

Enfant, handicaps et santé numérique Perspectives et applications pratiques

Santé numérique au XXI^{ème} siècle : comment protéger les données
personnelles ?

Stéphanie SAULNIER, Juriste, service de la santé, CNIL



Santé numérique au XXIème siècle : comment protéger les données personnelles ?

- 1. QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?**
- 2. QUELS SONT LES USAGES DES DONNÉES À CARACTÈRE PERSONNEL DANS LE DOMAINE DE LA SANTÉ ?**
- 3. QUELS SONT LES ENJEUX ?**
- 4. DANS CE CONTEXTE, COMMENT PROTÉGER LES DONNÉES DE SANTÉ ?**

Santé numérique au XXIème siècle : comment protéger les données personnelles ?

1. QU'EST-CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

Qu'est-ce qu'une donnée à caractère personnel ?



- **Données directement identifiantes :**
nom et prénom,
photo...
- **Données indirectement identifiantes :**
NIR / INS...
- **Recoupements d'informations :**
« le fils aîné du notaire
habitant au 11 bd
Raspail à Paris ayant
été hospitalisé dans le
service de cardiologie
du centre hospitalier
de... »

Santé numérique au XXIème siècle : comment protéger les données personnelles ?

2. QUELS SONT LES USAGES DES DONNÉES À CARACTÈRE PERSONNEL DANS LE DOMAINE DE LA SANTÉ ?

Quels sont les usages des données à caractère personnel dans le domaine de la santé ?

- **Améliorer la prise en charge du patient : outil d'aide au diagnostic**
 - Système permettant de lire un scanner ou un électrocardiogramme ou de repérer des anomalies
 - Test génomique où le sang est envoyé à un laboratoire qui le passe dans un séquenceur pour livrer un profil génomique
 - Programme de diagnostic
- **Développer la médecine prédictive**
 - Outils permettant de repérer des altérations et mutations de l'ADN, des prédispositions à certains cancers, maladies cardiaques ou métaboliques

Quels sont les usages des données à caractère personnel dans le domaine de la santé ?

- **Faciliter la recherche scientifique**
 - **Optimisation des essais cliniques grâce à une automatisation de la sélection des patients**
- **Améliorer la détection du risque sanitaire**
- ...

Santé numérique au XXIème siècle : comment protéger les données personnelles ?

3. QUELS SONT LES ENJEUX ?

Quels sont les enjeux ?

- **Quels impacts économiques ?**
 - **Création de nouveaux dispositifs**
 - **Automatisation de certaines tâches et des prises en charge médicale**
- **Jusqu'où aller dans la délégation de la prise de décision médicale, de l'homme à la machine ?**
 - **Réflexions du CNOM : seul l'homme est capable de transgression ; un patient ne se résume pas à une quantité de données (importance du colloque singulier, aspect psychologique notamment)**

Quels sont les enjeux ?

- **N'y a-t-il pas des risques de discrimination, d'exclusion ?**
- **Quelles données utiliser pour alimenter un algorithme ?**
- **Quel équilibre trouver entre les perspectives innovantes en santé et le respect de la vie privée ?**

Quels sont les enjeux ?

- **Et surtout ne pas oublier...**

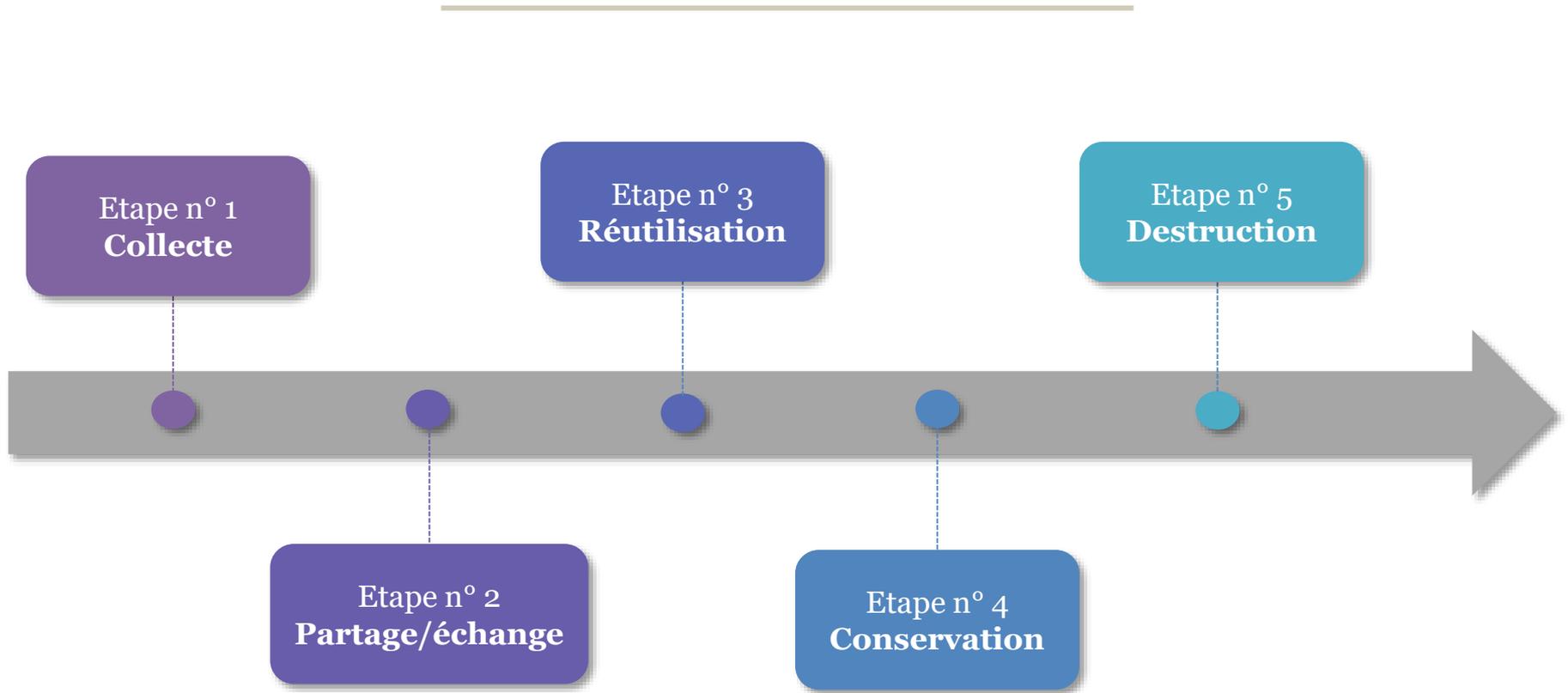
« L'informatique doit rester au service de chaque citoyen (...). Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi » (art. 1^{er} de la loi « Informatique et Libertés »)

Santé numérique au XXIème siècle : comment protéger les données personnelles ?

4. DANS CE CONTEXTE, COMMENT PROTÉGER LES DONNÉES DE SANTÉ ?

Dans ce contexte, comment protéger les données de santé ?



Dans ce contexte, comment protéger les données de santé ?



Etape n° 1
Collecte

Dans ce contexte, comment protéger les données de santé ?

Etape n° 1 : la collecte des données 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**

Dans ce contexte, comment protéger les données de santé ?

Etape n° 1 : la collecte des données de santé

Exemples de traitements de données de santé à caractère personnel

- Base de données PMSI de l'établissement de santé
- Dossier patient
- Utilisation d'un dispositif de téléexpertise
- PACS d'imagerie médicale
- Tableaux utilisés par des médecins pour réaliser des recherches
- Etc.

Dans ce contexte, comment protéger les données de santé ?

Etape n° 1 : la collecte des données de santé

Check-list des questions à se poser

- 1) Quelle est la **finalité** du traitement ?
- 2) Cette finalité est-elle **déterminé, 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 ?

Dans ce contexte, comment protéger les données de santé ?

Etape n° 1 : la collecte des données de santé

Check-list des questions à se poser



Toutes les questions
résultant de
l'application des
dispositions du code
de la santé publique
(identifiant national de
santé, référentiels de
sécurité, HDS, ...).

Dans ce contexte, comment protéger les données de santé ?



Dans ce contexte, comment protéger les données de santé ?

Etape n° 2 : l'échange et le partage des données de santé

Check-list des questions à se poser

- 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 ?

Dans ce contexte, comment protéger les données de santé ?

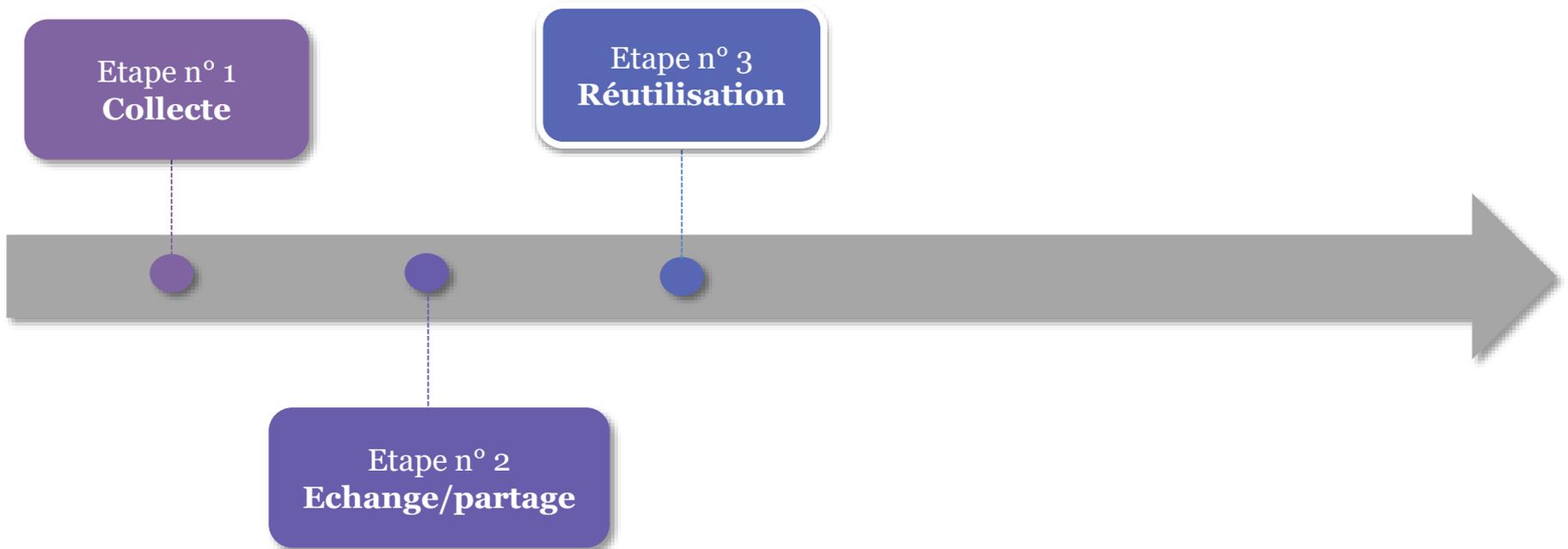
Etape n° 2 : l'échange et le partage des données de santé

Check-list des questions à se poser



Toutes les questions
résultant de
l'application des
dispositions du code de
la santé publique
(dossier médical partagé,
dossier pharmaceutique...).

Dans ce contexte, comment protéger les données de santé ?



Dans ce contexte, comment protéger les données de santé ?

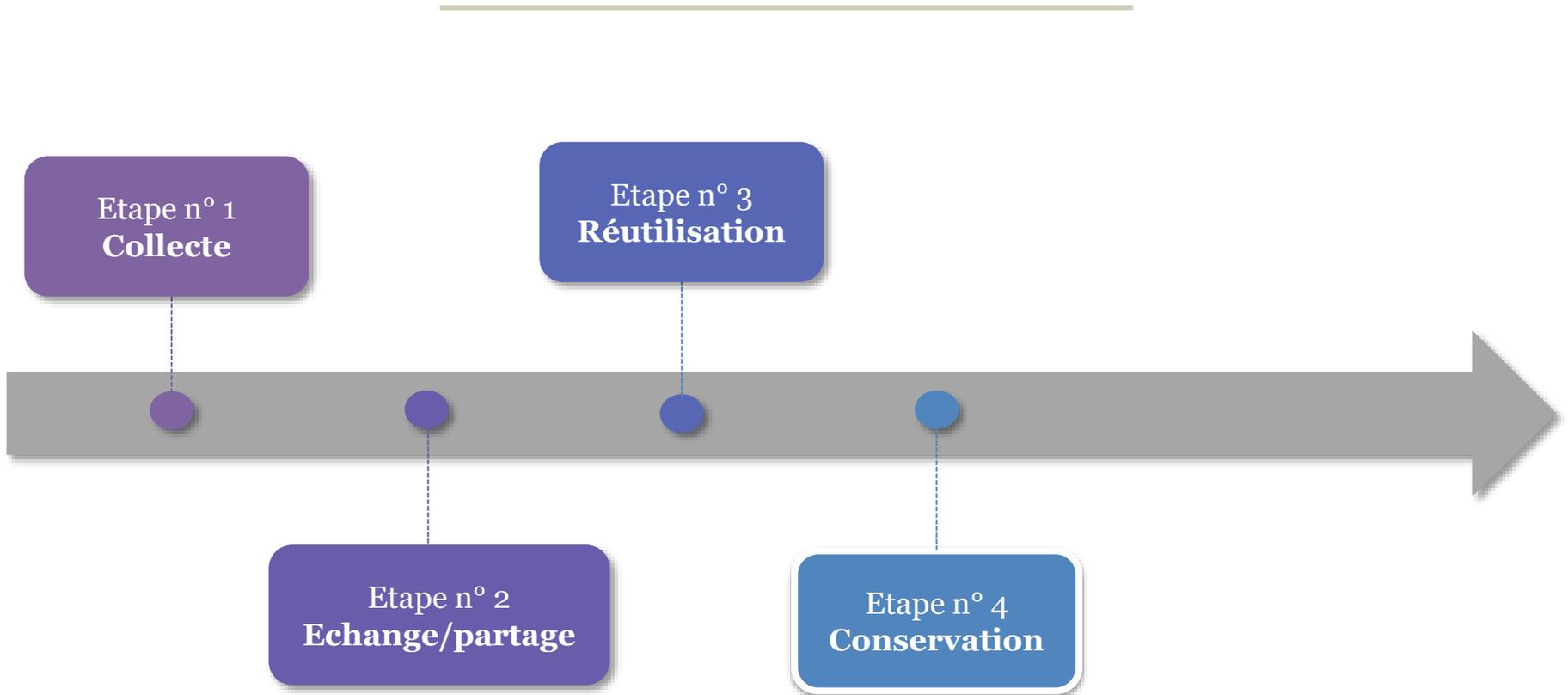
Etape n° 3 : la réutilisation des données de santé

La constitution des
entrepôts à des fins
de recherche
ultérieure

La réutilisation des
données de santé à
des fins de recherche
(intérêt public)

Focus sur des
éléments de doctrine
de la CNIL

Dans ce contexte, comment protéger les données de santé ?



Dans ce contexte, comment protéger les données de santé ?

Etape n° 4 : la conservation des données 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



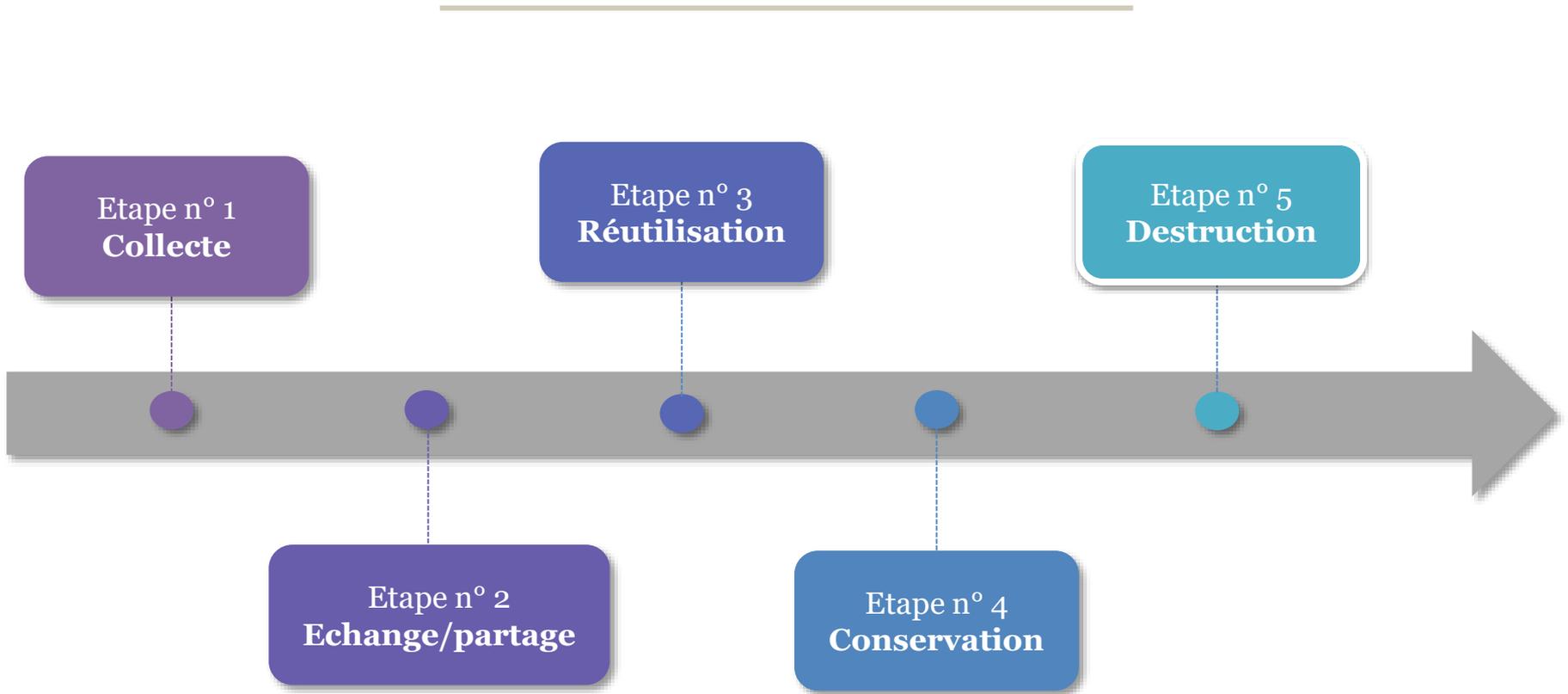
En
externe

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

Article L. 1111-8 CSP



Dans ce contexte, comment protéger les données de santé ?



Dans ce contexte, comment protéger les données de santé ?

Etape n° 5 : la destruction des données de santé

La réglementation applicable dans les établissements 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
Art. R.1112-7 CSP

Cas spécifiques :

Durée prolongée jusqu'au 28^{ème} anniversaire du patient mineur si elle s'achève avant cette date ;

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

La décision d'élimination est prise par le directeur de l'hôpital ou du groupe hospitalier **après avis** du médecin responsable de l'information médicale (DIM).

+

Obtention d'un **visa** de l'administration des archives



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

Dans ce contexte, comment protéger les données de santé ?

Les outils pour vous aider



Merci de votre attention !