AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP)

DNS/DAJMS/ANS/CNAM

Statut : Validé | *Classification : Publique* | *Version : v 0.1*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. INTRODUCTION

1.1. Qu'est-ce que le DMP ?

Le dossier médical partagé (DMP) est un espace de stockage personnel et sécurisé de données de santé, il permet à une personne de stocker et de partager ses documents de santé avec les professionnels de son choix.

Au titre de l'article L.1111-15 du code de la santé publique (CSP), les professionnels et établissements de santé doivent, sauf opposition de la personne pour un motif légitime, alimenter le dossier médical partagé des personnes qu'elles prennent en charge à l'occasion de chaque acte ou consultation. Un arrêté pris par le ministre chargé de la santé indique quels sont les documents soumis à cette obligation d'alimentation.

S'agissant des autres documents, les professionnels et établissements peuvent alimenter le DMP de la personne prise en charge, y compris avec des documents plus anciens qu'ils ont conservés dans leurs dossiers informatisés.

Enfin, les professionnels et établissements peuvent consulter le DMP des personnes qu'ils prennent en charge, après les avoir informés, suivant une matrice des droits d'accès au dossier médical partagé pour les professionnels autorisés (ou matrice d'habilitation) approuvée par arrêté, mentionnée par l'alinéa 6 de l'article R. 1111-46 du CSP. Cette matrice d'habilitation définit, pour chaque profil du professionnel, le niveau d'information consultable. Elle est complétée, adaptée ou modulée par les autorisations, masquages ou blocages éventuellement paramétrés directement dans Mon espace santé par le titulaire lui-même. Certains professionnels peuvent également consulter ces données dans des situations d'urgence, dans les conditions prévues au I de l'article L. 1111-17 du CSP, avec le périmètre d'habilitations prévu par la matrice et sauf opposition enregistrée par le titulaire lui-même dans Mon espace santé.

Le DMP ne remplace pas le dossier médical que tient le professionnel pour son patient localement, mais a vocation à centraliser une copie des données de santé les plus pertinentes afin que le titulaire puisse systématiquement avoir accès aux documents essentiels à sa prise en charge.

Le DMP est géré par l'Assurance Maladie, responsable du traitement.

Le matricule Identité Nationale de Santé (INS) mentionné à l'article L. 1111-8-1 I du CSP est l'identifiant des DMP des patients.

1.2. Par quels textes le DMP est-il encadré ?

Référence	Document
Articles L. 1111-14 à L. 1111-22 du CSP tels qu'issus de la loi du 7 décembre 2020 dite "loi ASAP"	https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000020889011/#LEGISCTA000038886983

Articles R. 1111-40 à R. 1111-52 du CSP tel qu'issus du décret n° 2021-1047 du 4 août 2021 relatif au dossier médical partagé	https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000043919276/#LEGISCTA000043919285
Article L. 1110-4 du CSP	Règles relatives au cercle de confiance et au partage de données de santé https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042656229/
Articles L. 1110-12 et R. 1110-2 du CSP	Définition de l'équipe de soins Article L1110-12 - CSP - Légifrance (legifrance.gouv.fr) Article R1110-2 - CSP - Légifrance (legifrance.gouv.fr)
Article L. 1470-5 du CSP	Règles relatives à l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043497489
Arrêté du XXX relatif à la matrice des droits d'accès au dossier médical partagé pour les professionnels autorisés	Règles relatives aux autorisations d'accès au DMP selon la profession
Arrêté du 26 avril 2022 fixant la liste des documents soumis à l'obligation prévue à l'article L. 1111-15 du CSP	Règles relatives aux documents devant obligatoirement être versés au DMP à l'occasion d'une consultation ou d'un acte

1.3. Quelle est l'articulation du DMP avec *Mon espace santé* ?

Le dossier médical partagé est intégré à Mon espace santé dont il constitue l'une des composantes (article L. 1111-13 du CSP).

Mon espace santé permet à chaque titulaire d'accéder à son DMP. Il peut notamment :

- Enregistrer des documents dans son DMP (ex : comptes-rendus médicaux, documents relatifs aux directives anticipées ou aux choix en termes de dons d'organes, etc.), directement ou via des applications référencées au catalogue[1] ;
- Consulter et/ou télécharger les documents de son DMP (y compris ceux alimentés par ses professionnels et établissements de santé) directement ou via des applications référencées au catalogue ;

[1] Autorisées à proposer de l'échange de données au vu de leur finalité (prévention, soin, diagnostic ou suivi social et médico-social) comme le prévoit l'article L 1111-13-1 III

- Personnaliser les conditions d'accès des professionnels à ses documents de santé (masquer des documents, autoriser ou bloquer l'accès de tout ou partie des professionnels, y compris pour les accès en cas d'urgence) ;
- Être informé et consulter les traces des accès à son DMP par ses professionnels et établissements de santé.

1.4. Quelle est la nature du présent référentiel ?

Ce référentiel constitue un référentiel de sécurité et d'interopérabilité, au sens de l'article L. 1470-5 du CSP, concernant l'accès au Dossier Médical Partagé par les professionnels et établissements intervenant en santé (cf. article 1.5 du présent référentiel).

Le référentiel détaille les exigences visant à garantir l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel traitées dans le cadre du DMP.

Il est approuvé par arrêté du ministre chargé de la santé, ce qui le rend opposable. Il fixe des exigences qui s'imposent aux professionnels et établissements qui souhaitent alimenter (écriture dans le DMP) des documents au DMP et/ou en consulter/télécharger (lecture du DMP), ainsi qu'à leurs éditeurs de logiciels sous-traitants.

Dans plusieurs situations qui sont détaillées dans le présent référentiel, les professionnels et établissements concernés devront s'engager à être conformes à ce référentiel. Un document d'engagement de conformité au référentiel DMP est proposé par l'Assurance Maladie sur son site internet.

Le présent référentiel est complété :

- Par les conditions générales d'utilisation du DMP pour les professionnels, publiées par l'Assurance Maladie, qui détaillent certaines exigences générales du présent référentiel ;
- Par le guide d'intégration 'Service DMP intégré aux LPS' publié par le GIE SESAM-Vitale, relatif aux exigences techniques applicables aux logiciels des professionnel ayant vocation à s'interfacer avec le DMP.

1.5. Quel est le périmètre d'application de ce référentiel ?

Ce référentiel encadre les modalités d'accès au DMP et à son contenu par les professionnels personnes physiques et personnes morales mentionnés aux 1° et 2° de l'article L. 1470-1 du CSP, et enregistrées dans les répertoires sectoriels de référence mentionnés à l'article L. 1470-4 du CSP. Il s'agit :

- Des professionnels de santé et des personnes exerçant sous leur autorité, des établissements et services de santé, du service de santé des armées et de tout organisme participant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le CSP ;
- Des professionnels des secteurs social et médico-social et des établissements ou services des secteurs social et médico-social mentionnés au I de l'article L. 312-1 du code de l'action sociale et des familles.

Ces derniers sont notamment les établissements et services sociaux et médico-sociaux qui délivrent des prestations à domicile, en milieu de vie ordinaire, en accueil familial ou dans une structure de prise

en charge. Ils assurent l'accueil à titre permanent, temporaire ou selon un mode séquentiel, à temps complet ou partiel, avec ou sans hébergement, en internat, semi-internat ou externat.

Le présent référentiel fait référence à ces professionnels lorsqu'il utilise l'appellation 'le professionnel'. Dans le cas des établissements, certaines exigences détaillées dans le présent référentiel concernent les personnes qui exercent au sein de l'établissement, vers qui l'établissement peut se retourner en cas de manquement (ex : défaut d'information du patient, etc.).

Même si le présent référentiel s'applique ainsi aux professionnels listés ci-dessus, les éditeurs de logiciels avec lesquels ils contractent sont également concernés, dans la mesure où certaines exigences ne peuvent être atteintes qu'au travers de leurs logiciels. Pour accompagner les professionnels :

- Les exigences qu'il contient sont réglementaires et prévalent aux contrats conclus entre le professionnel et les éditeurs, qui ne doivent pas comporter de mentions contraires ;
- Les éditeurs dont les produits sont utilisés pour des accès au DMP doivent être homologués préalablement par le centre national de dépôt et d'agrément (CNDA), sur la base d'un cahier des charges (guide d'intégration) déclinant les exigences du référentiel en spécifications techniques et de cahiers de tests détaillés ;
- La puissance publique conditionne les actions de financement qu'elle conduit vis-à-vis des éditeurs et des professionnels (ex : programme Ségur Numérique) à la compatibilité des logiciels.

1.6. Quelles sont les deux grandes modalités d'interaction avec le DMP pour les professionnels ? Quelles sont les modalités d'identification électronique associées ?

Deux modalités d'accès au DMP existent pour les professionnels : l'accès web et l'accès intégré à leur logiciel métier.

Un accès web, dénommé "Web PS DMP" est fourni par la puissance publique. Il consiste en un accès direct dans un navigateur sur l'URL https://www.dmp.fr/ps. Cette forme peut être intégrée partiellement aux logiciels métier des professionnels via un appel de contexte patient, permettant de directement visualiser le DMP du bon patient. Les professionnels peuvent s'y identifier électroniquement directement comme personnes physiques par les moyens d'identification électroniques prévus à l'article L. 1470-3 du CSP: le téléservice *Pro Santé Connect* (avec l'application mobile e-CPS ou la carte CPS) et la carte CPS. Ils peuvent alimenter des documents et/ou consulter/télécharger les documents du DMP du patient, sous réserve de leurs droits d'accès et du respect des droits du patient (droit d'opposition après information préalable ou recueil du consentement). Les droits d'accès des professionnels peuvent en outre être adaptés (réduits ou élargis) par le patient.

Un accès totalement intégré aux logiciels des professionnels de santé, dénommé "interfaces LPS DMP" permet aux professionnels d'interagir avec le DMP depuis leur logiciel métier, de manière optimisée. L'objectif est que les professionnels puissent interagir en écriture et en lecture avec le DMP au travers de leur logiciel métier, qui joue le rôle d'intermédiaire, avec différentes composantes relatives à ce rôle (gestion de l'identification électronique, contrôles de la qualité des documents, visualisation intermédiaire des documents pour sélectionner les documents pertinents à conserver, etc.).

Dans le cas où l'accès du professionnel est intégré à son logiciel, en ce qui concerne l'identification électronique au DMP, le professionnel peut :

- **Soit s'authentifier directement** par les moyens d'identification électronique prévus à l'article L.1470-3 du CSP. Le logiciel joue alors le rôle de passerelle pour véhiculer cette information au DMP ;

- **Soit s'authentifier indirectement**, en s'étant préalablement identifié à son logiciel en tant que personne physique (authentification primaire), avec des moyens d'identification électronique "locaux" (clefs FIDO, etc.), selon des modalités conformes aux exigences de sécurité en vigueur, notamment le référentiel d'identification électronique de la PGSSI-S, ainsi qu'aux exigences particulières du présent référentiel. L'identification électronique au DMP est alors effectuée par le logiciel avec des certificats appartenant à la structure dans laquelle le professionnel est employé (et dans le contexte de laquelle il effectue une prise en charge justifiant d'échanges avec le DMP) ;

- Soit bénéficier **d'échanges automatisés** effectués au travers du logiciel de l'éditeur sous-traitant du professionnel ou de sa structure (exemple : envoi nocturne de tous les comptes-rendus validés dans une journée, rapatriement automatisé des documents potentiellement pertinents pour les admissions du lendemain, etc.). L'identification électronique au DMP est alors également effectuée de manière indirecte avec les certificats, soit de la structure d'emploi dans laquelle le professionnel est employé (et dans le contexte de laquelle il effectue une prise en charge justifiant d'échanges avec le DMP), soit de l'éditeur du logiciel.

1.7. Quel régime pour les documents lors du transfert d'une copie entre traitements locaux et le DMP ?

Lorsque la copie d'un document est alimentée au DMP depuis un traitement local par un professionnel, cette copie ne relève plus du traitement local, mais du régime juridique applicable au DMP.

Inversement, lorsque la copie d'un document issu du DMP est enregistrée dans le traitement local d'un professionnel, cette copie ne relève plus du traitement DMP, mais des règles qui encadrent le traitement local.

Cette différence entre les deux traitements implique que les autorisations d'accès peuvent ne pas être les mêmes. Par exemple, un professionnel non autorisé au sens du DMP peut avoir accès à un document issu du DMP, une fois celui-ci intégré dans le logiciel, si celui-ci dispose d'un accès au dossier du patient dans le cadre des habilitations et accès locaux. A noter qu'en cas d'enregistrement local d'un document issu du DMP, il appartient au responsable du traitement local, le cas échéant, d'assurer le respect des dispositions du RGPD, notamment en ce qui concerne l'information de la personne concernée sur ses droits, ainsi que du respect de l'ensemble des obligations afférentes à sa pratique, et notamment le secret médical.

Néanmoins :

- Les règles d'autorisations d'accès au DMP s'appliquent pour les transactions avec lui (alimentation et consultation/téléchargement) ;

- Certaines exigences du présent référentiel portent sur les logiciels connectés au DMP, dépassent la stricte connectivité au DMP et s'appliquent aussi en partie transversalement à ces logiciels (sécurité, etc.). Ils relèvent généralement de rappels d'exigences déjà portées dans le RGPD.

2. EXIGENCES RELATIVES A L'INFORMATION DU PATIENT, L'EXERCICE DE SES DROITS, LES REGLES D'ACCES AU DMP

2.1. Information du patient et exercice de ses droits

Tout professionnel qui prend en charge un patient et qui appartient à son équipe de soins doit s'assurer que le patient est informé préalablement à la consultation et/ou au téléchargement (lecture) et/ou à l'alimentation (écriture) de son DMP.

Le tableau à l'Annexe 2 détaille les différentes informations à apporter selon les cas et précise les cas dans lesquels le consentement exprès du patient, ou le cas échéant de son représentant légal, devra être recueilli (cas du professionnel hors équipe de soins).

EXI 01 : le professionnel ou l'établissement **DOIT** veiller à ce que le patient soit informé des actions réalisées sur son DMP, conformément à la situation (alimentation de document ou accès en consultation/téléchargement) et de ses droits, de manière écrite, sur un support papier ou digital, sur la base des modèles annexés au présent référentiel (Annexe 4).

Cette information sur le DMP peut être réalisée au travers de mentions, éventuellement mutualisées avec d'autres traitements de données, au sein des documents de santé destinés aux patients (convocations, compte-rendu, etc.). Elle peut être effectuée dans le cadre des démarches en ligne effectuées par le patient en amont de sa prise en charge, en attachant une attention toute particulière au niveau de garantie de l'identification électronique du bon patient, et à la lisibilité des messages. Pour les établissements et structures, cette information peut être effectuée au nom de l'établissement ou du professionnel (personne physique) qui participera à la prise en charge.

Il est possible de considérer que la non-opposition est acquise immédiatement en cas d'une information 'synchrone', apportée dans une démarche en ligne (ex : case d'opposition à cocher dans un parcours de prise de rendez-vous ou de préadmission) ou une information en face à face ou par téléphone. En cas d'information 'asynchrone', par exemple par une mention figurant sur une convocation, on ne peut pas considérer que la non-opposition est acquise automatiquement au bout d'une certaine durée. Elle ne peut l'être que lorsque le titulaire reprend contact avec l'établissement (ex : accusé de réception de la convocation, etc.) ou au démarrage de l'épisode de soin. Cela implique que, dans certains cas, il ne sera pas possible de consulter/télécharger des documents du DMP en amont de la prise en charge.

En cas d'opposition du patient à l'accès par un professionnel, en alimentation et/ou en consultation/téléchargement, au DMP, le professionnel responsable de la prise en charge doit veiller à ce que cette opposition soit effectivement prise en compte. Il est à noter que le professionnel peut différencier les oppositions (une pour l'alimentation, une pour la consultation/ téléchargement) ou ne garder qu'une seule trace globale d'opposition à l'accès (en alimentation et en consultation/téléchargement) au DMP. Pour accompagner les professionnels, des guides pratiques sont mis à dispositions pour les différents cas d'usage (démarche en ligne en amont de l'épisode de santé, face à face, etc.) avec des exemples de mentions.

Dans tous les cas, il n'est pas recommandé de faire mention du motif de l'opposition dans le logiciel du professionnel, qu'il s'agisse d'une opposition pour motif légitime (alimentation) ou d'une opposition sans motif nécessaire (consultation).

EXI 02 : le professionnel ou l'établissement **DOIT** veiller à ce que l'éventuelle opposition du patient soit bien tracée dans son système d'information dans les champs adéquats, permettant ainsi de bloquer les transactions manuelles ou automatiques correspondantes.

2.2. Règles d'accès

Les accès en consultation/téléchargement (lecture) au DMP reposent sur une matrice d'habilitation (n'exonérant pas les professionnels habilités par défaut de se conformer aux règles d'information du paragraphe 2.1), basée sur un croisement des types de professions et rôles professionnels, et des types de documents auxquels ces professionnels peuvent avoir accès. Cette matrice est publiée par arrêté ministériel conformément à l'alinéa 6 de l'article R. 1111-46 du CSP.

En complément de ces autorisations d'accès en lecture par défaut, le titulaire du DMP peut autoriser ou bloquer l'accès aux documents contenus dans son DMP à tout ou partie des professionnels (avant-dernier alinéa de l'article R. 1111-46 du CSP). Il peut également masquer tout ou partie de ses documents aux professionnels qui consultent son DMP (article R. 1111-49 du CSP), y compris pour des situations d'urgence. Le professionnel auteur d'un document conserve la possibilité de le consulter et de le supprimer, même si le document a été masqué.

Le médecin traitant du patient, appelé 'médecin administrateur', déclaré par le patient dans son espace santé, conserve un accès total à l'ensemble des documents du DMP, y compris les documents masqués par le patient (article L. 1111-16 alinéa 2 du CSP).

L'ensemble de ces règles est récapitulé dans le tableau figurant à l'Annexe 3.

Le patient est systématiquement informé de tout accès à son dossier médical partagé, et peut consulter dans un historique toutes les traces d'accès (consultation/téléchargement et alimentation) à son DMP (articles R. 1111-43 et R. 1111-46 dernier alinéa du CSP). Les professionnels et les établissements sont informés que toutes les actions qu'ils effectuent sont horodatées et portées à la connaissance du titulaire du DMP concerné.

EXI 03 : Le professionnel **NE DOIT PAS** accéder au DMP d'une personne s'il n'est pas dans une situation de prise en charge et qu'il ne peut pas le faire dans le respect des règles d'accès.

2.3. Sanctions encourues

L'accès au DMP d'une personne est réservé aux professionnels ou établissements qui interviennent effectivement dans la prise en charge cette personne. Outre cette condition préalable de prise en charge, les modalités d'information de la personne ou de recueil de son consentement doivent être respectées (cf. Annexe 2)

Ainsi, tout professionnel qui consulterait un DMP sans respecter les règles d'information du patient (hors situation d'urgence), sans prendre en compte son opposition ou sans respecter les règles d'accès aux DMP s'expose à :

- 1 an de prison et 15 000 euros d'amende (violation du cercle de confiance – articles L. 1110-4 V. et L. 1111-18 du CSP) ;
- 5 ans de prison et 150 000 euros d'amende (accès frauduleux au DMP, système d'information mis en œuvre par l'Etat – article 323-1 du code pénal), ainsi que plusieurs peines complémentaires possibles (article 323-5 du code pénal).

Si le professionnel divulgue des données issues d'un DMP, il risque en outre 1 an de prison et 15 000 euros d'amende (violation du secret médical - article 226-13 du code pénal).

En complément, des sanctions disciplinaires sont également possibles.

3. EXIGENCES TRANSVERSES RELATIVES A L'ECHANGE ENTRE LES LOGICIELS METIER ET LE DMP

EXI 04 : Pour avoir des accès via interfaces LPS DMP, les professionnels et établissements **DOIVENT** être équipés d'un logiciel métier homologué par le CNDA pour l'alimentation et la consultation/le téléchargement du DMP, conformément au guide d'intégration DMP produit par le GIE SESAM-Vitale.

Il est à noter que le DMP respecte le cadre d'interopérabilité des systèmes d'information en santé (CI-SIS)[2]. Les logiciels qui s'y connectent doivent également respecter ce cadre, et notamment le volet structuration minimale des documents de santé, le volet partage des documents de santé, le volet transport synchrone pour client lourd et les volets de contenu qui concernent le périmètre fonctionnel des logiciels. Les éditeurs de logiciels peuvent utiliser l'espace de tests d'interopérabilité et les jeux de test mis à disposition par l'Agence du Numérique en Santé.

Cette exigence peut être satisfaite en combinant le logiciel métier du professionnel avec une plateforme d'intermédiation destinée à gérer les interfaces entre ce logiciel et le DMP. Il incombe alors à cette plateforme de vérifier que le logiciel métier satisfait bien les exigences qui relèvent de sa compétence.

Si le logiciel métier est hébergé et/ou administré par un sous-traitant du professionnel ou de l'établissement, ce dernier doit veiller à ce que le paramétrage associé n'aille pas à l'encontre des exigences du présent référentiel.

Le respect de cette exigence est essentiel pour les professionnels car il sécurise leur capacité à satisfaire une majorité des autres exigences du présent référentiel.

[2] https://esante.gouv.fr/offres-services/ci-sis/espace-publication

4. EXIGENCES SPECIFIQUES RELATIVES A L'ALIMENTATION DE DOCUMENTS VERS LE DMP

4.1. Documents alimentés au DMP

L'article L. 1111-15 du CSP prévoit l'obligation d'alimentation du DMP par les professionnels de santé quels que soient leur mode et leur lieu d'exercice à l'occasion de chaque acte ou consultation, des éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge. La liste des documents concernés est déterminée par l'arrêté du 26 avril 2022 fixant la liste des documents soumis à l'obligation prévue à l'article L. 1111-15 du CSP.

Il est à noter que, dans le contexte d'établissements sanitaires ou médico-sociaux, l'accord ou la consultation de la commission médicale d'établissement ne sont pas nécessaires préalablement à l'alimentation du DMP pour ces documents.

Cette alimentation peut être effectuée de manière manuelle ou automatisée, en excluant notamment les documents :

- Qui auraient déjà été alimentés au DMP ;
- De patients dont l'identité nationale de santé (INS) n'est pas qualifiée (voir paragraphe 4.2) ;
- Pour lesquels les patients se sont opposés à leur alimentation pour un motif légitime ;
- De patients décédés.

D'autres documents que ceux soumis à l'obligation prévue à l'article L. 1111-15 du CSP peuvent également être alimentés si les professionnels de santé estiment qu'ils peuvent être pertinents pour l'historique de santé du patient, ainsi que la coordination des soins. Des documents datant d'épisodes de santé antérieurs peuvent également être alimentés par les professionnels.

EXI 05 : Le professionnel ou établissement **DOIT** veiller à ce que le DMP soit alimenté systématiquement et automatiquement, sauf exceptions (opposition patient, etc.), avec tous les documents nécessaires à la coordination des soins de la personne prise en charge dans le respect de l'article L. 1111-15 du CSP et de l'arrêté précisant la liste des documents soumis à l'obligation d'alimentation.

Chaque document ayant fait l'objet d'une alimentation réussie au DMP doit être marqué comme tel, de manière visible, dans le logiciel du professionnel ou de l'établissement. Cette donnée peut être utile pour le professionnel dans ses échanges avec le titulaire du DMP, ainsi que pour éviter des alimentations en doublon vers le DMP.

4.2. Statut de l'identité des patients dont les documents sont alimentés au DMP

Afin de réduire le risque d'alimentation de documents dans le DMP d'un autre patient que le titulaire, seuls les documents relatifs à un patient dont l'INS a été qualifiée (se référer au référentiel INS[3] opposable) doivent être alimentés au DMP.

EXI 06 : Le professionnel ou l'établissement **DOIT** veiller à ce que le DMP ne soit alimenté qu'avec des documents relatifs à des patients dont l'Identité Nationale de Santé (INS) a été préalablement qualifiée.

La conduite à tenir en cas d'erreur d'identité sur les alimentations au DMP est explicitée au paragraphe 4.4.

4.3. Respect des règles de masquage d'un document par un professionnel

Le DMP prévoit, pour un professionnel ou un établissement habilité à verser des documents dans le DMP, des possibilités de masquage de ces documents, dans les cas suivants :

- **Un masquage (ou invisibilité) pour le patient lui-même :** lorsque le professionnel estime qu'une donnée de santé versée dans le dossier médical partagé ne doit pas être portée à la connaissance du patient sans accompagnement. Dans ce cas, le document est rendu invisible au patient pour une période de deux semaines à l'issue de laquelle le patient est informé qu'un document a été déposé et est invité à consulter un professionnel de santé pour en prendre connaissance. A l'issue d'un délai d'un mois suivant le dépôt du document et en l'absence de consultation d'annonce, le document est automatiquement rendu accessible au patient (article R. 1111-53 du CSP) ;
- **Un masquage aux titulaires de l'autorité parentale d'une personne mineure dans le cas où cette dernière demande à garder le secret sur son état de santé** (articles L. 1111-13-1 IV al. 4 et R. 1111-33 du CSP), parfois aussi appelé 'connexion secrète'. Les documents visés sont ceux relatifs :
  - Aux actions de prévention, de dépistage, de diagnostic, de traitement ou l'intervention qui s'imposent pour sauvegarder la santé d'une personne mineure ;
  - A l'interruption volontaire de grossesse (IVG) ;
  - Aux dépistages de maladies infectieuses transmissibles au moyen d'un test rapide d'orientation diagnostique (TROD).
- **Un masquage du document aux autres professionnels** : ce masquage ne peut être réalisé par un professionnel qu'à la demande et pour le compte du titulaire du DMP, dans le cas où ce dernier n'est pas en mesure de le faire lui-même dans son espace santé.

EXI 07 : Dans le cas de documents à masquer aux titulaires de l'autorité parentale ou de documents à masquer temporairement au patient le temps d'une consultation d'annonce, le professionnel **DOIT** veiller à ce que cette information soit bien tracée dans son logiciel dans les champs adéquats, permettant d'alimenter le DMP avec le masquage correspondant.

[3] https://esante.gouv.fr/offres-services/referentiel-ins

Une absence de démasquage après la consultation d'annonce serait préjudiciable au patient et reviendrait pour lui à une absence d'alimentation du document au DMP.

Aussi, le professionnel devra veiller à ce que le démasquage effectif du document soit bien réalisé après la consultation d'annonce, ou à défaut au bout d'un mois en l'absence de consultation d'annonce (en particulier tant que le mécanisme de démasquage par défaut au bout d'un mois n'aura pas été implémenté dans le DMP).

EXI 08 : Le professionnel **DOIT** veiller à ce que le démasquage effectif du document soit bien réalisé pour le patient après la consultation d'annonce.

4.4. Respect du RGPD et des obligations professionnelles en cas de détection d'erreurs dans une alimentation

Malgré toutes les précautions prises, il peut arriver qu'un document alimenté par un professionnel contienne une erreur dans son contenu ou qu'il ne concerne pas le bon titulaire (erreur d'identification). Des transactions de retrait d'un document ou de remplacement d'un document existent pour couvrir ces cas de figure.

EXI 09 : En cas d'erreur constatée sur un document alimenté au DMP, le professionnel ou l'établissement **DOIT** veiller à ce que le document alimenté au DMP soit supprimé ou remplacé, et en avertir les personnes concernées. Le professionnel ou l'établissement **DOIT**, en sa qualité de responsable de traitement, déterminer si une inscription au registre des violations, une notification à la CNIL et une information des personnes concernées, sont cumulativement ou alternativement nécessaires conformément aux articles 33 et 34 du RGPD.

4.5. Respect du RGPD en termes d'exercice des droits

Le patient dispose d'un certain nombre de droits qui s'exercent toujours la possibilité de demander la suppression d'un des documents auprès du professionnel qui en a fait l'alimentation, à condition d'invoquer un motif légitime.

EXI 10 : Le professionnel ou l'établissement **DOIT** avoir mis en place un processus permettant au patient d'exercer facilement ses droits de rectification et de suppression des documents alimentés par le professionnel ou l'établissement dans le DMP, notamment en cas de demande de suppression en invoquant un motif légitime. Ce processus précise la personne ou le service auprès duquel le patient peut exercer ses droits et les délais de réponse, conformément à l'article 12 du RGPD.

5. EXIGENCES SPECIFIQUES RELATIVES A LA CONSULTATION / AU TELECHARGEMENT DE DOCUMENTS DEPUIS LE DMP

5.1. Documents à conserver localement

Les documents contenus dans le DMP peuvent être consultés (via le Web PS DMP) ou téléchargés (localement via le Web PS DMP ou dans leur logiciel, via les interfaces LPS du DMP).

Ces transactions impliquent des recherches, généralement basées sur de filtres (types de documents, dates de l'épisode de santé documenté, contenu des documents, etc.).

En application des dispositions combinées du RGPD, de la loi « Informatique et Libertés » et des règles prévues par le code de la santé publique (article L. 1110-4 du CSP), seuls les documents pertinents à la prise en charge effective du patient peuvent être consultés et/ou téléchargés par le professionnel qui accède au DMP.

Le professionnel qui accède au DMP doit uniquement visualiser ou télécharger les documents dont le type et les dates lui paraissent pertinents pour la prise en charge du patient. Il peut être amené, en vue de préparer l'épisode de soins, à configurer son logiciel pour télécharger temporairement en amont de la prise en charge les documents dont le type et la date lui paraissent pertinents et strictement nécessaires à la prise en charge. Dans ce cas, seuls les professionnels responsables de la prise en charge peuvent consulter ces documents.

Les professionnels responsables de la prise en charge ne doivent conserver durablement une copie dans un traitement local (logiciel métier ou poste de travail) que pour les documents pour lesquels cela leur parait nécessaire, par exemple parce qu'il est essentiel qu'une information soit accessible à un autre membre de l'équipe de soins de la structure ou que les informations du document ont participé à orienter un diagnostic ou une action thérapeutique. Les documents téléchargés temporairement qui n'ont pas fait l'objet de cette sélection par le professionnel pour être sauvegardés dans le traitement local doivent être supprimés au plus tard une fois l'épisode de prise en charge terminé.

Cela permet ainsi de minimiser les données traitées localement, de ne pas dupliquer démesurément les documents, de limiter le risque de divulgation des données de santé du patient et de limiter le stockage et la consommation énergétique associée. Le choix des documents à conserver localement relève de la seule responsabilité des professionnels qui sont seuls compétents pour apprécier les critères de nécessité au regard de la prise en charge.

EXI 11 : Les professionnels **DOIVENT** veiller à ne conserver dans des traitements locaux que les documents qu'ils jugent strictement pertinents pour la prise en charge.

Les documents conservés sont des copies des documents du DMP, mais ne relèvent plus des règles propres au traitement DMP : ils sont conservés dans les logiciels des professionnels selon le même régime que les autres documents de santé qui y auraient été nativement produits. Dans le cas où le document provient du DMP, il est néanmoins obligatoire d'indiquer cette origine de manière visible dans le logiciel du professionnel, outre les caractéristiques propres du document (auteur, etc.) qui peuvent conduire à cette observation.

Par ailleurs, au travers du Web PS DMP, les professionnels peuvent consulter des documents et les télécharger localement sur leur poste de travail, afin de les stocker temporairement ou de les réimporter dans leurs logiciels, notamment pour le cas où ces derniers n'ont pas d'interfaces intégrées avec le DMP.

EXI 12 : Les professionnels ou les établissements **DOIVENT** conserver les documents issus du DMP dans un logiciel ou traitement de données qui offre des garanties de sécurité à l'état de l'art, notamment en termes de contrôle d'accès aux données, de modalités de conservation, d'intégrité et de confidentialité des données.

5.2. Exigence générale sur la sécurité sur les traitements locaux

Outre la 'DMP-Compatibilité' sanctionnée par l'homologation CNDA, il est essentiel que les traitements locaux aient un niveau de sécurité suffisant. L'éditeur du logiciel utilisé est également tenu, en tant que sous-traitant, de mettre en œuvre des mesures pour sécuriser le traitement des données personnelles de santé. Néanmoins plusieurs exigences sont portées sur les professionnels, responsables de ces traitements locaux.

EXI 13 : En tant que responsables du traitement des données en provenance du DMP (documents téléchargés dans le logiciel ou le poste du travail), les professionnels ou les établissements **DOIVENT** respecter l'article 32 du RGPD sur les mesures de sécurité mises en œuvre dans le cadre du traitement local dont ils sont responsables.

Le respect de cette exigence passe notamment par des échanges réguliers entre les professionnels ou établissement avec leurs éditeurs de logiciels à propos de la sécurisation du traitement de données dont les professionnels ou établissements sont responsables.

Pour les professionnels libéraux, il convient de se référer au référentiel de la CNIL relatif aux traitements de données personnelles pour les cabinets médicaux et paramédicaux[4].

5.3. Exigence sur la conduite d'une analyse d'impact sur la vie privée sur les traitements locaux

EXI 14 : En tant que responsables du traitement local de données dans lesquels seront éventuellement conservés des documents issus du DMP, les professionnels ou les établissements **DOIVENT** veiller à respecter l'article 35 du RGPD en conduisant et en mettant à jour régulièrement une analyse d'impact sur la vie privée des personnes dont les données sont traitées.

Cette analyse est propre à chaque traitement, même si le logiciel peut fournir des éléments standardisés permettant de contribuer à cette analyse. Plusieurs prestataires du marché proposent aux professionnels de les accompagner dans la réalisation de cette démarche.

[4] https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_cabinet.pdf

5.4. Exigence sur la conduite d'audit sur les traitements locaux ou les logiciels utilisés

EXI 15 : En tant que responsables du traitement local de données dans lesquels seront éventuellement conservés des documents issus du DMP, les professionnels ou les établissements **DOIVENT** veiller à ce que des audits réguliers soient effectués et tracés sur le traitement ou a minima sur la solution logicielle utilisée.

5.5. Exigences en termes de traçabilité dans les traitements locaux

Afin d'être en mesure d'identifier tout accès frauduleux ou utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il est impératif que l'organisme ou le professionnel qui alimente ou qui consulte le DMP mette en place un mécanisme de traçabilité des transactions effectuées en lien avec le DMP, des opérations de visualisation, et des actions de sauvegarde des documents issus du DMP.

Ce dispositif doit permettre d'enregistrer et de conserver l'identifiant local et, lorsque c'est possible, national, de l'accédant, la date et l'heure de l'accès, les données et documents concernés par l'accès et le détail des actions effectuées par l'utilisateur. Ces données ne doivent en principe pas être conservées plus de 6 mois selon les préconisations actuelles de la CNIL. Ces journaux doivent être disponibles sous 48h en cas de contrôle ou d'investigation par les autorités compétentes.

EXI 16 : Les professionnels ou les établissements **DOIVENT** veiller, en lien avec leur éditeur, à ce qu'il existe des processus documentés d'extraction des traces d'accès et aient été testés au moins une fois depuis trois ans avec succès. La conservation et l'accès à ces traces doivent être conformes à minima à l'état de l'art de la sécurité des systèmes d'information.

Il est à noter que cette traçabilité locale vient en complément de la traçabilité nationale dans le DMP, qui répertorie, quel que soit le type de certificat utilisé, les identifiants nationaux des personnes morales et physiques à l'origine ou en responsabilité des transactions.

5.6. Recommandation en termes de supervision

Afin d'être en mesure d'identifier des mésusages sur l'accès au DMP ou à des documents qui en sont issus, notamment dans le contexte de structures avec plusieurs professionnels salariés ayant accès au traitement local, il est recommandé :

- De mettre en place des mécanismes automatisés d'alerte sur la base de certains critères (nombre de dossiers consultés, récupération systématique de tous les documents, consultation de dossier de collègues, heures inhabituelles de consultation, etc.) ;
- D'avoir des processus d'investigation ;
- D'avoir des processus, éventuellement automatisés à caractère préventif, de blocage, en cas de mésusage constaté.

RECO 01 : Les professionnels ou les établissements **PEUVENT** implémenter, en lien avec leur éditeur, des processus de supervision des usages, et effectuer un point régulier avec leurs éditeurs sur les critères d'alertes et sur les incidents passés.

5.7. Exigences en termes d'identification électronique aux traitements locaux

La présence de mécanismes d'identification électronique robustes (entropie des mots de passe, facteurs de restriction d'accès, variété des facteurs d'authentification, etc.) aux logiciels impliqués dans la consultation et/ou le téléchargement de documents du DMP, est essentielle pour diminuer le risque d'usurpations et d'accès frauduleux aux données.

Les traitements locaux doivent être conformes au référentiel d'identification électronique de la PGSSI-S.

EXI 17 : Les professionnels ou les établissements **DOIVENT** veiller, en lien avec leurs éditeurs, à ce que les traitements locaux dans lesquels seront conservés des documents issus du DMP disposent de modalités d'identification électronique des utilisateurs conformes au référentiel sur l'identification électronique applicable[5].

La consultation/téléchargement de documents du DMP ne peut se faire qu'après une authentification directe, ou dans le cadre d'une authentification indirecte, dite 'AIR simplifié', avec des conditions particulières détaillées au paragraphe 6 du présent référentiel.

5.8. Exigences en termes de gestion des habilitations de traitements locaux

Dans le contexte de structures avec de nombreux professionnels salariés ayant accès au traitement local, il est essentiel que ce dernier ait des contrôles/autorisations d'accès (habilitations) paramétrés par le responsable de la structure ou son délégataire.

EXI 18 : Les professionnels ou les établissements **DOIVENT** veiller à ce que les traitements locaux dans lesquels seront conservés des documents issus du DMP disposent d'une gestion stricte, documentée et revue régulièrement des habilitations et autorisations d'accès, afin de garantir que seules les personnes impliquées dans la prise en charge médicale puissent accéder aux transactions d'échange avec le DMP et aux données de santé parmi lesquelles pourraient figurer des documents issus du DMP.

5.9. Exigences en termes de sensibilisation des utilisateurs des traitements locaux

Dans le contexte de structures avec de nombreux professionnels salariés ayant accès au traitement local, il est essentiel qu'une politique de sensibilisation soit mise en place vis-à-vis de la sécurité et du DMP.

EXI 19 : Les professionnels ou les établissements **DOIVENT** veiller à ce que les utilisateurs des traitements locaux dans lesquels seront conservés des documents issus du DMP soient sensibilisés (documents d'information, pop-ups dans les logiciels, mentions dans le contrat de travail, etc.) sur :

[5] https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

- Le présent référentiel ;
- La sensibilité des données du DMP ;
- L'hygiène numérique nécessaire lors du traitement de données de santé ;
- L'importance de ne pas consulter les données d'autres patients que ceux qu'ils prennent en charge, et en particulier de collègues ou de connaissances proches ;
- L'importance de ne pas prêter à d'autres personnes leurs moyens d'identification électroniques aux logiciels ;
- Le fait que l'ensemble de leurs accès sont tracés localement et au niveau national ;
- Les sanctions encourues en cas d'utilisations frauduleuses (cf. point 2.3 du présent référentiel).

5.10. Exigences en termes de respect de la durée de conservation dans les traitements locaux

EXI 20 : Les professionnels ou les établissements **DOIVENT** veiller à ce que les traitements locaux dans lesquels seront conservés des documents issus du DMP respectent les durées de conservation[6] applicables à ces traitements locaux.

[6] Voir le référentiels CNIL sur la conservation des données de santé (hors recherche) https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_traitements_dans_le_domaine_de_la_sante_hors_recherches.pdf

6. EXIGENCES SPECIFIQUES RELATIVES A LA CONSULTATION/AU TELECHARGEMENT DE DOCUMENTS VIA AUTHENTIFICATION INDIRECTE (AIR SIMPLIFIE)

Cette section détaille les exigences complémentaires qui s'appliquent si le professionnel ou l'établissement souhaite consulter et/ou télécharger des documents du DMP via une authentification indirecte (hors carte CPS et Pro Santé Connect), incluant les échanges automatisés avec le DMP, dans le cadre du mécanisme dénommé 'AIR simplifié'.

6.1. Authentification (primaire) à deux facteurs du professionnel au logiciel

Outre les exigences générales évoquées au paragraphe 5.7, une exigence complémentaire s'applique pour l'authentification (primaire) du professionnel au logiciel, afin de renforcer significativement la traçabilité et éviter les dérives fréquemment constatées de partage de mots de passe.

EXI 21 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), les professionnels **DOIVENT** veiller à avoir été préalablement identifiés électroniquement avec une authentification à deux facteurs.

6.2. Authentification (secondaire) de la structure ou du logiciel au DMP

EXI 22 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel ou établissement **DOIT** veiller, en lien avec son éditeur, que l'instance logicielle s'authentifie au DMP avec des certificats (authentification et/ou signature) de l'autorité de certification IGC-Santé contenant un identifiant FINESS de l'établissement.

Ce certificat **DOIT** contenir un identifiant autorisé pour l'accès au DMP (voir paragraphe 6.5 sur les structures autorisées).

EXI 23 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel ou établissement **DOIT** veiller à la sécurisation de ce type de moyens d'identification électronique conformément aux normes en vigueur (stricte confidentialité de l'accès à la clef privée, non duplication du certificat, révocation en cas de compromission, etc.).

6.3. Habilitation et Traçabilité des accès en cas d'authentification indirecte

Outre l'identifiant national porté par le certificat, deux identifiants sont transmis au DMP pour toute transaction :

- L'identifiant géographique de la structure (FINESS établissement) à l'origine de la transaction ;
- L'identifiant de la personne physique (RPPS) à l'origine de la transaction, ou, à défaut, de la personne physique désignée responsable de la prise en charge du patient ayant occasionné la transaction de consultation/téléchargement du DMP, notamment pour les transactions d'appel automatisées. L'identifiant RPPS transmis ne doit pas être générique (ex : médecin DIM de l'établissement, infirmier de coordination des entrées, etc.).

Cela permet :

- La gestion de la traçabilité, en permettant d'informer finement le titulaire du DMP des éventuels accès à son dossier ;
- L'application des règles d'accès au DMP (à la personne morale d'une part, et au professionnel d'autre part) ;
- La supervision nationale des mésusages.

Ces exigences sont directement déclinées dans le guide d'intégration DMP.

EXI 24 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel ou établissement **DOIT** veiller, à ce que les identifiants FINESS établissement de la structure et RPPS de la personne physique à l'origine de la transaction, ou, à défaut, de la personne physique désignée responsable de la prise en charge du patient ayant occasionné la transaction de consultation ou d'alimentation du DMP, soient transmis au DMP. L'identifiant RPPS transmis **NE DOIT PAS** être générique.

EXI 25 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel **DOIT** veiller à ce que la personne désignée via l'identifiant RPPS soit informée que son identifiant est transmis et sera utilisé pour la traçabilité nationale et le contrôle d'accès au DMP.

6.4. Contractualisation entre la structure et son éditeur sous-traitant

EXI 26 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), la personne morale ou physique responsable de traitement **DOIT** veiller à ce que le contrat avec son éditeur de logiciel inclut un paragraphe dédié au DMP, stipulant (i) *que le responsable de traitement s'engage à partager avec l'éditeur la liste des professionnels autorisés à s'identifier électroniquement auprès du DMP en son nom* et à transmettre les identifiants de personne morale et de personne physique correspondants, (ii) que le logiciel respecte bien le présent référentiel, en particulier en ce qui concerne l'identification électronique primaire, la traçabilité et le contrôle d'accès au logiciel et (iii) les modalités de restitution aux professionnels du récapitulatif régulier des accès au DMP.

6.5. Auto-homologation au référentiel DMP, constitution d'un procès-verbal et déclaration à l'Assurance Maladie pour mise en liste blanche du dispositif 'AIR Simplifié'

EXI 27 : Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel ou établissement **DOIT** avoir préalablement réalisé une auto-homologation vis-à-vis du présent référentiel, signé le procès-verbal (PV) de cette auto-homologation et déclarer à l'Assurance Maladie, gestionnaire du DMP, la réalisation de cette auto-homologation. Cette déclaration conditionne l'ajout des identifiants de l'établissement à une liste blanche d'accès par le dispositif 'AIR Simplifié'.

L'auto-homologation au référentiel DMP est une procédure interne, menée par un professionnel ou établissement, acteur de la prise en charge. L'éditeur de logiciels sous-traitant peut accompagner son client dans la réalisation de cette auto-homologation et participer à la commission d'auto-homologation. C'est néanmoins l'acteur de la prise en charge, responsable des accès au DMP, qui prononce et signe le PV de l'auto-homologation référentiel DMP.

D'un point de vue général, les acteurs pourront utilement s'inspirer des bonnes pratiques de l'ANSSI relatives à la démarche d'homologation d'un système d'information[7].

Pour l'auto-homologation référentiel DMP, cela consiste notamment à :

- Préparer un support documentaire, à minima sous format d'une présentation synthétique et intelligible ;
- Tenir une commission d'auto-homologation référentiel DMP, avec le responsable de l'établissement ou son représentant, avec les acteurs pertinents (délégué à la protection de données, direction des systèmes d'information, éditeur de la solution, représentants des patients, responsables de la cellule d'identitovigilance, etc.) ;
- Faire signer par le responsable de l'établissement le PV de la commission, avec la mention "le service est homologué pour [nombre] mois, [avec les (éventuelles) réserves suivantes : [réserves]]". La durée sera à l'appréciation du responsable de l'établissement qui pourra utilement prononcer une homologation courte si certaines réserves nécessitent de refaire un point à une brève échéance. Un rappel calendaire sera utilement programmé peu avant l'expiration pour organiser une nouvelle homologation ;
- Ajouter le PV de la commission dans le registre RGPD, au niveau du dossier concernant le traitement de données local amené à avoir des échanges de données avec DMP. Ce document est conservé et tenu à disposition des responsables du traitement, d'une part, ainsi que de tout organisme officiel qui aurait à en connaître (CNIL, ANSSI, etc.).

Le support documentaire de la commission devra notamment faire état des points suivants :

- Un récapitulatif des différents systèmes d'information qui auront accès au DMP en alimentation et en consultation / téléchargement ;

[7] Cf. https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/

- Pour chaque exigence du présent référentiel, une revue de son respect effectif, en détaillant les modalités associées, et en particulier en ce qui concerne :
    - Les modalités d'identification électronique à deux facteurs pour les transactions de consultation/téléchargement éventuelles ;
    - Des modalités de contrôle d'accès (habilitations) à ces outils, et de revue régulière de ces accès ;
    - Des méthodes mises en œuvre pour assurer la traçabilité des accès ;
    - Les modalités de sensibilisation des professionnels.
- Les risques principaux identifiés vis-à-vis du DMP, leur probabilité et leur criticité, ainsi que les mesures mises en œuvre, à date ou dans le futur, pour les réduire au maximum ;
- La procédure à suivre en cas de suspicion de violation de données.

Un modèle de PV est proposé en Annexe 1.

En termes de déclaration auprès de l'Assurance Maladie, il sera proposé aux établissements un formulaire en ligne, leur permettant notamment d'indiquer la date de la réalisation de l'auto-homologation. Le support documentaire de l'auto-homologation et le PV ne seront pas nécessaires pour cette déclaration.

Concernant le dispositif 'AIR Simplifié, l'Assurance Maladie :

- Se réserve le droit de retirer à tout moment un établissement et/ou un logiciel la possibilité d'être autorisé en liste blanche de 'AIR Simplifié', suite à une suspicion de mésusage – ce qui ne correspond néanmoins pas à une démarche d'audits aléatoires par l'Assurance Maladie ;
- Se réserve le droit de demander une nouvelle déclaration de bonne réalisation de l'auto-homologation à échéance régulière ou après une mise à jour substantielle du présent référentiel.

Annexe 1 : Exemple de procès-verbal d'auto-homologation au référentiel DMP

[Logo] [Libellé structure] [Identifiant juridique de la structure]

Suite à la commission tenue le [date], je soussigné [XX], responsable de la structure [XX], prononce l'homologation au « Référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) » version XX.XX pour [nombre] mois, [avec les réserves suivantes : [réserves]].

Liste des identifiants juridiques portés dans les certificats IGC-Santé utilisés pour l'accès en 'AIR Simplifié' :

Liste des établissements impliqués (FINESS établissement) :

En cas de besoin, le contact opérationnel pour l'Assurance Maladie sera [nom et coordonnées].

Date :

Signature :

Annexe 2 : Tableau récapitulatif des informations à apporter aux patients

Les modalités d'information et/ou de recueil du consentement propres à chaque catégorie de professionnel sont résumées dans le tableau ci -après :

Légende : ✗ Faux ✓ Vrai

	Droits d'accès		Droits du patient (information/consentement)		
Catégorie de professionnel	**Consultation (art. R. 1111-46 CSP)**	**Alimentation, en principe automatique et obligatoire (art. L. 1111-15 CSP)**	**Information préalable du titulaire (art. R. 1111-40 CSP)**	**Consentement à recueillir auprès du titulaire**	**Opposition possible par le titulaire**
Tous professionnels appartenant à une même équipe de soins (cf. liste des professionnels à l'art. L. 1110-12 CSP)	✓	✓	Obligatoire	Non nécessaire : consentement présumé (art. R. 1111-46 CSP)	Opposition possible à la **consultation** du DMP par un professionnel, en consultation. Opposition possible à **l'alimentation** du DMP, à condition d'invoquer un motif légitime (art. R. 1111-47 CSP) Opposition possible à **l'alimentation et la consultation** si le titulaire bloque le professionnel (art. L. 1111-19 et art. R 1111-46 CSP)

Les personnes exerçant sous la responsabilité d'un professionnel membre de l'équipe de soins	✗	✓	Obligatoire	Non nécessaire : consentement présumé (art. R. 1111-46 CSP)	Pas d'opposition à l'alimentation si le professionnel a été autorisé par le patient (art. R. 1111-46 al. 6 CSP)
Professionnel n'appartenant pas à l'équipe de soins	✓	✓	Obligatoire	Obligatoire (art. L. 1111-17 III, art. R. 1111-46 et art. D. 1110-3-1 CSP)	Le consentement recueilli est valable tant qu'il n'a pas été retiré (art. R. 1111-46 al. 3 CSP)

Annexe 3 : Tableaux récapitulatifs des autorisations de consultation de document du DMP

Les autorisations d'accès aux documents du DMP sont résumées dans le tableau ci-après :

	Tout professionnel (cf. matrice d'habilitation - art. R. 1111-46 CSP)	Professionnel auteur d'un document (art. R. 1111-49 CSP)	Médecin traitant (art. L. 1111-16 CSP) / médecin administrateur (art. R. 1111-54 CSP)	Professionnel de santé en situation d'urgence (art. L. 1111-17 I et art. R. 1111-48 CSP) **sauf opposition préalable du titulaire**	Professionnel bloqué par le titulaire (art. R. 1111-46 CSP)
Accès au document créé par un professionnel	✓	✓	✓	✓	✗ (sauf si auteur du doc)
Accès au document masqué (créé par un professionnel)	✗	✓	✓	✓	✗
Accès au document créé par le titulaire	✓	-	✓	✓	✗
Accès au document masqué (créé par le titulaire)	✗	-	✓	✓	✗
Accès au document alimenté par une application référencée	✓	-	✓	✓	✗

Accès au document pour lequel le titulaire mineur a demandé le secret	✅	✅	✅	✅	❌

Légende : ❌ Impossible ✅ Possible

Annexe 4 : Modèles de mention d'information et de recueil de consentement

Cas 1 (le plus fréquent) - Modèle de mention d'information préalable à l'accès (alimentation et/ou consultation/téléchargement) à Mon espace santé pour les professionnels membres de l'équipe de soins (art. R. 1111-46 du CSP)

Afin de participer efficacement à votre prise en charge, le professionnel de santé ou l'équipe de soins qui vous prend en charge a besoin d'accéder aux données de santé stockées dans votre compte Mon espace santé et d'y déposer les documents utiles à la prévention, la continuité et la coordination de vos soins, qui pourront être consultés par les autres professionnels autorisés qui vous prennent en charge dans le cadre de cet épisode de soins.

Vous pouvez vous opposer à la consultation de votre compte Mon espace santé et/ou, en invoquant un motif légitime, à son alimentation [*expliciter la méthode, qui peut être différente selon les canaux (information orale, plateforme en ligne, information sur des documents, etc.)*]), mais cela pourrait avoir des conséquences sur la qualité de votre prise en charge.

Vous avez la possibilité de gérer la confidentialité de vos données (par exemple masquer un ou tous vos documents, bloquer des professionnels de santé, ou clôturer complètement votre espace santé) sur le site internet https://www.monespacesante.fr/. Pour plus d'informations sur vos droits, vous pouvez consulter la foire aux questions (FAQ) de Mon espace santé disponible sur https://www.monespacesante.fr/questions-frequentes ou contacter le support Mon espace santé par téléphone au 34 22.

***

Cas 2 - Modèle de recueil du consentement préalable du patient à l'accès à son Mon espace santé pour les professionnels hors équipe de soins (art. D. 1110-3-1 du code de la santé publique)

Pour vous prendre en charge efficacement, j'ai besoin d'accéder aux données de santé stockées dans votre compte Mon espace santé, pour le consulter et y verser des documents utiles à la prévention, la continuité et la coordination de vos soins qui pourront être consultés par les autres professionnels qui vous prennent en charge.

En pratique, j'aurai besoin de partager avec eux les catégories d'informations suivantes : informations médicales, informations médico-sociales, informations administratives (*Rayer la mention inutile*), autres informations : …. (*Préciser*).

Ce partage de données se fera via votre compte Mon espace santé, dans les conditions optimales de sécurité qu'il offre, et au bénéfice des seuls professionnels habilités à y accéder (art. L. 1110-4 III du code de la santé publique).

En cochant la case ci-contre, vous déclarez consentir à ce que j'accède à votre compte Mon espace santé : ☐

***

Cas 3 - Modèle de recueil du consentement préalable du patient à l'accès à son Mon espace santé pour le professionnel membre de l'équipe de soins qui recueille le consentement du patient au bénéfice d'un professionnel hors équipe de soin (art. L. 1111-17 II du code de la santé publique)

Pour vous prendre en charge efficacement, un autre professionnel habilité va devoir accéder à votre dossier médical contenu dans votre profil Mon espace santé, pour le consulter et y verser des documents utiles à la prévention, la continuité et la coordination de vos soins qui pourront être consultés par les autres professionnels qui vous prennent en charge.

En pratique, ce professionnel aura besoin de partager les catégories d'informations suivantes : informations médicales, informations médico-sociales, informations administratives (*Rayer la mention inutile*), autres informations : …. (*Préciser*).

Ce partage de données se fera via votre compte Mon espace santé, dans les conditions optimales de sécurité qu'il offre, et au bénéfice des seuls professionnels habilités à y accéder (art. L. 1110-4 III du code de la santé publique).

En cochant la case ci-contre, vous déclarez consentir à un tel accès de ce professionnel à votre compte Mon espace santé : ☐