

Référentiel Force Probante des documents de santé

Document introductif

Version : V1.0 | Date : 22/03/2021

Documents de référence

1. Référence n° 1 : Référentiel force probante des documents de santé – Annexe 1 – Socle commun de principes techniques et organisationnels
2. Référence n° 2 : Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation
3. Référence n° 3 : Référentiel force probante des documents de santé – Annexe 3 – Mécanismes à mettre en œuvre dans le cadre de la production de documents nativement numériques
4. Référence n° 4 : Référentiel force probante des documents de santé – Annexe 4 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation de documents de santé numériques
5. Référence n° 5 : Référentiel force probante des documents de santé – Annexe 5 – Gestion des métadonnées
6. Référence n° 6 : Référentiel force probante des documents de santé – Annexe 6 – Classification des documents de santé
7. Référence n° 7 : eIDAS - Règlement du Parlement Européen et du Conseil n°910/2014 du 23 juillet 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
[<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR>]
8. Référence n° 8 : Politique de Sécurité des Systèmes d'Information du Ministère Chargé des Affaires Sociales (PSSI-MCAS) [<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031386468>]

Historique du document

Version	Date	Commentaires
V0.11	16/09/2019	Version diffusée pour la concertation
V1.0	22/03/2021	Version finale

SOMMAIRE

1. INTRODUCTION	4
1.1. Enjeux et problématiques	4
1.2. Réglementation	4
1.3. Objet du référentiel	5
1.4. Périmètre du référentiel	5
1.4.1. Documents concernés	5
1.4.2. Cas des documents émis par la personne prise en charge	6
1.5. Définitions	6
2. USAGE DE CONVENTION DE PREUVE	8
3. DOCUMENTS CONSTITUTIFS DU REFERENTIEL	9
4. PRINCIPES RELATIFS AUX DOCUMENTS NUMERIQUES	10
5. CAS D'USAGE ET EXIGENCES ASSOCIEES	11
5.1. Numérisation des documents papier comportant des données de santé	11
5.2. Production de document nativement au format numérique	12
5.3. Matérialisation des documents de santé nativement au format numérique	13

1. INTRODUCTION

1.1. Enjeux et problématiques

Les acteurs des secteurs de la santé, du suivi social et médico-social, quel que soit leur statut, produisent, partagent, échangent et conservent une grande quantité de documents comportant des données de santé à caractère personnel qu'ils soient au format papier ou numérique.

Ces documents doivent être conservés de manière sécurisée pendant une durée longue, fixée par la loi dans certains cas, pour répondre à la nécessité d'assurer dans le temps la continuité et la qualité de la prise en charge des patients. Ils peuvent également constituer des éléments de preuve décisifs dans le cadre de contentieux.

La gestion quotidienne et dans le temps des stocks de documents papier ainsi constitués est aujourd'hui un réel challenge pour de nombreux acteurs des secteurs sanitaire, social et médico-social. Plus particulièrement, l'accessibilité des informations de santé contenues dans ces documents, la gestion optimisée du stockage et des accès et la protection des documents contre les dégradations sont autant de problématiques auxquelles il est nécessaire d'apporter des réponses efficaces.

Si la réduction du volume de documents de santé¹ au format papier manipulés est désormais une réalité, la migration vers le numérique reste malgré tout progressive.

Afin d'aider à accélérer cette transition numérique et de limiter la gestion hybride du papier et du numérique, les articles L.1111-25 à 31 du code de la santé publique (issus de l'ordonnance n° 2017-29 du 12 janvier 2017) fixent les conditions de reconnaissance, pour les documents de santé, de la force probante des copies numériques, des documents nativement créés au format numérique et des documents nativement numériques matérialisés au format papier. Ils précisent également les modalités d'élimination des documents originaux au format papier après numérisation avant l'issue du délai légal de conservation du papier. La force probante des documents de santé est ainsi désormais indifférente au support, que le document soit sous format papier ou numérique.

1.2. Réglementation

Les articles L.1111-25 à L.1111-31 du code de la santé publique traitent des « **conditions de reconnaissance de la force probante** des documents comportant des données de santé à caractère personnel **créés ou reproduits sous forme numérique et de la destruction des documents** conservés sous une autre forme que numérique »

► **Champ organique** (Qui ?) [Art. L. 1111-25] :

- Un professionnel de santé, un établissement ou service de santé ;
- Un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le code de la santé publique ;
- Le service de santé des armées ;
- Un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles.

► **Champ matériel** (Quelles données ?) [Art. L. 1111-25] :

- Les données manipulées par les acteurs mentionnés ci-dessus dans le cadre des activités :
 - De prévention ;
 - De diagnostic ;
 - De soins ;
 - De compensation du handicap ;

¹ Dans tout le présent référentiel, par convention et commodité de lecture, la terminologie « document de santé » est utilisée pour définir un « document comportant des données de santé à caractère personnel » (cf. §1.5)

- De prévention de perte d'autonomie ;
- De suivi social et médico-social.

► **Les cas d'usages encadrés :**

- Numérisation des documents papier [Art. L. 1111-26] ;
- Création de documents nativement au format numérique [Art. L. 1111-27] :
 - Cas des documents nativement créés au format numérique devant être signés (documents nécessitant une signature conformément à la réglementation qui les encadre, que celle-ci soit effectuée de façon manuscrite ou numérique) ;
 - Cas dans lesquels ces documents sont signés de façon numérique [Art. L.1111-28] ;
- Mise en forme d'un document numérique à partir de un ou plusieurs documents numériques existants et sa matérialisation sur support papier [Art. L. 1111-29] ;
- Destruction éventuelle des documents papier originaux à la suite d'une opération de numérisation [Art. L. 1111-26] ;

- Le code de la santé publique **renvoie à l'ANS le soin de préciser dans un référentiel pris par voie d'arrêté du ministre chargé de la santé les conditions** (techniques et organisationnelles) d'application de chacune de ces dispositions [Art. L. 1111-30 et 31].

1.3. Objet du référentiel

Les objectifs de ce référentiel sont :

- de rappeler les **enjeux, problématiques et risques associés aux opérations** suivantes sur les documents de santé :
- Numérisation de documents de santé papier ;
 - Production de documents de santé nativement numériques ;
 - Matérialisation de documents de santé numériques ;
- de **fixer les règles, exigences et principes à respecter** par les professionnels de santé, les établissements et services de santé et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social, en application de l'article L.1110-4-1 du code de la santé publique.

1.4. Périmètre du référentiel

1.4.1. Documents concernés

Sont concernés par le présent référentiel tous les documents de santé qui font partie du champ matériel et organique de l'article L. 1111-25 du code de la santé publique (cf. §1.2) et incluent des informations relatives à une personne physique susceptible d'être identifiée de façon directe ou indirecte et strictement nécessaires à la coordination ou à la continuité des soins la concernant, à la prévention ou à son suivi médico-social et social (cf. article L. 1110-4 du code de la santé publique).

Le présent référentiel s'applique de la même façon à l'ensemble des documents de santé manipulés au sein d'une structure de santé, **y compris les documents à usage uniquement interne (documents n'ayant pas vocation à sortir de la structure de santé). Il appartient donc à la structure de santé d'appliquer les paliers décrits dans le présent référentiel à tous les documents manipulés en interne ou de définir des règles locales formalisées dans un document interne porté à la connaissance des personnels concernés** (cela peut prendre la forme d'une politique d'archivage par exemple). Dans ce dernier cas, le non-respect des exigences du référentiel force probante doit être justifié par chaque structure de santé à l'appui d'un argumentaire documenté. Celui-ci prendra un

format conforme aux processus de décision internes propres à la structure de santé concernée et pourra être complété par un plan d'action de mise en conformité au référentiel.

1.4.2. Cas des documents émis par la personne prise en charge

Toutes les règles décrites dans le référentiel Force Probante s'appliquent aux acteurs décrits dans le champ organique de l'article L.1111-25 du code de la santé publique (cf. §1.2). Les personnes prises en charge, bien qu'elles puissent être dans certains cas elles-mêmes émettrices de documents de santé du périmètre, n'y sont pas soumises.

Ce sont les structures du secteur santé-social qui se chargent de mettre en œuvre les mesures nécessaires lorsqu'elles demandent à une personne prise en charge de signer un document qu'elles ont produit (afin de recueillir son consentement par exemple). Toutefois, **un document produit par un individu à son domicile sans qu'aucune garantie ne soit mise en œuvre ne possède aucune valeur probante.**

Il est recommandé aux acteurs du secteur sanitaire, social et médico-social de communiquer à ce sujet avec les personnes qu'ils prennent en charge, afin de garantir la force probante des documents qu'elles reçoivent de leur part (directives anticipées par exemple). Ils pourront leur suggérer les bonnes pratiques suivantes lors de la production d'un document, dans cet ordre préférentiel :

1. Utiliser lorsqu'ils existent les services et outils institutionnels dédiés pour les déclarations (téléservices mis en œuvre par l'administration par exemple) ;
2. Dans la mesure où le document le justifie (enjeu important et/ou valeur probante essentielle), passer par un tiers de confiance afin de signer électroniquement le document ;
3. Confier le document produit à un professionnel de santé qui sera en mesure de le numériser et de l'ajouter au dossier patient ;
4. Ajouter le document au Dossier Médical Partagé (DMP).

1.5. Définitions

Acteur de santé	<i>Personne physique ou morale participant directement ou indirectement à la prise en charge médicale d'un patient</i>
Cachet électronique ou scellement	<i>Mécanisme qui permet de garantir l'origine et l'intégrité d'un document</i>
Document de santé	<i>Document comportant des données de santé à caractère personnel</i>
Donnée à caractère personnel	<i>Toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement</i>
Donnée de santé à caractère personnel	<i>Les données de santé à caractère personnel sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne</i>
Dossier de preuve	<i>Ensemble des éléments concourant à donner une force probante à un document ou une donnée. Il doit être conservé pendant toute la durée de vie du document ou de la donnée</i>

Empreinte numérique	<i>Terme de cryptologie désignant un ensemble de bits caractéristique d'un document numérique, obtenu par une fonction de hachage. Toute modification du document numérique entraîne la modification de son empreinte numérique. La comparaison d'empreintes permet de contrôler l'intégrité d'un fichier</i>
Force Probante	<i>Niveau de confiance que l'on peut accorder à un document ou une donnée. Dans le secteur du numérique en santé, la force probante des documents comportant des données de santé dématérialisées répond à un enjeu relatif au droit de la preuve mais avant de servir comme outil de preuve, elle est avant tout essentielle pour donner de la confiance dans la dématérialisation. Le degré de conviction que l'on peut accorder à un document dématérialisé varie en fonction des conditions de son élaboration et du maintien dans le temps de la réunion de ces conditions</i>
Identitovigilance	<i>Surveillance et prévention des erreurs et risques liés à l'identification des patients</i>
Intégrité	<i>Qualité d'un document ou d'une donnée qui n'a pas été altéré. Dans le monde numérique, un document ou une donnée est réputé intègre si son empreinte à un temps $t+n$ est identique à l'empreinte prise à un temps t</i>
Horodatage	<i>Mécanisme qui permet d'attester qu'une donnée ou qu'un document existe à un instant donné</i>
Métadonnées	<i>Ensemble structuré d'informations techniques, de gestion et de description attachées à un document servant à décrire les caractéristiques de ce document en vue de faciliter son identification, sa gestion, son usage ou sa préservation</i>
Moyen d'identité électronique	<i>Élément matériel et/ou immatériel (clé / carte avec ou sans contact, application d'authentification sur téléphone...) contenant des données d'identification d'une personne physique et utilisé pour s'authentifier sur un service en ligne</i>
Responsable de traitement de données à caractère personnel	<i>Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal</i>
Signature électronique	<i>Mécanisme qui permet l'identification de l'auteur d'un document électronique, la garantie de l'intégrité de ce document et le lien entre le document et la signature</i>

2. USAGE DE CONVENTION DE PREUVE

Le référentiel force probante des documents de santé fixe les règles à respecter afin qu'un document émis puisse être considéré comme recevable par le destinataire de ce document.

Il permet d'aider les responsables de traitement à identifier les différents niveaux de confiance et les moyens techniques associés pour donner une force probante selon différents niveaux à des documents numériques comportant des données de santé. Seul le recours à des moyens techniques dits qualifiés au sens du règlement eIDAS **[document de référence n°7]** permet de bénéficier d'un niveau de confiance instaurant une présomption de fiabilité. A défaut, les responsables de système d'information devront apporter la preuve de la fiabilité de leur dispositif dans le cadre d'un litige mettant en cause par exemple l'intégrité d'un document numérisé.

Les professionnels peuvent conclure des conventions de preuve entre eux afin d'aider le juge à apprécier la force probante des documents objet du litige (article 1368 du code civil). Une convention de preuve a pour finalité de permettre aux parties d'aménager la manière dont elles vont démontrer les droits qu'elles peuvent être amenées à invoquer l'une contre l'autre lors d'une procédure contentieuse. Elles déterminent pour cela par elles-mêmes les règles relatives à la charge de la preuve, la détermination des faits à prouver et les procédés de preuve admissibles en cas de litige.

Le juge peut être amené à statuer sur la validité de la convention de preuve et n'est pas lié par elle. En outre, une telle convention ne peut être opposée à l'utilisateur, elle ne vaut qu'entre les parties.

Enfin, la convention de preuve ne doit pas créer d'asymétrie trop forte entre les parties, le juge pouvant considérer que les clauses sont alors abusives. La mise à disposition de la documentation technique imposée par l'article L.1111-30 du code de la santé publique (voir les explications détaillées dans le socle commun du référentiel **[document de référence n°1]**) peut contribuer à éviter ce risque, en permettant à chaque partie de prendre connaissance des modalités de fonctionnement du processus de dématérialisation.

La convention de preuve doit notamment porter sur :

- ▶ la répartition des rôles et les moyens mis en œuvre pour la production ;
- ▶ la mise à disposition et la conservation des documents ;
- ▶ les règles de preuve (relatives à la charge de la preuve, la détermination des faits à prouver, les procédés de preuve admissibles) ;
- ▶ les conditions dans lesquelles seront réglés à l'amiable ou devant les tribunaux compétents d'éventuels conflits portant sur la valeur probatoire des documents échangés.

La convention de preuve est de nature contractuelle donc, s'il existe un contrat entre les parties concernées, il est naturel qu'elle y trouve sa place. Elle pourra sinon a priori s'intégrer à des conditions générales d'utilisation (CGU), leur acceptation permettant de formaliser le consentement. Il faudra dans ce cas veiller à tracer l'acceptation des CGU par chaque utilisateur concerné.

Quel que soit le palier retenu par le responsable de traitement, dès lors que les moyens mis en œuvre ne sont pas présumés fiables, il est préconisé de recourir à une convention de preuve. Cette recommandation est a fortiori applicable au cas dans lequel deux ou plusieurs structures amenées à échanger des documents de santé choisissent de ne pas se référer au référentiel force probante. Elles s'exposent néanmoins au risque de se voir reprocher par le juge de ne pas avoir mis en œuvre les exigences du référentiel force probante en cas de litige.

3. DOCUMENTS CONSTITUTIFS DU REFERENTIEL

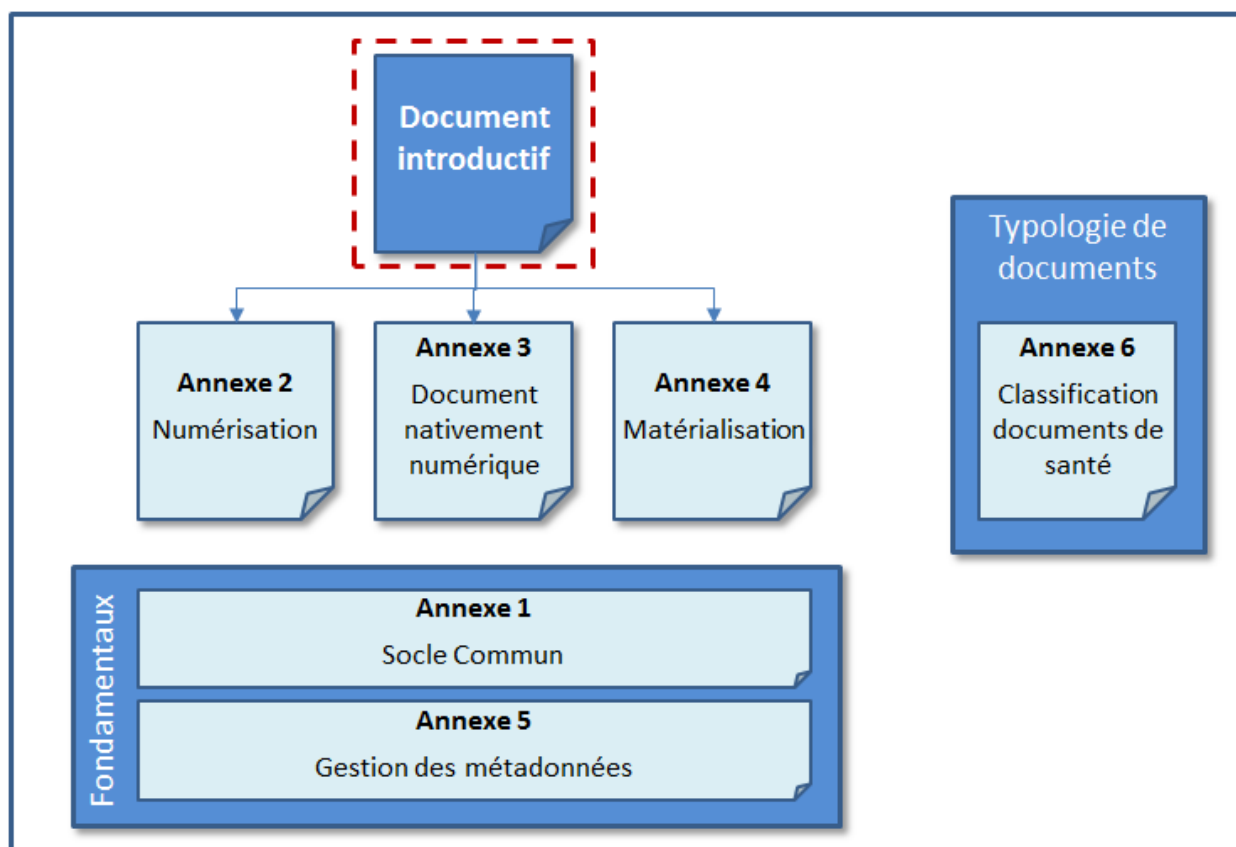
Le référentiel « force probante » des documents de santé est constitué :

► **Du présent document, composé de :**

- L'introduction du sujet de la valeur probante (enjeux, réglementation, objet du référentiel et périmètre) ;
- Informations relatives à l'usage de convention de preuve ;
- Une clarification des principes relatifs aux documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique ;
- Une présentation des enjeux et des risques relatifs à chacun des cas d'usage identifiés ;
- L'identification des annexes applicables en fonction du cas d'usage.

► **D'une série d'annexes et de documents de références, détaillant les mécanismes techniques, et procédures organisationnelles à mettre en œuvre en fonction des cas d'usages :**

- Annexe 1 - Socle commun de principes techniques et organisationnels
- Annexe 2 - Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation
- Annexe 3 - Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques
- Annexe 4 - Mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation de documents de santé numériques
- Annexe 5 - Gestion des métadonnées
- Annexe 6 - Classification des documents de santé



4. PRINCIPES RELATIFS AUX DOCUMENTS NUMERIQUES

Pour assurer la qualité juridique des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique, **il est nécessaire que les systèmes d'information** participant à leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, **respectent les principes ci-dessous** :

- ▶ Assurer la sécurité des processus et des opérations réalisées sur les documents électroniques originaux, ou issus d'une numérisation, **de bout en bout**, afin de leur conférer une force probante et de réduire les risques de contestation sur leur contenu ou leur origine. En ce sens, **l'homologation des systèmes d'information** associés est la bonne pratique, telle que promue par la PSSI-MCAS [**document de référence n°8**]. Il convient également à ce titre de veiller à ce que les éventuels fournisseurs de services intervenant dans le cadre de ces activités s'engagent à respecter les conditions de sécurité associées ;
- ▶ **Adapter les moyens aux enjeux**, en fonction des cas d'usages métier, et des risques associés. Les annexes au présent document identifient des paliers de mise en œuvre (ex : signature électronique simple, avancée, qualifiée), présentant des caractéristiques de sécurité plus ou moins avancées, mais induisant un niveau de complexité progressif de mise en œuvre et de déploiement. Il convient de s'appuyer sur la classification des documents de santé [**document de référence n°6**] afin d'identifier le palier de mise en œuvre minimum adapté à chaque document. Sur la base **d'analyses de risques** qu'il aura réalisées, le responsable de traitement peut mettre en œuvre des mesures de sécurité complémentaires afin d'ajuster au mieux la sécurité de son système d'information en fonction du contexte et des enjeux propres aux documents concernés ;
- ▶ **Analyser le contexte juridique propre au cas d'usage métier**. Le présent document et ses annexes définissent les exigences de mise en œuvre de la dématérialisation à vocation probatoire, mais ne constituent pas le seul cadre applicable aux documents de santé comportant des données à caractère personnel. Il appartient à la personne participant à la mise en œuvre de ces documents électroniques de veiller à respecter le cadre juridique existant pour le cas d'usage métier concerné. A titre d'exemple, les feuilles de soins électroniques sont encadrées par le code de la sécurité sociale et il convient de respecter celui-ci dans le contexte de mise en œuvre d'un projet de dématérialisation. En ce sens, une analyse juridique propre au cas d'usage métier est nécessaire, et elle participera au choix du ou des paliers à retenir, en sus des éléments décrits au point précédent ;
- ▶ **Utiliser des dispositifs et des services déjà disponibles et labellisés**. Dans le contexte du Règlement Européen « eIDAS » n° 910/2014 [**document de référence n°7**], l'ANSSI pour la France, et les organes de contrôle européens équivalents, labellisent des services et outils capables de produire, signer et horodater des documents électroniques. Il convient de veiller à les utiliser, autant que faire se peut, afin que la mise en œuvre de ces procédés de dématérialisation se fasse dans des conditions de sécurité adéquates ;
- ▶ Le cas échéant, s'assurer de **conserver le caractère « original électronique »** des documents produits, ou transmis, durant l'intégralité de leur cycle de vie, depuis leur création (originale électronique ou issu du papier) jusqu'à la fin de leur durée de vie utile (soit y compris pendant sa période de conservation). Les technologies et algorithmes techniques sous-jacents à la production des documents électroniques, à vocation probatoire, évoluant et devenant potentiellement vulnérables dans le temps, il est nécessaire de veiller à conserver la qualité des documents électroniques via des mécanismes de conservation sécurisée, tel que décrit dans le « Guide des mécanismes de protection de l'intégrité des données stockées » de la PGSSI-S ;
- ▶ Respecter un **socle commun de principes techniques et organisationnels**. Au-delà des aspects techniques strictement liés à la production et à la conservation de documents électroniques à vocation probatoire, la qualité juridique des documents produits nécessite également qu'ils soient produits dans des environnements « de confiance », respectueux d'un certain nombre de principes de sécurité communs. L'annexe « Socle commun de principes techniques et organisationnels » [**document de référence n°1**] est donc à considérer quels que soient les cas d'usage mis en œuvre, pour assurer un niveau de sécurité adapté au contexte.

5. CAS D'USAGE ET EXIGENCES ASSOCIEES

5.1. Numérisation des documents papier comportant des données de santé

La numérisation des documents de santé au format papier répond à plusieurs **enjeux pour les acteurs du secteur santé-social**, notamment :

- ▶ la possibilité de disposer d'un accès simplifié et plus rapide aux informations de santé et de procéder à la recherche des informations présentes dans les documents de santé initialement sur support papier ;
- ▶ la capacité d'indexation des informations stockées au format papier par les SI des acteurs du secteur santé-social ;
- ▶ La constitution progressive de dossiers patients permettant à partir d'un seul point d'accès, d'avoir une vision globale des informations formalisées relatives à l'état de santé d'un patient ;
- ▶ L'optimisation de la gestion des archives papier au sein du secteur et des coûts associés, dans l'hypothèse où le palier de mise en œuvre retenu permet la destruction des originaux papiers.

Toutefois, cette opération expose les acteurs du secteur santé-social à **divers risques, dont notamment**:

- ▶ la falsification des documents lors de leur numérisation ;
- ▶ l'erreur de reproduction fidèle des documents (numérisation partielle, non lisible, etc.) ;
- ▶ l'affectation erronée des documents numérisés au sein du SI Santé ;
- ▶ la modification non autorisée des copies numériques ;
- ▶ l'obsolescence des formats des copies numériques ;
- ▶ la non-reconnaissance de la force probante des copies numériques.

Il est ainsi primordial, dans le cadre de la mise en œuvre de la numérisation des documents de santé au format papier, de définir les moyens permettant de répondre aux **exigences ainsi posées** :

- ▶ **la fiabilité et qualité** du processus de numérisation ;
- ▶ **l'identitovigilance** au cours du processus de numérisation ;
- ▶ **l'identification et l'intégration** des copies numériques **au sein des SI** ;
- ▶ **la gestion des accès** aux documents numérisés et le respect de **leur intégrité** ;
- ▶ **la pérennité des copies numériques**.

Il appartient donc aux responsables de traitement concernés par ces procédés de numérisation de :

- ▶ **Analyser les risques relatifs à ces opérations de numérisation**, dans leur environnement, des documents de santé concernés ;
- ▶ **Respecter les principes et règles communs** à la manipulation de documents numériques tels que précisés au sein du document « Annexe 1 - Socle commun de principes techniques et organisationnels » **[document de référence n°1]** ;
- ▶ **Respecter les principes et règles de sécurité propres aux opérations de numérisation** tels que définies au sein de l'annexe « Annexe 2 - Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation » **[document de référence n°2]**. En particulier, il appartient au responsable du SI réalisant les opérations de numérisation de déterminer le « palier » le plus adapté au type de document (cf. annexe 6 **[document de référence n°6]**) ainsi qu'aux risques associés à son contexte métier.

5.2. Production de document nativement au format numérique

Les acteurs du secteur sanitaire, social et médico-social, quels que soient leur statut et leurs missions, produisent, partagent, échangent et conservent une grande quantité de documents créés nativement au format numérique et comportant des données de santé à caractère personnel.

Ces documents doivent être conservés pendant une durée longue, fixée par la loi dans certains cas, pour répondre à la nécessité d'assurer dans le temps la continuité et la qualité de la prise en charge des patients mais également pour constituer des éléments de preuve décisifs dans le cadre de contentieux.

Les documents créés nativement au format numérique doivent ainsi disposer de propriétés permettant de répondre aux enjeux suivants :

- ▶ **Identification de l'émetteur ;**
- ▶ **Intégrité et non répudiation ;**
- ▶ **Pérennité dans le temps ;**
- ▶ **Portabilité ;**
- ▶ **Traçabilité.**

L'ensemble de ces éléments contribuent à la force probante du document.

Par ailleurs, que le document soit au format papier ou numérique, il peut être exigé par un texte ou par convention qu'il soit signé (Art. L. 1111-28 du code de la santé publique). Lorsqu'il s'agit de faire signer le patient, la signature signifie que la personne prise en charge a pris acte du contenu du document et, le cas échéant, y consent. Lorsqu'il est imposé de faire signer le professionnel, la signature signifie que celui-ci valide le contenu du document (ex : certificats décès, naissance, arrêt de travail, etc.).

Des mesures organisationnelles, juridiques et techniques doivent être mises en œuvre et être documentées pour répondre à cette exigence dans le cadre de la dématérialisation des documents comportant des données de santé. En outre, des exigences particulières sont prévues par la loi lorsque le document est signé de façon électronique (conditions du second alinéa de l'article 1367 du code civil).

L'utilisation d'une signature ou d'un cachet électronique permet de garantir au destinataire du document :

- ▶ **Pour la signature électronique :**
 - L'identité et l'habilitation du professionnel de santé de façon non contestable (non répudiation) ;
 - L'intégrité du contenu.
- ▶ **Pour le cachet :**
 - L'origine du document de santé et l'organisation dont il émane ;
 - L'intégrité du contenu.

La signature et le cachet électroniques sont encadrés par le Règlement européen « eIDAS » n° 910/2014 du 23 juillet 2014 **[document de référence n°7]**. Ce texte s'applique depuis le 1^{er} juillet 2016 ; il fixe les bases de la mise en œuvre, de la valeur juridique et de la reconnaissance de 3 niveaux de mise en œuvre pour les « signatures électroniques » et « cachets électroniques » : simple, avancée, qualifiée.

Il appartient aux responsables des systèmes d'information concernés par ces procédés de production de documents nativement au format numérique de :

- ▶ **Analyser le cadre légal associé aux documents métiers produits** et à défaut de cadre précis, d'analyser les risques induits par les documents produits nativement au format numérique pour déterminer :
 - Si le document doit ou non être signé
 - Un texte le prévoit ;
 - L'importance du contenu du document a nécessité usuellement une signature de son auteur ;
 - Les moyens techniques à mettre en œuvre : la nécessité de mettre en œuvre une ou plusieurs signatures électroniques ou cachets électroniques ainsi que le niveau cible à retenir (simple, avancée, qualifiée) ;

- Les obligations (ou nécessités) éventuelles associées en matière d'horodatage, de forme pour ces signatures ou cachets (formats, types de signatures enveloppantes, enveloppées ou détachées) ;
- Le type d'authentification à mettre en place si besoin pour la signature ;
- ▶ **Respecter les principes et règles transverses** à la manipulation de documents numériques tels que précisés au sein du document « Annexe 1 - Socle commun de principes techniques et organisationnels » **[document de référence n°1]** ;
- ▶ **Respecter les principes et règles de sécurité relatifs aux documents nativement produits au format numérique**, tels que définis au sein de l'annexe « Annexe 3 - Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de document nativement numérique » **[document de référence n°3]**.

5.3. Matérialisation des documents de santé numériques

Des dizaines de milliers de documents sont matérialisés quotidiennement dans le secteur santé-social et n'ont pour preuve d'authenticité que le tampon de l'établissement ou la signature manuscrite au mieux d'une personne habilitée au sein de l'établissement (signature par ailleurs difficilement contrôlable).

La matérialisation des documents de santé créés nativement au format numérique (ou issus de la numérisation d'un document au format papier) est nécessaire pour répondre aux besoins de prise en charge des personnes, qu'il s'agisse de contribuer à la prise en charge de la personne concernée ou de lui permettre de faire valoir ses droits (entente préalable, certificat d'arrêt de travail, pour ne citer que ces exemples). Cette matérialisation de documents originaux électroniques est rendue complexe par le fait qu'une signature électronique, ou qu'un cachet électronique, n'ont pas de représentation visuelle comparable à la forme prise par les traditionnelles signatures manuscrites, ou tampon.

L'article L.1111-29 du code de la santé publique **fixe les conditions assurant à la copie matérialisée une force probante similaire à celle du document d'origine** (numérique). Les exigences énoncées portent sur :

- ▶ **L'insertion des métadonnées nécessaires à l'identification du document ;**
- ▶ **L'insertion d'informations permettant de préciser la date et le contexte de création du document matériel.**

La matérialisation des documents de santé numériques expose les acteurs du secteur santé-social principalement aux risques de **falsification** et **d'usage de faux**.

Ainsi, les principaux enjeux auxquels le processus de matérialisation doit répondre sont :

- ▶ **L'authenticité des documents matérialisés ;**
- ▶ **La garantie de la force probante.**

Sur le plan pratique, plusieurs mécanismes, prenant des formes diverses, permettent d'atteindre ces objectifs. Il appartient aux responsables des systèmes d'information concernés par ces procédés de matérialisation de document numériques de :


- ▶ **Analyser les risques relatifs à ces opérations de matérialisation**, dans le contexte de l'environnement et des documents de santé concernés ;
- ▶ **Respecter les principes et règles transverses** à la manipulation de documents numériques tels que précisés au sein du document « Annexe 1 - Socle commun de principes techniques et organisationnels » **[document de référence n°1]** ;
- ▶ **Respecter les principes et règles de sécurité relatifs aux opérations de matérialisation de documents nativement produits au format numérique**, tels que définis au sein de l'annexe « Annexe 4 - Mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation des documents de santé numériques » **[document de référence n°4]**. En particulier, il appartient au responsable du SI support des opérations de matérialisation de déterminer les moyens les plus adaptés aux possibilités opérationnelles de vérification de ces documents une fois ceux-ci matérialisés.



esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

 @esante_gouv_fr

 [linkedin.com/company/agence-du-numerique-en-sante](https://www.linkedin.com/company/agence-du-numerique-en-sante)

