qui sont à appliquer, **une démarche de sécurité ne s’improvise pas !**

SORBONNE UNIVERSITÉ SN@SU Santé Numérique Sorbonne Université

PLAN Assurer la cybersécurité des données de santé pour la recherche

1. Qu’est-ce que qu’une donnée de santé ?
2. Les données de santé sont sensibles, leur traitement implique d’assurer leur protection
3. Une démarche de cybersécurité encadrée par l’homologation
4. Qu’en est-il de l’AIPD ?
5. Des ressources pour encadrer la cybersécurité

Quand faut-il réaliser une AIPD pour évaluer le risque sur les données ?

Conformément à l'**article 35 du RGPD,** une **AIPD (analyse d'impact relative à la protection des données) est obligatoire** lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, **notamment dans le cas de traitement de données sensibles (dont les données de santé).**

Analyse globale du projet

- Finalités légitimes
- Cadre juridique adéquat
- Information correcte des personnes concernées
- Cycle de vie de la donnée conforme

Analyse des risques techniques

- Protection de l'intégrité des données
- Protection des réseaux
- Sécurité des serveurs
- Maintenance adéquate
- Supervision technique constante

Analyse des risques organisationnels

- Encadrement de l'accès aux données par les équipes
- Mise en place de plans de sauvegarde
- Formation continue

Pourquoi c'est important ?

- Sans évaluation adéquate du risque, impossible de **déterminer les mesures à prendre pour protéger** les personnes concernées et leurs données. C'est pourquoi la réalisation d'une **AIPD est obligatoire** avant tout traitement portant sur des données de santé

- Au-delà de son caractère juridique, l'analyse d'impact **impose des orientations techniques, organisationnelles et de gouvernance,** structurantes pour l'organisme qui porte le projet de recherche

Qu’est-ce que démontre l’AIPD ?

Evaluation et minimisation du risque de survenue d’un événement indésirable
ET
des conséquences encourues par les personnes concernées en cas de survenue de cet événement

Risque d’accès illégitime aux données (par un tiers non autorisé)	Risque de modification non désirée des données	Risque de suppression non désirée des données

Et après, on en fait quoi ?

- ➔ Si l’AIPD montre que le niveau de **risque résiduel reste élevé** malgré les mesures prises, elle doit être **transmise à la CNIL** pour consultation.
  La CNIL peut alors formuler des recommandations, demander des garanties supplémentaires, voire émettre un avis défavorable si les risques demeurent trop importants.

- ➔ Si l’AIPD ne présente **pas de risques résiduels** élevés, il constitue un **point d’appui pour l’équipe** chargée de la mise en œuvre du projet.
  Sa consultation régulière permet d’assurer la bonne prise en compte des mesures de sécurité.

Exemple d’une mesure de sécurité classique : la pseudonymisation

La pseudonymisation, c'est quoi ?

Ces deux concepts très proches cachent deux réalités juridiques et techniques très différentes.

L'anonymisation

Il s'agit d'un traitement qui consiste à retirer suffisamment d'éléments pour que la personne concernée **ne puisse plus être identifiée**. Elle doit être **irréversible** et aussi permanente qu'un effacement.

Les questions à se poser pour l'anonymisation :

- Est-il possible d'**isoler** un individu ?
- Est-il possible de **lier au moins deux informations** se rapportant à la même personne ?
- Est-il possible de **déduire des valeurs** avec un degré de probabilité élevé à partir d'un ensemble d'autres informations ?

Si la réponse est positive à l'une de ces trois questions, il faut conduire une **analyse de risque de réidentification pour démontrer que ce risque est nul**

Conséquence : **Ce ne sont plus des données personnelles** et le cadre juridique de la protection des données n'est pas applicable.

La pseudonymisation

L'anonymisation totale des données fait souvent perdre leur intérêt pour la recherche (par exemple lorsqu'on agrège les données, on perd la capacité à analyser les trajectoires individuelles). En revanche, il n'est pas nécessaire de garder le lien entre l'individu et ses enregistrements de santé pour faire de la recherche, on cherche donc à pseudonymiser

Il s'agit d'un traitement dont le but est de rendre impossible l'attribution de données à une personne physique identifiée sans informations supplémentaires.

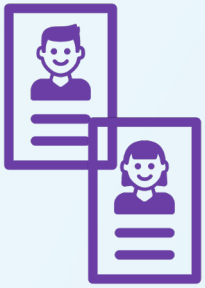
Une donnée pseudonymisée est une donnée indirectement identifiante. Prise isolément, elle ne permet pas d'identifier immédiatement la personne à qui appartiennent les informations, mais si elle est associée à d'autres données, il devient possible de retrouver son identité.

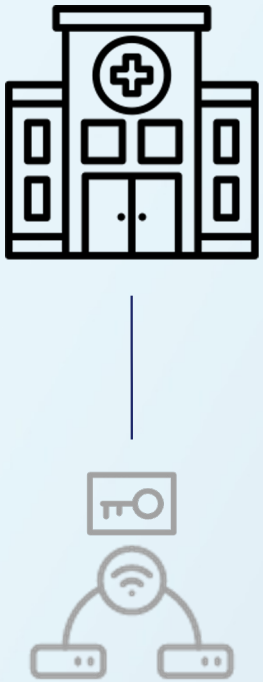
Conséquence : **Ce sont des données personnelles** et le cadre juridique de la protection des données s'applique.

Ex : un identifiant patient, un code…

La pseudonymisation, comment ça marche ?

1 Un hôpital tient des **fichiers patients** (Nom, Prénom, N° de sécurité sociale, Identifiant Patient Permanent ou IPP, description des actes...) avec lesquels les médecins peuvent retrouver les historiques médicaux de leurs patients.





2 L'hôpital définit un **code unique** pour chaque patient et retire toutes les informations directement identifiantes (ex : nom, prénom, adresse, numéro de sécurité sociale, IPP, etc.). Cela permet de **protéger la vie privée des patients** lors des analyses, tout en **permettant l'obtention d'informations complémentaires** auprès de l'hôpital et de lier les informations entre elles.

3 La base est alors enregistrée sur l'infrastructure de l'hôpital **sans donnée directement identifiante.**

Mais pourquoi "pseudo" ?
Simplement, parce que le code unique est un pseudonyme du patient. Ce n'est pas anonyme car, avec ce code, les médecins peuvent retrouver l'identité des patients de la base de données.

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

PLAN Assurer la cybersécurité des données de santé pour la recherche

1. Qu’est-ce que qu’une donnée de santé ?
2. Les données de santé sont sensibles, leur traitement implique d’assurer leur protection
3. Une démarche de cybersécurité encadrée par l’homologation
4. Qu’en est-il de l’AIPD ?
5. Des ressources pour encadrer la cybersécurité

Le RSSI, chef d'orchestre de la cybersécurité

1

Le **Responsable de la Sécurité du Système d'Information (RSSI)** occupe un poste central dans la protection cyber au sein d'une institution, notamment dans les établissements hospitaliers.
C'est un **spécialiste de la sécurité informatique et des réseaux**.

3

Le RSSI :
- audite et contrôle **la sécurité** en termes de **confidentialité, intégrité, disponibilité**
- contrôle l'application des **normes, standards et procédures** pour protéger les données et établir un environnement cyber conforme.

2

La mission du RSSI est de **concevoir et animer la démarche sécurité et confidentialité** des systèmes d'information (matériels, données et logiciels), en veillant à ce que les niveaux de sécurité et de confidentialité soient conformes à la réglementation externe et aux standards internes.

Il met notamment en œuvre les textes qui encadrent la cybersécurité en santé, comme par exemple :

- la **Politique de Sécurité des Systèmes d'Information pour les Ministères Chargés des Affaires Sociales (PSSI-MCAS)** ;
- la **Politique de Sécurité des Systèmes d'Information de Santé (PGSSI-S)**.

Votre établissement possède un RSSI, que vous pouvez consulter (lui ou son service) pour toute question ayant trait à la sécurité des réseaux, des systèmes informatiques et des données qu'ils hébergent.

SORBONNE UNIVERSITÉ

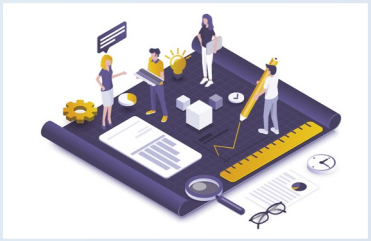
Le DPO, garant de la protection des données personnelles

1 Le correspondant informatique et liberté (aujourd'hui : **Délégué à la Protection des Données - DPO)** a été créé par la Loi informatique et libertés. En 2018, le RGPD l'a rendu **obligatoire** dans certains cas, notamment pour tout **établissement traitant des données de santé**.

DPO

2 Comme le RSSI, le DPO joue un rôle pivot dans la bonne mise en oeuvre des traitements de données :
- il **accompagne et conseille** les acteurs impliqués au sein de chaque service traitant des données
- il **contrôle** la bonne prise en compte du cadre légal et réglementaire

3 Le DPO assure le lien avec :
- les **personnes concernées** par le traitement
- les DPO des **partenaires** et des **sous-traitants**
- **l'autorité de contrôle** (la CNIL)



Votre établissement a forcément désigné un DPO : demandez ses coordonnées à votre administration centrale

DPO, RSSI, chef de projet, direction… : l'essentiel, c'est qu'ils se parlent ! La protection des données repose sur une vraie coordination entre tous les acteurs.

SORBONNE UNIVERSITÉ

SN@SU Santé Numérique Sorbonne Université

Informer les patients de l'utilisation de leurs données

Communiquer sur la réutilisation des données de santé est un enjeu important, mais comment informer efficacement l'ensemble des personnes concernées ?

Les personnes ont l'obligation d'être informées, **de façon individuelle et/ou collective** de la réutilisation possible de leurs données à des fins de recherche :

A travers des portails d'information

Certains établissements de santé ou organismes mettent également en place des **portails de transparence**, accessibles en ligne, permettant aux patients de consulter les projets utilisant leurs données, les finalités, les durées de conservation, et leurs droits (notamment le droit d'opposition).

ET

Par le biais d'affiches dans les locaux et/ou via des documents remis.

L'exemple d'une campagne de sensibilisation

Initialement affichés au CHU de Rouen Normandie, deux affiches de sensibilisation à la seconde vie des données ont été conçus grâce à des ateliers participatifs, rassemblant citoyens et experts. Elles sont aujourd'hui téléchargeables et accessibles à tous.

Des affiches réalisées en partenariat avec....

Des affiches qui peuvent par exemple constituer des outils pour les entrepôts de données de santé qui souhaitent contribuer à une meilleure information.

A quoi sert le répertoire des projets du Health Data Hub ?

Pour **consigner une trace de tous les projets** portant sur des données de santé, le HDH entretient un répertoire des projets de recherche sur des données de santé.

Tout responsable de projet utilisant des données de santé à l'obligation de soumettre à ce répertoire public, **AVANT la mise en œuvre**, les informations essentielles sur son traitement de données :
- la **nature et les caractéristiques de la recherche** envisagée,
- sa **finalité détaillée**,
- le **type de procédure réglementaire** sollicitée (autorisation CNIL, méthodologie de référence, etc.),
- la **méthode utilisée** pour la recherche,
- les **résultats enregistrés** par l'équipe projet.

Consultation tous publics sur :
https://www.health-data-hub.fr/projets

Et à quoi ça sert, tout ça ?

1. A répondre à l'**obligation de transparence** des projets mobilisant des données de santé

2. A apporter aux citoyens des **garanties sur la bonne utilisation** de leur données

3. A permettre à ces derniers de **suivre les évolutions de la recherche**

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

CPP & CESREES, qui fait quoi ?

Tout projet de recherche impliquant la personne humaine (RIPH) et des données du SNDS doit soumettre son protocole à un des 39 **Comités de Protection des Personnes (CPP)**, tiré au sort (la compétence des CPP n'est pas régionale).

Les projets non RIPH (portant uniquement sur les données du SNDS) doivent soumettre leur protocole au **Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES)**.

Les CPP s'assurent que les **projets RIPH** respectent des normes médicales, scientifiques, éthiques et juridiques. Ils sont composés de professionnels de la recherche, des Sciences Humaines et Sociales, de spécialistes de l'Ethique et de représentants des usagers (RU)

Le CESREES prend la place du CPP pour délivrer l'avis sur les **projets RNIPH.** Il est constitué de 20 membres dont 2 représentants des usagers du système de santé (RU)

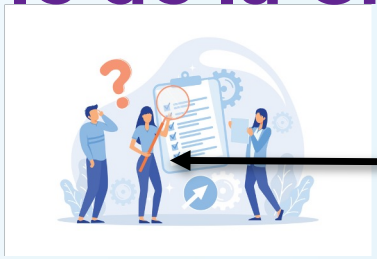
Les CPP ou le CESREES :

Rendent un **avis :**

- ➔ **impératif** et motivé,
- ➔ fondé sur une **"analyse collective pluridisciplinaire"**,
- ➔ incluant le cas échéant des **recommandations d'amélioration** pour un nouvel examen du projet,
- ➔ sur **plus de 5000 projets par an** (environ 300 pour le CESREES et 150 pour chaque CPP).

SORBONNE UNIVERSITÉ SN@SU Santé Numérique Sorbonne Université

Le rôle de la CNIL



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La mission de la **Commission Nationale Informatique et Liberté (CNIL)** est de **protéger les droits des personnes** sur leurs données, d'**accompagner la conformité** des traitements, de **conseiller les écosystèmes d'innovation**, de **contrôler et sanctionner les organismes** responsables de traitements.

Informe les personnes concernées sur les droits et mène des **actions de communication** grand public, notamment **sur les données de santé**

Dispose d'un **Service Santé** dédié, animé par des experts techniques et juridiques : **conseille, oriente et accompagne les projets** de recherche et les professionnels

Contrôle la **bonne mise en œuvre de la loi** dans les projets et sanctionne les manquements constatés

La CNIL analyse les **conditions de mise en œuvre des traitements de données de santé** afin de garantir leur sécurité et leur confidentialité, notamment **après avis du CPP ou du CESREES.**

Pour les projets de recherche, elle est **la seule autorité compétente pour autoriser l'accès aux données de santé, sauf lorsque le traitement est conforme à un référentiel préalablement approuvé** (comme les référentiels MR de la CNIL), auquel cas une déclaration de conformité suffit.

SORBONNE UNIVERSITÉ
SN@SU Santé Numérique Sorbonne Université

Qu'est-ce que l'engagement citoyen du Health Data Hub ?

Pour ajouter un **cadre éthique** aux garanties de sécurité juridiques et techniques, le HDH s'engage auprès des citoyens autour de **quatre axes majeurs**

1. L'intérêt général : des **comités éthiques indépendants** (le CESREES, dont le HDH assure le secrétariat, ou les CPP) valident le caractère d'intérêt général des projets. Toute utilisation de données de santé à des fins commerciales ou conduisant à l'exclusion de personnes d'une garantie est exclue.

2. La protection des données : **pseudonymisation des données** collectées par le HDH, pas de données en accès libre, **sécurité de la plateforme** maintenue au plus haut niveau possible, formation des utilisateurs.

3. Le respect des droits individuels : application stricte du **cadre légal** et réglementaire, **information claire** et directement compréhensible à travers le site internet, **appui aux personnes** concernées dans leurs démarches.

4. La transparence : information complète et à jour sur les bases, **répertoire des projets** public, **communication** régulière et adaptée.

SORBONNE UNIVERSITÉ SN@SU Santé Numérique Sorbonne Université

*Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre **de France 2030** portant la référence ANR-23-CMAS-0001*