



MINISTÈRE
DU TRAVAIL, DE LA SANTÉ,
DES SOLIDARITÉS
ET DES FAMILLES

*Liberté
Égalité
Fraternité*

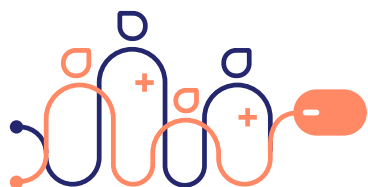
Délégation
au numérique
en santé

COMITÉ CITOYEN

SAISON 03

OCT / NOV

2024



COMITÉS
CITOYENS
DU NUMÉRIQUE
EN SANTÉ

DESSINONS ENSEMBLE
LA SANTÉ DE DEMAIN

ÉDITO

P. 3

LES MEMBRES DU COMITÉ CITOYEN

P. 4

INTRODUCTION

P. 5

RÉCAPITULATIF DES PROPOSITIONS

P. 6

01

LES DONNÉES DE SANTÉ ET LEURS USAGES

P. 11

02

CE QUE NOUS COMPRENONS DE L'UTILISATION DES DONNÉES DE SANTÉ ET L'INTÉRÊT QUE CELA REPRÉSENTE

P. 13

Utilisation primaire
des données de santé

–

Utilisation secondaire
des données de santé

03

CE QUE NOUS COMPRENONS DU RÈGLEMENT EUROPÉEN CONCERNANT LES DONNÉES DE SANTÉ

P. 16

Usage primaire
de la data

–

Usage secondaire
de la data

04

LES RISQUES QUE NOUS IDENTIFIONS CONCERNANT LES DONNÉES DE SANTÉ, NOTAMMENT EN CE QUI CONCERNE LEUR UTILISATION, ET LES QUESTIONS ÉTHIQUES.

P. 18

Utilisation primaire
des données de santé

–

Utilisation secondaire
des données de santé

05

PROPOSITIONS POUR MINIMISER LES RISQUES IDENTIFIÉS CONCERNANT LES DONNÉES DE SANTÉ

P. 21

Maîtrise technologique
et souveraineté

–

Sécurité et contrôle des
entreprises gestionnaires

–

Outils et méthodes pour
le contrôle et la sécurisation
des données de santé
à différentes échelles

06

LA NÉCESSITÉ D'UNE INFORMATION FACILE À COMPRENDRE, TRANSPARENTE ET ACCESSIBLE À TOUTES ET TOUS

P. 25

Diffusion et sensibilisation

–

Confiance, pédagogie,
transparence, éducation, ...

–

Garantir la transparence
de l'information

–

Mesurer le niveau
d'information des
personnes pour garantir
l'éthique de l'opt-out

07

L'ENJEU D'UN DISPOSITIF SIMPLE ET ERGONOMIQUE PERMETTANT À CHAQUE PERSONNE DE DÉCIDER DE L'USAGE PAR DES TIERS DE SES DONNÉES DE SANTÉ

P. 29

08

LE RÔLE DES CITOYENS DANS LA GOUVERNANCE FONCTIONNELLE ET DANS LA DÉFINITION DE L'ÉTHIQUE DE L'UTILISATION DES DONNÉES DE SANTÉ

P. 31

À l'échelle locale

–

À l'échelle française

–

À l'échelle européenne

09

LA QUESTION DE L'ENVIRONNEMENT, DE L'UTILISATION DES RESSOURCES ET DE LA CONSOMMATION D'ÉNERGIES ASSOCIÉE À LA GESTION DES DONNÉES DE SANTÉ

P. 34

Les différents impacts
écologiques du cycle
de vie des données de santé

–

Nos recommandations
pour limiter l'impact écologique
des données de santé

LE PROCESSUS DE DÉLIBÉRATION

P. 37

LES MEMBRES DU COMITÉ CITOYEN, SAISON 3

P. 38



La saison 3 du comité citoyen vient de s'achever avec une nouvelle fois un avis riche et éclairant !

Depuis 2019, la délégation au numérique en santé donne la parole aux citoyens pour construire un numérique en santé qui nous ressemble, qui réponde à nos espoirs et à nos exigences.

Pendant 3 mois, des citoyens tirés au sort, venant des 4 coins de la France sont investis d'une mission : répondre ensemble à une question de fonds sur le numérique en santé. À l'issue de cette expérience de démocratie participative, animée par une méthodologie robuste, leurs travaux sont autant de recommandation pour améliorer la politique publique que nous menons.

Avec engagement, nous suivons ces recommandations comme une véritable boussole dans nos actions. 78 % des recommandations issues du comité citoyen réuni en 2021 ont été mise en œuvre par les pouvoirs publics. Ces recommandations portaient sur Mon espace santé et continuent d'alimenter les évolutions du service ou son cadre juridique.

L'année précédente le comité citoyen s'est penché sur la question de la prévention et du numérique. Un an plus tard, plus de la moitié des recommandations ont déjà été mises en œuvre.

**HELA
GHARIANI**

**DAVID
SAINATI**

Cette année, le comité citoyen composé de 29 membres s'est prononcé sur la question suivante :

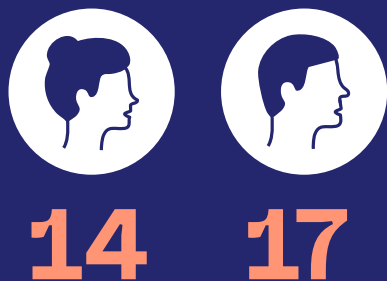
« Dans le cadre de la transcription en droit français du règlement européen sur les données de santé, quelles sont les règles et les conditions de mise en œuvre propres à la France qui permettront une bonne utilisation de ces données tout en générant la confiance des citoyens ? »

Le règlement européen sur données de santé va largement transformer les règles qui s'appliquent à l'usage des données de santé, dans le contexte du soin ou de la recherche. Au moment de traduire des décisions prises à Bruxelles dans le quotidien des français, il nous a paru essentiel d'associer des citoyens à la transposition d'un texte européen qui porte sur nos données les plus sensibles. Des experts français et européens ont été associés dans une démarche de pédagogie et de vulgarisation pour donner aux citoyens participants les clés de compréhension du règlement et de ses impacts. Ainsi, ils ont pu se familiariser avec le règlement et préciser les valeurs fondamentales à respecter pour l'appliquer en France.

À l'issue de trois weekends de travail, les citoyens ont produit 52 recommandations qui vont inspirer le futur cadre national sur l'usage des données de santé.

LES MEMBRES DU COMITÉ CITOYEN SAISON 3

GENRE



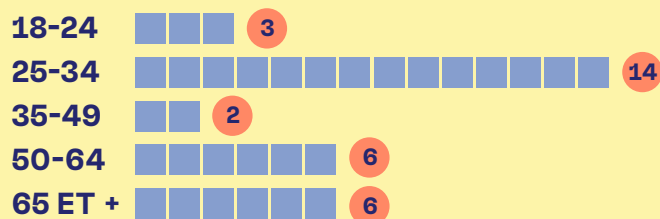
RÉGIONS



CATÉGORIES SOCIO- PROFESSIONNELLES



ÂGE



LIEU D'HABITATION



INTRO- DUCTION

Dans l'objectif commun de garantir une certaine sécurité numérique dans la santé, la Délégation au numérique en santé (DNS) a réuni un Comité citoyen composé de 30 personnes représentatives du territoire français. Nos débats ont été animés par le cabinet de conseil Res publica.

Durant 3 week-ends du mois d'octobre et de novembre 2024, le Comité s'est réuni pour échanger sur la question suivante : **Dans le cadre de l'intégration dans le droit français du règlement européen sur les données de santé, quelles sont les règles et conditions de mise en œuvre propres à la France qui permettront une bonne utilisation de ces données tout en générant la confiance des citoyens ?**

Après avoir assisté aux présentations des responsables de la Délégation ministérielle du numérique en santé, de représentants des professionnels de santé, d'experts en sécurité informatique et en protection des données personnelles, de spécialistes de l'éthique, de représentants d'entreprises de la e-santé (notamment des start-ups) ou de laboratoires pharmaceutiques ainsi que d'associations de patients et de représentants d'autres pays de l'Union européenne (Allemagne, Belgique, Estonie, Finlande), nous avons conduit une réflexion approfondie et collective sur le sujet.

À l'issue de ces interventions agrémentées par des périodes d'échanges et de débats, le comité citoyen a réussi à dégager un plan de travail composé de plusieurs thématiques. Différents axes de réflexions ont permis de synthétiser la volonté citoyenne vis-à-vis de la marge de manœuvre possible dans la transcription du droit européen en France afin de garantir au mieux la protection des données en santé.

Ce travail s'est d'abord fait autour de la notion même des données de santé en commençant par une analyse de leur nature, de leur utilité, et de leurs usages primaires et secondaires dans les contextes français et européen. L'objectif est de mettre en lumière leur rôle central dans les avancées médicales et la recherche, tout en interrogeant les règles actuelles qui encadrent leur utilisation.

Chaque partie de cette réflexion s'accompagne d'une analyse critique et de recommandations concrètes, avec un focus sur le règlement européen, ses avancées et les risques qu'il soulève en matière d'éthique, de sécurité et de stockage. Nous nous interrogeons également sur la capacité de renforcer la protection et le contrôle des données, tout en proposant des pistes d'amélioration pour répondre aux défis identifiés.

Une attention particulière est portée à l'implication citoyenne dans la gouvernance des données de santé, en explorant comment les citoyens peuvent participer à leur gestion et à la définition des règles éthiques. Nous recommandons des dispositifs transparents et accessibles permettant à chaque individu de mieux comprendre et maîtriser l'usage de ses propres données.

Outre les réflexions que nous avons développées en réponse à la question qui nous a été posée, nous avons élargi notre réflexion aux enjeux environnementaux en soulignant l'importance primordiale d'une vision écologique et durable.

À chaque étape, nous formulons des recommandations claires pour favoriser un cadre plus inclusif, transparent et respectueux de la volonté des citoyens.



Récapitulatif des propositions

**PROPOSITIONS
POUR MINIMISER
LES RISQUES IDENTIFIÉS
CONCERNANT
LES DONNÉES DE SANTÉ**

**➤ MAÎTRISE
TECHNOLOGIQUE
& SOUVERAINETÉ**

01

Développer des capacités françaises robustes pour la collecte, le stockage et le traitement des données de santé.

02

Prendre des engagements concrets, notamment en mobilisant des financements européens ou nationaux, pour créer des infra-structures souveraines.

03

Promouvoir une transparence totale sur la gestion des données collectées.

04

Évaluer périodiquement les services de stockage et les fournisseurs afin de garantir leur conformité aux normes de sécurité et de souveraineté qui évoluent constamment.

05

Localiser en priorité les données au sein de l'Union européenne.

**➤ SÉCURITÉ & CONTRÔLE
DES ENTREPRISES
GESTIONNAIRES**

06

Appliquer une surveillance stricte aux entreprises qui gèrent ou accèdent aux données de santé (audit réguliers, protocoles de sécurité renforcés).

07

Mettre en œuvre des systèmes d'incitation (financière ou autre) pour ceux qui signaleraient des failles de sécurité.

08

Adopter des sanctions dissuasives en cas de non-respect des règles.

**➤ OUTILS ET MÉTHODES
POUR LE CONTRÔLE
ET LA SÉCURISATION
DES DONNÉES DE SANTÉ
À DIFFÉRENTES ÉCHELLES**

**— À L'ÉCHELLE
INDIVIDUELLE**

09

Tout accès aux données de santé par un professionnel doit être encadré par une autorisation spécifique.

10

Pour les situations internationales, comme un voyage à l'étranger, une configuration globale des préférences doit permettre d'adapter les autorisations d'accès sans devoir les définir pays par pays.

11

Créer une plateforme centralisée où l'utilisateur pourrait :

- Consulter toutes les données utilisées à des fins secondaires.
- Modifier les autorisations facilement, par exemple en décochant les options de partage.
- Visionner des vidéos explicatives pour comprendre les implications du retrait d'une autorisation.

12

S'assurer que le pseudonymat reste la règle dans le cadre des recherches médicales.

— ÉCHELLE NATIONALE

13

Uniformiser les systèmes d'information entre médecins libéraux, hôpitaux et assurance maladie.

14

Renforcer la coordination des comités éthiques existants pour les entreprises et les structures de gestion de données de santé avec la CESREES pour une meilleure supervision.

15

Créer un système de consentement similaire à celui de la France, où les citoyens sont par défaut consentants et peuvent exercer leur droit de retrait (opt-out) pour l'utilisation secondaire de leurs données de santé.

16

Donner la possibilité aux citoyens de gérer leurs préférences via une plateforme centralisée.

17

Instaurer un dialogue structuré entre les comités éthiques nationaux et créer un comité éthique européen.

18

Travailler à l'uniformisation des normes de sécurité.

19

Développer une plateforme commune, inspirée du modèle du HDH en France, pour l'échange de données entre pays.

20

Soumettre toute demande d'accès à des données de santé par un professionnel de santé étranger à deux conditions : un consentement explicite du patient et une traçabilité complète des accès.

LA NÉCESSITÉ D'UNE INFORMATION FACILE À COMPRENDRE, TRANSPARENTE ET ACCESSIBLE À TOUTES ET TOUS

→ **DIFFUSION ET SENSIBILISATION : FORMER TOUTES LES PARTIES PRENANTES (MÉDECINS, TECHNICIENS, ASSOCIATIONS DE PATIENTS, ETC.) POUR S'ASSURER QUE LES DONNÉES PUISSENT ÊTRE EXPLOITÉES**

21

Équiper techniquement les parties prenantes (professionnels de santé et autres) pour qu'elles puissent faire remonter les données numériquement de manière équitable (équivalente pour tous les patients).

22

Motiver et éduquer les parties prenantes en leur démontrant l'intérêt commun de l'espace européen des données de santé et de l'utilisation des données (primaire ou secondaire).

23

Sensibiliser, former et suivre les parties prenantes à la gestion numérique des données de santé dès l'université.

24

Reclasser les visiteurs médicaux/délégués d'industrie pharmaceutique pour qu'ils forment les médecins, techniciens et associations en profitant de leur expertise et connaissances sur le domaine de la santé.

→ **CONFIANCE, PÉDAGOGIE, TRANSPARENCE, ÉDUCATION, FORMATION, SENSIBILISATION DES CITOYENS À L'UTILISATION PRIMAIRE ET SECONDAIRE DES DONNÉES**

25

Améliorer la connaissance du citoyen concernant ses données numériques de santé.

26

Utiliser un langage simplifié (principe de Feynman) pour informer les citoyens dans différentes langues à propos du traitement et de l'usage des données de santé, notamment en ce qui concerne le consentement par défaut et l'exercice du droit de retrait (opt-out).

27

Vulgariser les termes « utilisation primaire / secondaire des données de santé ».

28

S'assurer que l'information est apportée aux citoyens sans qu'ils aient besoin de la chercher.

29

Profiter de l'identification des assurés sociaux auprès de la sécurité sociale ou du remplacement d'une carte vitale perdue pour ouvrir «par défaut» l'espace santé des personnes concernées (si ce n'est pas déjà fait).

30

Informar les citoyens à l'aide d'une communication transparente sur les mesures de protection des données de santé.

➔ **GARANTIR LA TRANSPARENCE DE L'INFORMATION**

31

Rendre accessibles à tous les citoyens les projets et les résultats de l'utilisation secondaire des données de santé sur un site dédié.

32

Informar les citoyens à propos de toutes les étapes de la collecte de données, du stockage et de l'utilisation des données de santé de manière imagée et interactive.

33

Informar les citoyens concernés en cas de fuite de leurs données.

➔ **MESURER LE NIVEAU D'INFORMATION DES PERSONNES POUR GARANTIR L'ÉTHIQUE DE L'OPT-OUT**

34

Mettre en place des questionnaires et sondages auprès des citoyens pour évaluer leur compréhension des mécanismes de droit de retrait.

35

Remplacer le terme opt-out par «droit de retrait» ou «droit de rétractation» pour éviter un langage trop technique.

L'ENJEU D'UN DISPOSITIF SIMPLE ET ERGONOMIQUE PERMETTANT À CHAQUE PERSONNE DE DÉCIDER DE L'USAGE PAR DES TIERS DE SES DONNÉES DE SANTÉ

36

Faciliter la procédure de retrait de consentement sur Mon Espace Santé en cas de refus de réutilisation de données de santé et permettre de retirer le consentement à différents niveaux pour personnaliser au mieux leurs desiderata des citoyens.

37

Mettre en place un formulaire sur Mon espace santé qui permettra à chaque personne de piloter l'ensemble de ses choix.

LE RÔLE DES CITOYENS DANS LA GOUVERNANCE FONCTIONNELLE ET DANS LA DÉFINITION DE L'ÉTHIQUE DE L'UTILISATION DES DONNÉES DE SANTÉ

➔ **À L'ÉCHELLE LOCALE (LES ENTREPÔTS DE DONNÉES DE SANTÉ)**

38

Rendre obligatoire le comité scientifique et éthique pour chaque entrepôt de données de santé ; sa forme et son rôle doivent être clairement définis ; ils doivent être rattachés à la CNIL.

39

Mettre en place d'une plateforme publique centralisant les décisions rendues par l'ensemble des comités scientifiques et éthiques, au même titre, dans les mêmes conditions et au même endroit que les demandes qui ont été traitées par le HDH.

40

Imposer aux fournisseurs de logiciels d'entrepôt de données la mise en place d'espaces de travail de données isolés du reste de l'entrepôt.

41

Donner aux associations d'usagers un droit de regard sur l'ensemble des demandes d'accès aux données de santé, avec le CSE voire dans le cadre de ses travaux (si elles en sont membres).

42

S'assurer que toute recherche ayant abouti grâce à l'utilisation des données de santé sera partagée avec la communauté scientifique.

➔ À L'ÉCHELLE
FRANÇAISE
(HEALTH DATA HUB)

43

S'assurer l'ensemble des partages de données extérieurs à l'environnement d'un entrepôt passe par le HDH dans une volonté de rendre le HDH universel.

44

Rendre publics les audits réalisés par la CNIL au sein des entités qui gèrent un entrepôt. Nous souhaitons que ces audits concernent aussi les activités du CSE

➔ À L'ÉCHELLE
EUROPÉENNE

45

Un Comité Éthique Européen, il devra avoir des missions de contrôle et d'audit mais également être un interlocuteur que le citoyen pourra interpeller.

LA QUESTION
DE L'ENVIRONNEMENT,
DE L'UTILISATION
DES RESSOURCES ET
DE LA CONSOMMATION
D'ÉNERGIES ASSOCIÉE
À LA GESTION DES
DONNÉES DE SANTÉ

46

Obliger les entreprises et les administrations qui font appel à leurs services pour le stockage des données de santé de publier un rapport d'impact écologique comprenant un bilan carbone.

47

Créer un label national « Santé Numérique Responsable » qui pourrait certifier les infrastructures et services traitant des données de santé.

48

Créer un cadre juridique impliquant et responsabilisant sur ces questions écologiques autant les utilisateurs des données de santé (professionnels de santé, chercheurs, etc.) que les entreprises qui stockent les données.

49

Réutiliser la chaleur « fatale » produites par les data centers qui hébergent des données de santé.

50

Sensibiliser et former les citoyens à l'impact écologique des données en général et plus particulièrement des données de santé.

51

Optimiser l'utilisation des données de santé afin d'éviter les doublons ainsi que « les données inutiles ».

52

Promouvoir le recyclage et la réparation des équipements (des data centers, cloud...) afin de réduire les déchets et de préserver les ressources.

Les données de santé et leurs usages



Les données de santé sont des données personnelles de nature médicale ou administrative concernant l'état de santé de chaque individu ; elles sont fournies par les différents acteurs liés à son parcours de soins. Elles peuvent prendre un grand nombre de formes : un compte rendu médical, une imagerie, un dossier patient chez son médecin traitant, dans un hôpital ou une clinique ou encore l'ensemble des données récoltées par une montre connectée si celles-ci sont de nature médicale. Elles sont sensibles car elles permettent d'identifier facilement une personne unique. Ces données ont deux usages, primaire et secondaire.

Dans le cadre d'un rendez-vous médical, pour que le praticien puisse traiter son patient de manière optimale, il utilise les données de santé de ce dernier pour lui prescrire le meilleur traitement. On parle ici **d'utilisation primaire des données de santé**.

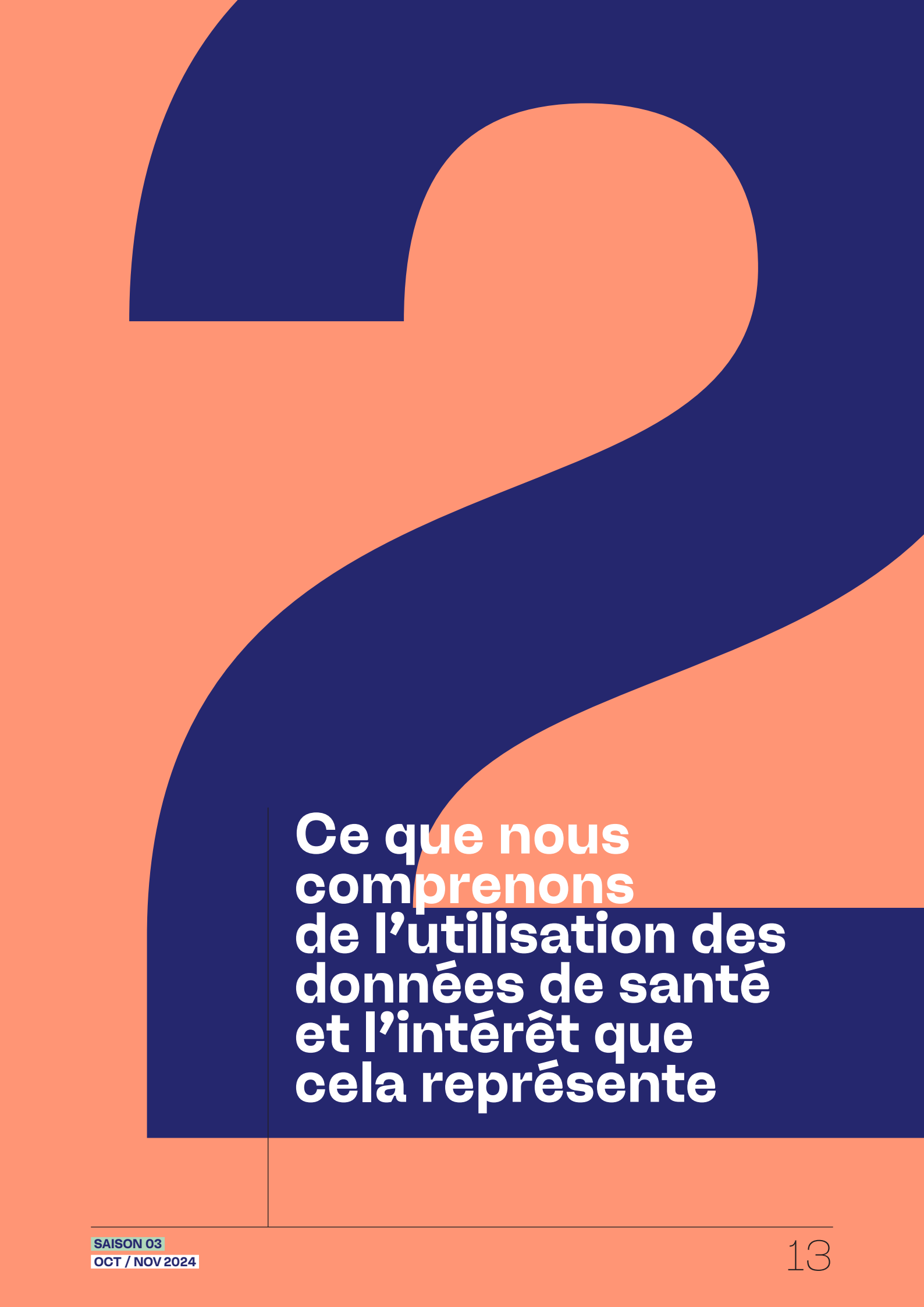
Dans le cadre d'une recherche, d'une étude, du développement d'un nouveau médicament, les données de santé sont utilisées par des professionnels de santé ou des chercheurs dans le but d'améliorer la santé de la population. C'est **l'usage secondaire des données de santé**.

Dans ce cas, les données personnelles de santé ne doivent pas permettre à l'entité les exploitant d'identifier directement les individus concernés. Pour cela les données sont soit pseudonymisées, soit anonymisées.

La **pseudonymisation** est un traitement de données personnelles qui a pour but de ne plus pouvoir attribuer les données à une personne physique identifiée sans information supplémentaire. Cela permet aux chercheurs de croiser les données pour les exploiter de façon à préciser leur recherche : dans ce cas, ils peuvent comparer plusieurs facteurs d'une population et, par exemple, identifier laquelle est la plus à risque.

L'anonymisation est un traitement de données personnelles qui rend impossible l'identification d'une personne. Ces données ne permettent pas de réaliser des croisements et réduit leur utilisation.

Dans les deux cas, même si des croisements peuvent être possibles, l'individu à la source de la donnée n'est pas identifiable sans la clef de chiffrement à l'origine.



**Ce que nous
comprendons
de l'utilisation des
données de santé
et l'intérêt que
cela représente**

UTILISATION PRIMAIRE DES DONNÉES DE SANTÉ

Les données de santé en France sont un atout précieux, notamment grâce à la base de données de la **Caisse Nationale d'Assurance Maladie (CNAM)** que nos voisins européens nous envient. **Mon Espace Santé**, un carnet de santé électronique qui centralise les informations médicales des patients est un outil qui facilite l'utilisation primaire des données de santé. Ce système permet au patient de gérer l'accès à ses propres données et de suivre son parcours de soins. Bien que toutes les données ne soient pas directement hébergées dans **Mon Espace Santé**, elles sont collectées et gérées par différents acteurs du système de santé, tels que les hôpitaux, les médecins et d'autres structures.

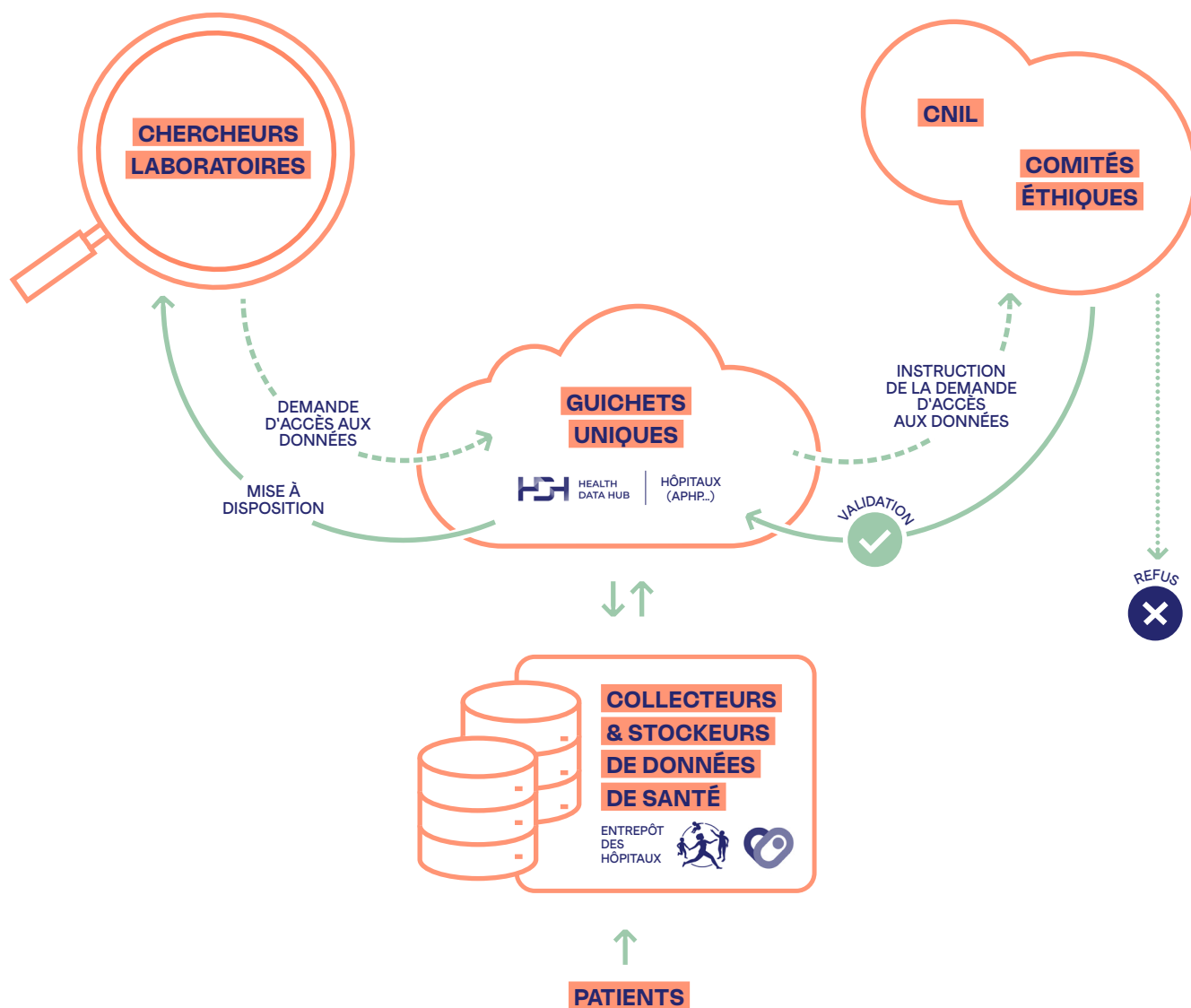
L'intérêt de l'utilisation primaire à l'échelle de l'Union Européenne réside dans la possibilité de garantir un suivi médical continu pour les citoyens européens. Cela est particulièrement important pour les **travailleurs frontaliers, les patients se faisant soigner dans un autre pays de l'Union européenne au cours d'un voyage par exemple ou les citoyens européens déménageant dans un autre pays de l'Union européenne**. Un tel système permettra de faciliter l'accès aux données médicales et d'assurer la continuité des soins dans ces différentes situations.

UTILISATION SECONDAIRE DES DONNÉES DE SANTÉ

— EN FRANCE

L'utilisation secondaire des données de santé concerne leur exploitation pour la recherche scientifique, l'analyse de la santé publique et le développement de nouveaux traitements ou technologies. Plusieurs organismes collectent ces données, tels que la **CNAM via le Système National des Données de Santé (SNDS)**, des hôpitaux comme **l'AP-HP** (→P38), des laboratoires et d'autres acteurs du secteur de la santé. Ces données sont accessibles via des plateformes comme le **Health Data Hub** (ou par exemple via l'AP-HP qui dispose de son propre guichet) centralisant et facilitant leur partage pour des projets de recherche.

Le processus pour obtenir l'accès à ces données est strictement régulé. **Les chercheurs et laboratoires doivent soumettre une demande d'accès via des guichets uniques tels que le Health Data Hub** ou directement auprès d'autres acteurs protéiformes qui détiennent de la donnée (hôpitaux, instituts de recherche publique, répartiteurs pharmaceutiques, autres acteurs privés...). Cette demande doit être validée par des **Comités Éthiques** (Ex : CESRESS (→P38) pour le HDH) et la **CNIL** (→P38), qui s'assurent que l'utilisation des données respecte les normes éthiques et légales. Si la demande est validée, les données sont mises à disposition pour les projets approuvés pour une durée déterminée.



— DANS L'UNION EUROPÉENNE

L'ouverture d'un **Espace Européen des Données de Santé (EEDS)** facilitera l'accès aux données de santé à travers l'Union européenne. Cela permettra de travailler avec des volumes de données plus importants et d'élargir les possibilités de recherche grâce à l'accès à des bases de données plus vastes et plus diverses. En facilitant l'accès transfrontalier aux données de santé, l'Europe pourra renforcer la compétitivité de ses chercheurs et maximiser les bénéfices pour la santé publique et les progrès médicaux. De plus, l'harmonisation des règles de gestion des données de santé entre les États membres contribuera à une recherche plus efficace et à une meilleure coordination dans la lutte contre les maladies rares (cf. ci-dessous).

► Le schéma ci-dessus illustre clairement ce processus de validation et d'accès aux données de santé qui est constitué de plusieurs étapes :

- 01 Les chercheurs/laboratoires soumettent leur demande d'accès aux données.
- 02 Cette demande est examinée par les Comités éthiques et la CNIL. Si la demande respecte les critères éthiques et légaux, elle est validée.
- 03 Une fois validée, les données sont mises à disposition via les guichets uniques, tels que le Health Data Hub ou d'autres institutions responsables.
- 04 En cas de non-validation, la demande est refusée.



Ce que nous comprendons du règlement européen concernant les données de santé

Le règlement européen sur l'Espace Européen des Données de Santé (EEDS)  (→ P38), prévoit **d'harmoniser la gestion des données de santé à travers l'Union européenne**, en permettant la circulation sécurisée des informations entre États membres. Il permet donc un meilleur partage des données entre les institutions de santé des États membres afin de favoriser la continuité des soins (usage primaire) en offrant la possibilité aux professionnels de santé d'accéder directement aux dossiers médicaux des patients à travers l'Union.

De créer un socle commun et d'harmoniser l'accès aux données de santé entre États membres dans le but d'améliorer la recherche scientifique (usage secondaire).

USAGE PRIMAIRE DE LA DATA

DES OBLIGATIONS POUR CHAQUE ÉTAT MEMBRE DISPOSANT D'UNE MARGE DE MANŒUVRE POUR L'APPLIQUER - ACCÈS DIRECT DES CITOYENS À LEURS DONNÉES DE SANTÉ ET ACCÈS AU DOSSIER MÉDICAL ENTRE ÉTATS MEMBRES

Le règlement garantit aux citoyens l'accès direct à leurs données de santé à travers un dossier médical électronique. Les individus pourront consulter et gérer leurs données, telles que les résultats médicaux, les prescriptions ou l'historique de leurs traitements, à tout moment et partout dans l'Union européenne.

Le règlement vise également à faciliter le partage transfrontalier des données de santé entre les professionnels de santé des différents États membres de l'UE, sous réserve de l'accord du patient.

Les opportunités que nous identifions associés à cette directive, sont :

- Une meilleure prise en charge au sein de l'Union Européenne pour les patients qui voyagent, qui déménagent au sein de l'UE ou qui sont transfrontaliers
- Une plus grande accessibilité pour tout patient européen à son dossier médical
- Un accès facilité aux documents de santé pour les patients
- Une réduction de l'utilisation du papier

USAGE SECONDAIRE DE LA DATA

**PARTAGE DES DONNÉES
ENTRE LES ÉTATS MEMBRES**

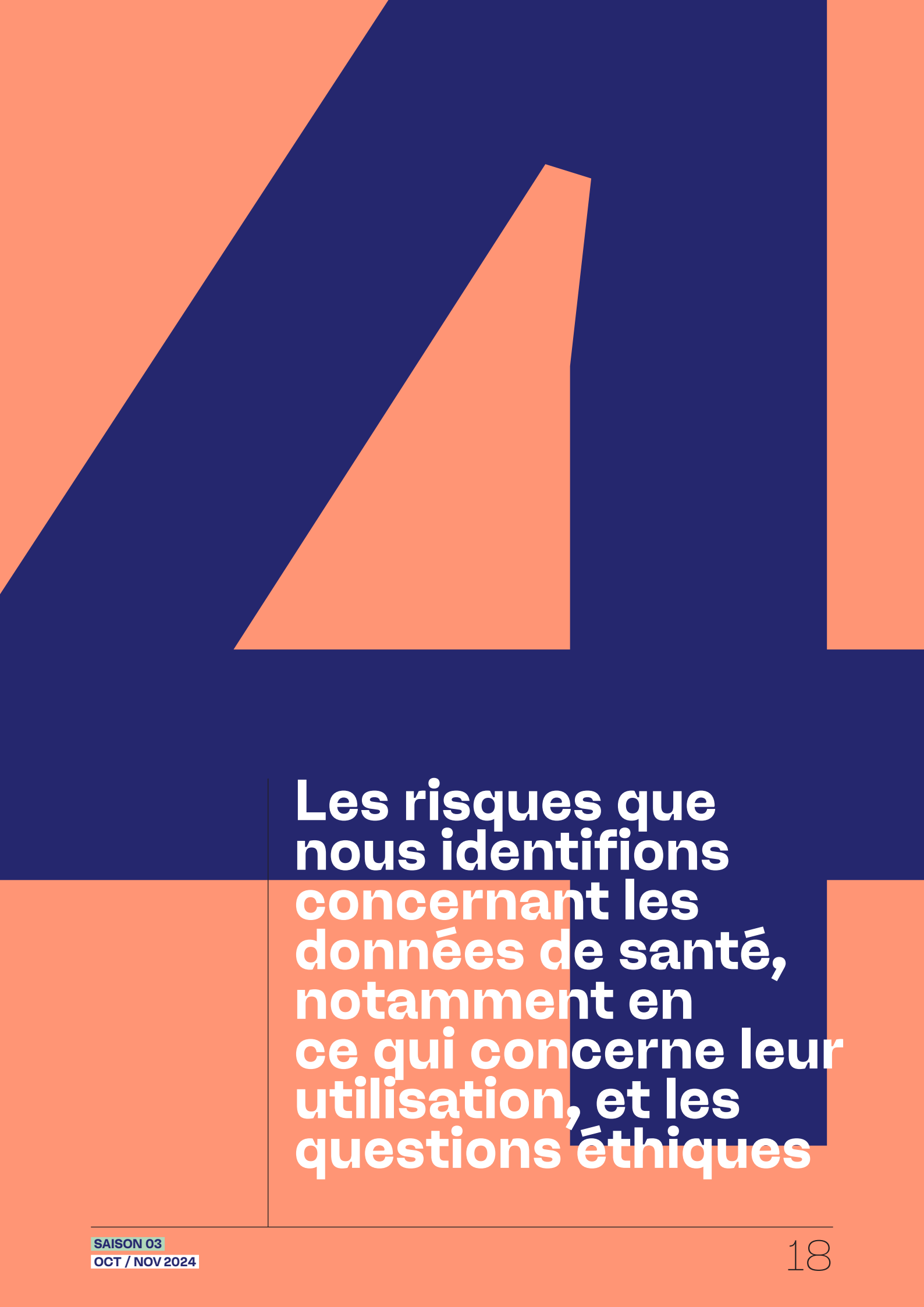
Le règlement instaure un **cadre juridique** pour la réutilisation des données de santé, notamment pour la recherche et les projets d'intérêt public. Cela permet de créer un espace sécurisé dans lequel les données anonymisées ou pseudonymisées peuvent être utilisées à des fins de recherche scientifique, de développement de nouveaux traitements et d'amélioration des politiques de santé.

Le règlement crée des **Organismes Responsables de l'Accès aux Données** (ORAD), qui sont chargés de gérer et d'autoriser l'accès aux données de santé dans le cadre de projets de recherche ou d'analyses. Ces organismes veilleront à ce que l'accès aux données soit strictement contrôlé et limité aux projets pertinents et conformes aux règles éthiques et juridiques.

La finalité n'est pas de créer une base de données commune à l'échelle européenne mais **d'harmoniser l'accès de tous les acteurs pertinents** des États membres de l'Union européenne à l'ensemble des données de santé européennes, avec le principe du guichet unique.

Les opportunités que nous identifions associés à cette directive, sont :

- **Une plus grande puissance d'analyse**, notamment pour les maladies rares qui nécessitent des jeux de données larges. À l'échelle de l'union européenne les chercheurs vont pouvoir faire avancer leurs recherches de manière exponentielle par rapport à leur capacité actuelle. Cela permet donc une meilleure souveraineté de l'Union européenne face aux autres puissances mondiales comme les USA et la Chine qui disposent déjà de jeux de données larges.
- **Une multitude de chercheurs supplémentaires** capables de travailler sur nos jeux de données.
- **Une amélioration de la collaboration** entre (les acteurs) des États membres.
- **Un guichet unique européen** permettra d'une part de faciliter les démarches administratives et d'autre part d'harmoniser l'accès aux données.



Les risques que nous identifions concernant les données de santé, notamment en ce qui concerne leur utilisation, et les questions éthiques

IL NOUS SEMBLE CAPITAL DE METTRE EN AVANT DES RISQUES ÉTHIQUES LIÉS À L'UTILISATION DE NOS DONNÉES DE SANTÉ, EN PARTICULIER AU REGARD DES PRINCIPES FONDAMENTAUX DE LIBERTÉ, DE CONSENTEMENT, DE DROIT À L'INFORMATION ET D'ÉGALITÉ.

UTILISATION PRIMAIRE DES DONNÉES DE SANTÉ

Nous identifions les risques suivants concernant l'utilisation primaire des données de santé.

— RISQUE 1 LE MANQUE D'INFORMATION

Si l'information concernant l'intérêt de l'utilisation de systèmes du type Mon espace santé est insuffisante, les citoyens risquent de ne pas voir l'intérêt de l'utilisation primaire des données de santé et donc de ne pas adhérer à la démarche (défiance, complotisme ...).

— RISQUE 2 L'ACCÈS PRÉCOCE AUX DOCUMENTS SENSIBLES

Nous percevons un double risque en cas de mise à disposition prématurée de comptes-rendus médicaux sensibles, dont l'annonce via Mon espace santé peut être violente pour le patient (dans le cas de maladies graves) : ne pas être informé de la bonne manière, voire de ne pas être informé du tout. Une consultation d'annonce nous apparaît obligatoire avant que le document soit accessible sur Mon espace santé.

— RISQUE 3 LE PROFILAGE ET LES DISCRIMINATIONS

Nous craignons que les données de santé puissent être utilisées pour profiler certaines catégories de citoyens, pour raisons de santé ou autre. Par exemple, identifier des populations ayant refusé un traitement ou un vaccin et utiliser ces informations pour modifier un remboursement et/ou une prise en charge de santé.

Nous nous inquiétons également du risque de discrimination dans l'utilisation des données de santé au sein de l'Union européenne. Les règles relatives au bris de glace prévu dans Mon espace santé et leur contrôle sont-ils aussi rigoureux dans tous les pays de l'Union qu'en France ?

Nous soulignons l'importance pour le patient de garder le contrôle sur l'accès à ses données dans Mon Espace Santé. Ainsi, nous proposons que le citoyen soit informé systématiquement via Mon espace santé lorsqu'un professionnel de santé, quel qu'il soit, a accédé à ses données de santé. Cette traçabilité des accès permettra de prévenir (ou sanctionner) les accès malveillants.

UTILISATION SECONDAIRE DES DONNÉES DE SANTÉ

Nous sommes vigilants relativement aux risques suivants :

— RISQUE 4 L'ÉTHIQUE

Tous les États membres sont libres de leurs règles éthiques d'accès aux données. Certains pays peuvent avoir des niveaux d'accessibilité moins restrictifs car l'éthique est à l'appréciation de chaque État membre, au regard de ses valeurs.

— RISQUE 5 L'IDENTIFICATION PAR CROISEMENT ET LE RISQUE RELATIF À LA CONFIDENTIALITÉ

Le croisement des données de santé pseudonymisées avec d'autres bases de données pourrait permettre de remonter jusqu'à certaines populations et de les cibler. Il y aurait alors un risque de réidentification par croisement de bases de données.

Par ailleurs, les données pseudonymisées permettent techniquement de retrouver l'identité de la personne concernée. Dans le cadre de l'espace européen des données de santé, cela sera possible non plus seulement au niveau national mais aussi européen. Nous craignons que les règles de confidentialité des données pseudonymisées ne soient pas uniformes dans tous les pays de l'Union européenne.

— RISQUE 6 LA DÉFIANCE DES CITOYENS

Les citoyens, en apprenant l'existence de l'usage secondaire de la donnée de santé, pourraient craindre l'utilisation que l'on en fait.

En outre, nous nous inquiétons d'une perte de confiance des citoyens si leur opposition à l'utilisation de leurs données n'est pas respectée, même en cas de force majeure. Si un tel cas se présentait, nous proposons que les citoyens soient informés des enjeux et de la possibilité de modifier leurs choix quant à l'utilisation de leurs données personnelles.

— RISQUE 7 LES PERTES D'OPPORTUNITÉ DE RECHERCHE

Le droit d'opposition peut être activé par chaque État membre afin que les personnes puissent refuser l'utilisation secondaire des données sous condition. Cela signifie, si la clause de droit d'opposition est massivement activée, qu'il existe un risque que les bases de données de certains États membres soient moins ouvertes que celles d'autres pays (qui n'auraient pas activé la clause).

Par ailleurs, les avis divergent entre nous concernant la possibilité de laisser au citoyen le choix du type de recherche auquel il contribue en partageant ses données de santé. Par exemple, à propos du droit d'opposition certains d'entre nous souhaiteraient que l'on puisse différencier les options de partage des données entre les acteurs publics ou privés (laboratoires pharmaceutiques, industries agro-alimentaires ...) ou selon le type de recherches. D'autres, parmi nous, s'y opposent.

— RISQUE 8 LE DÉTOURNEMENT DE L'UTILISATION DES DONNÉES ET RISQUE MERCANTILE

Nous souhaitons souligner l'indispensable vigilance à apporter au contrôle et au suivi des données accessibles via le HDH, afin d'éviter au maximum le détournement de leur utilisation. Exemple d'un organisme qui ferait un dépôt de projet de recherche au HDH et réutiliserait ces données pour un autre projet qui n'aurait pas été validé par la GESREES.

Par ailleurs, nous craignons que certains acteurs privés considèrent la donnée de santé plutôt en raison de ses objectifs financiers que du point de vue du bien commun.

— RISQUE 9 L'IDENTIFICATION ET L'INFORMATION CONTRE LA VOLONTÉ DE LA PERSONNE

Certains d'entre nous pointent l'existence d'un risque, dans le cas de la découverte d'une maladie à la suite de l'utilisation de données personnelles aux fins de recherche, d'être informé contre leur volonté. Nous proposons de laisser la possibilité de refuser la remontée d'informations au citoyen et de protéger son droit à ne pas être informé.

— RISQUE 10 LE MANQUE DE SÉCURITÉ LIÉ AU LIEU D'HÉBERGEMENT DES DONNÉES

Nous soulignons des risques d'utilisation moins encadrée de données de santé en cas de localisation des serveurs de stockage au sein de pays européens ayant des législations ou des pratiques différentes en termes de respect des données personnelles (accès, traitement, propriété, etc.). Par exemple, certains observateurs émettent des doutes quant à la réalité de la volonté de l'Irlande à faire respecter les données de santé, notamment en raison de la forte présence d'entreprises du numérique sur son territoire. On peut aussi craindre les risques liés à l'instabilité de certains pays en Europe. Il peut dès lors exister des problèmes de souveraineté si les serveurs ne sont pas en France.

Nous relevons également des risques d'espionnage industriel associés à l'utilisation de plateformes de gestion extra-européenne (Amazon, Microsoft ...) étant donné que le droit américain prévaut à l'étranger, ce qui peut aller à l'encontre de la souveraineté européenne.

Ce risque met en lumière l'importance du développement, au niveau européen, de services de gestion des serveurs (Cloud).



Propositions pour minimiser les risques identifiés concernant les données de santé

LA GESTION DES DONNÉES DE SANTÉ SUSCITE PLUSIEURS PRÉOCCUPATIONS, NOTAMMENT EN MATIÈRE DE STOCKAGE ET DE SÉCURITÉ. NOUS AVONS IDENTIFIÉ LES POINTS SUIVANTS DANS L'OBJECTIF DE GARANTIR UNE MAÎTRISE ET UNE PROTECTION OPTIMALES DE CES INFORMATIONS SENSIBLES.

MAÎTRISE TECHNOLOGIQUE ET SOUVERAINETÉ

Nous considérons qu'il est impératif de développer des **capacités françaises robustes pour la collecte, le stockage et le traitement des données de santé**. Si l'utilisation temporaire de serveurs américains, basés en Europe, peut être tolérée, l'objectif à long terme est de confier ces infrastructures à des entreprises européennes, idéalement françaises.

Nous demandons que soient pris des engagements concrets, notamment en mobilisant des financements européens ou **nationaux pour créer des infrastructures souveraines**. Cette stratégie vise à renforcer l'autonomie technologique de la France et de l'Europe tout en garantissant un contrôle accru sur ces données sensibles. Nous considérons que la priorité doit être donnée à la localisation des données au sein de l'Union européenne, conformément aux exigences du RGPD, afin de garantir une souveraineté totale sur les données sensibles.

Nous recommandons également **une réévaluation périodique** des services de stockage et des fournisseurs, à raison d'une fois tous les trois ans, afin de garantir leur conformité aux normes de sécurité et de souveraineté qui évoluent constamment.

Par ailleurs, nous demandons une **transparence totale sur la gestion des données collectées** : leur nature, les modalités de leur collecte et leur utilisation doivent être clairement décrites pour assurer un contrôle rigoureux à chaque étape.

Ce cadre général vise à répondre aux défis posés par le stockage et la sécurité des données de santé tout en garantissant leur protection et leur maîtrise à long terme.

SÉCURITÉ ET CONTRÔLE DES ENTREPRISES GESTIONNAIRES

Nous souhaitons qu'une surveillance stricte soit appliquée aux entreprises qui gèrent ou accèdent aux données de santé, même si ces usages restent peu fréquents. Cela inclut :

- **Des audits réguliers** pour évaluer leur conformité aux normes.
- **Des protocoles de sécurité renforcés** et un cadre réglementaire rigoureux pour prévenir tout risque de fuite ou d'abus.
- **Des systèmes d'incitation** (financiers ou autres) pour ceux qui signaleraient des failles de sécurité, notamment dans les centres de données (bien que cette mesure soit moins adaptée aux hôpitaux qui ne disposent que de peu de ressources).

Nous souhaitons que les sanctions, en cas de non-respect des règles, soient dissuasives :

- **Sanctions pour accès non autorisé** : Si un professionnel accède à des données non pertinentes, ces actes doivent être tracés et sanctionnés.
- **Suspension temporaire d'accès** : Les structures non conformes pourraient se voir retirer l'accès aux données pendant une période déterminée pour les inciter à corriger leurs pratiques.
- **Révocation des agréments** : Les certifications délivrées par des organismes comme la CNIL pourraient être retirées en cas de manquement.
- **Restrictions sur les projets publics** : Les entreprises ayant gravement violé les règles pourraient être interdites de participer à de nouveaux appels d'offres publics.
- **Publication des violations** : Les violations éthiques et légales pourraient être publiées dans un registre public pour renforcer la pression sur les entreprises à respecter les normes.

OUTILS & MÉTHODES POUR LE CONTRÔLE ET LA SÉCURISATION DES DONNÉES DE SANTÉ À DIFFÉRENTES ÉCHELLES

La sécurisation et le contrôle des données de santé requièrent des **approches adaptées aux échelles individuelle, nationale et européenne**. Voici une synthèse des réflexions et propositions selon ces trois niveaux.

— ÉCHELLE INDIVIDUELLE

① Gestion des accès aux données de santé

Tout accès aux données de santé par un professionnel doit être encadré par une autorisation spécifique. Pour simplifier les démarches, des accès prédéfinis pourraient être mis en place pour les consultations régulières. En cas d'urgence (bris de glace), une notification devrait être envoyée au patient et à son médecin traitant, offrant ainsi la possibilité de contester ou de signaler tout accès abusif à une instance dédiée.



Le pseudonymat devrait rester la règle dans le cadre des recherches médicales. Une levée du pseudonymat pourrait toutefois être envisagée si le patient consent explicitement à être recontacté.

② Contrôle renforcé du dossier médical

Pour les situations internationales, comme un voyage à l'étranger, une configuration globale des préférences doit permettre d'adapter les autorisations d'accès sans devoir les définir pays par pays.

③ Gestion des autorisations pour l'utilisation secondaire des données

Actuellement, s'opposer à l'utilisation secondaire des données exige de contacter chaque organisme collecteur. Une solution serait la création d'une plateforme centralisée où l'utilisateur pourrait :

- ➔ Consulter toutes les données utilisées à des fins secondaires.
- ➔ Modifier les autorisations facilement, par exemple en décochant les options de partage.
- ➔ Visionner des vidéos explicatives pour comprendre les implications du retrait d'une autorisation.

④ Maintien du pseudonymat dans les recherches médicales

Le pseudonymat devrait rester la règle dans le cadre des recherches médicales. Les chercheurs souhaitant accéder à des données supplémentaires doivent obtenir une validation préalable par le comité CESREES, garantissant ainsi un usage minimaliste et conforme au RGPD. Une levée du pseudonymat pourrait toutefois être envisagée si le patient consent explicitement à être recontacté, par l'intermédiaire de son médecin ou via des outils comme Mon espace santé.

⑤ Levée du pseudonymat en cas de découverte d'une maladie

Ce sujet reste débattu entre nous. Certains estiment que l'information devrait être transmise au patient via une procédure structurée impliquant le HDH et les professionnels de santé. D'autres s'y opposent, invoquant le principe de minimisation des données ou le droit à ne pas être informé (cf. ci-dessus). Un cadre clair reste à définir pour concilier ces approches divergentes.

① Réglementation française et mise en œuvre concrète

La gestion des données doit s'inscrire dans un cadre national clair, intégrant des principes comme l'intérêt général ou les cas de force majeure, par exemple lors de pandémies. Toutefois, des interrogations persistent quant à l'efficacité de l'application de ces réglementations en pratique.

② Harmonisation des données

L'uniformisation des systèmes d'information entre médecins libéraux, hôpitaux et assurance maladie est un enjeu majeur. Une plateforme unique pourrait être envisagée, mais une réflexion approfondie est nécessaire pour évaluer sa faisabilité et son utilité compte tenu de l'état actuel des pratiques.

③ Encadrement éthique et légal

Le CESREES, grâce à sa composition diversifiée, joue un rôle clé dans l'équilibre des enjeux. Les comités éthiques existants pour les entreprises et les structures de gestion de données doivent renforcer leur coordination avec cet organisme pour une meilleure supervision.

④ Rôle du HDH

Deux approches s'opposent au sein du Comité concernant le partage de bases de données dans une utilisation secondaire, lorsque plusieurs bases de données sont sollicitées :

- Une centralisation de la gestion des demandes d'accès aux données au niveau du HDH pour garantir une uniformité des procédures et une sécurité accrue.
- Une autonomie des comités éthiques des hôpitaux, qui pourrait accélérer les processus.

① Réglementation et gouvernance

L'harmonisation des cadres légaux est essentielle pour éviter que des divergences politiques ou juridiques entre États membres n'entravent la recherche scientifique. Nous proposons un système de consentement similaire à celui de la France, où les citoyens sont par défaut consentants et peuvent exercer leur droit de retrait (opt-out) pour l'utilisation secondaire de leurs données de santé et peuvent gérer leurs préférences via une plateforme centralisée.

② Harmonisation des pratiques

Pour favoriser une coopération européenne efficace, il est indispensable d'instaurer un dialogue structuré entre les comités éthiques nationaux, de créer un comité éthique européen et de travailler à l'uniformisation des normes de sécurité, en cohérence avec le RGPD.

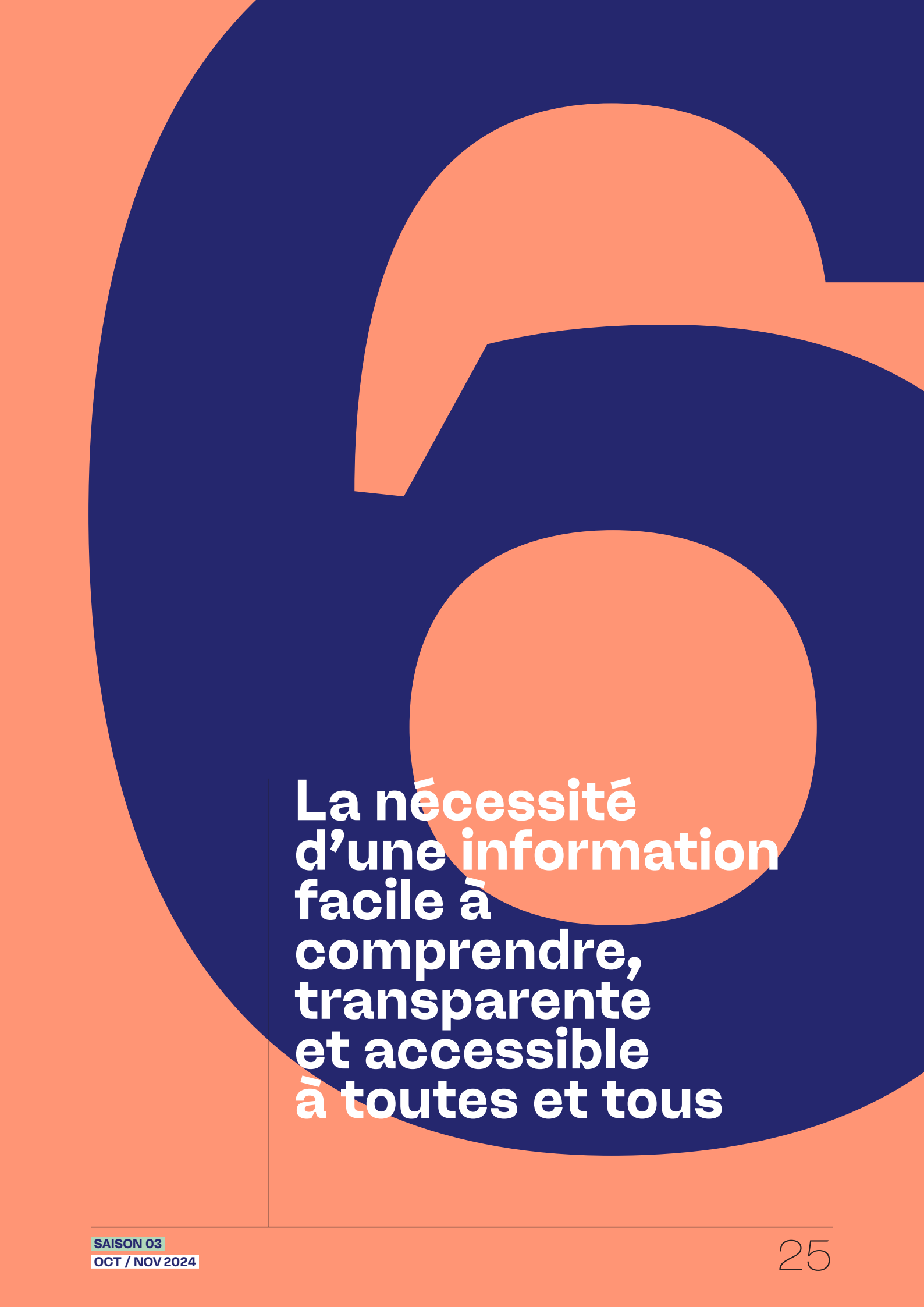
③ Outils partagés

Une plateforme commune, inspirée du modèle du HDH en France, pourrait être développée pour l'échange de données entre pays. Ces outils doivent garantir une sécurité maximale et restreindre tout usage non conforme au cadre défini par leur architecture.

④ Consultation des données à l'échelle européenne

Pour les accès transfrontaliers, une sécurisation stricte est indispensable. Toute demande d'accès par un professionnel de santé étranger doit être soumise à deux conditions : un consentement explicite du patient et une traçabilité complète des accès. Dans des cas exceptionnels, comme les situations d'urgence (« bris de glace »), des règles spécifiques doivent être prévues pour encadrer ces accès tout en préservant la sécurité des données.

Ces propositions visent à garantir la protection, la maîtrise et l'utilisation éthique des données de santé, en tenant compte des particularités de chaque échelle. Elles nécessitent une coordination entre les acteurs concernés et un effort commun pour harmoniser les pratiques à l'échelle nationale et européenne.



**La nécessité
d'une information
facile à
comprendre,
transparente
et accessible
à toutes et tous**

NOUS PRÉSENTONS DANS CETTE PARTIE LES RECOMMANDATIONS QUI PERMETTRONT DE PROMOUVOIR UNE BONNE COMPRÉHENSION PAR CHAQUE PERSONNE (CITOYENS, PROFESSIONNELS DE SANTÉ ET AUTRES ACTEURS) DE CE QUE SONT LES DONNÉES DE SANTÉ, DE LEURS DIFFÉRENTS USAGES ET DES INTÉRÊTS QU'ELLES REPRÉSENTENT AINSI QUE DES DROITS QUE CES PERSONNES DOIVENT POUVOIR EXERCER RELATIVEMENT À CES DONNÉES.

DIFFUSION & SENSIBILISATION : FORMER TOUTES LES PARTIES PRENANTES

(MÉDECINS, TECHNICIENS, ASSOCIATIONS DE PATIENTS, ETC.) POUR S'ASSURER QUE LES DONNÉES PUISSENT ÊTRE EXPLOITÉES

Nous préconisons d'équiper techniquement les parties prenantes (professionnels de santé et autres) pour qu'elles puissent faire remonter les données numériques de manière équitable **6** (→ P38), grâce à un outil commun. Le but serait à la fois d'uniformiser à l'échelle européenne les processus utilisés par les différents professionnels de santé ; et de simplifier leur formation à ces outils.

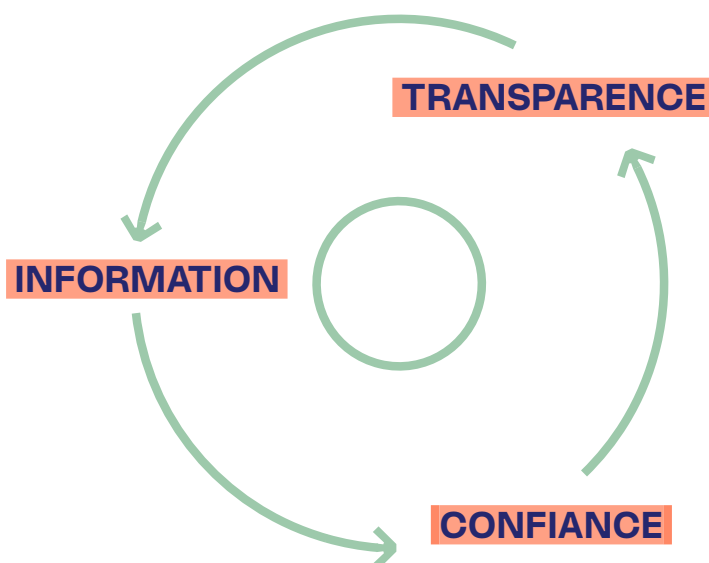
Il est **nécessaire de motiver et éduquer les parties prenantes** en leur démontrant l'intérêt commun de l'espace européen des données de santé et de l'utilisation des données (primaire ou secondaire) :

- ➔ Arguments pour l'utilisation primaire : Gain de temps pour un travail plus efficace, plus complet et avec moins de risques d'erreur, faciliter la prise en charge de patients, etc.
- ➔ Arguments pour l'utilisation secondaire : Possibilité de mener davantage de recherches, augmenter les volumes de données pour les maladies rares, croiser les résultats des différents pays de l'Union européenne pour des recherches plus complètes, etc.

Il nous semble pertinent de leur fournir l'information grâce à des formations, des contenus informatifs avec des données chiffrées pour démontrer l'intérêt public de la collecte de données ; un numéro de téléphone d'information à destination des professionnels serait aussi utile.

Selon nous, **il est nécessaire de sensibiliser, former et suivre les parties prenantes à la gestion numérique des données de santé dès l'université** ; les personnels déjà en activité doivent aussi être formés et suivis.

Nous suggérons de reclasser les visiteurs médicaux/délégués d'industrie pharmaceutique pour qu'ils forment les médecins, techniciens et associations en profitant de leur expertise et connaissances sur le domaine de la santé.



CONFIANCE, PÉDAGOGIE, TRANSPARENCE, ÉDUCATION, FORMATION, SENSIBILISATION DES CITOYENS

À L'UTILISATION PRIMAIRE ET SECONDAIRE DES DONNÉES

Améliorer la connaissance du citoyen concernant ses données numériques de santé est essentiel. En effet, un citoyen informé aura une meilleure maîtrise de ses données numériques de santé et sera plus enclin à s'impliquer dans la démarche du partage de ces données, que ce soit individuellement ou collectivement (dans le cadre d'associations de patients ou autres types d'organisations citoyennes ou de comités d'usagers par exemple). De cette manière, le citoyen pourra pleinement jouer son rôle.

Nous préconisons d'informer les citoyens par un langage simplifié (principe de Feynman) et dans différentes langues à propos du traitement et de l'usage des données de santé, notamment en ce qui concerne le consentement par défaut et l'exercice du droit de retrait (opt-out) et d'explicitier les différents types d'utilisation de ces données.

Nous recommandons de vulgariser les termes « utilisation primaire / secondaire des données de santé » pour permettre une compréhension par l'ensemble des utilisateurs (ex : le « carnet de santé » se réfère à l'utilisation primaire des données et les utilisations « à des fins de recherche » à l'utilisation secondaire des données)

Certains d'entre nous pensent qu'il faut écarter le droit de refuser l'utilisation secondaire des données dans certains cas particuliers qui correspondent au bien commun, par exemple en cas de crise sanitaire majeure. D'autres pensent que le droit de refus doit être possible quelle que soit la situation afin de ne pas affecter la confiance et pour que les personnalités « sceptiques/complotistes » ne puissent en tirer un argument politique pour rejeter l'exploitation secondaire de ces données.

Nous préconisons de motiver et éduquer les citoyens en leur démontrant l'intérêt commun de l'espace santé et de l'utilisation (primaire ou secondaire) de données de santé avec les mêmes arguments que pour les professionnels de santé et autres acteurs (cf. ci-dessus).

Nous considérons qu'il est essentiel que l'information soit apportée aux citoyens (sans qu'ils aient besoin de la chercher) en utilisant différents vecteurs de diffusion : spots télé et sur les réseaux sociaux, campagne d'affichage, présence dans les médias, formation des personnels de mairies et des acteurs de la fracture numérique, en suivant l'exemple du lancement de Mon espace santé, en janvier 2022. Il faudra également prévoir des formats adaptés à différents publics, notamment les personnes ayant des besoins spécifiques (supports visuels ou audio pour les malvoyants ou malentendants).

Nous proposons de profiter de l'identification des assurés sociaux auprès de la sécurité sociale ou du remplacement d'une carte vitale perdue pour ouvrir « par défaut » l'espace santé des personnes concernées (si ce n'est pas déjà fait). Il faudrait également les inciter à utiliser et à enrichir Mon Espace Santé afin que cela rentre dans leurs habitudes et que le volume de données récoltées soit important pour l'utilisation secondaire.

Au-delà des informations sur les utilisations des données de santé, nous préconisons d'informer les citoyens à l'aide d'une communication transparente sur les mesures de protection de ces données : montrer la volonté de protéger les données des citoyens et de respecter leur vie privée pour gagner leur confiance.

GARANTIR LA TRANSPARENCE DE L'INFORMATION

Nous proposons que les projets et les résultats de l'utilisation secondaire des données de santé soient accessibles à tous les citoyens sur un site dédié. Il serait possible d'accéder aux demandes de projets (validés ou non, avec justification en cas refus), au suivi des projets et aux résultats des études à l'échelle européenne, quel que soit le résultat positif ou négatif de la recherche.

Les citoyens devraient être informés de toutes les étapes de la collecte de données (cf. ci-dessous le «cycle de vie des données») de manière imagée et interactive dans un souci de transparence et de vulgarisation, pour qu'ils sachent de quelle manière les données de santé sont collectées, où elles sont stockées, mais aussi comment, par qui et dans quel but elles sont utilisées. Les citoyens se sentiront alors informés, impliqués, et rassurés.

Certains d'entre nous pensent que les risques liés à la collecte et à l'utilisation des données (qu'elle soit primaire ou secondaire) ne devraient pas être mis en lumière afin de ne pas complexifier la compréhension des citoyens sur l'utilisation des données, ni les alarmer ou les heurter. D'autres membres du comité, au contraire, seraient plutôt d'avis de prévenir les citoyens des risques dans un souci de transparence totale.

En cas de fuite de données, les citoyens devraient être prévenus au plus tôt pour ne pas entacher leur confiance. Cela pourra être fait à travers une communication emailing, par texto ou même via un message sur Mon Espace Santé.

Il faudrait ajouter un message de sensibilisation sur l'application pour rappeler aux patients les processus de Mon Espace Santé et prévenir les fraudes (par exemple : Attention aux fraudes, nous ne vous demanderons jamais votre numéro de sécurité sociale).

MESURER LE NIVEAU D'INFORMATION DES PERSONNES POUR GARANTIR L'ÉTHIQUE DE L'OPT-OUT

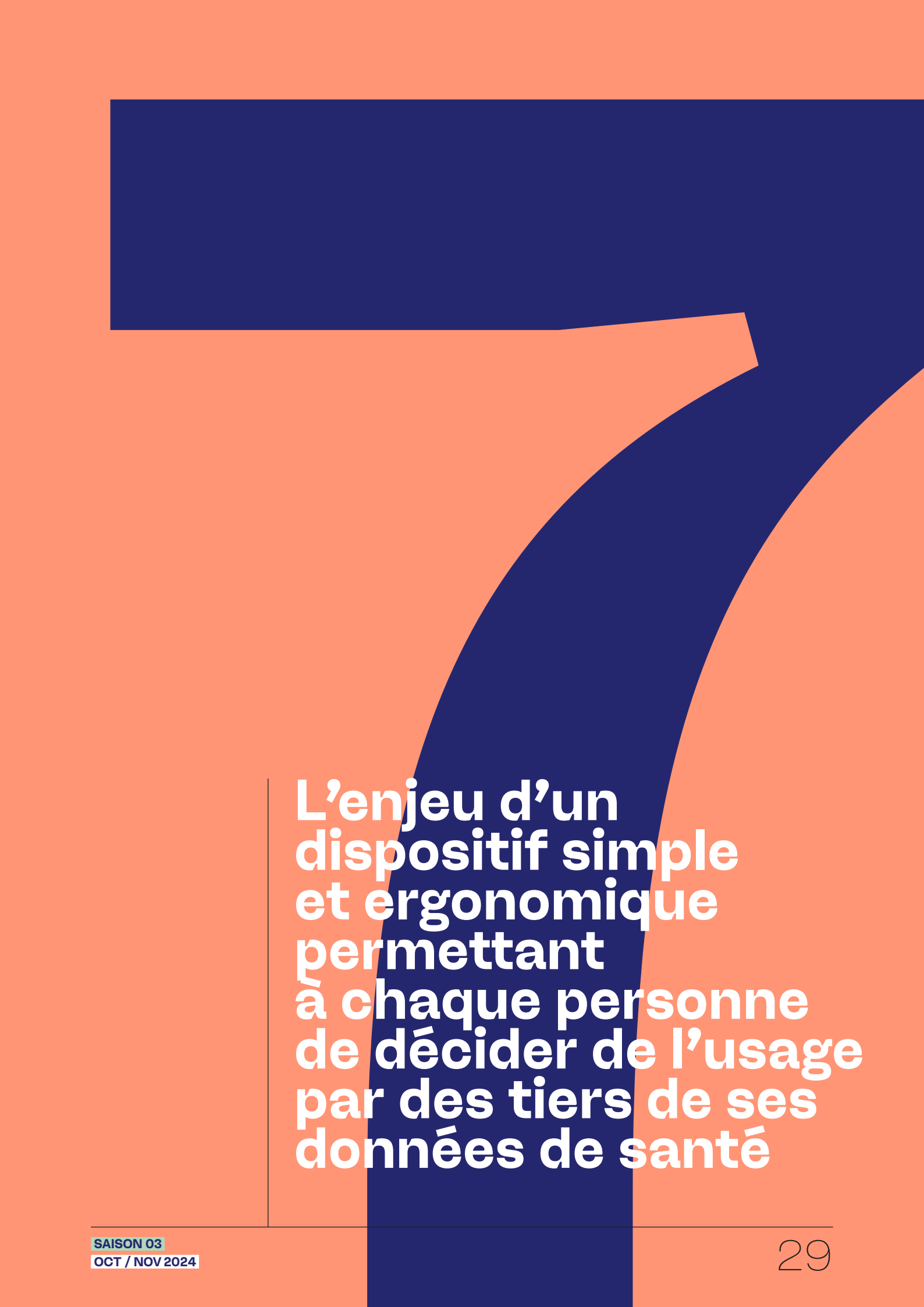
Comme indiqué précédemment, tous les messages informant sur les données de santé et particulièrement sur le droit d'opposition à l'usage des données devraient être rédigés dans un langage clair et facile à comprendre par tous.

Nous préconisons, en outre, de mettre en place des questionnaires et sondages auprès des citoyens pour évaluer leur compréhension des mécanismes de droit de retrait, par exemple : «Savez-vous que vos données de santé sont collectées pour des recherches médicales?», «Savez-vous comment exercer votre droit de retrait? »... Cela pourra passer par des campagnes emailing avec l'envoi des formulaires en ligne, pour faciliter l'analyse des résultats.

Enfin, nous recommandons de ne pas utiliser le terme opt-out mais plutôt «droit de retrait» ou «droit de rétractation» pour éviter un langage trop technique, qui pourrait induire les patients en erreur et gêner la bonne compréhension de ce que recouvre ce terme.

« Savez-vous que vos données de santé sont collectées pour des recherches médicales ? »

« Savez-vous comment exercer votre droit de retrait ? »



**L'enjeu d'un
dispositif simple
et ergonomique
permettant
à chaque personne
de décider de l'usage
par des tiers de ses
données de santé**

Nous souhaitons **faciliter la procédure de retrait de consentement sur Mon Espace Santé en cas de refus de réutilisation de données de santé**. Cela pourra par exemple être fait dès l'inscription sur l'application via une fenêtre pop-up ou un texte de survol. Il sera important de communiquer régulièrement sur ce droit pour que les citoyens ne se sentent pas « piégés » et qu'ils aient confiance dans la gestion des données. Nous demandons que les patients puissent retirer leur consentement à différents niveaux pour personnaliser au mieux leurs desiderata (utilisation primaire, secondaire, en fonction des pays, des organismes...). **Il est aussi nécessaire que les citoyens sachent que leurs choix sont modifiables**. Comme pour l'information, le dispositif permettant à chaque personne de piloter ses droits relatifs à l'accès à ses données de santé par des tiers doit être ergonomique et présenté dans un langage compréhensible par tous.

L'intérêt de ce dispositif sera d'une part de respecter la liberté individuelle de chaque citoyen et d'autre part de lui permettre d'avoir confiance dans le système car il y contribue. Le fait de pouvoir changer d'avis à tout moment et selon chaque situation (voyage à l'étranger, situation familiale qui évolue, changement d'opinion) permettra aussi d'établir un climat de confiance.

Il convient de **différencier l'utilisation primaire et secondaire des données** de santé même s'il y a un formulaire unique disponible. Nous proposons que ce formulaire soit **accessible sur Mon espace santé**.

Concernant l'utilisation des données de santé, nous suggérons une formulation simple de type « oui | non » et une explication des termes

employés. Ces termes pourraient être décrits par un texte (type « ? » à côté d'un mot – info-bulle) voire une courte vidéo pédagogique.

Par défaut les cases sont cochées « oui » pour exprimer le consentement par défaut. Si on est en désaccord (droit de retrait ou opt-out), il faut décocher la case « oui » et cocher la case « non ».

Il doit être possible :

- ➔ De choisir la durée (ou la période, de date à date) pour laquelle la personne ne souhaite plus donner son accord (notamment en cas de voyage)
- ➔ Revenir sur sa décision à tout moment (ex : possibilité de changer d'avis en cas de voyage à l'étranger) sans avoir à se justifier.
- ➔ Il doit être possible de demander la correction ou le retrait des données de santé.

Pour rassurer, le formulaire doit rappeler que les données ne permettent pas d'identifier la personne concernée (elles sont pseudonymisées, c'est-à-dire que l'utilisateur des données ne peut pas relier celles-ci à la personne concernée).

Nous demandons qu'il soit précisé qu'en aucun cas, le partage des données de santé ne peut être rémunéré : la personne concernée ne peut pas vendre ses données et personne ne peut les lui acheter (industriels, chercheurs...).

Nous nous posons la question : comment le citoyen qui ne souhaite pas partager ses données à l'assurance que ses volontés sont respectées ? (Suggestion : vérification par un algorithme du respect du choix ?)

➤ Exemple d'un formulaire de recueil de consentement à l'utilisation de mes données de santé disponible dans Mon espace santé

Types d'utilisation		oui	non
Carnet de santé (Utilisation primaire)	Bris de glace	☒	☐
	Partage de mes données avec le corps médical	☒	☐
À des fins de recherche (Utilisation secondaire)	Partage de mes données en France	☒	☐
	Partage de mes données en Europe	☒	☐
	Être informé en cas de découverte d'une maladie	☒	☐



Le rôle des citoyens dans la gouvernance fonctionnelle et dans la définition de l'éthique de l'utilisation des données de santé

LE BUT DU DISPOSITIF DE GOUVERNANCE À DÉFINIR EST D'AMÉLIORER DE FAÇON CONTINUE LA QUALITÉ DU SYSTÈME DE SANTÉ ET DES ORGANISATIONS QUI LE COMPOSENT. L'ESSENCE DE LA DÉMARCHE DOIT S'APPUYER SUR UNE VOLONTÉ DE SÛRETÉ, DE SOUVERAINETÉ ET DE TRANSPARENCE EN RENDANT DES COMPTES SUR SA RÉUSSITE.

DANS LE CADRE DE CETTE ACTION COLLECTIVE, ET AVEC POUR VOLONTÉ DE GARANTIR L'INTÉRÊT COMMUN, NOUS, CITOYENS, SOMMES ACTEURS DU PROCESSUS D'UTILISATION DES DONNÉES NUMÉRIQUES DE SANTÉ. LA GOUVERNANCE ET LE RÔLE DU CITOYEN SE DÉCLINENT À DIFFÉRENTES ÉCHELLES ET PERMETTENT DE RENFORCER LA CONFIANCE EN CHERCHANT À ACCROÎTRE LA COMPRÉHENSION ET L'ACCESSIBILITÉ DE LA DÉMARCHE.

VULGARISER LA GOUVERNANCE DE CES DONNÉES DOIT PASSER, D'UNE PART, PAR UNE CLARIFICATION DU RÔLE DES DIFFÉRENTS ACTEURS IMPLIQUÉS DANS LEUR PRODUCTION, LEUR COLLECTE, LEUR PARTAGE ET LEUR UTILISATION. D'AUTRE PART, CELA DOIT PASSER PAR UNE CLARIFICATION DES MODALITÉS (TECHNIQUES, JURIDIQUES) DE PRODUCTION, DE COLLECTE, DE PARTAGE ET D'UTILISATION DE CES DONNÉES.



À L'ÉCHELLE LOCALE

(LES ENTREPÔTS DE DONNÉES DE SANTÉ)

Même si chaque entité en charge d'un entrepôt est « propriétaire » de son dispositif de gestion des données, **le patient reste propriétaire de ses données personnelles jusqu'à anonymisation de ces dernières**. En ce sens, il a un certain nombre de droits déjà décrits dans le RGPD ; cependant les données de santé étant plus critiques que d'autres données personnelles, ses droits doivent être élargis de manière à le protéger plus amplement. Afin de répondre à des demandes d'accès à l'intérieur de l'entité qui a mis en place l'entrepôt, il existe déjà un comité scientifique et éthique (CSE).

Nous souhaitons que ce comité scientifique et éthique soit rendu obligatoire pour chaque entrepôt et que sa forme et son rôle soient clairement définis. Aussi, ces comités scientifiques et éthiques seront rattachés à la CNIL, afin de centraliser, historiser et communiquer sur l'ensemble des demandes traitées par les CSE.

De plus, le travail des CSE doit être rendu visible par la mise en place d'une plateforme publique centralisant les décisions rendues par l'ensemble de ces comités, au même titre, dans les mêmes conditions et au même endroit que les demandes qui ont été traitées par le HDH. Cette plateforme d'information mettra en avant la possibilité de questionner la CNIL sur les décisions rendues par les CSE. La CNIL devra produire des indicateurs pour mesurer le niveau d'information des citoyens.

Sur le même principe que le HDH dans le cas d'une mise à disposition d'un jeu de données, nous souhaitons que soit imposé aux fournisseurs de logiciels d'entrepôt de données la mise en place d'espaces de travail de données isolés du reste de l'entrepôt.

Il nous semble important de donner la capacité à une entité en charge d'un entrepôt de respecter les principes de minimisation et de pseudonymat ou d'anonymat dans le cadre d'accès aux données.

Dans un objectif de transparence, les associations d'utilisateurs doivent avoir un droit de regard sur l'ensemble des demandes d'accès aux données afin, avec le CSE voire dans le cadre de ses travaux (si elles en sont membres), de repérer des abus et d'avoir la capacité de les signaler. Si cela n'aboutit pas, les associations d'utilisateurs auront la possibilité de saisir la CNIL.

De même, nous souhaitons un partage à la communauté scientifique pour toute recherche ayant abouti grâce à l'utilisation des données de santé.



À L'ÉCHELLE FRANÇAISE

(HEALTH DATA HUB)

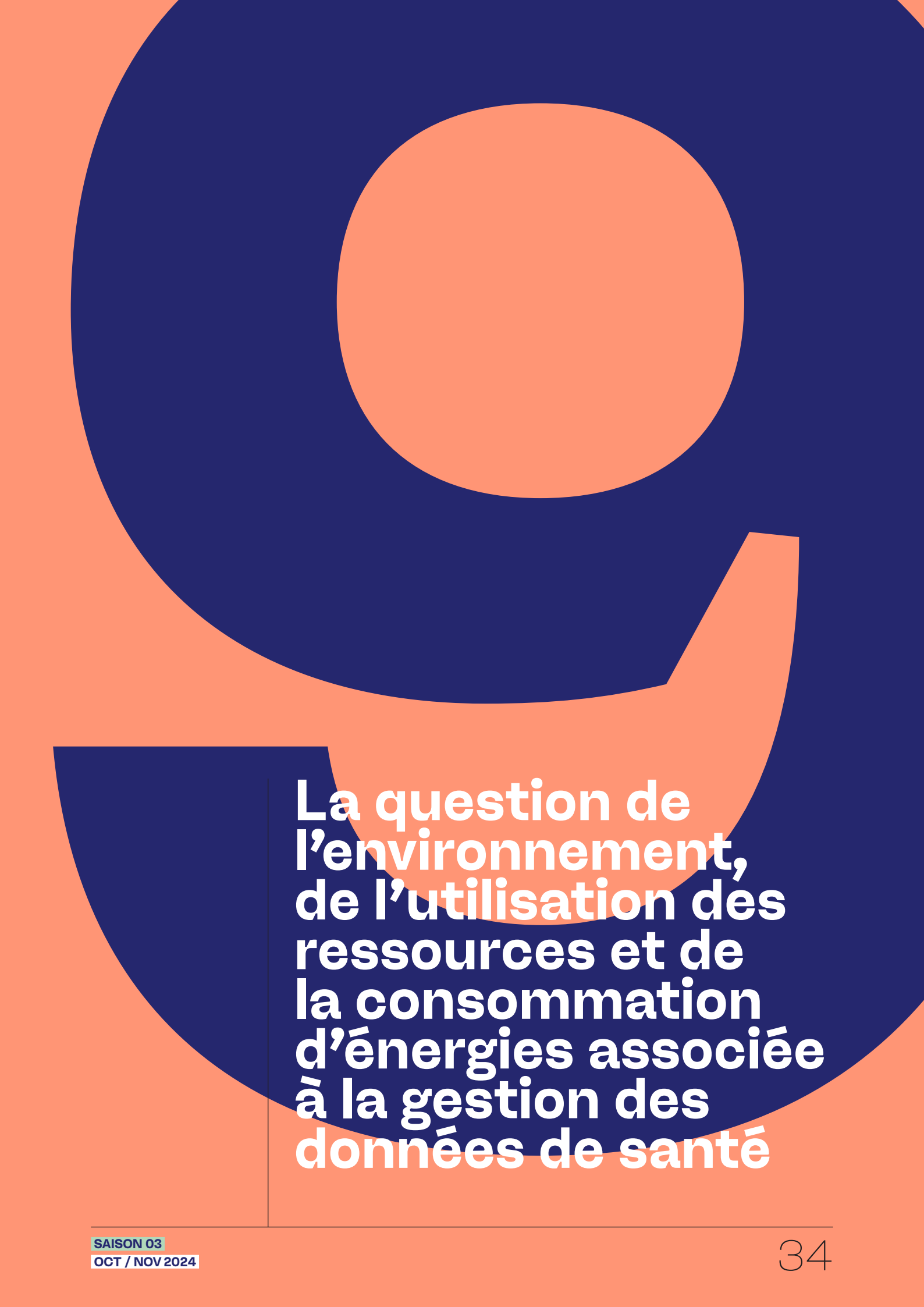
Dans une volonté de rendre le HDH universel nous souhaitons que l'ensemble des partages de données extérieurs à l'environnement d'un entrepôt passe par le HDH afin d'assurer le respect de l'ensemble des principes éthiques, de transparence et de sûreté énoncés par la législation.

Nous souhaitons que soient rendus publics les audits réalisés par la CNIL au sein des entités qui gèrent un entrepôt. Nous souhaitons que ces audits concernent aussi les activités du CSE. La CNIL doit être l'interlocuteur privilégié des citoyens à des fins de recours ou d'alerte, pour cela une méthode de saisine doit être identifiable et facile d'utilisation.



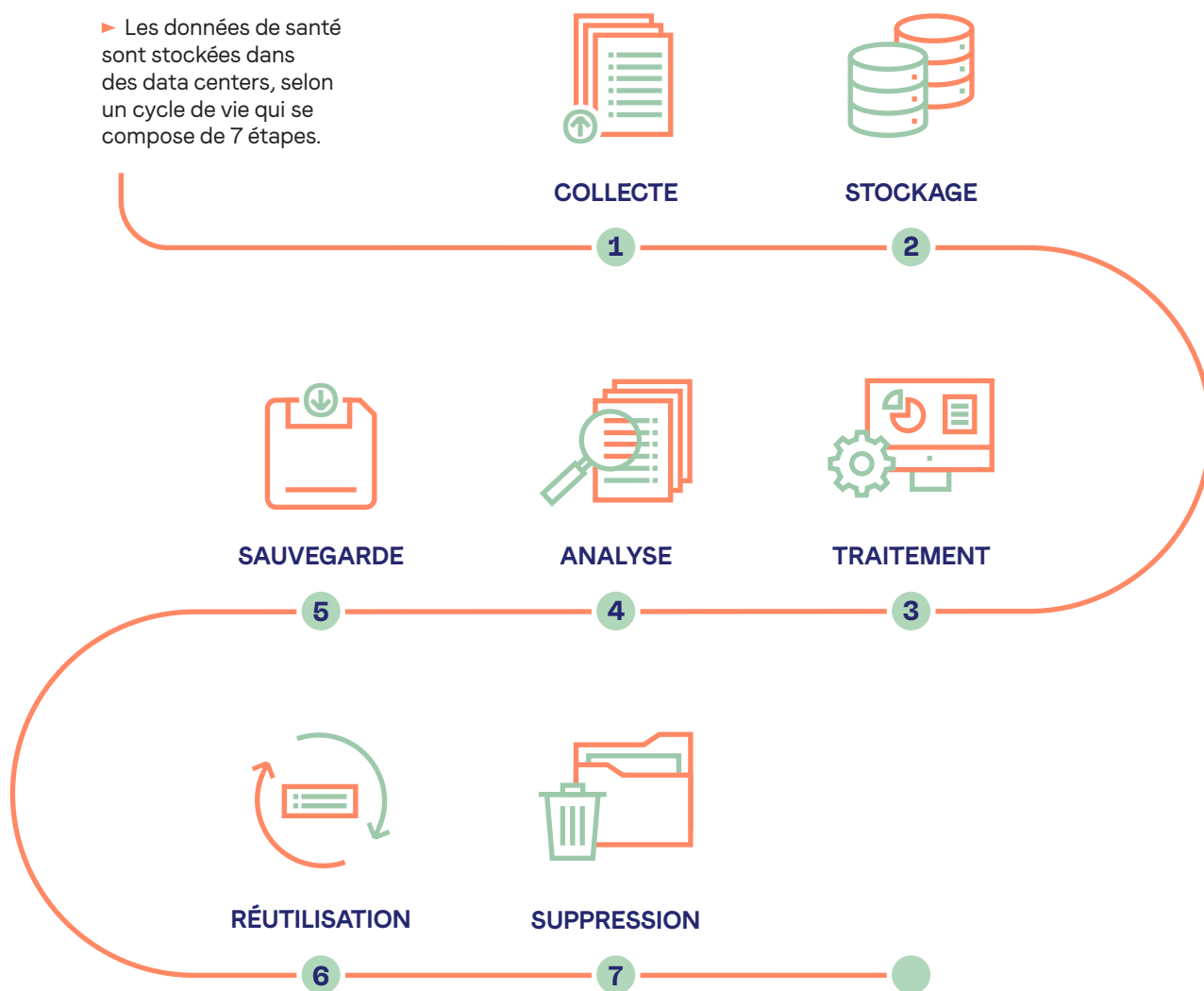
À L'ÉCHELLE EUROPÉENNE

Il nous semble que la structure déployée au niveau national répond de manière assez exhaustive aux besoins du citoyen dans son rôle d'acteur de ses données de santé. Un Comité Éthique Européen, devra avoir des missions de contrôle et d'audit mais également être un interlocuteur que le citoyen pourra interpeller s'il en ressent le besoin, par exemple en tant que lanceur d'alerte.



La question de l'environnement, de l'utilisation des ressources et de la consommation d'énergies associée à la gestion des données de santé

► Les données de santé sont stockées dans des data centers, selon un cycle de vie qui se compose de 7 étapes.



Les données de santé prennent de plus en plus de place dans les data centers en raison des nouvelles technologies médicales (imagerie) et de la numérisation. Sans action pour réduire l'impact écologique d'ici 2050, les conséquences pourraient être irréversibles pour l'environnement. C'est la raison pour laquelle l'enjeu écologique du cycle de vie des données de santé est un sujet d'actualité important. En effet, ce cycle de vie génère **différents impacts écologiques**, d'où la nécessité de **proposer des recommandations pour limiter la pollution**.



1%

2%

À l'échelle mondiale, les data centers représentent plus de 1% de la consommation d'électricité **6** (→ P38) en France, cela représente 2%.

LES DIFFÉRENTS IMPACTS ÉCOLOGIQUES DU CYCLE DE VIE DES DONNÉES DE SANTÉ

Les impacts écologiques liés au cycle de vie des données de santé sont nombreux et se distinguent selon deux catégories :

Les sources de pollutions :

- La pollution lors du refroidissement de serveurs
- Les déchets électroniques
- Les métaux lourds et produits chimiques
- L'émission de gaz à effet de serre
- La pollution liée à la construction et la maintenance

Les conséquences environnementales de ces sources de pollution :

- L'épuisement des ressources en eau
- La perte de biodiversité
- La contamination du sol et de l'eau
- La chaleur résiduelle
- Le réchauffement climatique

Ces impacts écologiques nous conduisent à formuler des recommandations afin de les limiter.

NOS RECOMMANDATIONS POUR LIMITER L'IMPACT ÉCOLOGIQUE DES DONNÉES DE SANTÉ

La pollution des data centers est une réelle question à l'échelle nationale comme à l'échelle européenne. La CSRD (Corporate Sustainability Reporting Directive) a vu le jour en janvier 2024 est une directive qui oblige les entreprises **7** (**→ P38**) à publier des informations sur la soutenabilité (durabilité) de leur fonctionnement.

Dans la même logique, nous recommandons d'obliger les entreprises et les administrations qui font appel à leurs services pour le stockage des données de santé de publier un rapport d'impact écologique comprenant un bilan carbone. Ceci favorisera la transparence en matière de responsabilité sociale et environnementale dans le domaine de la gestion des données de santé.

Nous recommandons aussi la création et la mise en place d'un label national « Santé Numérique Responsable ». Ce label pourrait certifier les infrastructures et services traitant des données de santé. Il comprendrait des critères combinant cybersécurité, éthique et durabilité environnementale, à l'image du Label Numérique Responsable français ou du Green Public Procurement au niveau européen.

Nous préconisons également qu'un cadre juridique prévoit que les utilisateurs des données de santé (professionnels de santé, chercheurs, etc.)

soient tout autant impliqués et responsabilisés sur ces questions écologiques que les entreprises qui stockent les données.

Nous recommandons de trouver une solution afin de réutiliser les énergies produites par les data centers. Nous savons, par exemple, qu'ils produisent une chaleur « fatale » qui nécessitent un système de refroidissement très performant et énergivore. Cette chaleur fatale pourrait être utilisée pour produire une autre forme d'énergie ou chauffer des équipements (comme le font déjà certains).

L'État a un devoir d'exemplarité face aux citoyens pour un avenir plus vert et durable. Il nous paraît important de sensibiliser et former les citoyens à l'impact écologique des données en général et plus particulièrement des données de santé. Il serait opportun de faire appel à l'intervention d'experts en écologie qui pourraient intervenir à ce sujet.

Il est indispensable d'optimiser l'utilisation des données de santé afin d'éviter les doublons ainsi que « les données inutiles ».

Nous recommandons également de promouvoir le recyclage et la réparation des équipements (des data centers, cloud...) afin de réduire les déchets et de préserver les ressources.

Enfin, l'intelligence artificielle, bien que prometteuse, soulève des défis écologiques majeurs. À titre d'exemple, Google ne pourra pas respecter ses engagements en termes d'émission de gaz à effet de serre en 2030 à cause de l'intelligence artificielles. Son impact dépasse largement le cadre des données de santé pour toucher l'ensemble des données numériques. Son utilisation croissante intensifie considérablement la consommation de ressources et d'énergie ; cela mérite une réflexion pour en limiter les effets.



Nous recommandons aussi la création et la mise en place d'un label national « Santé Numérique Responsable ».

LE PROCESSUS DE DÉLIBÉRATION

IIIIII

PREMIER
WEEK-END

- Constitution du groupe et découverte de la question posée
- Auditions d'experts - Information approfondie sur les éléments constitutifs de l'environnement de la question :
 - La réglementation sur la protection des données personnelles, (Gildine Croize, directrice juridique et de Marjolaine Cassar, Responsable du Département numérique, CNAM)
 - Présentation du Health Data Hub, (Eliza Régnier, cheffe de projet ouverture à la société, Health Data Hub)
 - En Belgique, un cadre éthique pour l'Espace européen des données de santé, (Wannes Van Hoof, chef du service de la santé, SCIENSANO - Belgique)
 - L'évolution du cadre juridique du numérique en santé, (Emma Miquel, doctorante en droit, Université de Lille)
 - Le règlement pour un espace européen des données de santé, (Emilie Passemard, directrice de projet, ministère de la Santé)
- Bilan des connaissances acquises et identification des nouvelles questions - discussions au sein du groupe

IIIIII

DEUXIÈME
WEEK-END

- Audition de témoins, d'acteurs et d'autres expériences européennes :
 - Le rôle des associations de patients (Arthur Dauphin, chargé de mission Numérique en santé à France Asso Santé, Alain Olympie, conseiller et militant en santé et Antoine Bessou, directeur du pôle « Données de santé » à Vaincre la mucoviscidose)
 - Les usages secondaires des données de santé, le point de vue de chercheuses (Sandra Malak, oncologue à l'institut Curie et Brigitte Séroussi, Professeure des universités et praticienne hospitalière)
 - Comment ça se passe dans d'autres États membres européens ? (Paula Nurmi, Finlande, Mari Luist, Estonie et Julia Jauer, Allemagne)
 - Le point de vue des entreprises (Mariuca De Hillerin, Lifen, Rémy Choquet, Roche et Thierry Chanet, Arkhn)
- Réflexions collectives sur les informations et préparation de la réponse à la question posée par la DNS

IIIIII

TROISIÈME
WEEK-END

- Discussions, préparation de la réponse à la question,
- Rédaction, par les membres du Comité citoyen, de la réponse à la question posée par la DNS

- L'ensemble du processus a été animé par le cabinet Res publica

LES MEMBRES DU COMITÉ CITOYEN SAISON 3

→ MIREILLE BALLEREAU

→ FREDERIC BERNARD

→ FANY BOUCEHABA

→ DYLAN BOUCHER

→ THOMAS CHAROLLES

→ FLORENCE CLOITRE-EMZIVAT

→ DANIEL COHEN

→ YVAN COTTA

→ DENIS GRENN

→ CLAIRE DAVIET

→ JEAN-LOUIS DEVOIZE

→ ALI DIDAOU

→ CÉLINE GRESSARD

→ NELLY GUERINEAU

→ JEAN-MARIE HUCHETTE

→ CORINNE IZQUIERDO

→ VALENTINE JALLAS

→ MOHAMED KRAMDI

→ ELOI LAWSON

→ YANNICK LEROY

→ DZEILLERE MAGHNI

→ MARYLINE MARCEL

→ AYMAN OUEDRAOGO

→ PIERRE PEREIRA-SALGUEIRO

→ JULIE PRESIER

→ XAVIER SENS

→ MICHEL TAPIE

→ MATTHIEU TERRIER

→ MAEVA TROUILH

→ CÉLIA YAO KOMISSA

Les membres du Comité citoyen ont été recrutés par Harris Interactive de manière à constituer un panel illustrant la société française relativement aux critères suivants : âge, genre, catégorie socioprofessionnelle, la région et le type de territoire d'habitation (rural, péri-urbain, urbain).

NOTES DE BAS DE PAGE

1 Assistance publique – Hôpitaux de Paris (→ P 14)

2 Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (→ P 14)

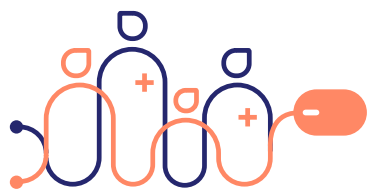
3 Commission nationale de l'informatique et des libertés (→ P 14)

4 Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final - https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0002.02/DOC_1&format=PDF (→ P 17)

5 C'est-à-dire équivalente pour tous les patients partout en Europe. (→ P 26)

6 Source : Agence internationale de l'énergie (→ P 35)

7 Seules les « grandes entreprises » sont concernées à partir de 2026 ; progressivement les moyennes puis les petites entreprises seront concernées dans les années suivantes. (→ P 36)



COMITÉS CITOYENS DU NUMÉRIQUE EN SANTÉ

DESSINONS ENSEMBLE
LA SANTÉ DE DEMAIN