

MEMO : Tout savoir sur le mode AIR

Le **mode AIR** est un dispositif **d'identification** et **d'authentification** des professionnels de santé permettant un **accès simplifié** et **sécurisé** au Dossier Médical Partagé (DMP). Il permet aux professionnels de **consulter directement** les documents du DMP depuis leur logiciel métier (DPI), sans avoir à se reconnecter à un service externe.

1 PRÉREQUIS VALIDÉS



2 CONTRACTUALISER



3 DÉPLOYER ET PÉRENNISER



Prérequis validés



Cellule d'auto-homologation validée

Avec l'Assurance Maladie

Le mode AIR donne accès à la liste blanche de l'Assurance Maladie et assure une traçabilité des échanges. Il renforce ainsi la sécurité, la conformité et la confiance dans les services utilisés.

Avec le GRADeS

Une fois l'accord établi, le GRADeS reste disponible pour mettre en place un plan d'accompagnement permettant de développer des usages au sein de votre structure.



LE RÔLE DU GRADeS INÉA

Le GRADeS est l'interlocuteur régional des établissements de santé pour le déploiement des usages du DMP

- ✓ Sensibilisation aux enjeux numériques
- ✓ Formation des équipes
- ✓ Suivi des usages



OBJECTIF FINAL

Faire du DMP un outil **intégré au quotidien** pour améliorer la coordination des soins et la qualité de prise en charge



Vous êtes prêt à contractualiser avec la CPAM de votre territoire ?

Votre chargé d'accompagnement vous accompagne et fait le lien avec l'Assurance Maladie

accompagnement.territoire@esante-hdf.fr

1

Comment valider les prérequis : les exigences du référentiel DMP

Le Référentiel de sécurité et d'interopérabilité du DMP comprend **29 exigences obligatoires** pour contractualiser. L'établissement se conforme aux exigences encadrantes, notamment :

- les modalités d'accès au DMP (web ou intégré aux logiciels métiers)
- les modes d'authentification des professionnels et les échanges avec les logiciels l'alimentation, la consultation et le téléchargement des documents, incluant la gestion de l'INS, des accès et des droits patients
- la sécurité et la traçabilité des traitements (habilitation, supervision, sensibilisation des utilisateurs)
- les exigences spécifiques du mode d'authentification indirecte AIR Simplifié.



Lien vers le [référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé](#)

QUESTIONS RÉCURRENTES

Mon logiciel DPI / PFI est-il référencé Ségur Vague 2 et/ou CNDA ?

Les **logiciels DPI / PFI** doivent être **référéncés Ségur Vague 2 et/ou homologués** par le **Centre National de Dépôt et d'Agrément (CNDA)** afin de garantir leur conformité aux exigences techniques et réglementaires nécessaires à l'utilisation du mode AIR Simplifié.



CONFORMITÉ

Dans le cadre du AIR DMP, le CNDA intervient notamment pour :

- **Tester la conformité** des logiciels aux spécifications nationales (DMP, INS, MSSanté, etc.).
- **Homologuer les connecteurs et services** permettant l'accès au DMP.
- **Valider les échanges** entre les logiciels des éditeurs et les services de l'Assurance Maladie
- **Délivrer un agrément** lorsque les tests sont concluants, permettant à l'éditeur de déployer son logiciel auprès des établissements de santé.

À noter : l'homologation CNDA est ouverte depuis octobre 2024.

Comment valider que les exigences du référentiel DMP sont atteintes ?



VIABILITÉ

Les exigences du référentiel DMP relèvent principalement de la conformité et du paramétrage de votre logiciel. Elles doivent donc être examinées en priorité avec votre **éditeur**, qui est en mesure de confirmer les fonctionnalités disponibles, leur configuration et les modalités de mise en œuvre.

Le GRADeS et l'ARS peuvent accompagner l'établissement dans la compréhension du dispositif ou du dossier de contractualisation, mais **ils ne peuvent pas se substituer à l'éditeur** pour valider les aspects techniques ou le paramétrage de la solution. Les réponses apportées au référentiel doivent également être le reflet de l'organisation interne de votre établissement et des pratiques effectivement mises en œuvre.

2

Comment valider les prérequis : L'authentification

L'authentification forte est un mécanisme de sécurité permettant de vérifier l'identité d'un utilisateur avant de lui donner accès à un système d'information ou à des données sensibles. Celle-ci repose sur la combinaison de minimum **deux facteurs d'identification** issus de catégories différentes pour accéder à l'appliquatif :

- **Ce que je suis** : biométrie (empreinte digitale, rétinienne), login
- **Ce que je sais** : mot de passe, code PIN ;
- **Ce que je possède** : carte CPx, clé FIDO, certificat.

ProSanté Connect est le **fournisseur d'identité des professionnels** de santé, permettant une **authentification forte** à double facteur grâce notamment au numéro RPPS. Cette authentification peut être réalisée via une carte CPS, une e-CPS ou être intégrée à une solution de gestion des identités et des accès (IAM/SSO), selon l'architecture retenue par l'établissement. Elle garantit un accès sécurisé aux services numériques de santé.

QUESTIONS RÉCURRENTES



SECURITÉ

Mon établissement dispose-t-il déjà d'une authentification forte ?

Tout dépend du mode d'authentification mis en œuvre. L'établissement peut s'appuyer sur ProSanté Connect ou sur un dispositif d'authentification à double facteur utilisant un code à usage unique (OTP), transmis par SMS, par e-mail ou généré via une application d'authentification (TOTP), telle que Microsoft Authenticator.



TRACABILITÉ

Comment mettre en place une authentification forte (MFA) ?

La mise en place d'une authentification forte dépend des solutions déjà déployées dans votre établissement et des capacités de votre logiciel. Pour les services numériques de santé, il est recommandé de s'appuyer sur des solutions conformes aux référentiels de l'Agence du Numérique en Santé, telles que Pro Santé Connect, la CPS ou la e-CPS.

Votre éditeur peut vous accompagner dans le choix de la solution la plus adaptée et dans son intégration au sein de votre système d'information.



INTEROPERABILITÉ

Le SSO est-il appelé à devenir obligatoire ?

Comment faire pour déterminer les SSO compatibles avec mon DPI ?

Bien que non obligatoire, cette solution améliore le confort d'utilisation en offrant un accès unifié à l'ensemble des applications du système d'information de l'établissement, grâce à une authentification unique, évitant ainsi des reconnections répétées.

Pour identifier les SSO compatibles avec votre DPI, rapprochez-vous de votre éditeur. Il pourra vous confirmer les solutions prises en charge et vous accompagner dans leur mise en place et leur paramétrage.



Vous avez d'autres questions sur l'Identification électronique (MIE) ? Rendez-vous sur notre FAQ



3

Comment valider les prérequis : L'auto-homologation

L'auto-homologation du référentiel DMP est une démarche par laquelle un établissement ou un professionnel de santé atteste que son système d'information respecte les exigences de sécurité et d'interopérabilité définies par l'Agence du Numérique en Santé pour l'accès au Dossier Médical Partagé (DMP).

Cette procédure comprend une évaluation de la conformité, la constitution d'un dossier de preuves et la signature d'un procès-verbal d'auto-homologation. Elle engage la responsabilité de l'établissement et constitue un prérequis pour certains modes d'accès au DMP.

Si besoin, des modèles et outils sont mis à votre disposition par le GRADeS, notamment un questionnaire d'auto-évaluation et un template de base documentaire.

QUESTIONS RÉCURRENTES

La mise en place d'une cellule d'auto-homologation est-elle obligatoire ?

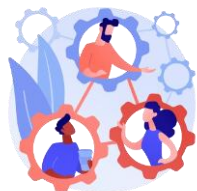


VALIDITÉ

Oui, la mise en place d'une cellule d'auto-homologation interne est **obligatoire**. Celle-ci doit être anticipée et structurée en amont, notamment par la constitution d'une **base documentaire complète** couvrant **l'ensemble des exigences du référentiel de sécurité et d'interopérabilité du DMP**, ainsi que sa mise en œuvre dans **l'organisation interne**.

Par ailleurs, cette étape doit permettre de définir de manière claire et documentée les habilitations et périmètres d'accès aux différents systèmes concernés (DPI, PFI, GAM et autres outils associés). Il est attendu une vision précise de « **qui a accès à quoi** », afin d'assurer la traçabilité des accès et la conformité du dispositif.

Quels membres composent l'instance d'auto-homologation ?



RESPONSABILITÉ

Cette cellule doit a minima réunir les principales parties prenantes impliquées dans la démarche : la **direction de l'établissement, la DSI et / ou le RSSI et/ou le DPO**, etc. ainsi que **les acteurs métiers** concernés. Cette gouvernance permet d'assurer une coordination efficace, un pilotage structuré et un suivi cohérent des actions engagées.

Comment formaliser la démarche d'auto-homologation ?



DURABILITÉ

La formalisation de la démarche repose sur la rédaction et la signature d'un procès-verbal d'auto-homologation, dans lequel doivent être mentionnées les éventuelles réserves identifiées. Ce document doit également préciser la durée de validité de l'homologation, qui ne peut excéder trois ans.