MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel Force Probante des documents de santé

Socle commun de principes techniques et organisationnels

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

Documents de référence

1. Référence n° 1 : Référentiel force probante des documents de santé - Document introductif
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 : Politique de Sécurité des Systèmes d'Information du Ministère Chargé des Affaires Sociales (PSSI-MCAS) [https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031386468]
8. Référence n° 8 : Référentiel Général de Sécurité V2 - Annexe B1 - Mécanismes cryptographiques (ANSSI) [https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs]

Historique du document

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

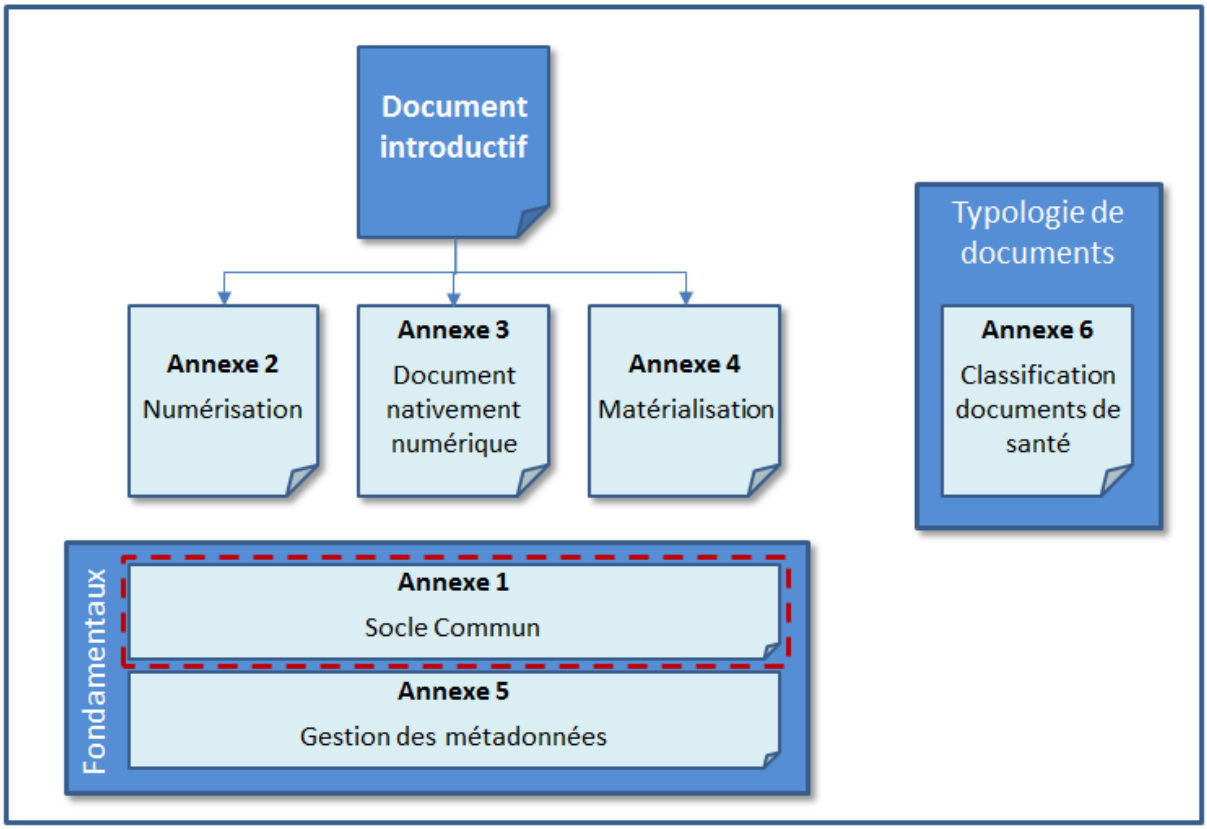
SOMMAIRE

1. INTRODUCTION

1.1. Objet du document

Ce document rassemble des principes techniques et organisationnels communs aux différents cas d'usage relatifs à la force probante des documents comportant des données de santé à caractère personnel.

Ce document constitue l'une des annexes du référentiel « Force probante » ainsi structuré :



Structure du référentiel Force Probante

Le référentiel « Force probante » répond aux attendus des articles L.1111-25 à 31 du code de la santé publique concernant les documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique. Il comprend notamment :

- Un document introductif qui présente la problématique, le périmètre et les enjeux **[document de référence n°1]** ;
- 3 annexes qui décrivent les exigences à appliquer dans les principaux cas d'usage
  - Cas de la dématérialisation (ou numérisation) de documents **[document de référence n°2]** ;
  - Cas de la production de documents nativement au format numérique **[document de référence n°3]** ;
  - Cas de la matérialisation (ou impression) de documents **[document de référence n°4]** ;
- 2 annexes présentant les principes fondamentaux à appliquer quel que soit le cas d'usage rencontré
  - Socle de principes communs à mettre en œuvre (présent document) ;
  - Explications relatives à la gestion des métadonnées **[document de référence n°5]** ;
- Une annexe qui propose une classification des documents de santé et fait correspondre à chaque classe de document de santé identifiée le niveau requis d'exigences de sécurité à appliquer **[document de référence n°6]**.

La présente annexe du référentiel centralise en un seul document des principes de sécurité qui s'appliquent quel que soit le processus mis en œuvre mettant en jeu la force probante des documents numériques comportant des

données de santé à caractère personnel. Elle évite la duplication de principes communs dans chacune des autres annexes et améliore la lisibilité de ces annexes en les recentrant sur un processus spécifique.

Ce document s'adresse aux personnes impliquées dans la mise en œuvre d'un processus relevant de l'un au moins des cas d'usage du référentiel, en particulier aux responsables des traitements qui devront veiller à leur application.

1.2. Champ d'application

Le champ d'application de ce référentiel est précisé dans le document introductif du référentiel « Référentiel force probante des documents de santé » **[document de référence n°1]**.

De façon générale, sont concernés tous les processus liés à la production ou l'échange de documents comportant des données de santé à caractère personnel, dans le domaine de la santé, du suivi social et du médico-social.

1.3. Présentation du document

La mise en place de mécanismes de sécurité destinés à renforcer la force probante de documents doit s'inscrire dans le cadre d'une démarche globale de sécurité du système d'information. Cela implique que la structure concernée dispose d'une politique de sécurité des systèmes d'information adaptée à son contexte, et en accord avec la **[PGSSI-S]**.

L'objet de ce document n'est pas de rappeler les exigences déjà applicables de la **[PGSSI-S]**. Les principes présentés dans la suite du document concernent uniquement des particularités associées aux cas d'usage du référentiel force probante.

1.4. Définitions

Acteur de santé	*Personne physique ou morale participant directement ou indirectement à la prise en charge médicale d'un patient*
Cachet électronique ou scellement	*Mécanisme qui permet de garantir l'origine et l'intégrité d'un document*
Document de santé	*Document comportant des données de santé à caractère personnel*
Donnée à caractère personnel	*Toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement (CNIL)*
Donnée de santé à caractère personnel	*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.*
Dossier de preuve	*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*

Empreinte numérique	*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*
Force Probante	*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*
Identitovigilance	*Surveillance et prévention des erreurs et risques liés à l'identification des patients*
Intégrité	*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*
Horodatage	*Mécanisme qui permet d'attester qu'une donnée ou qu'un document existe à un instant donné*
Métadonnées	*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*
Moyen d'identité électronique	*Elément 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*
Responsable de traitement de données à caractère personnel	*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*
Signature électronique	*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*

2. DOCUMENTS DE REFERENCE

Le référentiel « Force Probante » est basé sur un ensemble de documents des domaines juridique, technique et de sécurité des systèmes d'information.

2.1. Cadre juridique

Dans le domaine de la santé, des références juridiques générales sont données dans la **[PGSSI-S]**. Le référentiel « Force Probante » répond aux articles suivants du code de la santé publique :

- Articles L. 1111-25 à 31 issus de l'ordonnance n°2017-29 du 12 janvier 2017 : Ces articles fixent les conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel, et aborde notamment le cas de la numérisation en vue d'obtenir une copie fiable.

Ces articles renvoient aux dispositions du Code civil :

- Article 1366 du Code civil – Cet article traite de la force probante de l'écrit électronique
- Alinéa 2 de l'article 1367 du Code civil – Cet article traite de la signature électronique
- Article 1368 du Code civil – Cet article traite du conflit de preuve
- Article 1379 du Code civil – Cet article traite de la copie
- Décret n° 2016-1673 du 5 décembre 2016 : Ce décret définit les conditions permettant de présumer de la fiabilité d'une copie numérique en application de l'article 1379 du Code civil
- Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique

Concernant les services de confiance et la force probante, les textes suivants s'appliquent :

- Règlement européen **[eIDAS]** (Règlement (UE) n° 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014) : Ce règlement définit des exigences de sécurité applicables aux services de confiance (dont l'horodatage), en particulier les services qualifiés associés à la présomption de fiabilité des copies numériques
- Décision d'exécution 2015/1506 du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement 910/2014.
- Directive dite NIS[1] (Network and Information Security)

La protection des données à caractère personnel est encadrée par la loi française et européenne :

- Loi « informatique et libertés » **[CNIL]** : Cette loi règlemente la création et le traitement des fichiers contenant des données à caractère personnel. La loi n°2018-493 promulguée le 21 juin 2018 a modifié le texte de loi pour tenir compte du **[RGPD]**
- **[RGPD]** : Le Règlement Général sur la Protection des Données est un règlement européen ayant force de loi en France, et encadrant la protection des données à caractère personnel. Ce règlement est entré en application le 25 mai 2018

Des règles spécifiques sont prévues pour les données de santé. Il existe en outre une réglementation propre aux données de santé en droit européen et des règles spécifiques relevant du droit interne :

[1] Directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'union

- Directive relative aux soins transfrontaliers[2]
- Code de la santé publique (télémédecine, INS, secret / équipe de soins / échange et partage des données de santé, hébergement des données de santé, etc.)
- Code de l'action sociale et des familles (les dernières lois de santé dont la loi de 2016 ayant concouru au décloisonnement entre ce secteur et le secteur sanitaire)
- Code de la sécurité sociale (rôle et mission de la CNAM dans la gestion des remboursements des soins dispensés aux assurés, en tant que responsable de traitement du DMP, rôle et missions de la Haute Autorité de Santé, etc.)

Pour les documents appartenant au périmètre des archives publiques :

- la destruction du document d'origine au format papier après sa numérisation est encadrée par le code du patrimoine :
  - Champ des archives publiques : Article L.211-4
  - Autorisation de destruction après visa de l'administration des archives : Article L.212-3
- l'hébergement de données de santé à caractère personnel est encadré par le code de la santé publique :
  - Articles L1111-8, R1111-9 à R1111-15-1 et R1111-16
- Les agréments autorisant le tiers archivage d'archives publiques :
  - Décret 2020-733 du 15 juin 2020 relatif à la déconcentration des décisions individuelles dans le domaine de la culture

2.2. Référentiel de sécurité

Tous les SI santé faisant partie du périmètre décrit dans l'article L.1110-4-1 du code de la santé publique sont soumis à la **[PGSSI-S]**. Le corpus documentaire de la **[PGSSI-S]** se décline en un ensemble de documents à consulter sur le site de l'Agence du Numérique en Santé. On peut notamment citer les référentiels suivants :

- Référentiels d'identification et d'authentification des acteurs de santé qui fixe les bonnes pratiques à respecter sur ces thématiques (cf. §3.3) ;
- Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé ;
- Référentiel d'imputabilité : il définit les moyens utilisables afin d'assurer l'imputabilité des actions réalisées dans un système d'information santé. De nombreux concepts propres à garantir la force probante des documents sont développés au sein de ce document.

La PSSI-MCAS **[document de référence n°7]** constitue également un cadre aidant les porteurs de projet dans la définition des niveaux de sécurité attendus.

Le Référentiel Général de Sécurité émis par l'**[ANSSI]** contient des directives applicables dans le cadre de ce référentiel, notamment les directives en matière de mécanismes cryptographiques **[document de référence n°8]**.

[2] Directive 2011/24/UE du parlement européen et du conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers et les textes de transposition :

- Décret n° 2013-1216 du 23 décembre 2013 relatif à la reconnaissance des prescriptions médicales établies dans un autre Etat membre de l'Union européenne
- LOI n° 2014-201 du 24 février 2014 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la santé
- Décret n° 2014-1525 du 17 décembre 2014 relatif à la reconnaissance des prescriptions de dispositifs médicaux établies dans un autre Etat membre de l'Union européenne

2.3. Référentiel technique

L'ensemble des normes citées ci-dessous sont à utiliser dans leur dernière version en date (révision la plus récente publiée).

Le règlement **[eIDAS]** fait appel à des normes et à des rapports techniques de l'ETSI pour sa déclinaison technique et organisationnelle, en particulier :

- ETSI TR 119 000 V1.2.1 : Electronic Signatures and Infrastructures (ESI) - The framework for standardization of signatures: overview. Introduction aux documents du référentiel ETSI concernant la signature électronique
- ETSI EN 319 132 : **[XAdES]** digital signatures. Cette norme spécifie le format de signature **[XAdES]** pour les documents XML
- ETSI EN 319 142 : **[PAdES]** digital signatures. Cette norme spécifie le format de signature **[PAdES]** pour les documents PDF

Des normes AFNOR s'appliquent à la conservation de documents et à leur numérisation :

- Norme NF Z42-013 : Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes. Cette norme, non obligatoire, s'applique aux Système d'Archivage Electroniques **[SAE]**. La conformité à cette norme fait l'objet de la certification AFNOR NF461 « Systèmes d'archivage électronique ».
- Norme NF Z42-026 : Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations. Cette norme, non obligatoire, décrit des mesures de sécurité applicables à un processus de numérisation visant la possibilité de destruction des documents d'origine papier. La conformité à cette norme fait l'objet de la certification AFNOR NF544 « Service-Prestation de numérisation fidèle ».

2.4. Référentiel d'interopérabilité

L'Agence du Numérique en Santé maintient un cadre d'interopérabilité pour les systèmes d'information de santé nommé **[CI-SIS]**, disponible sur son site.

Le volet de structuration minimale de documents de santé doit notamment être suivi par tout acteur de santé, suivi social ou médico-social dans le cadre de l'élaboration de documents. L'annexe 5 de ce référentiel, qui traite de l'usage des métadonnées liées à la force probante fait notamment référence à ce document.

3. PRINCIPES TECHNIQUES ET ORGANISATIONNELS

3.1. Mesures organisationnelles

Tous les cas d'usage du référentiel Force Probante nécessitent en premier lieu une phase projet de définition et d'implémentation du processus. Durant cette phase, un responsable est chargé de prendre en compte les aspects métier, technique, juridique, organisationnel du projet pour aboutir à la solution la plus pertinente en fonction de l'environnement. Ce rôle est nommé « responsable de traitement » dans les annexes du référentiel. Il fait appel à des spécialistes de chacun des domaines si nécessaire, et s'appuie sur une analyse de risques pour effectuer ses choix.

Une fois le processus défini, son utilisation et son exploitation par les acteurs de santé doivent aussi être placées sous la responsabilité d'un comité de pilotage s'assurant du respect des mesures décidées en phase projet, et de l'évolution du processus dans le temps. Ce comité de pilotage doit faire auditer régulièrement les pratiques afin de mettre en place si besoin les mesures correctrices nécessaires.

3.2. Documentation des processus

Conformément à l'article L.1111-30 du code de la santé publique, une documentation des processus doit être établie et mise à la disposition des personnes prises en charge et des professionnels de santé.

Cette documentation doit permettre de comprendre les mesures juridiques, techniques et organisationnelles mises en œuvre pour assurer la sécurité des processus. Elle doit être rédigée de façon claire pour les personnes prises en charge et les professionnels de santé et ne nécessiter aucune connaissance technique ou réglementaire préalable. Ils doivent pouvoir obtenir facilement cette documentation (quel que soit son format).

La documentation des processus inclut notamment les informations relatives au dossier de preuve et il est recommandé qu'elle précise la durée de conservation des traces. Elle doit être conservée aussi longtemps que les documents qu'elle concerne. Elle peut utilement être mentionnée dans la convention de preuve, s'il en existe une.

En pratique, il n'est pas attendu de chaque acteur local de produire lui-même cette documentation concernant les services mis en œuvre qui sont mutualisés par des opérateurs de services nationaux, voire internationaux. Aussi, et dans le cas où les moyens mis en œuvre sont effectivement opérés par des tiers (fournisseurs, agences publiques), il leur appartiendra néanmoins de :

- **S'assurer que leurs fournisseurs de services de dématérialisation, numérisation (à titre d'exemples) disposent de cette documentation**, en ligne (exemple : Politique de Signature électronique, Politique d'Archivage électronique) ;
- **Indiquer dans les conditions d'usage (CGU) de leur solution les documents de référence applicables** (généralement en référençant le numéro du document applicable, son OID le cas échéant, au sein de ces conditions d'usage) ;
- **Veiller, par l'utilisation de clauses contractuelles, à ce que ces documents soient conservés par le fournisseur en ligne**, et par prudence, en sus, **collecter et conserver chaque nouvelle version de ces documents de référence** (en cas de défaillance du fournisseur par exemple).

A défaut d'usage de services tiers, non mutualisés (ex : mise en œuvre d'un service spécifique, dédié, en interne), **il appartiendra à son responsable de traitement d'assurer lui-même la production de la documentation associée**, et sa publication (selon les mêmes principes et obligations que ceux qu'il exigerait de son fournisseur).

3.3. Sécurité physique

Les mesures de sécurité physique doivent considérer les risques de vol, d'altération ou de divulgation d'informations imprimées sur documents papier, qui sont des risques différents de la seule protection des données informatiques. Ceci doit être pris en compte pour tous les aspects de la sécurité physique :

- Contrôle d'accès ;
- Détection d'intrusion ;
- Détection et extinction d'incendie ;
- Détection et prévention des risques associés aux dégâts des eaux ;
- Détection et prévention des risques liés aux rongeurs et autres nuisibles.

3.4. Identification et authentification des acteurs

Un processus de gestion de documents fait intervenir en général plusieurs acteurs. Dans une optique de contrôle d'habilitation et de production d'éléments de preuves, ces acteurs doivent être identifiés et authentifiés par des moyens adaptés. Ces mécanismes de sécurité doivent être définis pendant la phase de conception du processus. Les référentiels d'identification et d'authentification de la **[PGSSI-S]** (cf. §2.2) doivent être utilisés en l'absence de directives particulières dans le référentiel Force Probante.

En exploitation, les authentifications réussies ou en échec doivent être tracées à titre de preuve ou d'analyse des incidents de sécurité.

Les principes d'identitovigilance doivent être respectés dans le cadre de la prise en charge des patients. Les bonnes pratiques conformes à l'état de l'art en la matière sont à appliquer.

3.5. Traçabilité des opérations

Les traces des opérations réalisées constituent un facteur important pour le renforcement de la force probante, lorsqu'il s'agit d'apporter des éléments de preuve en cas de litige. Ces éléments sont donc à ajouter au dossier de preuve du document ou de la donnée.

La mise en place de la traçabilité est une règle générale à appliquer quel que soit le cas d'usage. Toutes les directives en la matière sont décrites au sein du référentiel d'imputabilité de la **[PGSSI-S]** (cf. §2.2).

Dans le cadre du présent référentiel, les opérations à journaliser sont au minimum celles qui impactent le contenu du document et ses effets juridiques, en particulier :

- Constitution du document par saisie de formulaire, import ou réception de données depuis un autre système, numérisation ;
- Conversion ou transformation du document : changement de format, insertion ou manipulation dans un document **[CDA]** ;
- Connexion (et éventuelle authentification) du signataire à l'application ou au service de signature ;
- Validation, approbation (ou consentement) d'un document par une personne physique ou morale ;
- Apposition d'une signature sur le document, quel que soit le niveau ;
- Remise ou transfert du document vers un patient ou un autre système ou entité juridique ;
- Stockage, déplacement, destruction du document papier ou électronique.

D'autres opérations ayant un impact juridique sur le document doivent être tracées en fonction du processus considéré et des risques techniques et juridiques identifiés lors de la conception de celui-ci.

Les traces doivent être conservées au moins aussi longtemps et dans les mêmes conditions que le document sur lequel elles portent. Lorsqu'elles sont susceptibles de contenir des données à caractère personnel, des précautions

particulières doivent être prises pour garantir leur confidentialité pendant la durée de conservation, puis pour les détruire une fois cette durée atteinte.

3.6. Mécanismes cryptographiques

Des mécanismes cryptographiques sont utilisés :

- Pour l'authentification de personnes physiques ou de systèmes (par exemple des certificats numériques) ;
- Pour le calcul d'empreintes numériques ;
- Pour la signature électronique de données (signature de personne physique ou morale);
- Pour le chiffrement de données.

Les mécanismes cryptographiques sont définis à un instant t pour présenter une résistance adaptée au potentiel d'un attaquant considéré, tout en étant accessibles et performants pour les utilisateurs.

Le choix des mécanismes de sécurité doit être réalisé en se conformant au **[RGS]** en vigueur, plus spécifiquement en suivant l'annexe B1 pour ce qui concerne la version v2 **[document de référence n°8]**.

Une veille de sécurité doit être menée par la structure qui met en œuvre des mécanismes cryptographiques afin de s'assurer que les mécanismes choisis à une date t sont toujours recommandés et suffisants pour les risques attachés au processus considéré. Lorsqu'une obsolescence est détectée, des mécanismes de sécurité plus récents et plus robustes sont à appliquer.

Pour le choix des autorités de certification, on se réfèrera au référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé de la **[PGSSI-S]** (sauf pour le cas du palier 3 de la numérisation de document **[document de référence n°3]**).

3.7. Recours à des prestataires externes

Le présent paragraphe rappelle quelques mesures de sécurité générales à appliquer lorsqu'un établissement fait appel à un prestataire externe pour réaliser tout ou partie d'une fonction détaillée dans ce référentiel. Les mesures présentées n'ont pas vocation à être exhaustives, mais évitent de répéter ces mesures générales qui peuvent s'appliquer sur chacune des annexes.

Un premier principe important est que, même en cas de sous-traitance complète d'une fonction, par exemple la numérisation ou l'archivage, l'établissement reste entièrement responsable des traitements exécutés, que ce soit d'un point de vue juridique, fonctionnel ou de sécurité. Une sélection attentive des prestataires est nécessaire, ainsi qu'un contrôle régulier (via des résultats d'audits déjà passés par le prestataire ou exigés expressément).

De ce fait, il convient de veiller à ce que les éventuels fournisseurs de services intervenant dans le cadre des activités décrites par le référentiel s'engagent à respecter les conditions de sécurité associées. En premier lieu, il est nécessaire de maîtriser les risques relatifs à l'infogérance en exigeant des fournisseurs tiers de produire une « Politique d'Assurance Sécurité » adaptée au contexte. Ensuite, il faut lister toutes les exigences de sécurité associées à une activité et identifier celles à reporter sur le prestataire, en fonction du périmètre pris en charge par celui-ci dans l'activité.

Etant donné le sujet traité par ce référentiel, deux problématiques sont notamment à adresser :

- La capacité du prestataire à manipuler des données de santé à caractère personnel. Une certification HDS (Hébergeur de Données de Santé) est obligatoire voire un agrément du Ministère de la Culture dans le cas spécifique où les données de santé concernées constituent une archive publique (se référer au §2.1 concernant le cadre juridique) ;
- Le respect du RGPD, le prestataire étant un sous-traitant du traitement des données à caractère personnel (potentiellement un cotraitant dans le cadre d'échanges de données entre des établissements de santé). Le respect des exigences induites se doit d'être contractualisé avec le prestataire.

Selon la fonction sous-traitée et le niveau de sécurité associé au palier choisi, d'autres exigences peuvent être imposées ou prises en considération, par exemple :

- La certification ISO 27001 du prestataire sur le périmètre des fonctions sous-traitées ;
- La qualification eIDAS pour le service approvisionné ;
- La certification de conformité du tiers archiveur à la norme NF Z 42-013 et son équivalent international ISO 14641-1 (certification Afnor N461 par exemple).

Ces indications sont à compléter dans tous les cas par les résultats de l'analyse de risque (cf. §3.1) associée aux traitements effectués.

3.8. Principe de transitivité de la force probante

Lorsqu'un document est produit par une structure de santé et remis à un individu (personne prise en charge, acteur sanitaire ou médico-social ou autre) ou une personne morale, il conserve un niveau de force probante identique lors d'un transfert à un tiers. C'est-à-dire que si l'individu ou la personne morale transmet ensuite le document à un tiers sans le modifier et en respectant les principes décrits au sein de ce référentiel, le document conserve son niveau de force probante initial.

3.9. Gestion des archives publiques

Certains documents de santé peuvent constituer des archives publiques et peuvent à ce titre être soumis à des règles spécifiques concernant tout ou partie de leur cycle de vie.

Il est donc essentiel pour toute structure de santé d'identifier, parmi l'ensemble des documents de santé sous sa responsabilité, ceux qui appartiennent au champ des archives publiques (voir §2.1 cadre juridique pour les articles du code du patrimoine).

Il est notamment essentiel d'assurer :

- La conservation de ces documents par des prestataires bénéficiant d'un agrément du Ministère de la culture pour la conservation d'archives publiques courantes et intermédiaires sur support numérique (la liste des prestataires agréés est consultable sur le portail national des archives francearchives.fr) ;
- La destruction de ces documents uniquement après visa de l'administration des archives suivant la procédure prévue au code du patrimoine (cf. §2.1 cadre juridique).

4. GLOSSAIRE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information Santé
CDA	Clinical Document Architecture
CNIL	Commission Nationale de l'Informatique et des Libertés
eIDAS	electronic IDentification, Authentication and trust Services
HDS	Hébergement de Données de Santé
IGC	Infrastructure de Gestion de Clés
PAdES	PDF Advanced Electronic Signature
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information Santé
RGPD	Règlement Général de Protection des Données
RGS	Référentiel Général de Sécurité
SAE	Système d'Archivage Electronique
SIAF	Service Interministériel des Archives de France
XAdES	XML Advanced Electronic Signature

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

AGENCE DU NUMÉRIQUE EN SANTÉ

Agence du Numérique en Santé
01 58 45 32 50
9, rue Georges Pitard
75015 PARIS