Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION

Arrêté du 26 octobre 2023 portant approbation du référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP)

NOR : *SPRD2325049A*

Le ministre de la santé et de la prévention,

Vu le 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu le règlement (UE) 910/2014 du Parlement européen et du conseil du 23 mars 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (règlement eIDAS) ;

Vu le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique ;

Vu la directive 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la santé publique, notamment ses articles L. 1470-5 et R. 1111-46 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu l'avenant modifiant la convention constitutive du groupement d'intérêt public « Agence du numérique en santé » prévu par l'article L. 1111-24 du code de la santé publique, approuvé par l'arrêté du 8 avril 2021 ;

Vu la notification n° 2023/358/F adressée à la Commission européenne le 9 juin 2023,

Arrête :

Art. 1er. – En application de l'article L. 1470-5 du code de la santé publique, le référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) annexé au présent arrêté est approuvé.

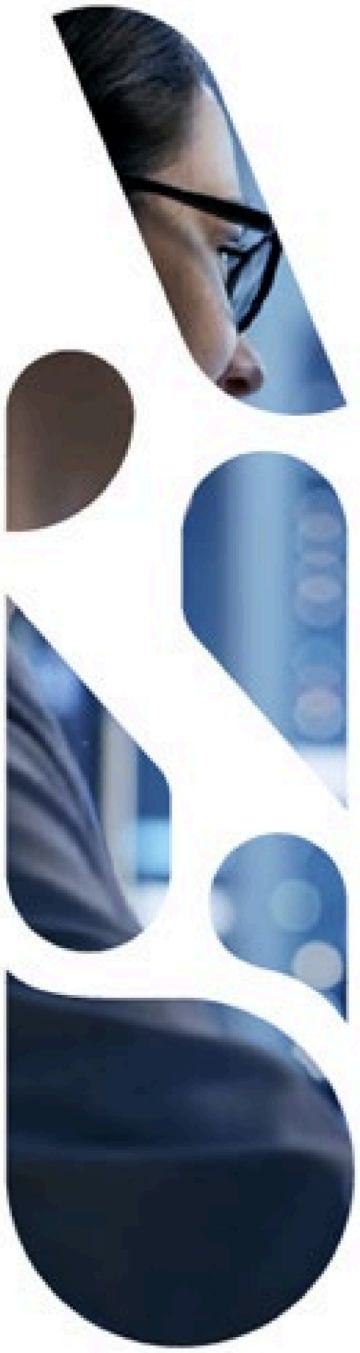
Art. 2. – Le référentiel et ses annexes peuvent être consultés sur le site internet du groupement mentionné à l'article L. 1111-24 du code de la santé publique.

Art. 3. – La déléguée au numérique en santé est chargée de l'exécution du présent arrêté qui sera publié au *Journal officiel* de la République française.

Fait le 26 octobre 2023.

Pour le ministre et par délégation :
La déléguée au numérique en santé,
H. Ghariani

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 : v1.0*

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 informées, 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 de 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 L. 1110-12 - CSP - Légifrance (legifrance.gouv.fr) Article R. 1110-2 - 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 mentionné par l'alinéa 6 de l'article R. 1111-46 du CSP, 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 ;

– 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.

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 professionnels ayant vocation à s'interfacer avec le DMP.

Cette première version du référentiel a été établie suite à de multiples échanges avec des professionnels de santé, représentants d'établissements de santé et éditeurs de logiciels, ainsi qu'à l'issue d'une concertation publique, quant aux attentes des professionnels et des usagers vis-à-vis de l'utilisation du DMP, puis d'échanges avec la CNIL.

Le référentiel sera mis à jour au plus tard 3 ans après la publication de cette version, compte tenu notamment :

- du renforcement de la sécurisation des moyens d'identification électronique des professionnels, conformément au référentiel d'identification électronique de la PGSSI-S (généralisation de l'authentification renforcée à 2 facteurs sur les services numériques en santé sensibles, au plus tard le 1er janvier 2026) ;
- des retours d'expérience des professionnels, sur :
  - l'utilisation effective du mode d'authentification indirecte pour la consultation et/ou le téléchargement de document du DMP dans les structures de prise en charge (mode « AIR Simplifié »présenté dans ce document, paragraphe 6) ;
  - l'utilisation des logiciels référencés dans le cadre du programme Ségur numérique, incluant des exigences s'appliquant aux logiciels pour l'alimentation et la consultation du DMP, ainsi que des exigences relatives à la sécurité des systèmes d'information en santé (dont les exigences présentées dans ce référentiel) ;
  - les nouveaux usages ouverts par le DMP dans l'exercice de leur profession, notamment sur :
    - les modalités d'accès aux documents pertinents du DMP depuis leur logiciel ;
    - le déploiement de nouveaux services numériques en santé permettant l'échange de données avec le dmp : services référencés pour les usagers au catalogue de services de mon espace santé, et/ou référencés pour les professionnels dans le bouquet de services aux professionnels (bsp) ;
    - les situations de prise en charge dans lesquelles les exigences du référentiel pourraient être réétudiées ou aménagées, afin de répondre à de nouvelles attentes des professionnels quant aux bénéfices potentiels du numérique en santé, tout en garantissant la sécurité des accès aux données du DMP ;
- de la possibilité de rendre obligatoire la détention d'un certificat de conformité pour les services numériques concernés, dès que les conditions de délivrance d'un tel certificat auront été définies par décret en Conseil d'Etat pris après avis de la CNIL, en application de l'article L. 1470-6 I du code de la santé publique.

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.

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

Plusieurs modalités d'accès au DMP existent pour les professionnels :

– l'accès web direct (depuis un navigateur) ;
– l'accès depuis leur logiciel métier, en mode « web contextuel » ;
– l'accès totalement intégré dans leur logiciel métier.

1.6.1. Accès web depuis un navigateur

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.

Les professionnels peuvent s'y identifier comme personnes physiques par les moyens d'identification électronique prévus à l'article L. 1470-3 du CSP: les moyens d'identification électronique disponibles sous *Pro Santé Connect* 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.

1.6.2. Accès depuis le logiciel métier

Deux modes d'accès peuvent être utilisés à travers les logiciels des professionnels :

Le « Web PS DMP » peut être appelé en mode **contextuel** depuis les logiciels métiers des professionnels avec un contexte patient, permettant de visualiser directement le DMP du patient déjà sélectionné dans le logiciel, en ouvrant une fenêtre du navigateur (externe ou encapsulée dans le logiciel).

L'accès peut aussi être totalement intégré aux logiciels des professionnels de santé, avec les « interfaces LPS DMP » qui permettent 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, alertes sur la présence de nouveaux documents, visualisation des documents avant de sélectionner éventuellement les documents à conserver, etc.).

Dans ces modes d'accès depuis les logiciels métiers, 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 : les moyens d'identification électronique disponibles sous *Pro Santé Connect* et la carte CPS. 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 », 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 (authentification à double facteur pour le mode AIR Simplifié présenté au chapitre 6). L'identification électronique au DMP est alors effectuée par le logiciel avec des certificats appartenant à la structure à laquelle le professionnel est rattaché (et dans le contexte de laquelle il effectue une prise en charge justifiant d'échanges avec le DMP).

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 à l'information du patient, l'exercice de ses droits, les règles d'accès 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 numérique, 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, le motif de l'opposition ne doit pas être enregistré 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. Le motif de l'éventuelle opposition **NE DOIT PAS** être enregistré dans le système d'information.

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 de se conformer aux règles d'information du paragraphe 2.1), qui indique les types de documents auxquels les professionnels peuvent avoir accès en fonction de leur profession. 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 à l'échange entre les logiciels métier 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.

4. **Exigences spécifiques relatives à 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 dans les conditions prévues à l'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 ;
  - à 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 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.

Suite aux retours des usagers et des professionnels, des adaptations réglementaires sont prévues pour encadrer tout mécanisme de démasquage automatisé éventuel, sans l'intervention d'un professionnel, d'un document rendu temporairement invisible au patient dans le DMP.

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

EXI 08 : le professionnel **DOIT** veiller à ce que le démasquage effectif d'un document temporairement invisible pour le patient soit bien réalisé dans son DMP, dès que les conditions sont réunies.

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 qu'il doit toujours pouvoir exercer. Il doit pouvoir demander auprès du professionnel qui en a fait l'alimentation, la rectification (si le document est erroné ou comporte une erreur) ou la suppression (à condition d'invoquer un motif légitime) d'un des documents du DMP.

Note : la rectification d'un document consiste pour le professionnel à supprimer la version erronée du document dans le DMP (pour qu'elle ne figure plus dans l'historique des documents du patient) et à publier une nouvelle version corrigée du document.

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 spécifiques relatives à la consultation et au téléchargement de documents depuis le DMP**

5.1. *Consultation, préchargement temporaire et enregistrement durable de données provenant du DMP*

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

Ces transactions impliquent des recherches, généralement basées sur les caractéristiques des documents (type de document, titre, version, date du document ou de l'épisode de soins, auteurs).

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 les caractéristiques lui paraissent pertinentes pour la prise en charge du patient.

Selon les pratiques propres à chaque profession et au contexte d'exercice des professionnels, les logiciels des professionnels pourront donc proposer des fonctionnalités différentes pour la recherche, la consultation, le préchargement et l'enregistrement durable des caractéristiques ou du contenu de documents du DMP.

5.1.1. Caractéristiques d'un document du DMP

Elles sont véhiculées par les métadonnées associées au document lors de son alimentation dans le DMP : type, titre, date(s), auteur(s), version(s).

Elles peuvent être utilisées comme critères de recherche ou pour l'affichage d'une liste de documents du DMP. Ces caractéristiques des documents peuvent être affichées à l'écran de l'utilisateur, par exemple sous forme d'une liste de documents, en mode Web ou de manière intégrée dans son logiciel. Elles peuvent donc être enregistrées dans le logiciel (sans toutefois y enregistrer le contenu des documents associés).

Lorsqu'une recherche est effectuée par un professionnel sur les métadonnées des documents présents dans le DMP, elle est tracée dans l'historique des accès au DMP, que le patient peut retrouver dans Mon espace santé (onglet « Autres activités » de la rubrique « Historique d'activité ») : *« Date et heure - [Professionnel XXX] - a recherché des documents »*.

Dans certains cas, le professionnel responsable de la prise en charge peut être amené, en vue de préparer un épisode de soins, à configurer son logiciel pour précharger temporairement les caractéristiques des documents qui lui paraissent pertinents et nécessaires pour la prise en charge, avec un filtrage sur des critères pré-paramétrés (patient, type, date, auteur …). Il peut ainsi être informé de l'existence d'un nouveau document par une alerte dans son logiciel ou accéder rapidement à une liste de nouveaux documents.

EXI 11 : dans le cas où les caractéristiques (métadonnées) des documents sont préchargées dans un traitement local, le professionnel pour le compte duquel ces métadonnées ont été préchargées **DOIT** être le seul à pouvoir y accéder dans le traitement local (avec un mode d'authentification à 2 facteurs). Cette liste de caractéristiques **DOIT** être préchargée au plus tôt 3 jours avant la prise en charge, et **DOIT** être supprimée au plus tard 3 jours après le préchargement.

5.1.2. Contenu d'un document du DMP

Lorsque le contenu d'un document du DMP est affiché à l'écran ou téléchargé par un professionnel, en mode Web ou de manière intégrée dans son logiciel, cette action est tracée dans l'historique des accès au DMP, que l'usager peut retrouver dans Mon espace santé (onglet « Autres activités » de la rubrique « Historique d'activité ») : *« Date et heure - [Professionnel XXX] - a consulté le document XXXXX »*.

Dans certains cas, le professionnel responsable de la prise en charge peut être amené, en vue de préparer un épisode de soins, à configurer son logiciel pour précharger temporairement le contenu des documents du DMP qui lui paraissent pertinents et nécessaires pour la prise en charge, avec un filtrage sur des critères pré-paramétrés (patient, type, date, auteur …). Il peut ainsi, sans clics additionnels et de manière récurrente pour le même type de document, être alerté et visualiser instantanément le contenu des documents essentiels, voire prérequis pour la prise en charge (exemple : dernier compte rendu de biologie médicale datant de moins d'un mois, certificat de test

Covid-19 avant hospitalisation, etc.), sans qu'il soit forcément nécessaire de les conserver durablement dans le traitement local.

Afin de s'assurer d'un filtrage effectif des documents essentiels, le nombre de documents préchargés doit, quoi qu'il arrive, être limité à 10 documents par patient et le préchargement temporaire doit être limité dans le temps. Les logiciels qui intègreront ces fonctionnalités de préchargement temporaire devront permettre aux professionnels de configurer le filtrage effectif des documents et le respect de ces limitations.

Ces documents dont le contenu est préchargé ne sont accessibles dans le traitement local qu'au professionnel à l'origine du préchargement (authentifié à 2 facteurs), au plus tôt 3 jours avant la prise en charge. Sans action manuelle de ce professionnel pour enregistrer durablement ces documents, ils ne sont pas accessibles à d'autres utilisateurs du traitement local et sont supprimés automatiquement une fois l'épisode de soin terminé ou au plus tard 3 jours après le préchargement.

EXI 12 : dans le cas où le contenu d'un document est préchargé de manière temporaire dans un traitement local, le professionnel pour le compte duquel ce préchargement temporaire a été effectué **DOIT** être le seul à pouvoir accéder au contenu de ce document dans le traitement local (avec un mode d'authentification à 2 facteurs), au plus tôt 3 jours avant la prise en charge du patient concerné.

Il **DOIT** s'assurer (en lien avec l'éditeur de son logiciel) :

- que le contenu d'un document préchargé temporairement, s'il ne l'a pas sélectionné spécifiquement pour un enregistrement durable dans son logiciel par une action manuelle, est bien supprimé automatiquement de son traitement local une fois l'épisode de soin terminé, ou au plus tard dans les 3 jours suivant le préchargement temporaire ;
- de ne pas précharger temporairement dans le traitement local plus de 10 documents pour un même patient ;
- de ne pas précharger temporairement dans le traitement local, en 24 heures, des documents concernant plus de 50 patients (pour un même professionnel).

5.1.3. Préchargement temporaire automatique

Le préchargement temporaire dans les traitements locaux des caractéristiques ou du contenu de documents du DMP peut faire l'objet de traitements automatiques. Un professionnel peut paramétrer dans son logiciel, s'il le permet, des critères de préchargement automatisé de documents pertinents dans le DMP en amont de la prise en charge d'un ou de plusieurs patients (par exemple pour les patients ayant un rendez-vous le lendemain).

L'exécution des préchargements des caractéristiques ou du contenu des documents peut être déclenchée automatiquement :

- dès la connexion de l'utilisateur à son logiciel (mode d'authentification directe à 2 facteurs) ;
- en amont de la connexion de l'utilisateur, avec le mode d'authentification indirecte AIR Simplifié (présentée au paragraphe 6 du présent référentiel).

L'enregistrement durable du contenu d'un document du DMP dans un logiciel ne peut pas faire l'objet d'un traitement automatique.

5.1.4. Enregistrement durable du contenu d'un document du DMP

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.

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.

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.

L'enregistrement durable d'un document du DMP dans un traitement local résulte d'une action manuelle de l'utilisateur, spécifique à ce document, dans les situations suivantes :

- document affiché à l'écran avec son contenu (en mode Web ou dans le logiciel) ;
- document sélectionné dans une liste de documents déjà filtrée, dont les caractéristiques ont été préchargées (dans les limites présentées au 5.1.1) ;
- document sélectionné parmi des documents préchargés temporairement (dans les limites présentées au 5.1.2).

EXI 13 : les professionnels **DOIVENT** veiller :

– à ne sélectionner spécifiquement pour enregistrement durable dans des traitements locaux que les documents qu'ils jugent strictement pertinents pour la prise en charge du patient ;
– à ce que les documents téléchargés depuis le DMP soient clairement identifiés dans leur logiciel comme provenant du DMP (par opposition aux documents produits localement).

Par ailleurs, au travers du Web PS DMP, les professionnels peuvent consulter des documents et les télécharger localement sur leur poste de travail, de manière transitoire avant de les réimporter dans leurs logiciels, pour le cas où ces derniers n'ont pas d'interfaces intégrées avec le DMP. Le cas échéant, les documents téléchargés sur le poste de travail doivent être supprimés immédiatement et définitivement après leur importation dans le logiciel.

EXI 14 : 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 15 : 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 établissements 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 16 : 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.

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

EXI 17 : 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, des actions de sauvegarde des documents issus du DMP et de leur suppression éventuelle à posteriori dans le traitement local.

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 18 : 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 qu'ils 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 d'une structure avec plusieurs professionnels exerçant sous sa responsabilité et 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 19 : 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 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 20 : 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 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 21 : 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 (par exemple : documents d'information, contenu mis en ligne dans les logiciels, mentions dans le contrat de travail, etc.) sur :

- 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 22 : 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. **Exigences spécifiques relatives à la consultation et au téléchargement de documents via authentification indirecte (air simplifié)**

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 Pro Santé Connect), incluant les échanges automatisés avec le DMP, dans le cadre du mécanisme dénommé « AIR simplifié ».

6.1. *Authentification 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 23 : 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 de la structure au 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, en lien avec son éditeur, à ce que l'instance logicielle s'authentifie au DMP avec des certificats de l'autorité de certification IGC-Santé contenant un identifiant FINESS de l'établissement.

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

EXI 25 : 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 à l'origine de la transaction (FINESS établissement) ;
– l'identifiant de la personne physique (RPPS) à l'origine de la transaction de consultation/téléchargement de documents du DMP.

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.

Note : la possibilité d'utiliser des identifiants de structures de type SIRET et/ou RPPS-rang avec le mode AIR simplifié pourra être étudiée dans une prochaine version du référentiel.

EXI 26 : 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 de consultation ou d'alimentation du DMP, soient transmis au DMP.

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 l'établissement **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 28 : 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, 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 29 : dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel ou le responsable de l'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 du ou des identifiants FINESS établissement à une liste blanche d'accès par le dispositif « AIR Simplifié », pour une durée maximale de 3 ans, à l'issue de laquelle la démarche devra être renouvelée.

L'auto-homologation au référentiel DMP est une procédure interne, menée par un professionnel ou établissement, acteur de la prise en charge. Les éditeurs de logiciels sous-traitants peuvent accompagner leur 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 au 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), ainsi qu'à la solution MonServiceSécurisé de l'ANSSI (8).

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 (responsable de la sécurité des systèmes d'information (RSSI), délégué à la protection de données (DPO), 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. Dans tous les cas, la durée d'homologation ne pourra excéder 3 ans, délai au bout duquel la procédure devra être obligatoirement être renouvelée ;
- 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 ;
- 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 (en lien avec l'engagement de sécurisation des modalités d'identification électronique des utilisateurs, conformément au référentiel d'identification électronique de la PGSSI-S) ;
  - des modalités de contrôle d'accès (habilitations) à ces outils, et de revue régulière de ces accès ;
  - les cas d'usage pour lesquels il est prévu d'automatiser le préchargement des caractéristiques et/ou du contenu de certains documents du DMP ;
  - 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. Il appartiendra au responsable de la structure de désigner une personne responsable de la démarche, qui devra saisir également l'identité du RSSI et du DPO de la structure.

Ce formulaire en ligne rappellera toutes les obligations et sanctions encourues, qu'il s'agisse d'une déclaration erronée (documents non conformes) ou d'un mésusage. Il ne sera pas exigé de fournir le support documentaire de l'auto-homologation et le PV de la commission lors de la déclaration en ligne.

La procédure d'auto-homologation et l'inscription en ligne devront être renouvelées régulièrement, notamment dans les cas suivants :

- dépassement de la durée maximale d'auto-homologation (3 ans) ;

– publication d'une nouvelle version du présent référentiel ;
– évolution de l'un des éléments du support documentaire de l'auto-homologation en regard des exigences du présent référentiel, ou de l'engagement de sécurisation des modalités d'identification électronique des utilisateurs (PGSSI-S) ;
– modification de la configuration logicielle mise en œuvre par un éditeur, susceptible de modifier les modalités de respect effectif des exigences du présent référentiel.

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 l'expiration de la durée d'homologation définie par l'établissement ou de la durée maximale d'homologation (3 ans), ainsi que dans les cas mentionnés ci-dessus.

7. **Synthèse des exigences et recommandations**

Exigence n° 01

[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 numérique, sur la base des modèles annexés au présent référentiel (annexe 4).

Exigence n° 02

[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. Le motif de l'éventuelle opposition **NE DOIT PAS** être enregistré dans le système d'information.

Exigence n° 03

[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.

Exigence n° 04

[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.

Exigence n° 05

[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.

Exigence n° 06

[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.

Exigence n° 07

[EXI 07] Dans le cas de documents à masquer aux titulaires de l'autorité parentale ou de documents à masquer temporairement au patient, 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.

Exigence n° 08

[EXI 08] Le professionnel **DOIT** veiller à ce que le démasquage effectif d'un document temporairement invisible pour le patient soit bien réalisé dans son DMP, dès que les conditions sont réunies.

Exigence n° 09

[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.

Exigence n° 10

[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.

Exigence n° 11

[EXI 11] Dans le cas où les caractéristiques (métadonnées) des documents sont préchargées dans un traitement local, le professionnel pour le compte duquel ces métadonnées ont été préchargées **DOIT** être le seul à pouvoir y accéder dans le traitement local (avec un mode d'authentification à 2 facteurs). Cette liste de caractéristiques **DOIT** être préchargée au plus tôt 3 jours avant la prise en charge, et **DOIT** être supprimée au plus tard 3 jours après le préchargement.

Exigence n° 12

[EXI 12] Dans le cas où le contenu d'un document est préchargé de manière temporaire dans un traitement local, le professionnel pour le compte duquel ce préchargement temporaire a été effectué **DOIT** être le seul à pouvoir accéder au contenu de ce document dans le traitement local (avec un mode d'authentification à 2 facteurs), au plus tôt 3 jours avant la prise en charge du patient concerné.

Il **DOIT** s'assurer (en lien avec l'éditeur de son logiciel) :

- que le contenu d'un document préchargé temporairement, s'il ne l'a pas sélectionné spécifiquement pour un enregistrement durable dans son logiciel par une action manuelle, est bien supprimé automatiquement de son traitement local une fois l'épisode de soin terminé, ou au plus tard dans les 3 jours suivant le préchargement temporaire ;
- de ne pas précharger temporairement dans le traitement local plus de 10 documents pour un même patient ;
- de ne pas précharger temporairement dans le traitement local, en 24 heures, des documents concernant plus de 50 patients (pour un même professionnel).

Exigence n° 13

[EXI 13] Les professionnels **DOIVENT** veiller :

- à ne sélectionner spécifiquement pour enregistrement durable dans des traitements locaux que les documents qu'ils jugent strictement pertinents pour la prise en charge du patient ;
- à ce que les documents téléchargés depuis le DMP soient clairement identifiés dans leur logiciel comme provenant du DMP (par opposition aux documents produits localement).

Exigence n° 14

[EXI 14] 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.

Exigence n° 15

[EXI 15] 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.

Exigence n° 16

[EXI 16] 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.

Exigence n° 17

[EXI 17] 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.

Exigence n° 18

[EXI 18] 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 qu'ils 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.

Recommandation n° 01

[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.

Exigence n° 19

[EXI 19] 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.

Exigence n° 20

[EXI 20] 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.

Exigence n° 21

[EXI 21] 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 (par exemple : documents d'information, contenu mis en ligne dans les logiciels, mentions dans le contrat de travail, etc.) sur :
- 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).

Exigence n° 22

[EXI 22] 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 (9) applicables à ces traitements locaux.

Exigence n° 23

[EXI 23] 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.

Exigence n° 24

[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, en lien avec son éditeur, à ce que l'instance logicielle s'authentifie au DMP avec des certificats de l'autorité de certification IGC-Santé contenant un identifiant FINESS de l'établissement.
Ce certificat **DOIT** contenir un identifiant FINESS d'établissement autorisé pour l'accès au DMP (voir paragraphe 6.5 sur les structures autorisées).

Exigence n° 25

[EXI 25] 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.).

Exigence n° 26

[EXI 26] 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 de consultation ou d'alimentation du DMP, soient transmis au DMP.

Exigence n° 27

[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 l'établissement **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.

Exigence n° 28

[EXI 28] 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, la traçabilité et le contrôle d'accès au logiciel et (iii) les modalités de restitution aux professionnels du récapitulatif régulier des accès au DMP.

Exigence n° 29

[EXI 29] Dans le cas d'une authentification indirecte pour une consultation et/ou un téléchargement de documents du DMP (AIR simplifié), le professionnel ou le responsable de l'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 du ou des identifiants FINESS établissement à une liste blanche d'accès par le dispositif « AIR Simplifié », pour une durée maximale de 3 ans, à l'issue de laquelle la démarche devra être renouvelée.

(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 du CSP.
(2) https://esante.gouv.fr/offres-services/ci-sis/espace-publication.
(3) https://esante.gouv.fr/offres-services/referentiel-ins.
(4) https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_cabinet.pdf.
(5) https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire.
(6) Voir le référentiel 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.
(7) *Cf.* https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/.
(8) *Cf.* https://www.ssi.gouv.fr/actualite/monservicesecurise-une-nouvelle-solution-de-lanssi/.
(9) 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.

ANNEXES

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 est [nom et coordonnées].
Le responsable de la sécurité des systèmes d'information (RSSI) est [nom et coordonnées].
Le délégué à la protection de données (DPO) est [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 :

	Accès des professionnels au DMP		**Droits du patient (information/consentement)**		
Professionnels appartenant à une même équipe de soins art. L. 1110-12	**Consultation possible** selon matrice d'habilitation sauf opposition art. R. 1111-46	**Alimentation Obligatoire** en principe automatique sauf opposition art. L. 1111-15	**Information préalable obligatoire** art. R. 1111-40	**Consentement présumé** art. R. 1111-46	Opposition possible à la **consultation** du DMP par un professionnel. Opposition possible à **l'alimentation** du DMP, à condition d'invoquer un motif légitime (art. R. 1111-47) Opposition possible à **l'alimentation et la consultation** si le titulaire bloque le professionnel (art. L. 1111-19 et art. R. 1111-46)
Personnes exerçant sous la responsabilité d'un professionnel membre de l'équipe de soins	**Consultation non autorisée** hors matrice d'habilitation	**Alimentation Obligatoire** en principe automatique sauf opposition	**Information préalable obligatoire**	**Consentement présumé**	Pas d'opposition à l'alimentation si le patient ne s'y est pas opposé pour le professionnel concerné art. R. 1111-46 al. 6 CSP
Professionnel n'appartenant pas à l'équipe de soins	**Consultation possible** selon matrice d'habilitation sauf opposition	**Alimentation Obligatoire** en principe automatique sauf opposition	**Information préalable obligatoire**	**Consentement à recueillir** art. L. 1111-17 (III) art. R. 1111-46 art. D. 1110-3-1	Le consentement recueilli est valable tant qu'il n'a pas été retiré art. R. 1111-46 al. 3 CSP

La notion d'équipe de soin est définie par l'article L. 1110-12 du code de la santé publique. Il s'agit d'un ensemble de professionnels qui participent directement à la prise en charge d'un même patient par la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie ou aux actions nécessaires à la coordination de plusieurs de ces actes et qui :

1° Soit exercent dans le même établissement ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ;

2° Soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient ;

3° Soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé.

L'article R. 1110-2 du code de la santé publique précise qui sont les professionnels susceptibles d'échanger ou de partager des informations relatives au patient pris en charge. Ils appartiennent à deux catégories : les professionnels de santé mentionnés à la quatrième partie du code de la santé publique (médecin, infirmier, pharmacien, etc.) et d'autres professionnels mentionnés au sein de ce même article (assistantes sociales, assistantes maternelles, psychologues, etc.).

Quelques exemples :

– un médecin généraliste prescrit des actes de rééducation et des soins d'hygiène. Le masseur kinésithérapeute et le service de soins infirmiers à domicile (SSIAD) choisis par le patient constituent une équipe de soin, à laquelle le médecin appartient ;
– un médecin généraliste souhaite demander un avis sur l'état de santé de son patient à un confrère qui exerce dans un établissement hospitalier et qui ne connaît pas le patient : ce confrère ne fait pas partie de l'équipe de soins du patient ;
– une équipe de soins peut être constituée de médecins, psychologues et assistantes sociales exerçant au sein du même établissement de santé ou qui n'exercent pas au sein du même établissement mais qui ont été reconnus comme tels par le patient lui-même ;
– un infirmier exerçant dans un autre établissement que celui au sein duquel le patient est pris en charge, ne fait pas partie de son équipe de soins si celui-ci est inconnu du patient.

ANNEXE 3

TABLEAU RÉCAPITULATIF DES AUTORISATIONS DE CONSULTATION DE DOCUMENT DU DMP

Les autorisations d'accès aux documents du DMP sont résumées dans le tableau ci-après (**X** Impossible ✓ Possible) :

	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	✓	✓	✓	✓	**X** (sauf auteur)
Accès au document masqué (créé par un professionnel)	**X**	✓	✓	✓	**X**
Accès au document créé par le titulaire	✓	-	✓	✓	**X**
Accès au document masqué (créé par le titulaire)	**X**	-	✓	✓	**X**
Accès au document alimenté par une application référencée	✓	-	✓	✓	**X**
Accès au document pour lequel le titulaire mineur a demandé le secret	✓	✓	✓	✓	**X**

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) au dossier médical (DMP) de 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 soins (art. L. 1111-17 (II) du code de la santé publique)

Pour vous prendre en charge efficacement, ce professionnel : ..... *(préciser l'identité du professionnel pour le compte duquel l'autorisation est demandée, sa fonction et son service)* 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 : ☐