# PIA
# ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES

## Programme Prédice

**PARTAGER et ÉCHANGER** l'information pour mieux se coordonner et **FACILITER L'ACCÈS** au système de santé.

# ÉTUDE DU CONTEXTE

## VUE D'ENSEMBLE

### Quel est le traitement qui fait l'objet de l'étude ?

Le programme Prédice propose aux professionnels et aux établissements de santé un bouquet de services dans le but d'améliorer l'organisation et la qualité de la prise en charge. Prédice positionne également l'usager en santé comme acteur de sa santé en lui permettant, par le biais de services numériques, de co-construire son parcours de santé en interaction avec les professionnels et les structures de santé.

Il est construit en cohérence avec les orientations nationales et est interopérable avec l'ensemble des services numériques en santé. Les services de Prédice sont conformes aux standards nationaux en termes de sécurité et d'interopérabilité et respectent une charte éthique.

Les différents services de Prédice sont structurés autour de 3 piliers:

- Les services de mise en relation ;
- Les services de coordination ;
- Les services de télésanté.

**Le présent PIA s'intéresse aux deux premières catégories de services (mise en relation et coordination).**

Un autre PIA sera réalisé pour les services de télésanté.

Le programme prévoit également, à terme, un observatoire des données de santé qui fera l'objet d'un PIA spécifique.

Les services de mise en relation et de coordination proposent les fonctionnalités majeures suivantes :

- Accès à un portail usager (en lien avec l'approche « Ma santé 2022 ») ;
- Accès à un portail pour les professionnels ;
- Rendez-vous en ligne ;
- Pré-admission en ligne ;
- Echange d'information via le dossier de coordination ;
- Partage d'information via le dossier de coordination ;
- Présentation du parcours sous forme d'une « ligne de vie » ;
- Echange instantané ;
- Outillage des parcours de situation complexe.

### Quelles sont les responsabilités liées au traitement ?

➔ Responsables conjoints de traitement

**Agence régionale de santé (ARS) Hauts-de-France**

L'ARS Hauts-de-France détermine la politique de santé régionale et notamment la stratégie régionale en matière de e-santé (Schéma directeur régional des SI de santé). A ce titre, elle a lancé mi-2018 le programme Prédice avec l'ambition d'offrir à l'ensemble des acteurs du système de santé un bouquet de services numériques, qui permet la mise en relation, la coordination des

acteurs et la télésanté. L'objectif de Prédice est de permettre aux usagers/patients, à leur entourage et aux professionnels de santé de mieux interagir avec l'ensemble des composantes du système de santé. L'ARS Hauts-de-France exerce par ailleurs une responsabilité de traitement sur le futur observatoire des données de santé *(cf. supra)*

**Sant& Numérique Hauts-de-France (S&N)**

Le groupement d'intérêt public Sant& Numérique Hauts-de-France est l'assistance à maitrise d'ouvrage en matière d'e-santé de l'ARS. Il décline la stratégie régionale en e-santé de façon opérationnelle, fédère les acteurs, et conduit les projets. Au regard du droit des marchés publics, en tant que pouvoir adjudicateur, S&N établit les cahiers des charges et interagit avec le sous-traitant titulaire de l'Accord-cadre chargé de la mise en œuvre des traitements du programme Prédice, la société Maincare Solutions. S&N agit aux côtés des établissements de santé publics et ESPIC dans une logique de responsabilité conjointe de traitement. S&N est membre du GCS (Groupement de Coopération Sanitaire) AMEITIC.

**Les établissements de santé publics et ESPIC**

Les établissements de santé publics et ESPIC de la région Hauts-de-France sont bénéficiaires directs de l'Accord-cadre et bénéficiaires indirects pour les services managés (regroupant l'activité opérationnelle de gestion de l'infrastructure informatique d'un Système d'Information, notamment l'hébergement).

**Répartition des rôles entre les responsables conjoints de traitement :**

La répartition des rôles est formalisée selon un modèle RACI validée par l'ensemble des responsables impliqués. Le modèle RACI repose sur les principes explicités ci-dessous :

*Les valeurs :*

- R : Responsible (réalise l'activité) ;
- A : Accountable (approuve et rend compte) ;
- C : Consulted (est consulté) ;
- I : Informed (est informé).

*Explications et règles :*

- Le ou les R (le A peut aussi avoir un rôle de R) réalisent l'activité. Il doit y avoir au moins un R pour chaque activité. Le A peut déléguer la réalisation de l'activité au(x) R, mais est responsable du résultat.
- Le A est donc celui qui doit rendre des comptes sur l'avancement de l'activité et qui la définit. Il y a toujours un A (et un seul) pour chaque activité. « Avoir le A » signifie être totalement responsable des résultats d'une activité (de sa bonne fin) et de sa définition.
- Les C sont les acteurs (entités, personnes, groupes …) qui doivent être consultés, avant ou au cours de la réalisation de l'activité.
- Les I sont les acteurs qui doivent être informés.

Dans le cas d'une responsabilité conjointe, les périmètres de responsabilité sont précisés dans la colonne « Observations ».

La colonne « ES » décrit les responsabilités des établissements de santé publics et ESPIC tels que présentées ci-dessus.

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| **Elaboration et évolution du cadre contractuel de Prédice** | | AR | C | RC | |
| **Modèle de Registre des activités de traitement des Services Prédice** | | I | I | AR | S&N transmet aux MEMBRES BENEFICIAIRES et à l'ARS les éléments leur permettant de compléter leur propre registre des traitements. |
| **Registre des activités de traitement des Services Prédice** | | R | R | AR | Les Parties et les MEMBRES BENEFICIAIRES s'engagent à tenir un registre des activités de traitement effectuées sous leur propre responsabilité. Ce registre devra comporter toutes les informations prévues par la réglementation. |
| **Adéquation des Services Prédice aux besoins des membres** | | A | C | RC | S&N est chargé par l'ARS de recueillir les besoins des MEMBRES BENEFICIAIRES et de s'assurer que le développement du programme Prédice répond à ceux-ci. |
| **Utilisation des services Prédice dans le respect de la règlementation et des relations contractuelles** | | C | R | AR | S&N fournit la politique de sécurité et les règles de bon usage de la plateforme Prédice que les MEMBRES BENEFICIAIRES se chargent de faire appliquer à leur niveau. |
| **Définition et évolution de l'Observatoire régional des données** | | A | IC | RC | L'ARS définira, autant que de besoin avec le support de S&N en tant qu'assistance à maitrise d'ouvrage, ses attentes concernant l'Observatoire régional des données. |

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| **Exploitation de l'Observatoire régional des données** | | AR | | RC | Le rôle de S&N pourra éventuellement être réévalué en R si l'ARS décide d'une délégation de tout ou partie de l'exploitation à S&N. |
| **Exploitation du serveur régional de rapprochement d'Identité** | | C | R | AR | S&N met en place un Service Régional de Rapprochement d'Identité (SRRI) chargé de la gestion des rapprochements d'identités à l'échelon régional. Les personnels du SRRI sont placés sous l'autorité d'un professionnel de santé et leur contrat de travail prévoit une clause de confidentialité renforcée. Le SRRI échange au quotidien avec les établissements afin de résoudre les problématiques de rapprochement. Les établissements réalisent les modifications nécessaires dans leur GAM. L'ensemble des MEMBRES BENEFICIAIRES est impliqué dans la définition et l'amélioration continue de la politique régionale de rapprochement. |
| **Exploitation du serveur de rapprochement d'Identité au niveau de la Plateforme Prédice de Territoire** | | | AR | C | Les établissements au sein de chaque plateforme Prédice de territoire gèrent leur politique de rapprochement en tenant compte de la politique définie à l'échelon régional. L'activité des cellules d'identitovigilance (CIV) de chaque MEMBRE BENEFICIAIRE et, le cas échéant, de la CIV de territoire sont placées dans le périmètre d'un médecin DIM (à défaut, |

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| | | | | | sous l'autorité d'un professionnel de santé). Le contrat de travail des personnels de CIV prévoit une clause de confidentialité renforcée. Les identités du SRI de territoire sont transmises automatiquement au SRI régional. |
| **Gestion des habilitations des Services Prédice** | Définir et faire évoluer la matrice des droits et habilitations | IC | AR | RC | Les établissements décident, dans le cadre d'une comitologie mise en place par S&N, de la matrice des droits et habilitations pour l'accès aux services Prédice et de ses évolutions. Des modalités de contrôle sont mises en œuvre. |
| | Création des comptes des professionnels de santé | | R | A | Les comptes sont créés automatiquement grâce au connecteur mis en place entre le ROR et l'ODS. Les établissements alimentent le ROR. |
| | Activation, modification des droits d'accès, suppression des droits d'accès des professionnels des établissements de santé | I | R | AR | Les établissements de santé gèrent les droits de leurs professionnels via « Ideodirectory ». |
| | Activation, modification des droits d'accès, suppression des droits d'accès des autres professionnels (professionnels de santé libéraux, professionnels des ESMS, paramédicaux) | I | R | AR | *Pour ces catégories de professionnels, les modalités d'activation sont encore en cours de définition. Ces modalités seront définies par S&N au regard des attentes de ces catégories de professionnels.* |
| | Création, activation, modification des droits d'accès, suppression des droits | AR | | R | |

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| | des professionnels de l'ARS | | | | |
| | Création, activation, modification des droits d'accès, suppression des droits d'accès des usagers | I | | AR | *Les modalités de création et d'activation sont encore en cours de définition. Ces modalités seront définies par Sant& Numérique au regard des attentes* |
| **Information des Personnes concernées** | Usagers utilisateurs des Services Prédice | I | AR | R | Les professionnels de santé restent le premier interlocuteur de l'usager pour l'informer et recueillir son consentement. S&N se charge de fournir la documentation, les éléments de langage et les CGU nécessaires. |
| | Equipes de soins et sous-traitants habilités des MEMBRES BENEFICIAIRES | I | AR | R | Les structures de santé s'assurent de l'information de leur personnel. Sant& Numérique se charge de fournir la documentation, les éléments de langage et les CGU nécessaires. |
| | Utilisateurs et sous-traitants habilités de S&N | | | AR | S&N s'assure de la bonne information des personnels relevant de son périmètre (personnel et sous-traitants) ayant des comptes d'accès à Prédice |
| | Utilisateurs et sous-traitants habilités de l'ARS | AR | | R | L'ARS s'assure de la bonne information de ses personnels ayant des comptes d'accès à Prédice (notamment dans le cadre de l'observatoire des données). S&N se charge de fournir la documentation, les éléments de langage et les CGU nécessaires. |

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| **Exercice des droits des utilisateurs des services Prédice** | | I | IR | AR | Exercice des droits d'accès, rectification, limitation, opposition, suppression et sur le périmètre des Services Prédice.<br>Les MEMBRES BENEFICIAIRES prennent en compte les demandes d'exercice des droits adressés à leur niveau et les transmettent à S&N pour traitement. |
| **Durée de conservation et d'archivage des données** | Données personnelles relevant des MEMBRES BENEFICIAIRES | | A | R | Les MEMBRES BENEFICIAIRES sont responsables des durées de conservation et d'archivage des données concernant leurs activités propres. Ils mettent en œuvre les mesures techniques et organisationnelles appropriées pour protéger ces données. |
| | Données de coordination relevant du niveau régional | | R | A | S&N est responsable des données de coordination régionales. |
| | Données relatives au recueil du consentement | | AR | R | Les MEMBRES BENEFICIAIRES mettent en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données archivées et s'assurer de leur authenticité et de leur intégrité. |
| **Transfert hors UE** | Aucun transfert hors UE autorisé | I | I | AR | S&N s'assure qu'il n'y aucun transfert hors UE |
| **Sécurité au niveau du MEMBRE** | Mise en place d'une politique interne de protection des données à caractère | I | AR | I | |

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| **BENEFICIAIRE** | personnel dans le respect de l'état de l'art du moment. | | | | |
| **Sécurité au niveau du MEMBRE BENEFICIAIRE** | En cas de Violation de données à caractère personnel :<br>- notification auprès des autorités compétentes (CNIL)<br>- Information des personnes concernées | I | AR | I | |
| **Sécurité des services Prédice** | Analyse d'impact | I | I | AR | |
| | Mise en place d'une politique interne de protection des données à caractère personnel adossée à une PSSI dans le respect de l'état de l'art du moment. | I | R | AR | |
| | Information et notification auprès des autorités compétentes et le cas échéant des personnes concernées en cas de la Violation de données à caractère personnel | I | R | AR | |
| | Identification et production d'indicateurs sur la qualité des services et sur la satisfaction des utilisateurs | I | AR | RI | |

| Activités | Description | ARS | ES | S&N | Observations |
|---|---|---|---|---|---|
| **Qualité des services Prédice** | relevant de la responsabilité des membres (délivrance de l'information, procédures mises en œuvres, satisfaction utilisateurs professionnels et usagers…) | | | | |
| | Identification et production d'indicateurs sur la qualité des services et sur la satisfaction des utilisateurs relevant de la responsabilité de S&N (indicateurs sécurité, indicateurs disponibilité, indicateurs satisfaction sur la plateforme…) | I | I | AR | |
| | Identification et production d'indicateurs sur la qualité des services et sur la satisfaction des utilisateurs relevant de la responsabilité de l'ARS | AR | I | R | |

### ➜ Sous-traitant principal

**Maincare Solutions**

Maincare Solutions est une société spécialisée dans la fourniture de prestations de services informatiques dans le domaine de la santé. Titulaire de l'Accord-cadre conclu avec le GCS AMEITIC ainsi que des marchés subséquents, Maincare Solutions est partenaire industriel du programme. Il agit en tant que sous-traitant principal des responsables conjoints de traitement précités.

### ➜ Autres acteurs impliqués dans le programme Prédice

**Les autres acteurs de santé de la région**

Acteurs de ville, établissements de santé privés, établissements et services médico-sociaux bénéficient de l'accord-cadre de manière indirecte en qualité de membres de S&N.

**GCS AMEITIC**

Le GCS AMEITIC est la centrale d'achat ayant élaboré l'accord-cadre Prédice avec Maincare Solutions. Il est le porteur du projet au sens FEDER.

**CHEOPS Technology**

Spécialiste des infrastructures informatiques sécurisées, agréé hébergeur de données de santé (HDS), sous-traitant ultérieur auprès de Maincare Solutions.

### ➜ Gouvernance du programme Prédice

La gouvernance du programme s'articule autour de plusieurs instances de pilotage, de coordination et d'animation.

- Le **comité de pilotage** réunit les représentants des différents bénéficiaires ainsi que des représentants des usagers autour de l'ARS.

- Le **comité de coordination** est d'ordre technique. Il réunit des représentants spécialisés des bénéficiaires ainsi que le sous-traitant (Maincare Solutions).

Différents **ateliers** ont été mis en place permettant d'exprimer les spécificités territoriales et d'adapter la mise en place des outils proposés aux besoins sur chaque territoire, 14 thématiques d'échanges ont été définies, dont celle liée au thème « SSI/RGPD ».

## Quels sont les référentiels applicables ?

**Référentiels spécifiques santé :**

- Art. L. 1110-4 CSP : prise en charge du patient ;
- Art. L. 1110-12 CSP : définition de l'équipe de soin ;
- Art. L. 1111-8 CSP : hébergement de données de santé ;
- Art. L. 1111-8-1 CSP : utilisation du NIR pour l'identification des dossiers patients ;
- Art L. 1434-12 : définition de la communauté professionnelle territoriale de santé;
- Art. R. 6316-1 à 6316-11 CSP : télémédecine ;
- Art R1110-1 à R1110-3 ;
- Décret n°2016-994 du 20 juillet 2016 et n°2016-1349 du 10 octobre 2016 ;
- Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé.

**Référentiels généraux :**

- RGPD
- Loi Informatique et Libertés

**Référentiels sécurité des SI :**

- RGS
- PGSSI-S
- PSSI-E
- PSSI-MCAS

# DONNÉES, PROCESSUS ET SUPPORTS

## Quelles sont les données traitées ?

**Données des usagers:**

- Données d'identification de l'usager : nom de naissance, nom d'usage, prénoms, date de naissance, genre, NIR ou NIA, INS-C (optionnel), lieu de naissance (code INSEE ou code postal), coordonnées (électroniques, postales, téléphoniques) ;
- Données relatives à la vie personnelle : habitudes de vie ;
- Données de santé : pathologies, affections, antécédents familiaux, données relatives aux soins (données nécessaires à la coordination ville/hôpital, données liées aux parcours de situation complexe, données d'imagerie médicale, données de biologie en format pdf ou structuré…) ;
- Données sur l'équipe de soins : liste des professionnels participants à la prise en charge de l'usager et épisodes de soins associés, données PMSI ;
- Données de connexion : identifiants des terminaux, identifiants de connexion, informations d'horodatage, identification des actions.

**Données des professionnels de santé :**

- Données d'identification : nom, prénom, profession, spécialités, coordonnées (postales, électroniques, téléphoniques), numéro RPPS, établissement de rattachement le cas échéant ;
- Données de connexion : identifiants des terminaux, identifiant de connexion, informations d'horodatage, identification des actions ;
- Données relatives à la vie professionnelle : période d'absence, plage de disponibilité (par exemple période d'absence), réunion (avec le nom/prénom des participants, date/heure, lieu, objet), rappel par SMS ou courriels envoyés à l'usager/patient avant un rendez-vous, type de rendez-vous (domicile, cabinet, établissement, téléconsultation,…), rôle du professionnel vis-à-vis de chaque usager/patient aux différents épisodes de soin associés (ex : médecin traitant).

**Données des aidants ou autres personnes tierces:**

- Données d'identification : nom, prénom, coordonnées (postales, électroniques, téléphoniques) ;
- Type de relation avec la personne concernée : conjoint, aidant, famille, tuteur, personne de confiance ;
- Données de connexion : identifiants des terminaux, identifiants de connexion, informations d'horodatage, identification des actions.

**Données des représentants :**

- Données d'identification : nom, prénom, coordonnées (postales, électroniques, téléphoniques) ;
- Type de relation avec la personne concernée ;

- Données de connexion : identifiants des terminaux, identifiant de connexion, informations d'horodatage, identification des actions.

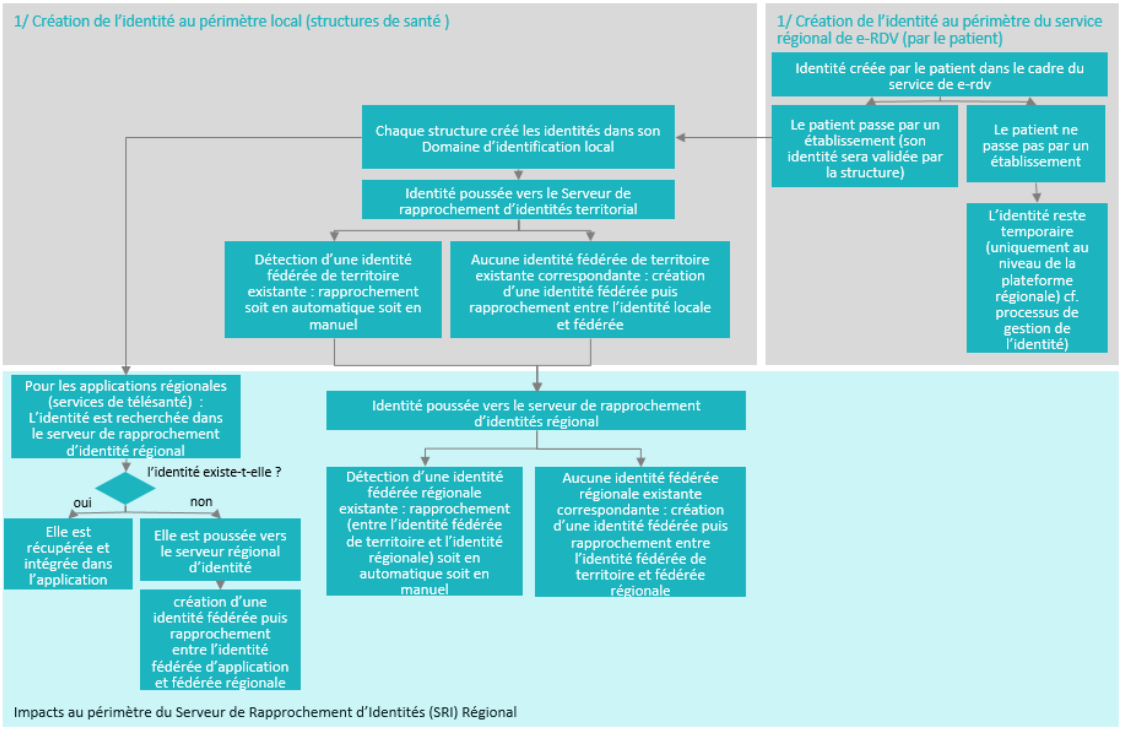
Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

## Introduction

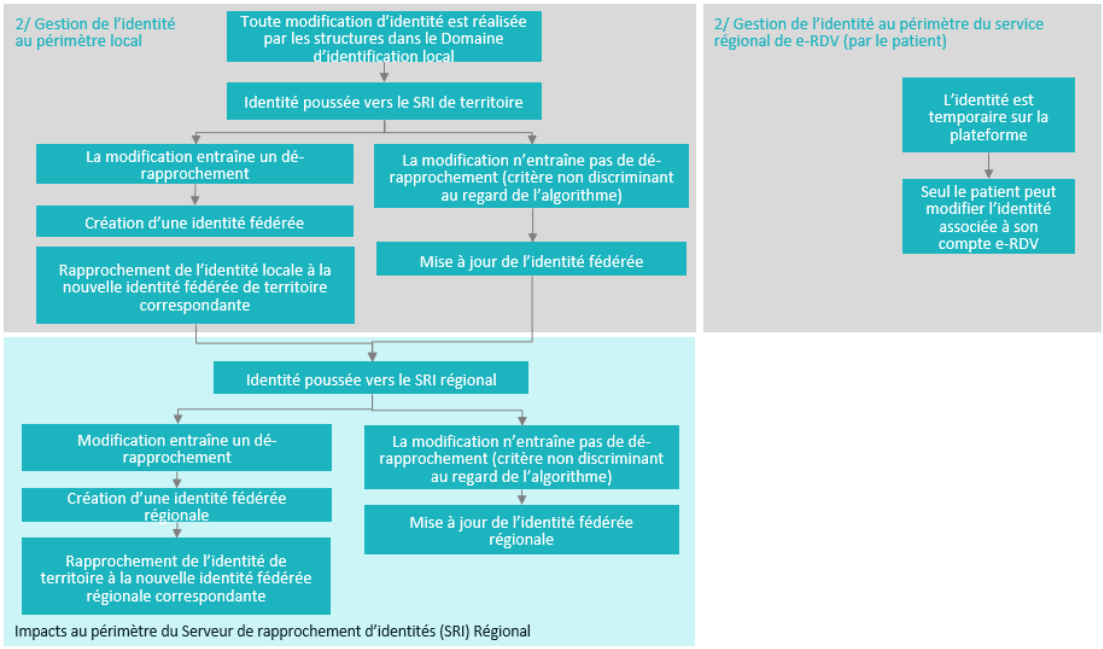
Les cycles de vie vont concerner : les données d'identité, les données du dossier de coordination, les données des professionnels et des utilisateurs.

## 1 Les cycles de vie associés aux données d'identités

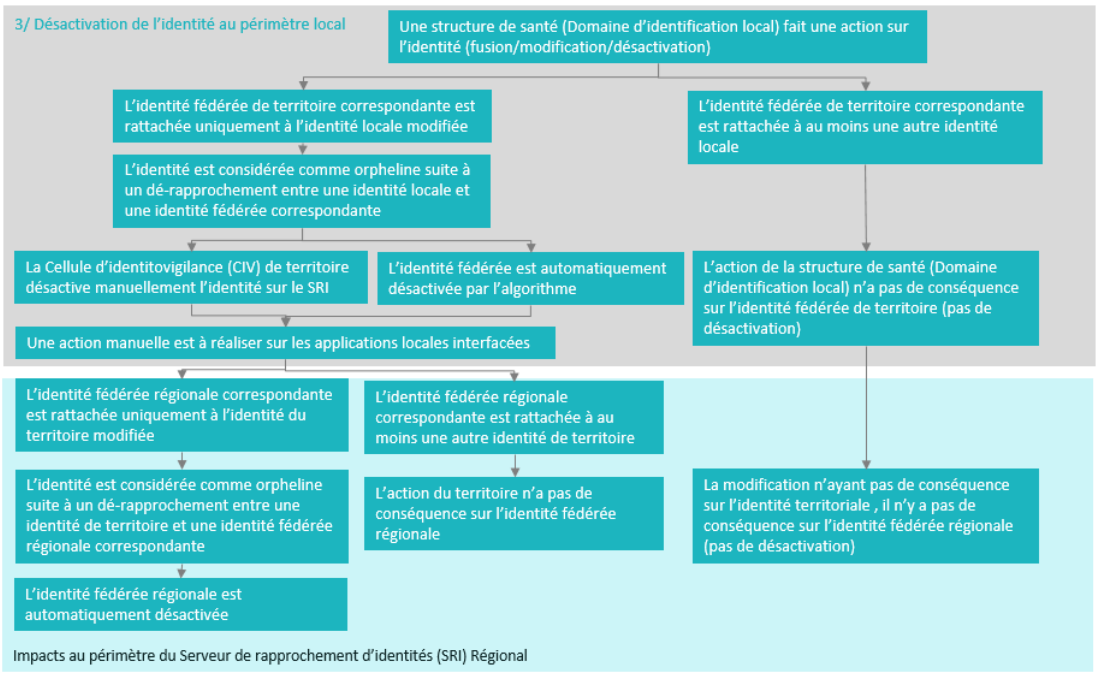
Cycle de vie de la **création** d'une identité usager



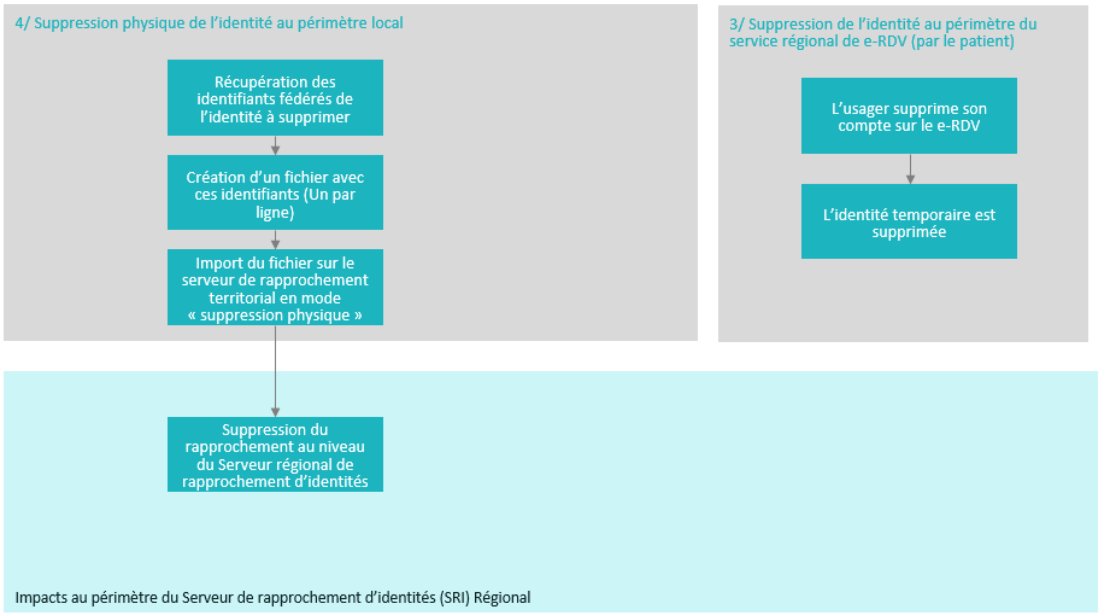
## Cycle de vie de **gestion** des identités usager




## Cycle de vie de la **désactivation** d'une identité usager

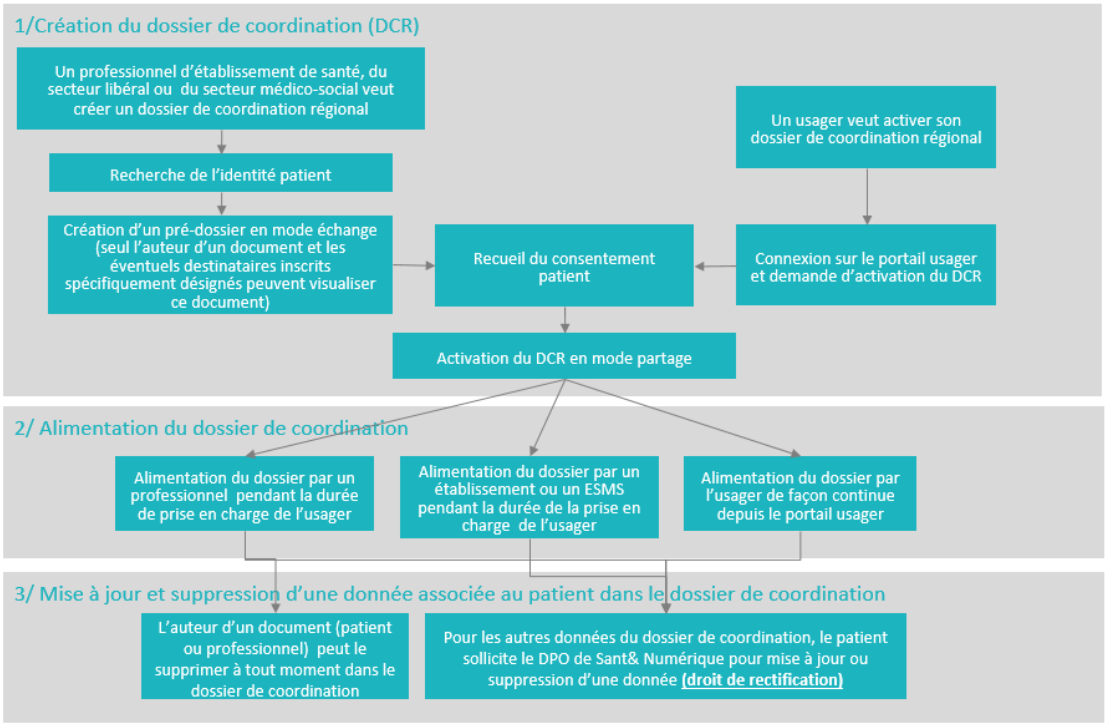


Cycle de vie de la **suppression** d'une identité usager

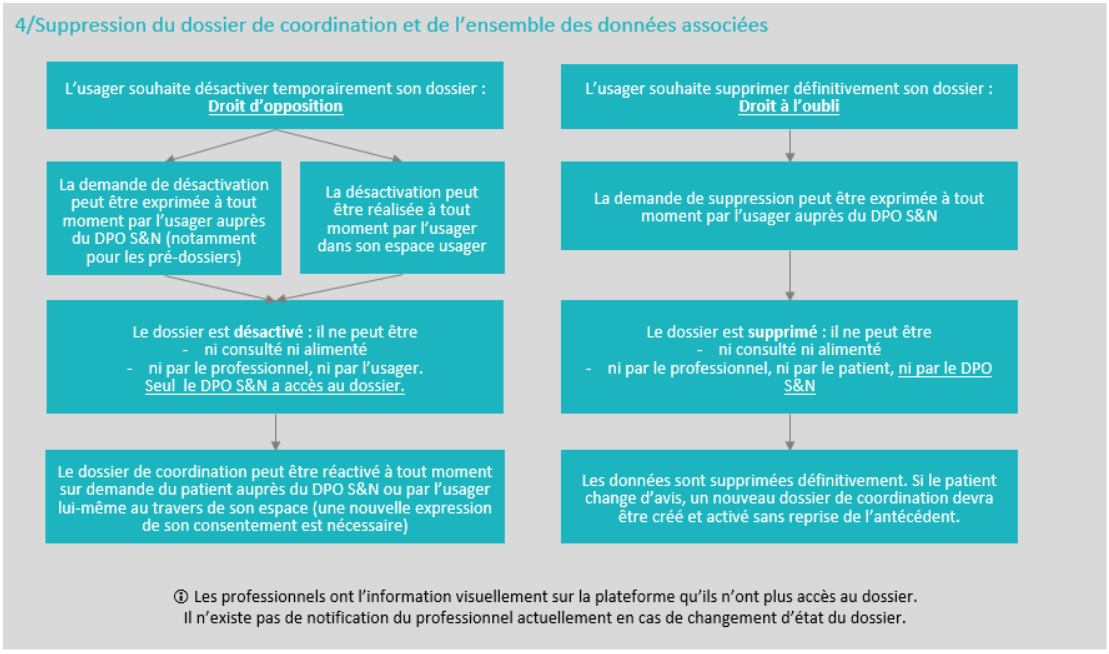



## 2 Les cycles de vie associés aux données du dossier de coordination

Cycle de vie de la **création et la gestion** des données –Dossier de coordination

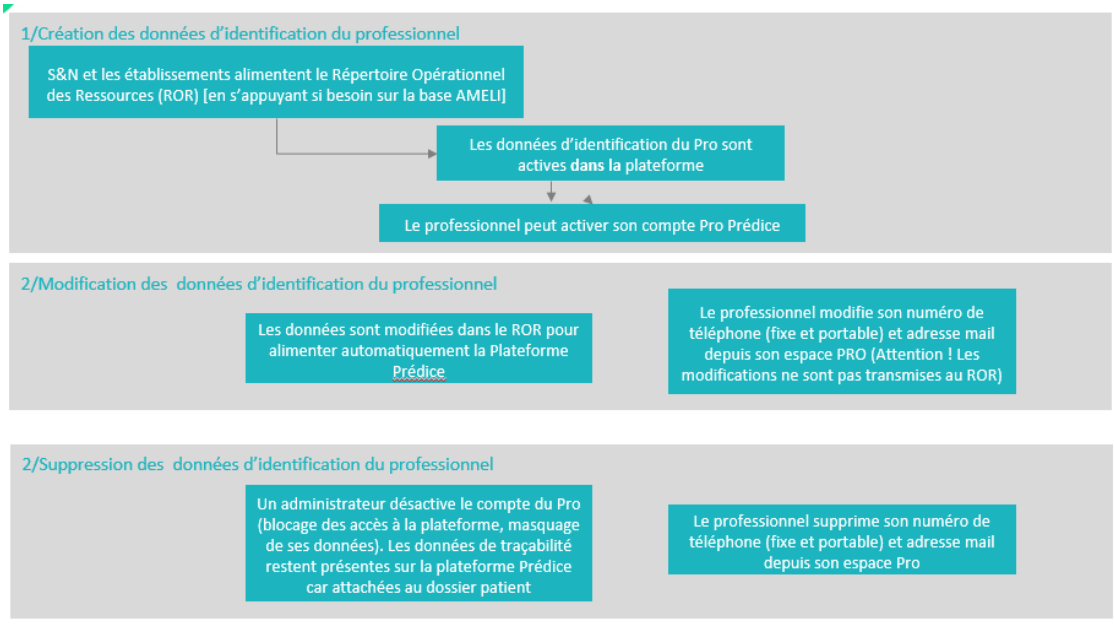


Cycle de vie de la **suppression** du dossier de coordination et des données associées

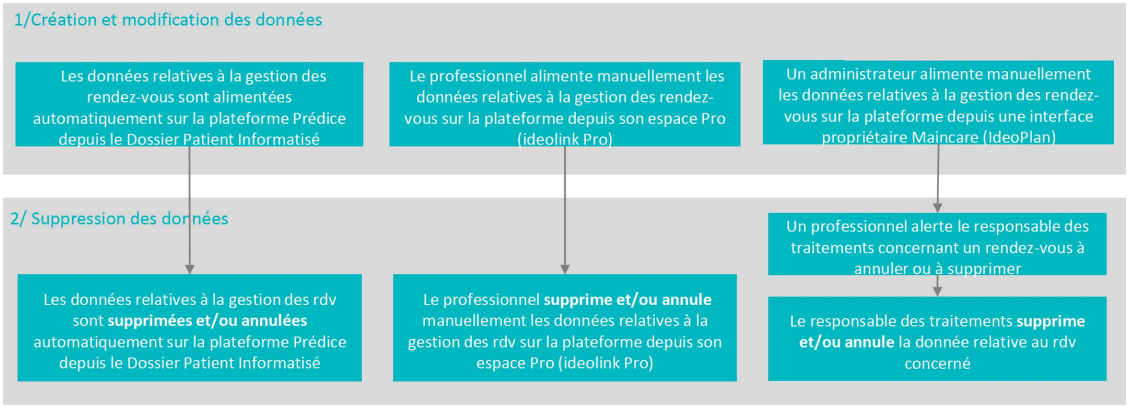



## 3 Les cycles de vie associés aux données des professionnels

Cycle de vie de la **création, modification et suppression** des données des professionnels



Cycle de vie de la **création et modification, suppression** des données – Professionnels / données de gestion des rendez-vous




## QUELS SONT LES SUPPORTS DE DONNÉES ?

- Serveurs
- Postes de travail des différents acteurs de santé
- Postes de travail au sein de S&N

# PRINCIPES FONDAMENTAUX

## PROPORTIONNALITE ET NECESSITE

### Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

La finalité du traitement analysé dans ce PIA est la coordination/mise en relation. Il s'agit donc de permettre l'amélioration de la prise en charge et de la continuité des soins à l'échelle du territoire régional.

Les sous-finalités poursuivies sont les suivantes :

1. **Alimentation identité usager:** Alimenter les plateformes territoriales et la plateforme régionale avec les identités des usagers nécessaires à l'ouverture de services à destination des professionnels de santé et des usagers/patients. Ces identités peuvent provenir des différentes structures de santé.
2. **Rapprochement des identités :** Rapprocher les identités des usagers qui passent dans plusieurs structures de santé afin d'offrir une vision consolidée de ligne de vie;
3. **Echange autour du cas d'un usager :** Permettre l'échange entre professionnels de l'équipe de soins autour du cas d'un usager ;
4. **Alimentation Documents et Images :** Alimenter les plateformes territoriales et le la plateforme régionale avec les documents des usagers et les liens pointant sur les images des PACS des établissements pour permettre l'ouverture de services à destination des professionnels de santé et des usagers. Les usagers peuvent également alimenter la plateforme via le portail usager;
5. **Consultation de la ligne de vie :** Permettre à un professionnel d'accéder en fonction de ses habilitations à la ligne de vie consolidée d'un usager ; permettre à l'usager d'accéder à sa ligne de vie.
6. **Prise de rendez-vous :** Permettre à un usager (ou à un professionnel de santé pour le compte de celui-ci) de prendre un rendez-vous avec un professionnel de santé en fonction de ses besoins et de l'offre en santé d'un territoire ;
7. **Alimentation de l'offre de soins (référentiel technique) :** Sur la base du ROR, alimenter la plateforme avec le référentiel des structures et professionnels permettant d'utiliser les services proposés (ex: prise de rendez-vous) ;
8. **Alimentation DMP :** Alimenter le DMP avec les documents propres au dossier de coordination (les structures alimentent à leur niveau le DMP avec les documents hors dossier de coordination régional).

## Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Les traitements de données réalisés dans le cadre de Prédice s'inscrivent dans le périmètre des traitements liés à une mission d'intérêt public (amélioration de la qualité de la prise en charge des usagers par une meilleure coordination des acteurs régionaux du système de santé). Ces traitements sont donc fondés sur l'article 6, §1, point e) du RGPD :

« le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ».

Le développement de Prédice s'inscrit dans le cadre de la stratégie régionale de l'ARS en matière de e-santé (schéma directeur régional des SI de santé), en cohérence avec les orientations nationales conformément à la feuille de route Ma Santé 2019-2022.

Le considérant 45 du RGPD énonce que lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public, le traitement devrait avoir un fondement dans le droit de l'Union ou des États membres. Toutefois, le règlement n'exige pas de disposition légale spécifique pour chaque traitement individuel.

**En l'espèce, le programme Prédice s'inscrit pleinement dans la mise en œuvre des missions d'intérêt public convergentes incombant à chacun des porteurs de projet, lesquels assument conjointement la responsabilité des traitements.** Le caractère d'intérêt public de ces missions ressort des dispositions législatives, réglementaires, statutaires et conventionnelles régissant ces organismes :

L**'ARS Hauts-de-France** (établissement public à caractère administratif) est chargée, aux termes de l'article L. 1431-2 du CSP, de mettre en œuvre la politique de santé définie au niveau national et de réguler, d'orienter et d'organiser l'offre de services de santé. Elle a notamment pour mission de veiller à ce que la répartition territoriale des offres de services de soin de santé permette de satisfaire les besoins en santé de la population (notamment via le schéma régional de l'organisation des soins) et à la qualité des services de prévention et de soin.

Le **GIP Sant& Numérique Hauts-de-France** s'est vu confier par l'ARS la coordination du programme régional visant à contribuer à la transformation numérique du système de santé. Conformément à l'arrêté d'approbation de sa convention constitutive, l'action du groupement s'inscrit dans une politique d'intérêt général au service de la modernisation du système de santé grâce à la transformation numérique dans les champs du sanitaire, du médico-social et du social. S&N conduit les projets que l'ARS lui confie, en particulier ceux relatifs au socle commun minimum de services numériques en santé, et contribue à l'urbanisation, à la sécurité, et l'interopérabilité des systèmes d'information de santé à l'échelle régionale.

Concernant **les établissements de santé**, leur implication dans le programme Prédice s'inscrit dans le prolongement des missions d'intérêt public qui leur incombent au titre de l'article L. 6111-1 du CSP. Outre leurs missions de prévention, de diagnostic, de surveillance et de soin, les établissements de santé participent également à la mise en œuvre de la politique de santé et à la coordination des soins dans le cadre défini par l'ARS.

Par ailleurs, le traitement de données de santé dans le cadre de **Prédice** est fondé sur l'article 9, §2, point h) du RGPD. En effet, le traitement des données de santé impliqué par l'utilisation de la plateforme par les usagers/patients et les professionnels de santé est nécessaire à la gestion des systèmes et services de soins de santé.

## Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

- **Données d'identité d'un usager :** ces données sont nécessaires à la qualité et à la sécurité des soins (identitovigilance) ; le traitement du NIR est indispensable à cette fin. Les données d'identité d'un usager sont nécessaires à l'activation ou la désactivation de son dossier de coordination suite au recueil de son consentement (un usager = un dossier de coordination).
  Dans le cadre de la recherche d'un usager, le professionnel n'a accès ni aux éléments liés à la création des identités (ni date, ni motif, ni identification du professionnel ou de la structure à l'origine de la saisie), ni au contenu du dossier de la personne concernée.

  Seuls les personnels des CIV et du SRRI peuvent associer une identité à un domaine d'identification (structure à l'origine de la saisie). Dans ce cadre, différentes garanties sont posées : ces personnels sont placés sous l'autorité d'un professionnel de santé ; leur contrat de travail prévoit une clause de confidentialité renforcée ; Prédice met en place une matrice des droits et habilitations et un premier niveau de contrôle a minima.
- **Données relatives à la vie personnelle :** ces données sont nécessaires à la prise en charge de l'usager/patient et à la coordination des soins ;
- **Données de santé :** ces données sont nécessaires à la prise en charge de l'usager/patient et à la coordination des soins. Les professionnels s'assurent de ne partager que les données strictement nécessaires à la prise en charge et de n'échanger qu'avec les personnes habilitées;
- **Données relatives aux professionnels de santé :** ces données sont nécessaires à l'identification du professionnel sur la plateforme, à l'organisation et à la prestation des soins mais ne sont pas directement accessibles aux autres utilisateurs;
- **Données de connexion :** ces données sont nécessaires à la traçabilité, à l'imputabilité de la responsabilité et à la garantie de l'intégrité des données

## Les données sont-elles exactes et tenues à jour ?

- **Données d'identité de l'usager/patient :** possibilité de noter le caractère provisoire ou validé des données, la validation de l'identité étant réalisée par la présentation d'un document d'identité en cours de validité auprès des établissements (cf. préconisations de la charte d'identitovigilance s'imposant à chaque structure de santé). Chaque modification est propagée automatiquement sur les différentes plateformes concernées via le flux IHE-PAM. En outre, les cellules d'identito-vigilance à chaque niveau (établissement, GHT, région) sont chargées de s'assurer de la qualité de l'identité et donc l'unicité de chaque usager/patient sur la plateforme et appliquent toutes la charte d'identification de l'usager dans son parcours de santé mise en place à l'échelon régional;
- **Données relatives aux professionnels de santé :** Prédice s'appuie sur le Répertoire Opérationnel des Ressources (ROR) et AMELI pour la création des comptes des professionnels de santé ;
- **Autres données (hors données de connexion) :** l'exactitude et la mise à jour des données découlent de la prise en charge des usagers/patients par les professionnels de santé et/ou structures de santé.

L'intégrité des données est assurée techniquement par des sauvegardes quotidiennes et fonctionnellement grâce à la traçabilité des actions de mise à jour de l'information (journalisation permettant de retrouver l'état d'une information à un instant donné).

## Quelle est la durée de conservation des données ?

En phase de production, la durée de conservation des données sera déterminée par catégorie en fonction des usages :

- Les données de connexion (traces techniques) seront accessibles pendant 1 an aux utilisateurs habilités, elles seront ensuite archivées pendant 10 ans aux fins de couvrir le délai de prescription prévu par l'article L. 1142-28 du Code de la santé publique en matière de responsabilité médicale (dix ans à compter de la consolidation du dommage) ;
- Les données reçues depuis les systèmes externes (transmis des structures de santé ou de l'usager/patient vers les différentes plateformes Prédice) et les données saisies directement sur Prédice seront conservées 5 ans à compter de la clôture du compte usager (dossier inactif) en base active, puis 5 ans en base archive ;
- Les données d'ordre administratif saisies sur la plateforme seront conservées durant 5 ans à compter de la clôture du compte utilisateur ;
- Le NIR est conservé pendant les durées prévues par les dispositions législatives et réglementaires applicables à la conservation des dossiers médicaux en tant que trait fort d'identito-vigilance.

A l'issue de ces délais, les données seront détruites.

# MESURES PROTECTRICES DES DROITS

## Comment les personnes concernées sont-elles informées à propos du traitement ?

Les portails d'accès usager et professionnel permettent d'avoir accès facilement (à partir du menu principal) et à tout moment aux éléments suivants:

- Conditions générales d'utilisation (CGU) ;
- Politique de confidentialité ;
- Publication du présent PIA (dans une version allégée);
- Notice d'information spécifique pour les usagers (délivrée par les acteurs de la prise en charge et accessible sur le site Internet)

Les CGU détaillent les obligations du professionnel de santé en matière d'information de l'usager/patient, de recueil du consentement et d'exercice des droits prévus par la réglementation applicable (loi Informatique et Libertés, RGPD, Code de la santé publique).

Le contenu de l'information délivrée concerne les caractéristiques des traitements, y compris l'information sur l'hébergement des données de santé renseignées sur la plateforme. La notice d'information précise que l'usager/patient est tenu d'informer les autres personnes pour lesquelles les données sont renseignées au bénéfice de son compte (aidants).

L'information délivrée sera adaptée au niveau de compréhension de la personne.

## Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Les opérations de traitement étant fondées sur l'exercice des missions d'intérêt public incombant aux responsables de traitement et les finalités poursuivies étant compatibles avec les finalités initiales pour lesquelles les données des usagers/patients ont été collectées, le consentement des usagers/patients n'est pas nécessaire pour la mise en œuvre de la plateforme.

Le respect des règles d'échange et de partage au sein de l'équipe de soins est assuré par une politique fine de droits et d'habilitations (cf. infra, « Organisation »). Toutefois, certains cas d'usage amèneront à sortir du cadre de l'équipe de soins, telle que définie par l'article L. 1110-12 CSP et ne permettront pas de garantir une étanchéité complète au niveau de ces équipes de soins.

Il a donc été choisi **de mettre en œuvre un recueil du consentement généralisé auprès des usagers/patients pour l'ensemble des cas d'usage de partage de données** liées à Prédice. Ce consentement portant sur l'ensemble des usages de partage liées au dossier de coordination Prédice, une fois délivré, est réputé valide dans l'ensemble des structures de santé de la région et pour l'ensemble des acteurs habilités intervenant dans la prise en charge.

Au regard des exigences d'obtenir un consentement libre, éclairé, spécifique et univoque (article 7 du RGPD), l'information mise en place à destination des usagers présente le cadre et les objectifs du partage, les droits dont dispose l'usager ainsi que la possibilité de retirer son consentement à tout moment et les modalités pratiques permettant de retirer ce consentement *(cf. schémas ci-dessous)*

- Applicabilité du consentement

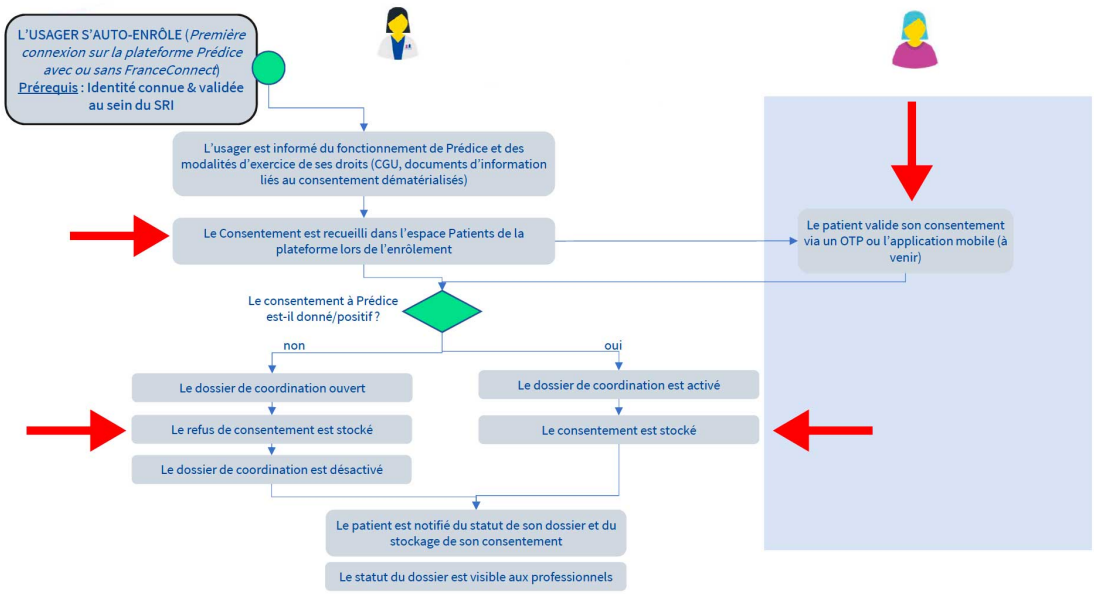
| Cas d'usage (Dossier de coordination / Messagerie instantanée) | Information/Consentement |
|---|---|
| Un professionnel partage du contenu (message instantané, document, information) avec N professionnels du même territoire ou d'un autre territoire. | Information et consentement |

- Modalités de recueil du consentement

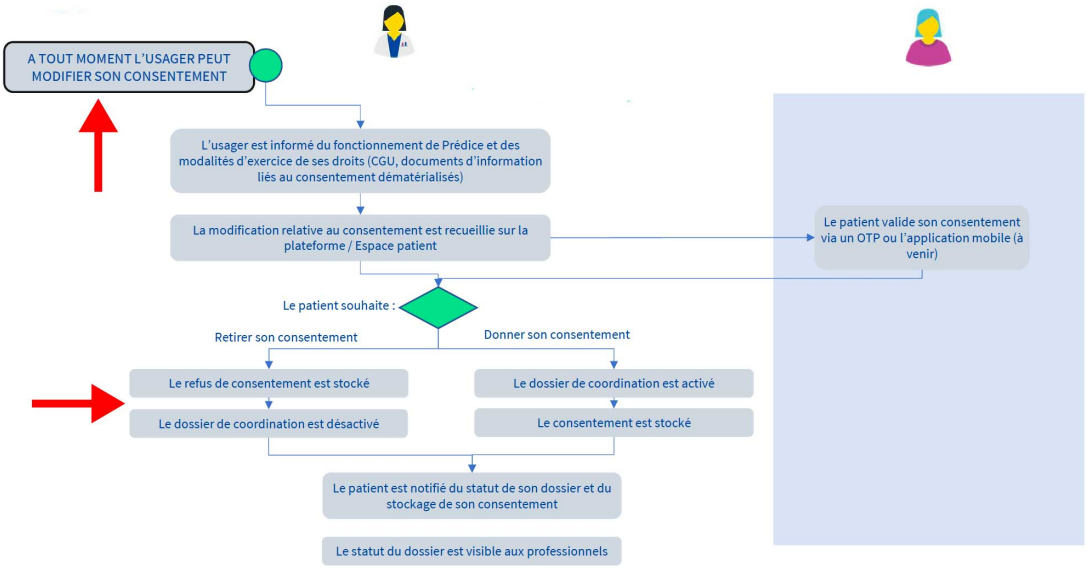
| Dossier de coordination en mode partage | Modalités de recueil du consentement usager |
|---|---|
| **Professionnels hospitaliers** | **Établissements dotés de Docaposte :**<br>Consentement recueilli dans Docaposte et transmis à Prédice<br>**Établissements non dotés de Docaposte :**<br>Consentement recueilli directement dans Prédice et associé à l'identité : recueil de manière totalement dématérialisée ou formulaire papier stocké dans la ligne de vie de l'usager<br>**Modalités dérogatoires en amont de la mise en œuvre du consentement Docaposte & Prédice :**<br>Consentement recueilli via formulaire papier, scanné et stocké dans le dossier temporaire de l'usager et activation/désactivation du dossier selon le choix de l'usager. Le formulaire papier est conservé par le professionnel, le scan n'ayant pas valeur probante. |
| **Professionnels libéraux** | **Consentement recueilli directement dans Prédice et associé à l'identité :**<br>recueil de manière totalement dématérialisée ou formulaire papier conservé par le professionnel, scanné et stocké dans la ligne de vie de l'usager |
| **Professionnels – établissements** | **Consentement recueilli directement dans Prédice et associé à l'identité :** |

| | |
|---|---|
| **médico-sociaux** | Recueil de manière totalement dématérialisée ou formulaire papier conservé par le professionnel, scanné et stocké dans la ligne de vie de l'usager |
| **Recueil pour les personnes dans l'incapacité physique d'exprimer leur consentement** | **Recueil a posteriori** lorsque la personne retrouve ses capacités ou recueil auprès du responsable légal |
| **Recueil pour les personnes dans l'incapacité juridique d'exprimer leur consentement** | **Recueil auprès du responsable légal :** nécessite au préalable la création d'un compte pour le responsable légal afin de pouvoir lui affilier le compte de la personne dans l'incapacité juridique d'exprimer son consentement |

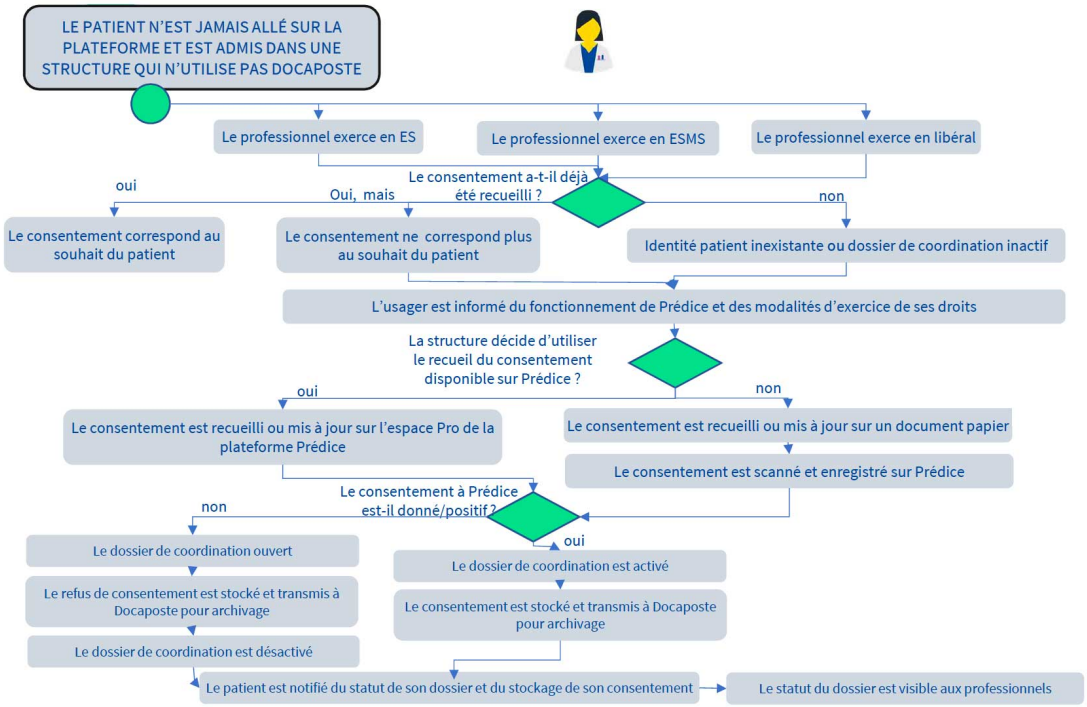
- Modalités de recueil du consentement dans le cas de l'auto-enrôlement de l'usager



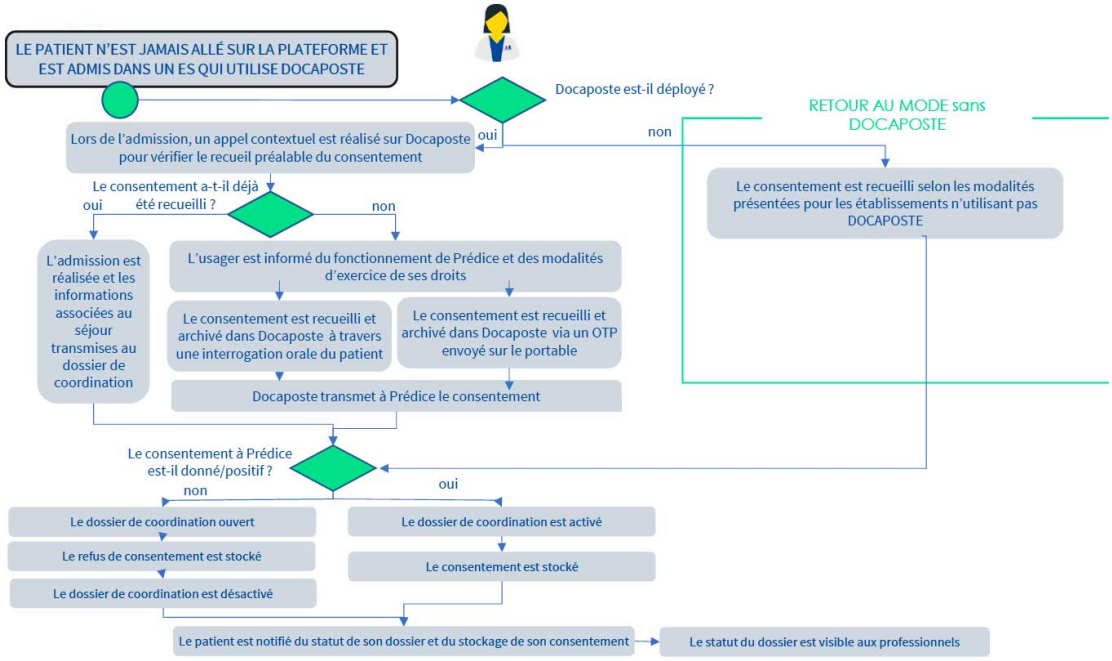
## Cas de la gestion du consentement par l'usager




## Cas de l'usager admis en structure n'utilisant pas DOCAPOSTE



## Cas de l'usager admis en structure utilisant DOCAPOSTE



## Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

En qualité de responsable de traitement pilotant l'administration de la plateforme et assistance à maîtrise d'ouvrage, S&N s'acquitte des réponses aux demandes d'exercice de droit des personnes concernées relatives aux données renseignées sur la plateforme.

Le sous-traitant Maincare Solutions s'est engagé contractuellement à aider le responsable de traitement à s'acquitter de son obligation de donner suite à ces demandes. En particulier, lorsque les personnes exercent auprès du sous-traitant ces demandes, celui-ci s'engage à adresser celles-ci dès réception par courrier électronique à l'adresse communiquée par S&N.

S'agissant des demandes relatives au dossier usager, ces demandes demeurent gérées par les établissements de santé concernés. S&N et le sous-traitant aident les établissements de santé à s'acquitter de leurs obligations en la matière en transmettant dès réception les demandes qui leur sont adressées à l'adresse communiquée par chaque établissement.

Seul le médecin de CHEOPS Technology est habilité à désarchiver les données pour faire droit aux demandes d'exercice des droits d'accès, de rectification, d'effacement et d'opposition pour des motifs légitimes des personnes concernées ou de leurs ayants-droit.

Les traitements étant fondés sur l'exercice d'une mission d'intérêt public, le droit à la portabilité n'est pas applicable. (article 20 §3 du RGPD – voir également les règles directrices du G29 sur le droit à la portabilité : WP242)

## Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

En qualité de responsable de traitement pilotant l'administration de la plateforme et assistance à maîtrise d'ouvrage, S&N s'acquitte des réponses aux demandes d'exercice de droit des personnes concernées relatives aux données renseignées sur la plateforme.

Le sous-traitant Maincare Solutions s'est engagé contractuellement à aider le responsable de traitement à s'acquitter de son obligation de donner suite à ces demandes. En particulier, lorsque les personnes exercent auprès du sous-traitant ces demandes, celui-ci s'engage à adresser ces demandes dès réception par courrier électronique à l'adresse communiquée par S&N.

S'agissant des demandes relatives au dossier usager, ces demandes demeurent gérées par les établissements de santé concernés. S&N et le sous-traitant aident les établissements de santé à s'acquitter de leurs obligations en la matière en transmettant dès réception les demandes qui leur sont adressées à l'adresse communiquée par chaque établissement.

.

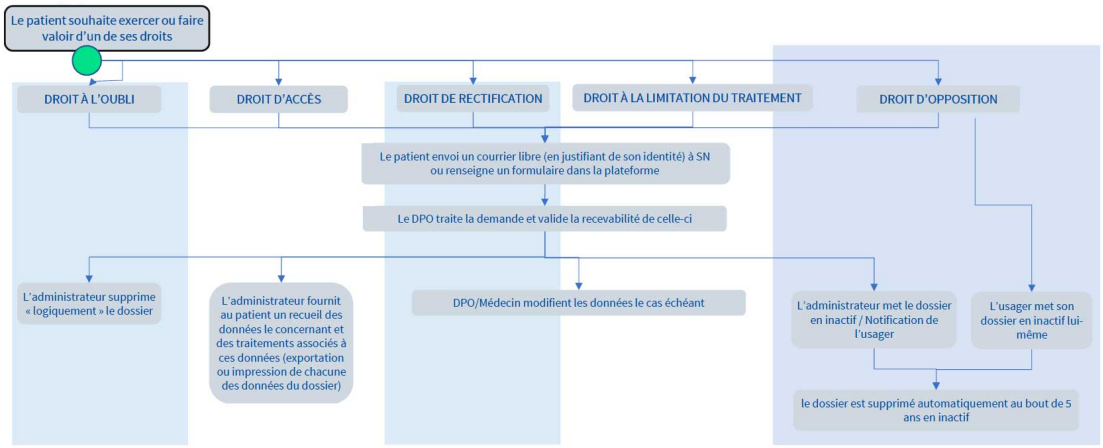
## Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

En qualité de responsable de traitement pilotant l'administration de la plateforme et assistance à maîtrise d'ouvrage, S&N s'acquitte des réponses aux demandes d'exercice de droit des personnes concernées relatives aux données renseignées sur la plateforme.

Le sous-traitant Maincare Solutions s'est engagé contractuellement à aider le responsable de traitement à s'acquitter de son obligation de donner suite à ces demandes. En particulier, lorsque les personnes exercent auprès du sous-traitant ces demandes, celui-ci s'engage à adresser ces demandes dès réception par courrier électronique à l'adresse communiquée par S&N

S'agissant des demandes relatives au dossier usager, ces demandes demeurent gérées par les établissements de santé concernés. S&N et le sous-traitant aident les établissements de santé à s'acquitter de leurs obligations en la matière en transmettant dès réception les demandes qui leur sont adressées à l'adresse communiquée par chaque établissement.

### L'EXERCICE DES DROITS EN RÉSUMÉ



## Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Les obligations du sous-traitant sont contractualisées via le mémoire technique (document à valeur contractuelle) soumis par Maincare Solutions à S&N au cours de la procédure d'adjudication.

Les obligations du sous-traitant ultérieur (hébergeur CHEOPS Technology) sont contractualisées entre Maincare Solutions et CHEOPS Technology. Le sous-traitant initial demeure garant du respect de ses obligations (notamment au titre de la sécurité des traitements) par le sous-traitant ultérieur.

# RISQUES

## PREAMBULE

Dans le cadre de la politique de sécurité mise en œuvre sur le projet, un premier audit de sécurité (audit d'architecture et tests d'intrusion) a été mené au dernier trimestre 2019 aboutissant à la conclusion que la plateforme Prédice, au périmètre des éléments audités, présent un niveau de sécurité élevé.

## Mesures existantes ou prévues

### CHIFFREMENT

Des mécanismes permettant des échanges sécurisés et vérifiant l'intégrité des données échangées sont utilisés.

Les établissements de santé se connectent à Prédice par le biais de réseaux sécurisés

### Traçabilité

Toutes les actions sont tracées afin de piloter le bon usage des accès et de mettre œuvre des règles de bon usage afin de remonter des alertes automatiques avec levées de doute en cas de suspicion d'usage anormal ou déviant.

### Contrôle des accès utilisateur

**Maincare Solutions :** Les accès d'administration et d'exploitation de la Plateforme Client par les équipes Maincare Solutions, dans le cadre d'un hébergement de données de santé, sont réalisés par le biais d'un mécanisme central déployé au sein du Cloud Santé de Maincare Solutions et permettant la gestion & le suivi des actions réalisées.

**Établissements de santé :** Les établissements de santé traitant les données « Patient » dans le cadre du programme Prédice sont responsables :

- Des habilitations et des accès applicatifs.
- Du respect des préconisations faites par l'hébergeur (notamment l'authentification forte type CPS ou tout autre dispositif équivalent).

**Sant& Numérique Hauts-de-France :** se devra d'informer les établissements de santé des recommandations de l'hébergeur quant à la sécurité des accès (authentification et habilitations)

S&N est responsable pour les autres acteurs de santé :

- des habilitations et des accès applicatifs ;
- du respect des préconisations faites par l'hébergeur

S&N est également responsable des habilitations, accès applicatifs et du respect des préconisations pour son propre personnel.

### Cloisonnement

Au niveau du stockage des données, l'intégrité et de la durabilité du stockage des données de la plateforme est garantie.

### Contrôle d'intégrité

Des mécanismes permettant les échanges sécurisés et vérifiant l'intégrité des données échangées (Services Web ou autres) sont utilisés.

Sant& Numérique Hauts-de-France s'assure de la cohérence et l'intégrité des données sauvegardées.

### Archivage

Les traces et horodatages des accès et actions seront conservées dans une base séparée pendant 1 an, puis archivées pendant 10 ans. A l'issu de ce délai, les données seront détruites.

### Sécurisation

La certification ISO 27001 détenue par CHEOPS Technology (partenaire hébergeur de Maincare Solutions) apporte la garantie d'une organisation gérant la Sécurité de l'Information :

- Sécurité physique.
- Sécurité logique.
- Sécurité des ressources humaines

### Surveillance

Les mesures de sécurité devant être mises en œuvre par les établissements lors de l'implémentation du projet Prédice sont décrites dans la politique de sécurité du projet et fournie aux établissements.

Cette politique de sécurité sera mise à jour en fonction de l'évolution technologique du projet et des recommandations de Maincare Solutions.

### Éloignement des sources de risques

Maincare Solutions : la gestion de l'éloignement des sources de risques est garantie par la qualité d'hébergeur agréé HDS de Chéops technology (partenaire hébergeur), *« pour l'hébergement d'applications fournies par ses clients et gérant des données de santé à caractère personnel collectées à des fins de suivi médical, via des offres d'hébergement dédié ou mutualisé ».*

Les emplacements géographiques des 2 Datas center et la sécurisation des infrastructures garantissent un haut niveau d'imperméabilité aux risques humains et non humains, au même titre que les certifications ISO20000 et ISO27001.

## Protection contre les sources de risques non humaines

La protection contre les risques non humains liés aux serveurs est sous la responsabilité de Maincare Solutions et Cheops technology.

Les établissements intégrant le programme Prédice sont responsables de la protection de leurs propres serveurs hébergeant les données.

## Politiques interne de protection des données

Maincare Solutions dispose d'une politique interne de protection des données éditée sous la responsabilité de son DPO.

## Organisation

L'accès aux données à caractère personnel est restreint à une liste d'employés de Maincare Solutions et Chéops technology prédéfinie selon les taches qui leur sont affectées.

Ils ont tous un compte d'accès aux serveurs, unique et limité à leurs fonctions.

Les politiques de gestion des habilitations de Maincare Solutions et CHEOPS technology définissent et décrivent ces accès.

La politique de gestion des habilitations d'accès au dossier de coordination a été construite en étroite collaboration avec le sous-traitant Maincare Solutions, pour tenir compte des contraintes législatives et réglementaires spécifiques afférentes aux données de santé.

Différents niveaux d'habilitation sont ainsi définis :

- L'habilitation de périmètre, qui vise l'habilitation d'un utilisateur donné à accéder au dossier de l'usager/patient qui est déterminée par un mandat ;
- L'habilitation de fonction, qui vise l'habilitation d'un utilisateur donné sur une fonction ou un type d'information spécifique (ex: compte rendu d'hospitalisation, résultats de biologie…) qui est déterminée par la profession du professionnel et son affectation ou non au « cercle de confiance » de l'usager/patient.

Le mandat représente l'autorisation donnée à un utilisateur ou à une entité (établissement ou réseau de santé) d'accéder au dossier d'un usager/patient spécifique pendant une durée (déterminée ou non).

Il existe plusieurs types de mandat :

1. Les mandats individuels liés aux professionnels appartenant à l'équipe de soin et, le cas échéant, au cercle de confiance (= sous-ensemble de l'équipe de soins regroupant les professionnels de confiance ayant accès aux documents restreints)
2. Les mandats liés à un établissement (=l'ensemble des professionnels de santé d'un établissement) ou à un groupe d'établissements (prévu pour 2020)

3. Les mandats individuels liés à l'accès de l'usager (par un non-professionnel)

Le mandat est complété par l'attribution de droits fins via la gestion des profils et l'appartenance au cercle de confiance.

L'ensemble des accès au dossier de l'usager/patient est défini par la matrice d'habilitation.

Un réglage des niveaux d'accès aux documents permet d'affiner davantage la visibilité pour chaque utilisateur de chaque information contenue dans le dossier. Cette granularité assure une maîtrise effective du périmètre d'habilitation. Trois niveaux sont disponibles:

- Confidentialité normale
- Confidentialité restreinte.
- Confidentialité privée

Par défaut, le professionnel de santé a accès aux documents placés en confidentialité normale.

Ce projet est cofinancé par l'Union européenne avec le Fonds européen de développement régional (FEDER)