Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère des solidarités et de la santé

Direction générale de l'offre de soins

Sous-direction du pilotage de la performance
Bureau systèmes d'information des
acteurs de l'offre de soins (PF5)

Personnes chargées du dossier :
Michel Raux, Adjoint à la Cheffe de bureau
Tél: 01 40 56 70 95
Marie Vallas, Chargée de mission
Tél: 01 40 56 58 89
dgos-pf5@sante.gouv.fr

La ministre des solidarités et de la santé

Le directeur général de la caisse nationale d'assurance maladie

à

Mesdames et Messieurs les directeurs généraux des agences régionales de santé (pour information)

Mesdames et Messieurs les directeurs de caisse primaire d'assurance maladie (pour information)

Mesdames et Messieurs les directeurs des établissements de santé (pour mise en œuvre)

NOTE D'INFORMATION N° DGOS/PF5/CNAM/2020/2 du 06 janvier 2020 relative à l'appel à projets auprès des établissements de santé pour l'expérimentation de méthodes alternatives à la carte de professionnel de santé (CPS) pour la consultation du dossier médical partagé (DMP).

Date d'application : immédiate
Classement thématique : établissements de santé

Inscrite pour information à l'ordre du jour du CNP du 22 novembre 2019 – N° 130

Catégorie : Directives adressées par le ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.
Résumé : Modalités de mise en œuvre de l'appel à projets pour l'expérimentation de méthodes alternatives à la CPS pour la consultation du DMP par les professionnels de santé en établissements.
Mots-clés : DMP ; Systèmes d'information ; Etablissement de santé ; Accès ; Dossier Patient Informatisé ; CPS ; Authentification ; Sécurité ; interopérabilité
Textes de référence : - Décret n° 2016-914 du 4 juillet 2016 ; - Article L. 1110-4-1 du code de la santé publique ; - Article R. 1111-29 du code de la santé publique ; - Référentiel d'authentification des acteurs de santé, extrait de la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S).
Annexes : Annexe 1 : Détermination du montant unitaire de soutien financier par établissement ; Annexe 2 : Description de la cible d'usage ; Annexe 3 : Convention de collaboration entre les établissements et la Cnam dans le cadre de l'expérimentation de méthodes alternatives à la CPS pour la consultation du DMP ; Annexe 4 : Document-type d'EIVP à compléter par les établissements expérimentateurs.
Diffusion : Les établissements de santé, par l'intermédiaire des agences régionales de santé.

Cette note d'information vise à décrire les modalités de l'appel à projets pour l'expérimentation de méthodes alternatives à la carte de professionnel de santé (CPS) pour la consultation du dossier médical partagé (DMP) par les professionnels de santé en établissements.

1. Contexte de l'appel à projets

1.1 Le dossier médical partagé

Le dossier médical partagé (DMP) est un dossier médical informatisé sécurisé, accessible sur internet et à partir de logiciels compatibles, et que l'on peut considérer comme le carnet de santé numérique du patient.

Sa conception, sa mise en œuvre et son administration sont confiées à la Cnam par le décret n° 2016-914 du 4 juillet 2016. L'hébergement du DMP est externalisé chez un hébergeur agréé données de santé.

L'article R. 1111-29 du code de la santé publique dispose que le dossier médical partagé est accessible aux professionnels de santé **par voie électronique** notamment **depuis un site internet ou via des logiciels respectant les référentiels d'interopérabilité et de sécurité** mentionnés à l'article L. 1110-4-1 du même code, selon les modalités techniques et organisationnelles définies par la Caisse nationale de l'assurance maladie.

Les référentiels d'interopérabilité et de sécurité sont décrits dans le corpus documentaire de la **Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)** qui définit et organise les exigences incontournables en matière de sécurité s'appliquant à tout système d'information de santé.

Au sein de ce corpus, le référentiel d'authentification des acteurs de santé décrit les exigences à respecter en matière d'authentification des professionnels de santé et définit différents paliers de sécurité correspondant au niveau de confiance accordé à un dispositif d'authentification donné.

Actuellement, au regard du caractère particulièrement sensible des données que contient le DMP, la **consultation du DMP par les professionnels de santé n'est autorisée qu'en authentification directe**, avec lecture de la CPS (respect du palier 3 de l'authentification publique défini dans le référentiel d'authentification).

Notons que la **création et l'alimentation** de DMP sont quant à elles accessibles par des modes d'authentification indirecte.

1.2 Les difficultés liées à la consultation du DMP par lecture de la CPS en structures de soins

La CPS reste très peu utilisée en établissements de santé et son utilisation se confronte à plusieurs contraintes fortes en milieu hospitalier.

Dans le cas des professionnels de santé de ville, la CPS est requise pour les besoins de la facturation et ce moyen d'authentification s'impose naturellement. Les professionnels en établissements de santé n'ont pas nécessairement cette obligation.

Dans les établissements de santé, les postes de travail sont souvent partagés entre professionnels de santé, avec des changements d'utilisateurs qui peuvent être très fréquents. L'insertion de la CPS dans un lecteur et la saisie d'un code PIN peuvent être jugés contraignants dans ces situations de travail.

Enfin, la CPS comme moyen d'authentification est difficile à accepter lorsqu'elle vient s'ajouter à d'autres moyens déjà mis en œuvre au sein des établissements.

1.3 La première expérimentation des méthodes alternatives à la CPS

Pour lever les freins liés à l'utilisation de la CPS et faciliter ainsi l'usage du DMP par les praticiens hospitaliers, la DGOS a souhaité **expérimenter de nouvelles méthodes d'authentification pour la consultation de DMP en structures de soins**.

La DGOS et la Cnam ont donc lancé en 2018 un appel à candidatures auprès des établissements de santé et éditeurs de logiciels afin que ces derniers proposent **des méthodes d'authentification alternatives à la CPS, en authentification indirecte**.

Les solutions alternatives des candidats pouvaient être de deux types, correspondant à deux modes d'accès distincts au DMP :

— **Accès depuis un « logiciel de professionnel de santé » (LPS)** : l'appel des transactions DMP se fait depuis le ou les LPS du système d'information hospitalier (SIH).

— **Accès via l'interface webPS** : l'accès au DMP se fait par appel de l'URL[1] par le navigateur d'un poste du SIH.

Quel que soit le mode d'accès envisagé, les méthodes alternatives ne devaient pas avoir d'impact sur l'utilisation du DMP : **une fois authentifiés, les professionnels de santé devaient avoir accès aux mêmes fonctionnalités**, leur usage demeurant inchangé.

Suite à cet appel à candidatures, une **dizaine d'établissements** a été retenue pour **expérimenter différentes méthodes alternatives sur le terrain**. Etant donné l'intérêt porté par de nombreux établissements à ce projet et la volonté de la DGOS de faciliter la consultation du DMP dans les structures de soins, il a été décidé de procéder à un **appel à projets.**

2. Objectifs de l'appel à projets

Cet appel à projets a pour objectif d'élargir l'expérimentation à un plus grand nombre d'établissements de santé, de contextes métiers et de méthodes d'authentification différent(e)s.

Ainsi, la DGOS et la Cnam pourront envisager une phase de généralisation en se basant sur une expérimentation plus riche et plus représentative.

3. Critères d'éligibilité

3.1 Les prérequis

Pour candidater, les structures de soins, publiques ou privées, doivent :

- Avoir atteint les prérequis du programme Hôpital Numérique[2] ;
- Avoir atteint les cibles d'usage du domaine D2 du programme Hôpital Numérique : DPII (Dossier patient informatisé et interopérable) et communication extérieure ;
- Atteindre l'indicateur D6.1 (Taux de documents publiés dans le DMP pour les patients disposant d'un DMP au moment de leur admission) du programme HOP'EN[3] au plus tard à la date d'atteinte de la cible d'usage du présent appel à projets.

Chaque établissement peut présenter sa candidature seule ou s'associer avec d'autres établissements. Les établissements peuvent s'associer à des partenaire(s) industriel(s), éditeurs de logiciel et fournisseurs de solutions d'authentification.

Les établissements ayant été financés dans le cadre de la première expérimentation ne sont pas éligibles sauf dans le cas où ils proposeraient une méthode de consultation du DMP via leur LPS.

---

[1] Uniform Resource Locator : adresse internet.

[2] Lien vers le guide des indicateurs des prérequis et des domaines prioritaires du socle commun du programme Hôpital Numérique :

https://solidarites-sante.gouv.fr/IMG/pdf/DGOS_Guide_d_indicateurs_Programme_Hopital_Numerique_-_avril_2012-2.pdf

[3] Le guide des indicateurs des domaines prioritaires du programme HOP'EN est disponible à l'adresse : https://solidarites-sante.gouv.fr/hopen

Les éditeurs des applications mises en œuvre dans le cadre du projet devront être référencés dans la base RELIMS (Référencement des éditeurs de logiciels et intégrateurs du marché de la santé) de la DGOS.

Les candidats peuvent soumettre une ou plusieurs méthodes. **Chacune d'entre elles doit répondre aux exigences techniques et juridiques définies conjointement par la Cnam et la CNIL** - et précisées en 3.2 - pour être autorisées puis mises en œuvre.

3.2 Les exigences techniques et juridiques

Cadre technique

Les exigences techniques et de sécurité sont définies par la Cnam en accord avec les principes de **la PGSSI-S de l'ASIP Santé** [4] et les **recommandations des services techniques de la CNIL**.

Pour participer à l'expérimentation, les établissements doivent fournir à la Cnam une description de la solution proposée. Les établissements doivent également, conformément à la règlementation en vigueur, fournir à la Cnam **une étude d'impact sur la vie privée (EIVP)**[5] **comprenant une analyse des risques résiduels identifiés**[6].

Une authentification forte des professionnels de santé et **l'utilisation d'identifiants publics** en lien avec les référentiels de l'ASIP Santé font partie des principes forts à respecter.

La solution mise en œuvre par l'établissement et son éditeur partenaire devra également obtenir un agrément du centre national de dépôt et d'agrément (CNDA), basé sur un **guide d'intégration spécifique à l'expérimentation**. Ce guide sera transmis aux établissements retenus.

Cadre juridique

Pour participer à l'expérimentation, les établissements s'engagent donc à respecter un **ensemble d'exigences organisationnelles, techniques, de sécurité et juridiques**, en signant avec la Cnam une **convention juridique spécifique**. En cas de non-respect de leurs engagements, **la responsabilité des établissements sera mise en cause, et non celle de la Cnam.**

[4] https://esante.gouv.fr/securite/politique-generale-de-securite-des-systemes-d-information-de-sante

[5] La fourniture de cette EIVP et sa validation par la Cnam est nécessaire au déploiement de la solution dans les services expérimentateurs, et constitue donc un prérequis à la validation de l'atteinte de la cible d'usage. En revanche, cette EIVP ne constitue pas un prérequis à la candidature de l'établissement à l'appel à projet.

[6] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

4. Modalités de l'appel à projets

4.1 Candidature des établissements de santé

Les établissements de santé candidatent en déposant leur dossier de candidature par voie dématérialisée sur l'espace de candidature disponible sur le site démarches-simplifiées à l'adresse suivante : https://www.demarches-simplifiees.fr/commencer/aap-cps-dmp. Afin de pouvoir accéder à cet espace et remplir le formulaire de candidature, chaque établissement doit désigner le référent du projet qui devra demander la création d'un compte usager directement sur le site.

L'objectif du dossier de candidature est de présenter succinctement les grands principes de la solution proposée, et notamment :

- Les acteurs impliqués ;
- Les deux facteurs d'authentification ;
- Les grandes briques applicatives utilisées ;
- Le mode d'accès au DMP (intégré logiciel ou par appel du portail web).

Il appartient aux établissements de santé de s'assurer qu'ils satisfont l'ensemble des critères d'éligibilité définis dans le 3) avant de présenter leur candidature.

A l'initiative de la Cnam, une phase d'échanges entre les services de la Cnam (notamment la Direction de la Sécurité) et l'établissement candidat pourra avoir lieu pour préciser certains éléments du dossier.

4.2 Modalités de sélection des projets

Une cinquantaine de projets sera retenue.

Le processus de sélection, assuré par la DGOS et la Cnam, prévoit deux vagues de sélection :

- Une première vague de sélection de candidats interviendra en janvier 2020 ;
- Une seconde vague de sélection de candidats interviendra en avril 2020.

La DGOS et la Cnam veilleront à sélectionner les dossiers afin d'assurer une diversité de projets en termes d'organisation (méthodes d'authentification alternatives) et en termes techniques (industriel) permettant ainsi de prendre en compte la quasi-totalité de l'offre du marché.

5. Modalités de mise en œuvre du projet et atteinte de la cible d'usage

Dans le cadre de la mise en œuvre du projet, l'établissement déploie la solution dans 2 services pilotes au moins, dont un service d'hospitalisation.

Pour chacun des services, la cible d'usage à atteindre est un nombre de consultations de DMP fixé à 100 sur une période de 3 mois.

L'établissement devra fournir un calendrier prévisionnel de généralisation de la solution intégrant l'ensemble des services concernés de l'établissement sur une période de 6 mois à compter de la date d'atteinte de la cible d'usage pour les services pilotes.

6. Modalités de suivi des établissements sélectionnés

Un suivi des établissements et de leurs éditeurs partenaires sera assuré tout au long de l'expérimentation par le GIE SESAM Vitale. Différents points réguliers seront organisés :

- Des points individuels, dont la fréquence pourra être adaptée aux besoins de l'établissement ;

- Des comités regroupant plusieurs voire la totalité des établissements, dans le but de partager les bonnes pratiques et points de vigilance.

Un support sera également proposé par le GIE SESAM Vitale aux établissements et aux éditeurs.

7. Dispositions pour le financement

Tout projet validé sera accompagné financièrement selon un mécanisme de financement à l'usage.

Ce mécanisme prévoit un financement d'aide à la contractualisation sous forme :

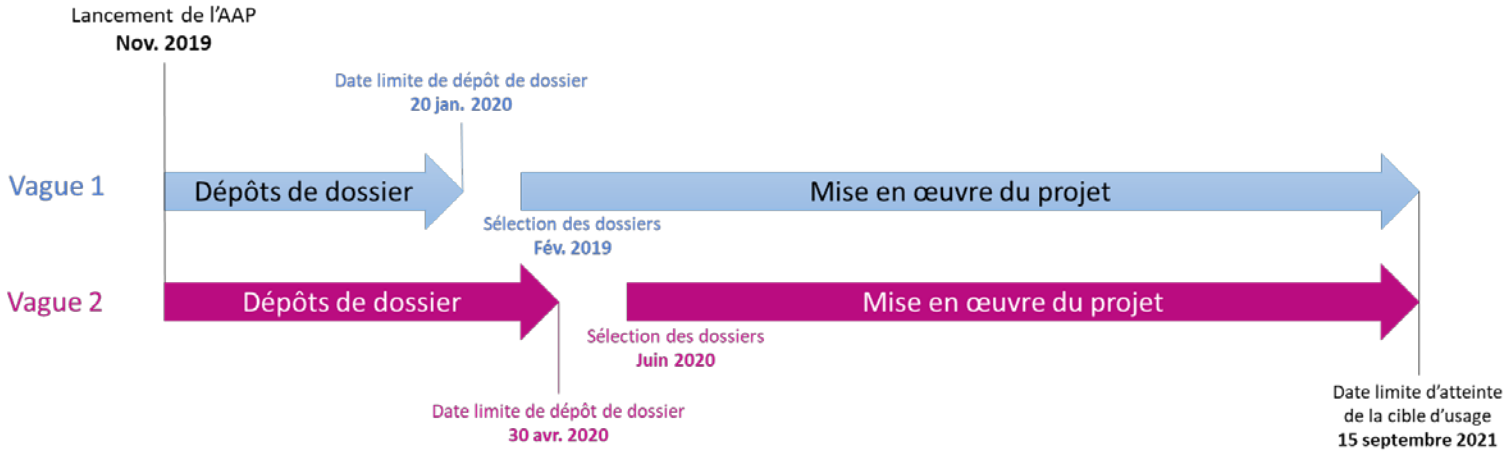
- D'un financement à l'amorçage du projet à hauteur de 50 % de l'accompagnement prévu versé dans le cadre de la première circulaire budgétaire de 2020 (pour les établissements retenus dans le cadre de la première vague) et de la deuxième circulaire budgétaire de 2020 (pour les établissements retenus dans le cadre de la seconde vague).

- D'un financement à l'usage du projet à hauteur de 50 % de l'accompagnement prévu versé a posteriori aux seuls établissements pouvant justifier de l'atteinte de la cible d'usage. Il est rappelé que le déploiement de la solution dans les services expérimentateurs, et donc l'atteinte de la cible d'usage, est conditionnée à la validation par la Cnam de l'EIVP réalisée par l'établissement.

La méthode de détermination du montant unitaire du soutien financier par établissement est décrite en annexe 1.

8. Calendrier prévisionnel de l'appel à projets

Lancement de l'appel à projets	Novembre 2019
Clôture des candidatures à l'appel à projets : - Première vague - Seconde vague	 20 janvier 2020 30 avril 2020
Sélection : - Première vague - Seconde vague	 7 février 2020 12 juin 2020
Date limite d'atteinte de la cible d'usage pour les 2 vagues	15 septembre 2021



Je vous prie de bien vouloir assurer la diffusion de cette note d'information et de ses annexes à vos services.

Je vous invite à me faire part des difficultés éventuelles que vous pourriez rencontrer dans sa mise en œuvre, en prenant contact le cas échéant avec le Bureau des systèmes d'information des acteurs de l'offre de soins (dgos-pf5@sante.gouv.fr).

Vu au titre du CNP par la Secrétaire Générale des ministères chargés des affaires sociales

Pour la ministre et par délégation

signé

Katia JULIENNE
Directrice générale de l'offre de soins

signé

Nicolas REVEL
Directeur général de la caisse nationale de l'assurance maladie

ANNEXE 1

Détermination du montant unitaire de soutien financier par établissement

1. L'activité combinée de l'établissement

L'activité combinée correspond à une mesure de l'activité des établissements fondée sur le nombre de journées et séances. L'activité combinée de chaque établissement est calculée au niveau national, une fois au début du programme. Les données utilisées sont celles de l'année 2017, fournies par l'ATIH (données PMSI), quelle que soit l'année de candidature ou de sélection.

Les différents champs d'activité sont mis en équivalence selon les modalités suivantes :

- 1 séance MCO équivaut à 0,5 journée MCO.

- 1 hospitalisation de jour de chirurgie ambulatoire équivaut à 1,5 journée MCO.

- 1 journée SSR, 1 journée PSY ou 1 journée HAD équivalent à 0,5 journée MCO.

- 1 hospitalisation de jour, hors chirurgie ambulatoire, équivaut à 1 journée MCO.

Les valeurs de l'activité combinée des établissements de sa région sont fournies à chaque ARS.

2. Montant du soutien financier pour chaque établissement

Les montants exacts des soutiens financiers sont forfaitaires et définis au niveau national :

- En fonction de l'activité combinée de l'établissement, qui correspond à une mesure de l'activité des établissements fondée sur le nombre de journées et séances avec une mise en équivalence des différents champs d'activité.

Seuil d'activité combinée	**Montants de soutien financier par catégorie d'établissements**
Cat. A : 0 - 7000	40 k€
Cat. B : 7 000 – 22 500	60 k€
Cat. C : 22 500 – 230 000	80 k€
Cat. D : 230 000 - max	100 k€

ANNEXE 2

Cible d'usage

Définition de l'indicateur	
Définition	Nombre de DMP consultés
Valeur cible	100
Production de l'indicateur	
Unité	Nombre
Période	3 mois révolus
Restitution de l'indicateur	
Remontée de l'information	Fournie par la Cnam

ANNEXE 3

Convention de collaboration entre les établissements et la Cnam dans le cadre de l'expérimentation de méthodes alternatives à la CPS pour la consultation du DMP

Convention de collaboration entre les établissements et la Cnam dans le cadre de l'expérimentation de méthodes alternatives à la CPS pour la consultation du DMP

Entre :

La Caisse Nationale d'Assurance Maladie (Cnam)	
Type d'entité	Établissement public national de l'État
Adresse	50 avenue du Professeur André Lemierre – 75020 Paris
Représenté par	Monsieur Nicolas REVEL, dûment habilité pour la signature des présentes en sa qualité de Directeur général
Ci-dessous dénommée	La Cnam

Et :

[Nom de l'établissement]	
Type d'établissement	[CHU, CH, Clinique privée…]
N° FINESS – N° SIRET	[A compléter]
Adresse	[Adresse du siège social]
Représenté par	Monsieur/Madame [Prénom NOM], dûment habilité pour la signature des présentes en sa qualité de Directeur de l'établissement
Ci-dessous dénommée	L'établissement (ou Ets)

Préambule :

Le Dossier Médical Partagé (DMP) est un dossier médical informatisé sécurisé, accessible sur internet et à partir de logiciels compatibles ayant pour objectif de « *favoriser la prévention, la coordination, la qualité et la continuité des soins* » ;

L'article L. 1111-14 du code de la santé publique confie sa conception, sa mise en œuvre et son administration à la Cnam et prévoit que son hébergement doit être réalisé auprès d'un hébergeur de données de santé à caractère personnel dans le respect de l'article L. 1111-8.

Le décret n° 2016-914 du 4 juillet 2016 vient préciser les conditions d'encadrement opérationnel du DMP. L'article R. 1111-29 dispose que le dossier médical partagé est accessible aux professionnels de santé par voie électronique notamment depuis un site internet ou via des logiciels respectant les référentiels d'interopérabilité et de sécurité mentionnés à l'article L. 1110-4-1 du code de la santé publique, selon les modalités techniques et organisationnelles définies par la Caisse nationale d'assurance maladie.

Le DMP est également soumis aux référentiels de sécurité qui sont décrits dans le corpus documentaire de la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) qui définit et organise les exigences incontournables en matière de sécurité s'appliquant à tout système d'information de santé.

Au sein de ce corpus, le référentiel d'authentification des acteurs de santé décrit les exigences à respecter en matière d'authentification des professionnels de santé et définit différents paliers de sécurité correspondant au niveau de confiance accordé à un dispositif d'authentification donné.

Actuellement, au regard du caractère particulièrement sensible des données que contient le DMP, la consultation du DMP par les professionnels de santé n'est autorisée qu'en authentification directe, avec lecture de la Carte de Professionnel de Santé ou CPS (palier 3 de l'authentification publique défini dans le référentiel d'authentification).

Pour développer l'usage du DMP en établissement, souvent freiné par l'utilisation de la CPS, la DGOS et la Cnam souhaitent expérimenter d'autres méthodes d'authentification des Professionnels de Santé (PS) pour la consultation de DMP dans les structures de soins.

Ces méthodes alternatives reposeront sur un mode d'authentification indirecte, qui s'inscrira dans le palier requis de la PGSSI-S.
Aussi, un nouveau mode d'authentification, l'Authentification Indirecte Renforcée, sera éprouvé lors de cette expérimentation, et sera intégré à la PGSSI-S en cas de généralisation.

Article 1 : Définitions

- **LPS :** Logiciel de Professionnel de Santé.
- **Service (web) :** désigne un ensemble de fonctionnalités exposées sur internet ou sur un intranet, par et pour des applications ou machines, permettant la communication et l'échange de données entre applications et systèmes hétérogènes dans des environnements distribués.
- **Fournisseur :** organisme mettant à disposition des services. Dans notre cas, pour l'accès au DMP, la Cnam est le fournisseur du service.
- **Client :** organisme sollicitant un service. Dans notre cas, pour l'accès au DMP, l'Ets est le client du service.
- **PGSSI-S :** Politique Générale de Sécurité des Systèmes d'Information de Santé. Fixe le cadre de la sécurisation des Systèmes d'Information de Santé (SIS).
- **Utilisateur** : Professionnel de santé intervenant pour le compte de l'Ets et ayant accès aux applications proposées par la structure qui lui sont nécessaires dans sa pratique.
- **SIH** : Système d'information hospitalier. Ensemble des composants logiciels et d'infrastructure mis en œuvre au sein de l'ETS.
- **Jeton VIHF :** Vecteur d'Identification et d'Habilitation Formelles. Objet technique utilisé dans le cadre de la sécurisation des échanges de données entre SIS. Il porte entre autres les éléments permettant l'identification, l'authentification d'un organisme ou d'un utilisateur.
- **IGC (PKI en anglais) :** Infrastructure de Gestion de Clés. Ensemble de composants physiques (ordinateurs, équipements cryptographiques logiciels ou matériel), de procédures humaines (vérifications, validation) et de logiciels (système et application) destiné à gérer les clés publiques des utilisateurs d'un système.

Article 2 : Objet des Présentes

La présente convention a pour objet de déterminer les exigences organisationnelles, techniques, de sécurité et juridiques auxquelles l'établissement accepte de se soumettre afin d'entrer dans le dispositif de l'expérimentation sur la consultation du DMP à l'aide de moyens alternatifs à la CPS.

La signature de la présente convention vaut adhésion aux modalités d'utilisation du service et aux exigences qui sont décrites ci-après.

Un **audit des établissements** aura lieu au lancement des expérimentations, pour vérifier que les exigences organisationnelles et techniques décrites dans la présente convention sont bien respectées par l'Etablissement. Cet audit permettant à la Cnam de veiller au respect des exigences de sécurisation des accès au DMP dont elle est responsable de traitement.

Les parties s'engagent sur les documents suivants :

- La présente convention
- L'**Annexe 1** : tableau récapitulatif des exigences
- L'**Annexe 2** : moyens d'authentification primaires autorisés pour l'expérimentation
- L'**Annexe 3** : liste des FINESS géographiques associés aux certificats de personne morale

Les annexes font partie intégrante de la présente convention et ont la même valeur juridique que cette dernière.

Art. 2.1 : Engagements spécifiques de la Cnam

La Cnam s'engage à assurer et maintenir une bonne qualité de service en termes de disponibilité et de performance, pour les services dont elle a la charge.

L'ouverture à des méthodes alternatives à la carte CPS doit s'accompagner d'un renforcement de la vigilance quant aux accès abusifs au DMP.
→ La mise en place de **mécanismes de détection des mésusages** est apportée par la Cnam au SI-DMP qui ne demande **pas d'action spécifique de la part des établissements et de leurs éditeurs** partenaires.
→ Les actions de signalement ou de blocage engagés en cas de détection de mésusages pourront cibler le professionnel de santé ou l'établissement selon les cas, avec des mesures telles que l'interdiction de consultation dans l'attente de l'analyse des causes.
→ Les mésusages seront détectés par l'observation de données volumétriques sur les accès au DMP par un utilisateur (un professionnel de santé) ou un établissement donné, qui traduiraient une activité anormale.

Art. 2.2 : Engagements spécifiques de l'Ets

Plusieurs prérequis sont nécessaires avant la conclusion de la présente convention, aussi l'établissement reconnaît avoir satisfait à l'ensemble des conditions ci-après imposées :

L'Etablissement, qu'il s'agisse d'une structure de soins publique ou privée, doit avoir atteint les prérequis Hôpital Numérique.

Pour l'accès de ses utilisateurs au DMP, l'Etablissement engage sa responsabilité sur le respect des **exigences imposées par la Cnam** et décrites dans la présente convention, qui sont rappelées en **Annexe 1**.

En cas de non-respect de leurs engagements, la responsabilité de l'établissement sera mise en cause, et non celle de la Cnam.

L'établissement s'engage également, conformément à la règlementation en vigueur, à avoir fourni à la Cnam préalablement à la signature de la présente convention les éléments nécessaires à la constitution d'un dossier CNIL, **et notamment une description détaillée du ou des moyen(s) d'authentification primaire(s) qu'il utilisera pendant l'expérimentation.** Ce ou ces moyen(s) sera(ont) rappelé(s) en **Annexe 2**.

A ce titre, l'établissement déclare avoir réalisé pour chaque méthode alternative proposée, une Etude D'Impact sur la Vie Privée (EIVP) ainsi qu'une analyse des risques résiduels identifiés.
L'établissement s'engage par ailleurs à n'utiliser qu'un logiciel (d'un éditeur ou le sien propre) spécifiquement homologué par le CNDA dans le cadre de la présente expérimentation pour le mode d'authentification indirecte renforcée.

Article 3 : Authentification Indirecte Renforcée (AIR)

Pour l'expérimentation, l'établissement s'inscrit dans un schéma d'authentification indirecte dite « renforcée », entendue comme s'appuyant sur une authentification primaire de ses utilisateurs, assurée par et sous sa seule responsabilité et soumise à des contraintes imposées par le système DMP (SI-DMP).

Les solutions alternatives d'authentification peuvent être mises en œuvre sur deux canaux d'accès au DMP :

- via un logiciel intégré (LPS), par l'appel des transactions DMP depuis une application du SIH
- via l'interface Web dédiée aux PS (WebPS), par appel de l'URL dans le navigateur d'un poste du SIH

La consultation d'un DMP en mode AIR offre à un PS les mêmes fonctionnalités que la consultation en authentification directe.

Le mode AIR est réservé à la fonctionnalité « Consultation » du SI-DMP et donc uniquement accessible à certaines qualifications professionnelles, conformément à la matrice d'habilitation en lecture de documents. Les autres fonctionnalités (« Création et gestion administrative », « Alimentation ») sont à mettre en œuvre avec les modes d'authentification classiques (directe et/ou indirecte).

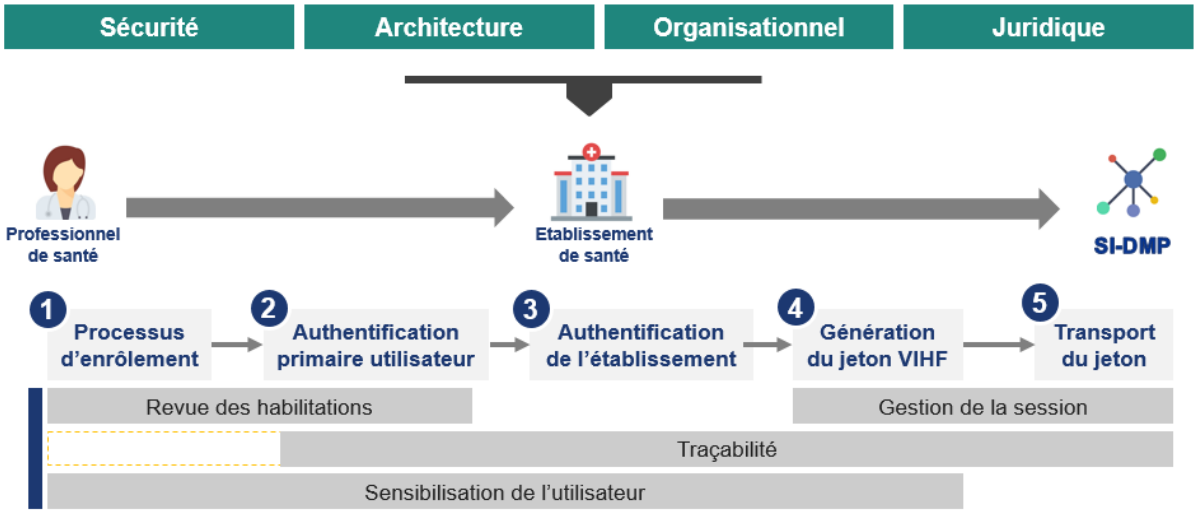
Les exigences techniques et de sécurité ont été définies par les experts de la Cnam en accord avec les principes de la PGSSI-S de l'ASIP Santé et les recommandations des services de la CNIL.

Art. 3.1 : Cadre général du fonctionnement de l'Authentification Indirecte Renforcée (AIR)

Le mode AIR fait intervenir trois acteurs : Le professionnel de santé (PS), utilisateur du service, la structure qui l'accueille et l'habilite et le SI-DMP qui rend le service

L'enjeu de l'authentification indirecte renforcée est de permettre à l'Ets une plus grande liberté dans le choix des moyens d'authentification forte des PS, pour l'accès au DMP.

Les exigences, qu'elles soient d'ordre organisationnel, technique ou sécurité, portent sur toute la chaîne d'authentification de l'utilisateur, depuis le processus d'enrôlement jusqu'au transport du jeton VIHF (Vecteur d'Identification et d'Habilitation Formelles) pour l'accès au DMP. Cela passe notamment par une authentification primaire forte de l'utilisateur.



Art. 3.2 : Processus d'enrôlement

L'un des enjeux clefs de l'authentification des utilisateurs est le processus d'enrôlement qui permet de vérifier l'identité de la personne physique (le professionnel de santé), sa qualité professionnelle (médecin, infirmier, …) et ce dans le but de :

- l'associer au dispositif d'authentification alternatif, qui assure son authentification forte pour l'accès au DMP (carte, téléphone mobile, etc.)
- le référencer pour lui attribuer des habilitations aux différentes applications de l'Ets

L'Etablissement est le garant de l'adéquation entre l'identifiant national du PS (RPPS/ADELI) utilisé pour l'accès au DMP, le PS utilisateur, et les moyens d'authentification mis à sa disposition.

Pour garantir l'identité de la personne physique, l'authentification de l'utilisateur lors du processus d'enrôlement du dispositif alternatif doit s'effectuer, autant que possible, avec la carte CPS.

Art. 3.3 : Gestion des habilitations

L'accès au DMP doit faire l'objet d'une gestion des habilitations particulières qui prend en compte la qualité professionnelle, les mouvements des personnels, le service d'exercice, etc.

Art. 3.4 : Authentification primaire des PS

Art. 3.4.1 : Identification

Pour accéder au DMP en consultation, l'identification du professionnel de santé doit être de portée nationale. Elle s'appuie sur un identifiant issu d'un référentiel national, tel que le référentiel RPPS ou ADELI de l'ASIP santé. L'identifiant national du PS est présent dans le VIHF transmis au SI-DMP.

Art. 3.4.2 : Authentification

Pour accéder au DMP en consultation, l'authentification des professionnels de santé doit être forte, c'est-à-dire être réalisée à partir d'une combinaison de deux facteurs de natures différentes qui peuvent correspondre à :

- « ce que je sais » (ex : un mot de passe) ;
- « ce que je possède » (ex : une carte, un terminal mobile,…) ;
- « ce que je suis » (ex : une caractéristique biométrique du PS).

Art. 3.4 : L'authentification de l'établissement

L'authentification de l'Ets auprès du SI-DMP s'effectue au moyen d'un certificat d'authentification pour personne morale, par la mise en œuvre d'une liaison sécurisée TLS en authentification mutuelle.

Un certificat de cachet pour personne morale est utilisé pour signer le jeton VIHF généré par l'établissement.

Art. 3.5 : Génération du VIHF

La construction du jeton VIHF est réalisée sous la responsabilité de l'Ets. Elle peut s'appuyer sur la solution logicielle d'un partenaire industriel.

L'infrastructure de génération des VIHF doit par conception permettre de préserver sa propre intégrité (mésusages, duplication et compromission des certificats). Cette infrastructure et son intégrité sont de la responsabilité de l'établissement. Le maintien en conditions opérationnelles ainsi que le maintien du niveau de sécurité de la solution doivent être assurés tout au long de l'expérimentation.

La durée de vie des jetons d'authentification des professionnels de santé doit être limitée dans le temps et s'adapte au contexte de consultation du DMP – services d'urgence, consultation, *etc.*

Art. 3.6 : Gestion des traces

La génération du jeton VIHF et son transport doivent permettre l'émission de **traces probantes au sein du SI-DMP**, permettant d'identifier clairement le Professionnel de santé et l'établissement de santé.

L'établissement est responsable de l'authentification primaire des PS sur ses systèmes d'information, et doit être en mesure d'assurer la **traçabilité de cette authentification** primaire.

Ces traces sont conservées par l'Ets et peuvent être fournies sur demande à l'Assurance Maladie.

L'Ets doit être en mesure de respecter la durée légale de conservation des traces. Celle-ci est alignée sur la durée de conservation du DMP. Les traces doivent être conservées 10 ans après la clôture du DMP puis détruites.

L'Ets doit être en mesure de garantir l'intégrité et la complétude des traces.
Sur demande de l'assurance maladie, l'établissement doit être en mesure d'envoyer par courriel (les modalités seront définies lors de la demande) toutes les traces d'un PS ou de plusieurs PS sur une période donnée en moins d'une semaine.

Art. 3.7 : Sensibilisation des utilisateurs

Pour participer à l'expérimentation du mode AIR, les établissements doivent avoir une politique de sécurité des systèmes d'information adressant la sensibilisation des utilisateurs – mesures existantes dans la majorité des cas.

La sécurité d'un système d'information repose également sur le comportement et les pratiques des utilisateurs qui manipulent les applications et données de la structure.

Article 4 : Sécurité

Art. 4.1 : Sécurité Physique

Les parties doivent mettre en œuvre et maintenir respectivement des procédures et des mesures de sécurité afin d'assurer la protection de leurs matériels (serveur de jeton), de leurs locaux, et de leurs services.

Les parties doivent respectivement mettre en œuvre et maintenir des procédures et des mesures de sécurité afin d'assurer la protection des accès au service proposé contre les risques d'accès non autorisés, de modification, de destruction ou encore de perte de données y figurant.

Art. 4.2 : Sécurité logique

Les parties utilisent des certificats générés par une infrastructure de gestion de clés validée par les deux parties. Ces certificats doivent être issus de l'IGC-Santé et délivrés par l'ASIP Santé.

Dans le cadre de l'expérimentation, l'Ets ne pourra utiliser que les certificats délivrés sur les FINESS géographiques renseignés en Annexe 3.

Fermeture des accès au service :

La Cnam se réserve le droit d'interrompre le service ou de fermer les accès au service de façon conservatoire dès lors qu'elle considère que les actions de l'ES peuvent représenter un danger pour le SI-DMP ou les données qu'il contient.

Article 5 : Confidentialité et protection des données

Les règles édictées au sein de cet article viennent s'ajouter à l'ensemble des règles relatives aux conditions de création, d'accès (alimentation comme consultation) aux DMP prévues par les articles L. 1111-14 et s. ; R. 1111-26 et s. du code de la santé publique. Ces règles sont notamment reprises au sein des conditions générales d'utilisation du DMP opposables à l'ensemble des professionnels et établissements de santé.

Art. 5.1 : Confidentialité et secret professionnel

Les parties sont tenues, ainsi que l'ensemble de leur personnel, au secret professionnel, à l'obligation de discrétion et à l'obligation de confidentialité durant toute l'exécution des présentes et après son expiration.

Les données mises à la disposition du PS exerçant au sein de l'Etablissement qu'elles soient ou non à caractère personnel, sont des données confidentielles et couvertes par le secret professionnel et médical, tel que défini aux articles 226-13 et s. du code pénal et L. 1110-4 et s. du Code de la santé publique.

Les parties conviennent que les données mises à la disposition des PS exerçant au sein de l'Etablissement, ne doivent en aucun cas être divulguées ou retransmises à des personnes physiques ou morales non autorisées.

Les parties s'engagent à respecter de façon absolue lesdites règles et obligations, et à les faire respecter par les PS utilisateurs qu'ils auront autorisés à accéder au service.

Si pour l'exécution des présentes modalités d'utilisation du service, les parties ont recours à des prestataires de services, ceux-ci doivent présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité.

Dans ce cas, les parties s'engagent à faire souscrire à ces prestataires de services les mêmes engagements que ceux figurant dans le présent article. A défaut, un engagement spécifique doit être signé avec lesdits prestataires mettant à la charge de ces derniers les obligations sus-énoncées.

En outre, les parties s'engagent à faire souscrire à ces prestataires de services, en plus des engagements contenus dans le présent article les engagements suivants :

- ils ne doivent pas utiliser les documents et supports d'information confiés par l'une des parties à des fins autres que celles spécifiées aux présentes ;
- ils ne doivent conserver aucune copie des documents et supports d'information confiés par l'une des parties après l'exécution des prestations ;
- ils ne doivent pas communiquer ces documents et informations à d'autres personnes que celles qui ont qualité pour en connaître ;
- ils doivent prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers en cours d'exécution des présentes ils doivent prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la convention ;
- ils doivent reconstituer les documents et les fichiers qui leur sont confiés et qui viendraient à être perdus ou inutilisables par leurs fautes.

Dans le cas où les prestataires de services sous-traiteraient l'exécution des prestations à un tiers, ce dernier serait soumis aux mêmes obligations.

Art. 5.2 : Protection des données à caractère personnel

Les Parties à la présente convention s'engagent à respecter, en ce qui les concerne, les dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi que celles du Règlement (UE) 2016-679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

De manière générale, chacune des Parties à la convention reconnaît être tenue, pour la partie du traitement qui la concerne, de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au règlement précité.

Comme rappelé par l'article R. 1111-27 du code de la santé publique et dans les conditions encadrées notamment par le décret n° 2016-1545 du 16 novembre 2016 autorisant la création d'un traitement de données à caractère personne dénommé « dossier médical partagé », la Cnam est responsable du traitement de données « DMP ». La Cnam a désigné un Délégué à la protection des données.

L'Etablissement est responsable du traitement qu'il met en œuvre pour permettre la consultation, par les professionnels strictement habilités exerçant en son sein, du DMP à l'aide de moyens alternatifs à la CPS.

A ce titre, la Cnam et l'établissement ont réalisé une étude d'impact vie privée (EIVP) conforme aux exigences du RGPD et des exigences publiées par la Cnil.

Pour ce faire, l'établissement conduit son étude sur la sécurité du dispositif global (c'est-à-dire de l'intégration du composant forgeant le jeton au SIH, et non une évaluation du risque lié à la solution d'authentification d'une part et du risque auquel est exposé le SIH d'autre part). S'il s'est associé à un éditeur et que la solution n'est pas interne, cette analyse est menée en partenariat avec cet éditeur. Tout recours à un sous-traitant dans le cadre du traitement des données nécessite l'information et l'acceptation de la Cnam.

L'établissement s'engage à transmettre à la Cnam son EIVP préalablement à la mise en œuvre de l'expérimentation et respecter l'ensemble des éléments techniques organisationnels qu'il a avancé pour prouver sa conformité à l'ensemble du panel normatif encadrant la protection des données.
L'établissement s'engage également à informer la Cnam de toute modification des conditions de réalisation de l'expérimentation pouvant impacter le contenu de l'EIVP et donc les conditions de conformité du traitement de données.

Conformément aux exigences du RGPD, chacune des parties s'engagent :

- à informer au plus tard dans les 48 heures l'autre partie de tout incident de sécurité au titre du DMP et plus particulièrement de la présente expérimentation pouvant aboutir à une violation de données personnelles accidentelle ou non ;
- de tout manquement à la règlementation applicable en matière de protection des données impliquant le DMP ;
- Garantir de manière coordonnée le respect des obligations quant à la notification de violation de données à caractère personnel auprès de l'autorité de contrôle et des personnes concernées si nécessaire, également en ce qui concerne l'analyse d'impact relative à la protection des données, compte tenu de la nature du traitement et des informations ;
- Mettre à la disposition de l'autre partie toutes les informations nécessaires pour démontrer le respect des obligations ;

- Assurer de manière coordonnée l'exercice des droits des personnes (droit à l'information, droit d'accès, droit de rectification, droit de limitation, droit d'opposition, notamment) ;
- Procéder aux formalités requises par loi susvisée.

Article 6 : Conditions de fonctionnement et d'utilisation du service

Art. 6.1 : Surveillance du niveau de service

Art 6.1.1 : Veille sécurité

Chaque partie assure une veille sécurité active sur tous les éléments concernés de son système d'information.

Art. 6.1.2 : Gestion des correctifs de sécurité

Chacune des parties s'engage à apporter tout correctif de sécurité identifié sur ses systèmes. Cela relève plus généralement du processus de gestion des changements avec une urgence adaptée à la vulnérabilité

Chaque partie s'engage à communiquer en toute transparence les vulnérabilités découvertes, les correctifs apportés avec les délais.

Art. 6.2 : Gestion des incidents et des problèmes

En cas de dysfonctionnement, le fournisseur et le client s'engagent à mettre tous les moyens dont ils disposent pour rétablir une situation normale dans les meilleurs délais.

L'Etablissement s'engage à informer dans les meilleurs délais les équipes de la Cnam de toute anomalie ou dysfonctionnement constaté sur les services qu'il opère, dans la mesure où le problème identifié serait de nature à mettre en jeu la sécurité des services opérés par la Cnam ou la confidentialité des informations échangées.

Tous les incidents sur les services en ligne considérés sont tracés. A chaque incident ouvert est associé un niveau de priorité défini en fonction des critères suivants :

- L'impact de l'incident sur le service aux utilisateurs,
- L'urgence qui reflète l'évaluation de la rapidité avec laquelle un incident doit être résolu, en solution définitive ou de contournement.

Il n'y a pas d'outil partagé entre le client et le fournisseur sur la traçabilité et le suivi des incidents. Ce partage est assuré par une communication par courriel ou téléphone entre les parties.

Les parties s'engagent à s'informer mutuellement de l'indisponibilité de l'un ou l'autre de leurs services.

Article 7 : Propriété intellectuelle des logiciels, applications et matériels

Les parties demeurent propriétaires des logiciels et applications qu'elles mettent en œuvre pour l'application du présent service.

La signature des présentes ne saurait entraîner de plein droit une quelconque cession de droit de propriété intellectuelle sur les logiciels et matériels, marques et noms de domaines utilisés pour la mise en œuvre du service.

Article 8 : Conditions financières

Pour accompagner les établissements dans leur démarche, les structures de soins retenues bénéficient de financements du Ministère, versés en deux temps – au début de l'expérimentation, puis une fois l'expérimentation débutée.
Le Ministère de la santé rend l'arbitrage final concernant les candidats retenus pour l'expérimentation, sur la base des informations transmises par la Cnam et du respect des exigences définies.

Compte tenu de ces éléments il est rappelé que la présente convention intervient à titre gracieux.

Article 9 : Durée

La présente convention entre en vigueur à compter de sa signature par les parties pour la durée de l'expérimentation et prendra fin en tout état de cause **le 31/12/2021**, et cela quelle que soit la date d'émission du premier flux.
A l'issue de cette période, les parties devront se rencontrer à nouveau afin de convenir des modalités d'une nouvelle collaboration.

Cependant, la Cnam se réserve le droit de faire un bilan global de l'expérimentation **1 an à partir du premier flux**.

Article 10 : Résiliation de la convention

Art. 10.1 : Résiliation par déclaration unilatérale de volonté d'une partie

Chaque partie peut, à tout moment, résilier la présente convention par lettre recommandée avec demande d'avis de réception adressée à l'autre Partie.

La résiliation de la convention prend effet à l'issue d'un délai défini en commun par les parties qui ne peut être inférieure à une durée de six mois.

Les parties conviendront des prestations à engager ou à réaliser pour la bonne fin de la présente convention, afin notamment de trouver une solution de remplacement pour ne pas que cette résiliation ait d'effet pénalisant sur l'une ou l'autre des parties.

Les parties restent tenues des engagements pris en matière de confidentialité et visés à l'article 5 qui survivent à la résiliation des présentes.

Art. 10.2 : Résiliation pour inexécution des obligations

En cas de manquement par l'une des parties à ses obligations, non réparé dans un délai de trente jours calendaires à compter de la réception de la lettre recommandée avec demande d'avis de réception lui notifiant le ou les manquements en cause et valant mise en demeure, l'autre Partie pourra résilier de plein droit les présentes, sans autre formalité que l'envoi d'une notification par lettre recommandée avec demande d'avis de réception adressée à la Partie défaillante.

Cette résiliation ne fait pas obstacle à toute demande de dommages et intérêts auxquels la Partie lésée pourrait prétendre en vertu des présentes.

Les parties restent tenues des engagements pris en matière de confidentialité et visés à l'article 5 qui survivent à la résiliation des présentes.

Les parties conviendront des prestations à engager ou à réaliser pour la bonne fin de la présente convention, afin notamment de trouver une solution de remplacement pour ne pas que cette résiliation ait d'effet pénalisant sur l'une ou l'autre des Parties.

Art. 10.3 : Règlement des litiges

Les parties conviennent de rechercher une solution amiable à tout différend qui pourrait survenir dans le cadre de la présente convention.

A défaut, tout litige résultant de l'application de la présente convention sera soumis à la juridiction compétente.

Fait à Paris en 2 exemplaires, le

Pour la Cnam, Pour l'établissement,

Annexe 1 : Tableau récapitulatif des exigences

N°	Libellé
#1	Lors de l'enrôlement du PS utilisateur, l'Ets est garant et doit s'assurer de : - L'adéquation entre la personne physique utilisatrice du compte local (le PS) et son identifiant national associé pour l'accès au DMP - L'appariement de l'utilisateur avec l'outil utilisé comme moyen d'authentification forte sur son système d'information hospitalier.
#2	Gestion des habilitations : les droits d'accès au DMP des différents types de PS utilisateurs du SIH doivent être documentés et régulièrement revus au regard de la qualification professionnelle et du contexte (mouvements, services, etc.).
#3	L'identification de l'utilisateur doit être publique, c'est-à-dire être un identifiant de portée nationale attribué lors de l'enregistrement dans un référentiel national (RPPS ou ADELI).
#4	L'authentification primaire du PS pour l'accès au DMP doit être forte et reposer sur deux facteurs distincts.
#5	Les méthodes d'authentification primaires du PS doivent être celles déclarées et autorisées pour l'Ets, et être précisées dans l'**Annexe 2**.
#6	L'authentification de l'Ets doit être effectuée par un certificat de personne morale valide, délivré par l'ASIP Santé sur un des FINESS géographiques déclarés dans l'**Annexe 3**.
#7	Pour accéder au DMP, l'Ets doit utiliser une solution logicielle homologuée AIR par le CNDA.
#8	La génération du jeton VIHF est sous la responsabilité de l'Ets et doit se faire dans un espace sécurisé.
#9	L'identification et l'authentification des utilisateurs et de la structure, portées par le jeton VIHF, doivent permettre la production de traces probantes au sein du SI-DMP. Localement, l'Ets doit être en mesure de tracer les sollicitations du système DMP.
#10	L'Ets doit sensibiliser les utilisateurs (ceux accédant au DMP et les intervenants techniques du SIH) participant à l'expérimentation aux risques liés à l'accès aux données de santé du DMP.
#11	L'Ets assure la protection logique et physique des éléments logiciels et d'infrastructure du SIH.

Annexe 2 : Liste des moyens d'authentification primaires autorisés pour l'expérimentation

Est attendu ici que l'Ets précise les moyens d'authentification primaire qu'il mettra en œuvre dans le cadre de l'expérimentation, en les cochant dans le tableau ci-dessous. L'Ets ne peut cocher que des moyens qu'il a décrits dans le dossier qu'il a transmis à la Cnam.
Ce tableau précise, pour chaque moyen, les deux champs (*AuthnContextClassRef* et *AuthnContextDecl*) que l'Ets devra renseigner dans le jeton VIHF lorsqu'il le met en œuvre pour accéder au DMP en mode AIR.

N°	Libellé	Valeur correspondante à renseigner dans le champ *AuthnContextClassRef* du jeton VIHF	Valeur correspondante à renseigner dans le champ *AuthnContextDecl* du jeton VIHF	Moyens utilisés par l'Ets
#1	Lecture de la CPS + saisie du code PIN	SmartCardPKI	CPS	☐
#2	Utilisation d'une carte d'établissement sans contact + saisie d'un code PIN	SmartCardPKI	CARTE_ETS	☐
#3	Lecture initiale de la CPS (avec saisie du code PIN) puis authentification en lecture sans contact	PreviousSession	CPS:CPSSANSCONTACT	☐
#4	Login/mot de passe + saisie d'un code OTP reçu par SMS	MobileTwoFactorContract	OTP_SMS	☐
#5	Login/mot de passe + saisie d'un code PIN sur une application mobile	MobileTwoFactorContract	APP_MOBILE_AUTH	☐
#6	Login/mot de passe + saisie d'un code PIN sur un navigateur web	InternetProtocolPassword	APP_BROWSER_AUTH	☐

Annexe 3 : Liste des FINESS géographiques associés aux certificats de personne morale

Est attendu ici que l'Ets précise les **FINESS géographiques** associés aux certificats utilisés pour l'accès au DMP en mode AIR, en les renseignant dans le tableau ci-dessous. Dans le cadre de cette expérimentation, l'Ets peut renseigner jusqu'à 3 FINESS différents.

N° FINESS géographique	Nom/libellé de la structure
[A compléter par l'Ets]	[A compléter par l'Ets]

Ne peuvent être indiqués que les FINESS des établissements pour lesquels le signataire de la présente convention dispose du pouvoir d'engagement plein et entier de la responsabilité.

ANNEXE 4

Document-type d'EIVP pour l'expérimentation « Consultation du DMP sans carte CPS »

à compléter par les établissements expérimentateurs

Document-Type d'EIVP pour l'expérimentation consultation du DMP sans carte CPS

à compléter par les établissements expérimentateurs

Cnam – Mission DMP

Juillet 2018
V1

LE DOSSIER MÉDICAL PARTAGÉ

1 Etude d'impact sur la vie Privée

1.1 Introduction

L'établissement doit conduire pour cette expérimentation, conformément à la réglementation en vigueur une étude d'impact sur la vie privée (EIVP), aussi appelée Privacy Impact Assessment (PIA).

L'établissement conduit en partenariat avec l'éditeur une analyse des risques sur la sécurité du dispositif global (c'est-à-dire de l'intégration du composant forgeant le jeton au SIH, et non une évaluation du risque lié à la solution d'authentification d'une part et du risque auquel est exposé le SIH d'autre part).

Avertissement :

Cette section du document fournit un exemple de structure pour la réalisation de l'étude d'impact sur la vie privée, à compléter par les établissements et leurs partenaires, et constitue ainsi un accompagnement à la réalisation de l'étude d'impact sur la vie Privée.

Aussi, la structure proposée et les exemples d'éléments à fournir dans chacun des paragraphes doivent être adaptés et précisés par les établissements autant que de besoin, afin d'assurer la pertinence et la complétude de leur analyse.

La responsabilité de la réalisation de l'EIVP (l'analyse de risques sécurité, la description des mesures de sécurité compensatoires, des scénarios d'événements indésirables, de l'évaluation des risques résiduels, …) revient aux établissements.

1.2 Principe général d'évaluation des risques *A compléter par l'établissement*

Est attendue ici la description des principes structurants de l'évaluation des risques. En particulier, peuvent être listés les principaux critères de l'expérimentation qui influencent les risques et sont pris en compte dans l'évaluation, la liste des principales menaces retenues et identifiées pour l'analyse, les axes d'évaluation des risques, ainsi que l'échelle de probabilité des menaces.

Des exemples sont fournis ci-après :

Illustration

Les risques sont évalués en prenant en compte les conditions spécifiques à l'expérimentation,

- *Le type de méthode d'authentification alternative utilisée (dispositifs, technologies, architecture…) ;*
- *L'implémentation de la méthode au sein du SIH ;*
- *Le processus d'enrôlement ;*
- *La protection du certificat ;*
- *L'environnement technique et organisationnel des établissements qui implémentent les méthodes ;*
- *Le nombre de PS éligibles à l'expérimentation ;*
- *Autres, à compléter*

L'estimation des risques porte sur les menaces et vulnérabilités pondérées par les mesures mises en œuvre pour l'expérimentation.

L'échelle de probabilité des menaces est présentée dans le paragraphe Echelles.

L'impact est évalué selon deux axes :

- *Impact VP (pour Vie Privée), sur une l'échelle définie plus loin dans ce document ;*
- *Risque pour votre établissement.*

1.3 Principes retenus pour l'évaluation des impacts sur la vie Privée *A compléter par l'établissement*

Sont décrits ici principes qui ont guidé l'évaluation des impacts sur la vie privée dans les principaux cas de figure correspondant aux grandes catégories de risques encourus. Il s'agit d'identifier les risques encourus par les patients comme par l'établissement, et d'en évaluer la criticité des impacts pour la vie privée, par exemple en cas de divulgation des données de santé du DMP d'un patient, de consultation du DMP d'un patient par une personne non habilitée, indisponibilité du service, etc.

Illustration

Exemple – Cas de figure : les données de santé du DMP d'un patient sont divulguées :
Les données stockées dans le DMP et/ou dans le SI-DMP contiennent des informations de santé. Elles sont constituées de la manière suivante :

- *Pour le patient (hors données de santé) : NIR, Nom, Prénom, date de naissance, rang de naissance, adresse e-mail, numéro de téléphone, numéro de sécurité sociale*
- *Pour le patient (données de santé) : données sur les traitements pris, les pathologies diagnostiquées, les allergies, les résultats d'examens biologiques, etc.*

En cas d'attaque de ces données, l'impact est évalué à critique pour la vie privée.

1.4 Synthèse des niveaux de risque *A compléter par l'établissement*

Est attendue ici la description exhaustive des risques identifiés, qui pourra être représentée sous forme de tableau de synthèse de l'ensemble des risques traités. Ces risques peuvent être classés en catégories (par exemple, risques liés au SIH, à l'enrôlement, au SI-DMP, à l'authentification, à la fraude, etc.) et comprennent également les risques liés non aux données personnelles (indisponibilité du service).
Pour chaque ligne du tableau décrivant un risque, un niveau de risque est attribué (voir sections échelles), et la nature ou les impacts du risque sont identifiés en colonne (voir exemple tableau).

Illustration

Le niveau de risque utilisé pour les travaux de conception et d'identification des mesures de protection est le niveau le plus élevé entre l'évaluation sur l'échelle CNIL (Vie privée) et l'échelle Cnam ; On retrouve ce niveau de risque dans le ***Erreur ! Source du renvoi introuvable.****,* ***Erreur ! Source du renvoi introuvable.*** *;*

Exemples de nature ou impacts du risque à évaluer en colonne – à adapter par l'établissement :

« DDP» : Divulgation des données à caractère personnel des patients, mais également atteinte à la disponibilité de ces données ; Si ce dernier type de risques est réellement rencontré, il est noté que le PS a toujours recours à l'authentification par carte CPS pour assurer la continuité du service actuel.

« DDP – S » : Divulgation des données à caractère personnel de santé des patients, mais également atteinte à la disponibilité de ces données ; Si ce dernier type de risques est réellement rencontré, il est noté que le PS a toujours recours à l'authentification par carte CPS pour assurer la continuité du service actuel.

« CDMP » : Consultation du DMP par une personne non habilitée…

Illustration

Type	Risque	Description du risque	Niveau de risque	DDP	DDP-S	CDMP
SI DMP	_R01	— Les données à caractère personnel de patients stockées dans le DMP sont divulguées.	4	…	…	…
SI DMP	_R02	— Les données à caractère personnel de patients stockées dans le DMP sont « aspirées »	4	…	…	…
SIH	_R01	— Un jeton réputé fiable est rejoué	..	…	…	…
ENROL	_R01	— Vol d'un dispositif tiers authentificateur enrôlé (smartphone, carte personnelle d'établissement, etc. du PS),	…	…	…	…

ENROL	_R02	– Usurpation d'identité pour l'enrôlement du dispositif tiers authentificateur	…	…	…	…
…	….	– …	…	…	…	…

1.5 Détails des risques *A compléter par l'établissement*

Est attendue ici la description détaillée des risques, rassemblée par catégories de risques (risque de sécurité liés à l'enrôlement, risques de sécurité relatifs à l'intrusion au sein du SIH, risques de sécurité relatifs à l'utilisation abusive ou frauduleuse du dispositif d'authentification, risques règlementaires liés à la vie privée…).

Pour chaque catégorie de risques, chaque risque est présenté dans le détail, par exemple dans un tableau comme celui-ci :

1.6 Couverture des risques *A compléter par l'établissement*

Illustration

SI_DMP_R01 : Divulgation des données à caractère personnel de santé stockées dans le DMP de patients	**Impact VP**	**Probabilité**	**Risque VP**
	..	..	**..**
	Impact pour l'établissement		**Risque pour l'établissement**
	..		**..**
Description d'un scénario de réalisation du risque, de sa probabilité d'occurrence, et de l'analyse de ce risque qui conduit aux évaluations chiffrées situées en en-tête de tableau.			
Conséquences Vie Privée	…		
Conséquences Etablissement	…		
Type de menaces	*Liste des menaces associées au risque décrit*		

Cette section a pour objectif de décrire, pour chacun des risques identifiés, les mesures de sécurité compensatoires mises en œuvre afin de les maîtriser et limiter.

Cette description s'effectue par catégories de risques identifiés, dans l'ordre identique à celui utilisé aux paragraphes précédents (synthèse de niveaux de risques et couverture des risques).

Pour chaque catégorie de risque identifiée, un tableau comme celui-ci pourra être réalisé :

Illustration

Risques de la catégorie (ex. risques liés au processus d'enrôlement)	**Mesures de sécurité compensant les risques liés à la catégorie**	**Mesure de sécurité compensatoire 1**	**Mesure de sécurité compensatoire 2**	**Mesure de sécurité compensatoire 3**	…	…				
Libellé du risque 1		x	x	x					x	
Libellé du risque 2		x			x					
Libellé du risque 3				x				x		

1.7 Plan d'action *A compléter par l'établissement*

Est décrit dans cette section le plan d'actions à mettre en œuvre dans le cas où l'ensemble des mesures compensatoires n'aurait pas été décrit dans les sections précédentes. Les autres mesures envisagées dans le cadre de l'expérimentation sont alors décrites ici.

1.8 Validation de l'étude d'impact sur la Vie Privée *A compléter par l'établissement*

L'évaluation du PIA passe par la vérification des mesures juridiques, techniques et contractuelles.

Le Responsable de traitement doit s'assurer qu'il n'est pas utile ou possible de les améliorer dans le traitement et leur mise en œuvre. Il doit également décider de l'acceptabilité des risques résiduels de manière argumentée.

Le Responsable de traitement doit s'engager à appliquer les mesures prévues et détaillées dans le PIA.

Dans cette section sont évalués les niveaux de risque résiduels après prise en compte des mesures de sécurité compensatoires, et selon les critères touchés (Disponibilité, Intégrité, Confidentialité ou Preuve DCIP).

Illustration

ID	Libellé du risque	Critères touchés	Niveau risque résiduel DCIP	Acceptabilité et arguments
	–			

1.9 Base de connaissances

1.9.1 Catégories de données à caractère personnel courantes

Types de DCP	Catégories de DCP
DCP courantes	État-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses…)
	Vie professionnelle (CV, scolarité formation professionnelle, distinctions…)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale…)
	Données de connexion (adresses IP, journaux d'événements…)
	Données de localisation (déplacements, données GPS, GSM…)
DCP perçues comme sensibles	Numéro de sécurité sociale (NIR)
	Données biométriques
	Données bancaires
DCP sensibles	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, **données de santé**, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle.
	Infractions, condamnations, mesures de sécurité

1.9.2 Liste des menaces

1.9.2 Liste des menaces retenues *A compléter par l'établissement*

Est présentée ici la liste des menaces retenues dans le cadre de cette étude d'impact sur la vie privée, parmi les menaces EBIOS 2010.

Les menaces peuvent être présentées par catégories (Menaces sur les matériels, sur le logiciel, etc.) dans un tableau comme celui-ci (où l'impact est évalué sous la forme de critères touchés parmi Disponibilité, Intégrité, Confidentialité ou Preuve - DCIP) :

Illustration

ID	Intitulé de la menace	Description de la menace	Critères touchés
M2	– Espionnage d'un matériel	Le matériel, généralement un périphérique, est observé ou écouté, sans être endommagé, avec ou sans équipement d'amplification sensorielle ou de capture, depuis l'intérieur ou l'extérieur de locaux. Les informations et traitements peuvent ainsi être compromis.	C

Les menaces sont notamment renseignées dans les descriptions détaillées des risques.

1.9.3 Exemples de suite d'événements redoutés *A compléter par l'établissement*

Est attendu dans cette section la description d'exemples de suites d'événements redoutés. Le scénario peut décrire des étapes de gravité croissante d'événements indésirables. Cette description peut se présenter sous la forme d'un tableau tel que celui présenté ci-dessous :

Illustration

Evénements redoutés	Etapes	Description
Accès illégitime aux données à caractère personnel	Consultation	…
	Stockage	
	Rediffusion	…
	Exploitation	…

1.10 Echelles

1.10.1 Echelle de probabilité des menaces *A adapter au besoin par l'établissement*

Un tableau résumant l'échelle de probabilité des menaces est proposé ci-après.

Illustration

Niveau Dénomination	Critère compétences et moyens	Critère motivation	Profil de l'attaquant	Décision Etablissement
0	Impossible à mettre en œuvre dans la pratique ou possibilité extrêmement faible de se réaliser	Stratégique ou politique	Organisations criminelles ou étatiques	Non pris en compte : risque acceptable
1 Très improbable, ne surviendra proba-blement jamais	Demande des moyens très importants et/ou des connaissances très élevées dans le domaine considéré	Frauduleuse, stratégique, politique	Organisations criminelles ou étatiques Concurrents	À prendre en compte au cas où : zone de risque résiduel acceptable
2 Possible bien qu'improbable	Demande des matériels disponibles commercialement et/ou des connaissances de base sur le domaine considéré Pourrait arriver pendant le cycle de vie du système	Frauduleuse	Fraudeur	À prendre en compte. Toléré au cas par cas.
3 Probable, devrait arriver un jour	Demande peu de moyens et peut être réalisé avec peu de connaissances du domaine concerné	Ludique vénale	Hacker lambda	À prendre en compte obligatoirement
4 Très probable. Surviendra sûrement à court terme.	Ne demande aucun matériel particulier et peut être réalisé sans connaissances particulières du domaine concerné	Ludique occasionnel	Hacker lambda	À prendre en compte obligatoirement

1.10.2 Echelle d'impact sur la vie privée *A adapter au besoin par l'établissement*

L'évaluation de l'impact des risques sur la vie privée se base sur l'échelle suivante issue des recommandations de la CNIL, à laquelle a été ajouté le niveau 0.

Illustration

	Description générique de l'impact	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemple d'impacts moraux
0 – Aucun	Les personnes concernées ne seront pas impactées	-	-	-
1 – Négligeable	Les personnes concernées pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle), maux de tête passagers	Perte de temps pour réitérer des démarches, réception de publicités ciblées non sollicitées pour des produits courants	Simple contrariété par rapport à l'information reçue ou demandée, sentiment d'atteinte à la vie privée sans préjudice réel
2 – Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Affection physique mineure (ex. : maladie bénigne suite au non-respect de contre-indications), absence de prise en charge causant un préjudice minime mais réel (ex : handicap), diffamation donnant lieu à des représailles physiques ou psychiques	Paiements non prévus, frais supplémentaires, refus d'accès à des services administratifs ou commerciaux, promotion professionnelle manquée publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel	Affection psychologique mineure mais objective (diffamation), difficultés relationnelles avec l'entourage personnel ou professionnel (réputation ternie), intimidation sur les réseaux sociaux
3 – Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	Affection physique grave causant un préjudice à long terme (aggravation de l'état de santé suite à une mauvaise prise en charge), altération de l'intégrité corporelle par exemple à la suite d'une agression ou d'un accident	Détournements d'argent non indemnisés, difficultés financières temporaires, opportunités uniques perdues (prêt immobilier, études, emploi), interdiction bancaire, perte d'emploi, divorce	Affection psychologique grave (dépression, développement d'une phobie), , développement d'une phobie, victime de chantage, de harcèlement moral, assignation en justice, atteinte à la liberté d'expression
4 – Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	Affection physique de longue durée ou permanente, décès, altération définitive de l'intégrité physique	Péril financier, dettes importantes, impossibilité de travailler ou de se loger, perte de preuves dans le cadre d'un contentieux, perte d'accès à une infrastructure vitale (eau, électricité)	Affection psychologique de longue durée ou permanente, sanction pénale, enlèvement, perte de lien familial, changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

1.10.3 Echelle d'impact sur l'établissement *A adapter au besoin par l'établissement*

L'impact tient compte du niveau de sensibilité du bien ciblé par l'attaque sur la caractéristique impactée.

L'échelle de valeur d'impact proposée pour les différentes menaces retenues par type d'acteurs est indiquée dans le tableau ci-dessous :

Niveau Libellé	Impact sur l'organisation Périmètre atteint
0 Aucun impact	Aucun impact sur le fonctionnement de l'organisme.
1 Faible Impact insignifiant	Susceptible de gêner le fonctionnement de l'établissement (pertes financières faibles, nuisances organisationnelles, …). Fonctions secondaires ou accessoires Attaque sans conséquence importante sur le système
2 Sensible Impact significatif	Susceptible d'amoindrir notablement les capacités de l'organisme (pertes financières, sanctions administratives, …). 30% des fonctions courantes sont indisponibles
3 Critique Impact très grave	Menace susceptible de provoquer une modification importante des structures et la capacité de l'organisme (perte d'image de marque, pertes financières importantes, révocation de dirigeants, …). (+50% fonctions courantes +) ou certaines fonctions critiques
4 Stratégique Impact extrêmement grave	Atteinte majeure susceptible de mettre en cause la pérennité de l'organisme (perte d'image de marque, pertes financières inacceptables, poursuites judiciaires, …). Système complet – ne peut plus remplir ses missions de base

1.10.4 Echelle de gravité des risques *A adapter au besoin par l'établissement*

La gravité d'un risque est obtenue par le croisement entre la probabilité et l'impact de la menace :

Impact ⇨ Probabilité ⇩	0	1	2	3	4
0	0	0	0	1	2
1	0	1	1	2	3
2	0	1	2	3	4
3	1	2	3	4	4
4	2	3	4	4	5

L'échelle de gravité utilisée est présentée ci-dessous :