

Données de santé : droits d'usage

Congrès SFIL – Montpellier – 28 mars 2019

Erik Boucher de Crèvecœur - Ingénieur expert à la CNIL

La notion de données de santé

Article 4 du RGPD

« données 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** »

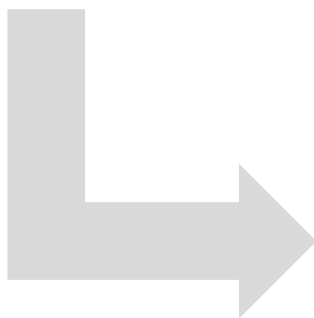
Pour vous aider, voir la fiche pratique [« Qu'est ce qu'une donnée de santé ? »](#)

Le principe : l'interdiction de traiter des données de santé



Interdiction de traiter des données relatives à la santé

- **article 9-I du RGPD**
- **article 8-I de la loi I&L**



Pour traiter des données de santé, il faut justifier de l'une des **exceptions** de l'article 9.2 du RGPD

Attention ! Ne pas confondre ces exceptions avec la **base légale** du traitement (article 6 RGPD).

Les exceptions à ce principe d'interdiction (article 9.2 RGPD)

- (...)
- **Médecine préventive, médecine du travail, diagnostics médicaux**, prise en charge sanitaire ou sociale ou **gestion des systèmes et services de soins en santé**
- (...)
- **Motifs d'intérêt public** dans le domaine de la **santé publique**
- **Recherche scientifique**, fins archivistiques ou statistiques



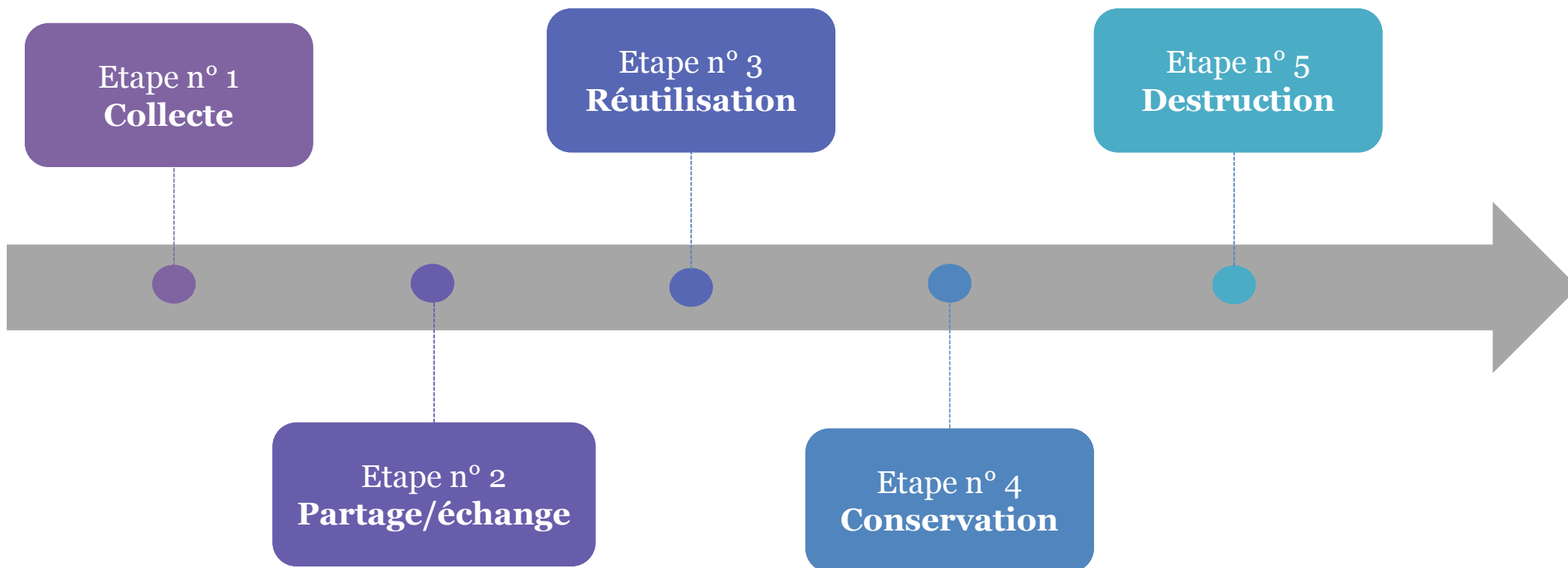
Article 8-II-8 LIL : traitements comportant des données concernant la santé justifiés par **l'intérêt public** et conformes aux dispositions du **chapitre IX LIL**



Droit d'usage des données de santé

LES TRAITEMENTS DE DONNÉES DE SANTÉ DANS UN LABORATOIRE DE BIOLOGIE MÉDICALE

Le parcours de la donnée de santé



Etape n° 1 : la collecte de la donnée de santé

Etape n° 1
Collecte

A diagram illustrating the first step of a process. It features a long, horizontal grey arrow pointing to the right. A purple rounded rectangle callout box is positioned above the arrow, containing the text 'Etape n° 1' and 'Collecte'. A vertical dashed line connects the bottom of the callout box to a small purple circle on the top edge of the arrow.

Etape n° 1 : la collecte de la donnée de santé

La prise en charge médicale du patient génère la **production** de **données de santé à caractère personnel** concernant ce patient.

3 catégories de données de santé

Données de santé **par nature**

Données de santé du fait d'un **croisement avec d'autres données**

Données de santé du fait de **l'utilisation des données**

Etape n° 1 : la collecte de la donnée de santé

Check-list des points à vérifier



Code de la santé publique (identifiant national de santé, référentiels de sécurité, HDS, ...).

- 1) Quelle est la **finalité** du traitement ?
- 2) Cette finalité est-elle **déterminée, explicite et légitime** ?
- 3) Quelle est la **base légale du traitement** ?
- 4) A quel titre puis-je **déroger au principe d'interdiction de la collecte des données de santé** ?
- 5) Les données collectées sont-elles **adéquates, pertinentes et nécessaires** au regard de la finalité du traitement ?
- 6) Les données collectées sont-elles **exactes et mises à jour** ?
- 7) Le patient est-il **informé** au moment de la collecte ?
- 8) La **durée de conservation** des données est-elle adaptée à la finalité du traitement ?
- 9) Des **mesures de sécurité** sont-elles mises en place pour garantir l'intégrité et la confidentialité des données ?

Etape n° 2 : le partage et l'échange de la donnée de santé



Etape n°2 : le partage et l'échange de la donnée de santé

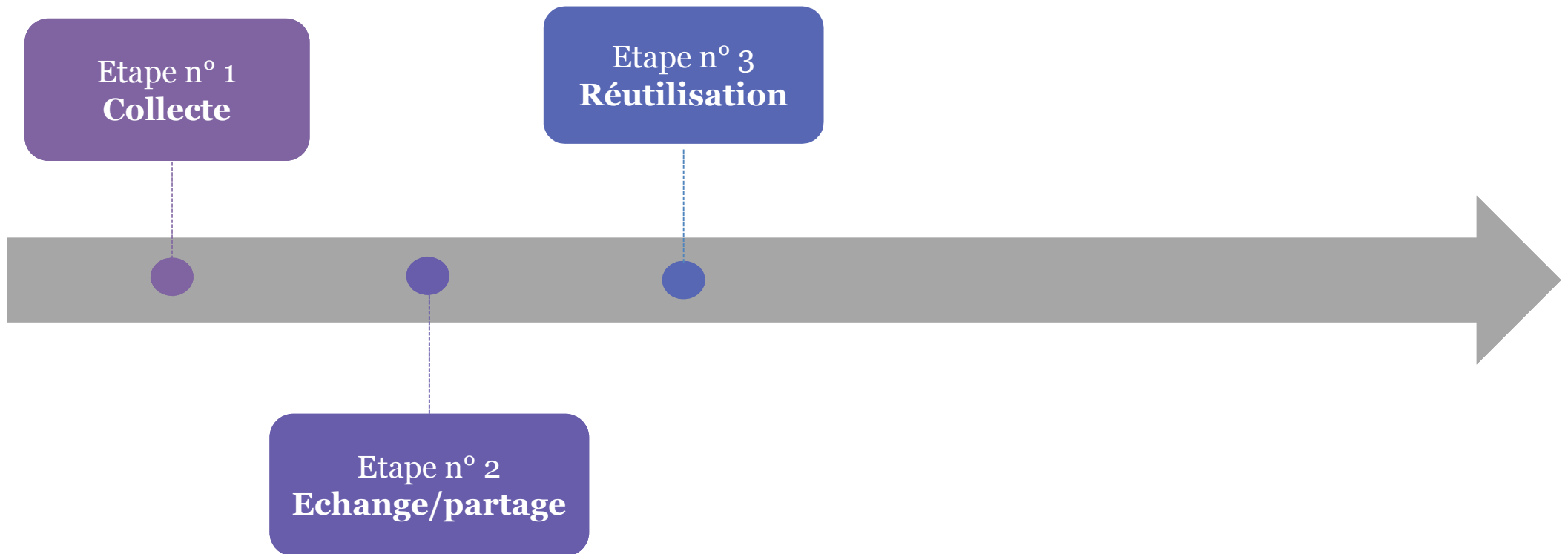
Check-list des points à vérifier



Code de la santé publique (dossier médical partagé, dossier pharmaceutique, ...).

- 1) Le patient est-il bien **informé** en amont du partage/de l'échange de ses données ?
- 2) Ce partage intervient-il dans le cadre de **l'équipe de soins** ou **en dehors de celle-ci** ?
- 3) Le partage / l'échange des données est-il **licite** ?
- 4) Les personnes sont-elles bien **autorisées à accéder** aux données de santé du patient ?
- 5) Une procédure de **gestion des habilitations et des accès** est-elle mise en place ?
- 6) Les professionnels de santé utilisent-ils la **messagerie sécurisée** pour échanger entre eux ?

Etape n°3 : la réutilisation de la donnée de santé



Etape n°3 : la réutilisation de la donnée de santé

Motifs d'intérêt public dans le domaine de la santé publique (entrepôts, vigilances)

Recherche scientifique : recherche, étude ou évaluation dans le domaine de la santé

Études non interventionnelles de performances des DM DIV (MR-002)

Les entrepôts de données

- Bases de données de santé constituées et utilisées dans l'**intérêt public**, principalement à des fins de recherches ultérieures, avec les enjeux du respect des droits des personnes et des finalités.
- Doctrine de la CNIL :
 - Délibération du 19/01/2017 autorisant la mise en œuvre de l'entrepôt de données de santé (EDS) de l'AP-HP
 - Fixe le cadre applicable pour la création de ce type d'entrepôt
 - Délibérations IQVia, OpenHealth (Entrepôts privés, 2017)
 - Délibération CHU Nantes (EHOP) du 19 juillet 2018

Les entrepôts de données

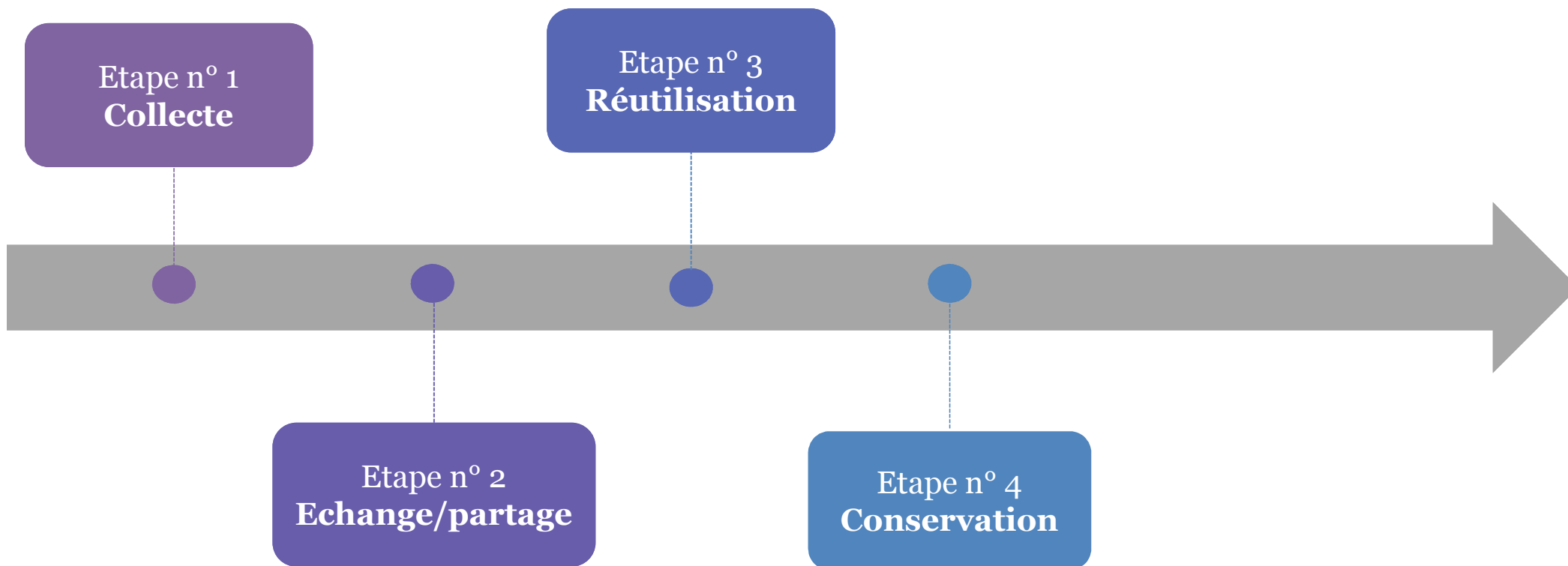
- ◊ Gouvernance par un **comité scientifique et éthique chargé** :
 - ◊ d'évaluer les projets de recherche
 - notamment de vérifier leur **caractère d'intérêt public**
 - ◊ de donner les autorisations d'accès aux données de l'entrepôt
- ◊ Principes RGPD à intégrer, notamment « privacy by design » :
 - ◊ Accès de l'entrepôt à une équipe restreinte et dédiée
 - ◊ Profils d'habilitation avec différents niveaux d'accès
 - ◊ Pseudonymisation / anonymisation
 - ◊ Limitation des extractions de données
 - ◊ Traçabilité et surveillance

Anonymisation et pseudonymisation

- Un **processus d'anonymisation est un traitement de données** à caractère personnel (soumis aux obligations). Il implique un **appauvrissement** des données brutes et une **restriction** du champ des exploitations possibles.
- Une donnée anonyme (selon les critères du G29) **n'est plus** une donnée à caractère personnel. Elle peut être diffusée et utilisée largement (Recherche, Open data).
- **Pseudonymiser** un jeu de données protège la vie privée (dé-identification) mais cela ne le rend **pas anonyme**. Il permet le **chaînage et l'appariement des données personnelles d'un individu**.



Etape n°4 : la conservation de la donnée de santé



Etape n°4 : la conservation de la donnée de santé

En
interne

Conservation au moyen des systèmes d'information conformes aux **référentiels d'interopérabilité et de sécurité élaborés par l'ASIP Santé**

Art. L. 1110-4-1 CSP



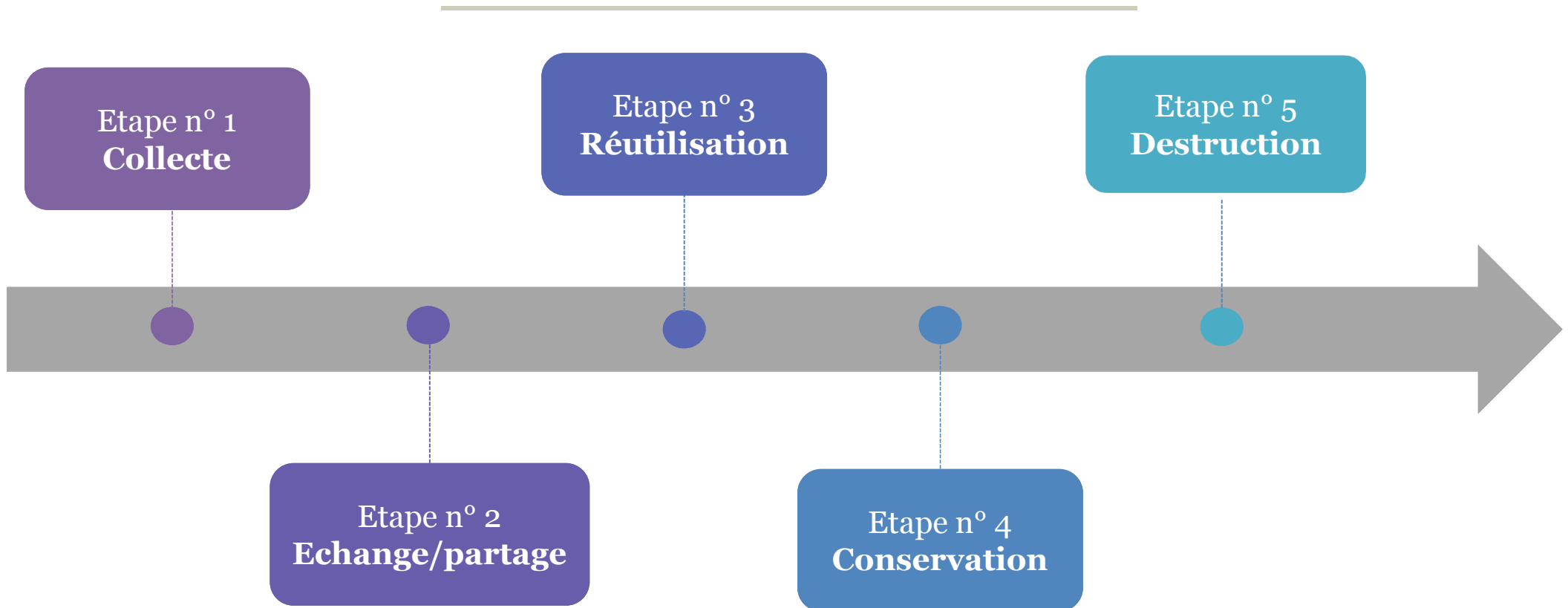
En
externe

En cas d'externalisation de l'hébergement des dossiers médicaux : recours à un **hébergeur agréé/certifié**

Article L. 1111-8 CSP



Etape n°5 : la destruction de la donnée de santé



Etape n°5 : la destruction de la donnée de santé

Durée

Destruction à l'issue des délais de conservation : **20 ans** à compter de la date du dernier séjour ou de la dernière consultation du patient dans l'établissement ; **30 ans** pour les examens génétiques et transfusion

Cas spécifiques :

Durée prolongée jusqu'au 28^{ème} anniversaire du patient mineur ;

Durée réduite à 10 ans à compter de la date du décès du patient si celui-ci décède moins de 10 ans après son dernier passage dans l'établissement;

Délais suspendus par tout recours tendant à mettre en cause la responsabilité de l'établissement ou du professionnel de santé.

Modalités

Conservation **5 ans en base de production**

Puis **archivage automatique** dans une base distincte à accès limité

Puis **purge** automatique ou manuelle des données ayant atteint leur durée de conservation



Exception possible pour des raisons d'intérêt scientifique, statistique ou historique.

Les outils pour vous accompagner

Méthodologie de référence MR-002

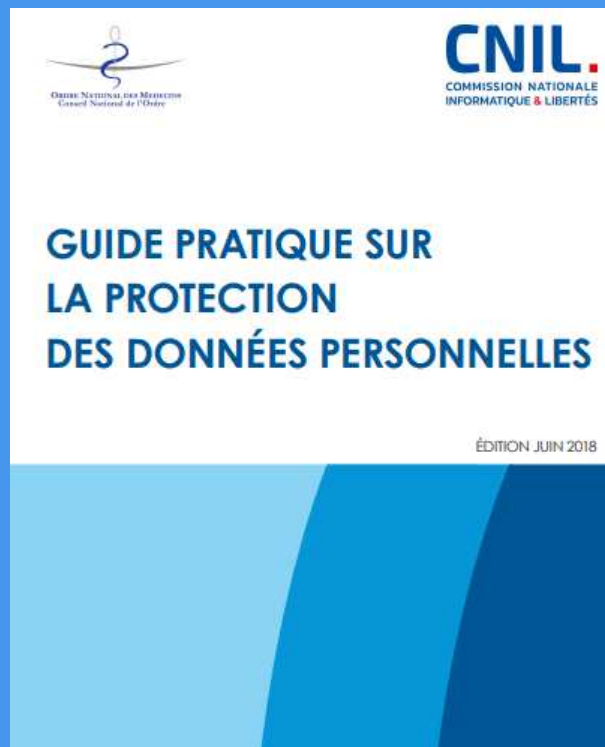
Études non interventionnelles de performances concernant les dispositifs médicaux de diagnostic in vitro

La méthodologie de référence MR-002 concerne les études non interventionnelles de performances menées sur les dispositifs médicaux in vitro (DM DIV) en vue de leur mise sur le marché.

Sont exclues du champ de cette méthodologie de référence les recherches biomédicales, les études faisant apparaître l'identité complète des personnes participant à l'étude, les études épidémiologiques, les études en génétique ayant pour objet d'identifier les personnes par leurs caractéristiques génétiques.

TEXTE OFFICIEL

Délibération n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic ...

The image is a screenshot of a web application interface titled 'Captoo'. It displays a checklist for 'Principes fondamentaux' (Fundamental Principles) and 'Risques' (Risks). The 'Principes fondamentaux' section includes 'Proportionnalité et nécessité' (checked) and 'Mesures protectrices des droits' (checked). The 'Risques' section includes 'Mesures existantes ou prévues' (checked), 'Accès illégitime aux données' (checked), 'Modifications de données' (checked), 'Disparition de données' (checked), and 'Vue d'ensemble des risques' (checked). Below the checklist is a 'VALIDATION DU PIA' section with a 'Plan d'action' and 'Cartographie des risques', and a 'Valider le PIA' button. At the bottom, there is a 'PIECES JOINTES' section with a file named 'Admin_serveur.pdf' and an 'Ajouter' button. On the right side, there are three text input fields with prompts: 'Quelles sont les finalités de la collecte et l'utilisation des données par le service?', 'Comment les données sont-elles minimisées?', and 'Qui sont les destinataires des données?'. The top right corner shows 'Principes fondamentaux PROPORTIONNALITE ET NECESSITE' and a 'Speech' icon.

Merci de votre attention 😊

Dossiers complets sur notre site :
www.cnil.fr/fr/sante