RÉSEAU présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

Dématérialisation et signature électronique en SPSTI
Synthèse du référentiel de l'ANS
« *Force probante des documents de santé* »

La numérisation des documents en SPSTI est largement utilisée pour moderniser la gestion de l'information et assurer le suivi des entreprises et de leurs salariés.

Le référentiel « ***Force probante des documents de santé*** », élaboré par l'Agence du Numérique en Santé (ANS) établit des normes strictes pour garantir la force probante des documents numérisés.

La Commission Système d'Information de Présanse a fait l'analyse de ce référentiel et met à la disposition des SPSTI, qui sont invités à se mettre en conformité avec le référentiel pour toute prestation de dématérialisation, cette synthèse de son contenu ainsi qu'un diaporama illustrant les points saillants à mettre en œuvre en SPSTI.
Les acronymes figurant dans ce document sont explicités en dernière page.

Objet et périmètre

Le référentiel « ***Force probante des documents de santé*** » se compose d'un document introductif et de six annexes et s'applique à toutes les structures du secteur santé-social et donc aux SPSTI.

Il a pour objet de répondre aux enjeux posés par la dématérialisation des documents papier et de leur validité et leur opposabilité, ainsi que de fixer des règles et mécanismes à respecter pour qu'un document ait une force probante.

Le référentiel aborde trois aspects, **la numérisation** des documents papier, **la matérialisation** des documents de santé numériques et **la création de documents nativement au format numérique**.

Force probante d'un document de santé

Pour avoir une **force probante**, un document doit **répondre au règlement européen eIDAS** ou à défaut il convient d'**apporter**, dans le cadre d'une procédure, **la preuve de la fiabilité des dispositifs**.

Ainsi, il est possible de mettre en place une **convention de preuve** qui décrit la répartition des rôles et moyens mis en œuvre pour produire le document, les process de mise à disposition et de conservation, les règles de preuve, ainsi que les conditions de règlement des conflits portant sur la valeur probatoire d'un document échangé.

Dématérialisation et signature électronique en SPSTI
Synthèse du référentiel de l'ANS
« *Force probante des documents de santé* »

Principes généraux et organisationnels

Un socle commun de principes techniques et organisationnels y est décrit et plusieurs annexes détaillent en fonction des traitements les :

1. mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation, (*DMST papier par exemple*) ;
2. mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques, (*avis d'aptitude par exemple ou DMST numérique*) ;
3. mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation de documents de santé numériques (*impression d'un extrait d'un DMST par exemple*).

Les principes généraux relatifs aux documents numériques sont :

- D'assurer la sécurité des processus de numérisation (recommandation de l'ANSSI : PSSI-MCAS).
- D'adapter les moyens aux enjeux par une analyse de risque.
- De prendre en compte les risques juridiques propres au contexte des SPSTI.
- D'utiliser les services labélisés par l'ANSSI ou à défaut permettant de conserver le caractère original d'un document.
- De respecter un socle de principes techniques et organisationnels.

Parmi les points à retenir, il faut prendre en compte des prérequis que sont le **respect des référentiels de sécurité** (PGSSI-S, PSSI-MCAS…), **techniques** (normes eIDAS et AFNOR) et **d'interopérabilité** (CI-SIS).

En termes d'organisation, il convient de **mettre en place une organisation et d'en assurer le suivi, de disposer d'une documentation des processus** à disposition des personnes prises en charge et d'**assurer la sécurité physique des données**.

D'un point de vue technique, il faut pouvoir **identifier et authentifier les acteurs**, **mettre en place des mesures garantissant la traçabilité et des mécanismes cryptographiques**.

En cas de **recours à des prestataires externes**, ceux-ci sont entièrement responsables des traitements et doivent respecter le référentiel et le RGPD. Des contrôles réguliers doivent donc être faits.

Formats des métadonnées

Il est recommandé que les métadonnées soient **au format CDA R2** (obligatoire pour le DMP) **ou au format PDF/A** (archive).

Lorsqu'un document est produit nativement au format numérique, les métadonnées concernent le type de document, son titre, sa date de création, un identifiant unique, l'auteur et la personne morale (SPSTI), ainsi que l'identification de la personne prise en charge et des métadonnées de signature.

Dans le cas d'une numérisation, les métadonnées concernant le document d'origine sont les mêmes, auxquelles s'ajoutent des données de numérisation (identifiant unique, auteur, personne morale, date, lot de numérisation, lieu, dispositif de numérisation).

Pour la matérialisation, il convient d'ajouter au document papier des métadonnées rattachées.

Dématérialisation et signature électronique en SPSTI
Synthèse du référentiel de l'ANS
« *Force probante des documents de santé* »

Catégories des documents numérisés et paliers de sécurité

Le référentiel décrit trois catégories de documents auxquelles sont attachées des paliers minimums à mettre en œuvre :

- Expression de la volonté du patient – **Palier 3** (copie fiable (copie conforme aux exigences du décret n°2016-1673)).
- Information communiquée par la personne prise en charge – **Palier 1** (copie simple (numérisation simple respectant au minimum les impératifs de l'identitovigilance et de la protection des données personnelles)).
- Autre document du périmètre (traitement par défaut) – **Palier 2** (copie sécurisée (numérisation dans des conditions maîtrisées d'intégrité et de traçabilité suffisantes pour pouvoir détruire le document original)).

Mécanismes de sécurité dans le cadre de la numérisation

En Santé au travail, les documents numérisés produits et utilisés **ne semblent être concernés que par les paliers 1** (pour les documents non originaux, par exemple les copies apportées par un salarié) **et 2** (pour les documents originaux et nécessitant une intégration dans les logiciels métiers). Le palier 3 pourrait être appliqué pour les documents originaux nécessitant un archivage sur le long terme mais sans lien avec le logiciel métier (par exemple, les dossiers numérisés).

Le choix du palier dépend du cadre juridique du document d'origine, de la réalisation de la numérisation et de l'usage qui en est fait (conservation longue (palier 2), copie intégrée au système d'information (palier 2), destruction de l'original (palier 3). C'est le responsable du traitement qui définit le palier à prendre en compte pour un document donné. Ce palier influe sur la conception et la documentation du processus, la numérisation et le contrôle, la protection de l'intégrité de la copie numérique et sa conservation et le traitement du document d'origine.
Des mesures de sécurités doivent en outre être mises en place.

Mécanismes de sécurité des documents nativement numériques

Pour les **documents nativement numériques**, une **signature numérique ou un cachet numérique** peut être apposé. En Santé au travail, la finalité de la signature électronique est la validation du contenu. Elle peut être simple (palier 1 : identifiant unique du document signé, date, nom et prénom du signataire), avancée (palier 2 : certificat numérique (signature simple avec scellement) ou qualifié (palier 3 : équivalente à une signature manuscrite par les moyens délivrées par l'ANSSI).

Le cachet numérique quant à lui a pour finalité de garantir l'origine et l'intégrité des données. Il est rattaché à une personne morale et dépend des mêmes niveaux de sécurité que la signature électronique.
En outre, le document doit être horodaté.

Mécanismes de sécurité pour la matérialisation des documents

Des mécanismes de sécurité doivent aussi être mis en œuvre pour la matérialisation des documents de santé numériques. La matérialisation consiste à créer un nouveau document à partir d'un ou plusieurs documents numériques sans en modifier le sens et le contenu.

Des **métadonnées peuvent y être ajoutées de même qu'une signature électronique** si aucun autre document n'est signé.

Comme pour les autres types de documents, des paliers existent. Le palier 1 correspond à une impression simple garantissant l'identitovigilance et la confidentialité des données. Pour le palier 2 est ajouté un cartouche et des métadonnées (identifiant unique, date de génération du document, nom de la structure qui constitue le document. Ce palier concerne notamment les dossiers médicaux. Le palier 3 nécessite la publication du document sur une plateforme, du type « *Mon espace santé* », permettant son contrôle.

Dossier de preuve

Le **dossier de preuve** attendu pour un document numérique doit contenir toutes les traces numériques ou papier retraçant le processus de signature, et il doit être consultable durant toute la période de conservation d'un document.
La **conservation** doit permettre de retrouver facilement le document, de garantir son intégrité (aucune modification ou altération) et son niveau de confidentialité.

Préconisations aux SPSTI

Il conviendra à chaque SPSTI :

- **D'exiger la conformité au référentiel** et aux références citées dans celui-ci (PGSSI-S, ...) pour toute prestation ou solution en lien avec la dématérialisation.
- **De documenter les processus de dématérialisation** dans les SPSTI – volet technico-organisationnel.
- **De définir des conventions de preuve** – volet technico-juridique.

Pour information : la numérisation d'un DMST réalisée par un organisme certifié devrait permettre que le document numérisé soit force probante et ainsi que le document papier soit détruit.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
L'ANSSI est l'autorité française en charge de la sécurité et de la défense des systèmes d'information.

CDA R2 : Clinical Document Architecture Release 2
Norme de l'HL7 (Health Level Seven International) utilisée pour la structuration, le formatage et l'échange des documents cliniques électroniques.

CI-SIS : Cadre d'Interopérabilité des Systèmes d'Information en Santé
Il s'agit d'un ensemble de normes, de protocoles, et de directives visant à assurer la communication, l'échange et l'utilisation harmonieuse des données entre différents systèmes d'information de santé

eIDAS : electronic IDentification, Authentication and trust Services
Cadre juridique adopté par l'Union européenne pour réguler l'identification électronique et les services de confiance pour les transactions électroniques renforçant la sécurité et la fiabilité des transactions électroniques entre les citoyens, les entreprises et les administrations publiques.

PDF/A : Portable Document Format for Archiving
Norme ISO (International Organization for Standardization), dérivé du format PDF (Portable Document Format) pour l'archivage de documents électroniques et la possible reproduction à l'identique indépendamment du logiciel et du matériel utilisés.

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé
Cadre de référence établi par l'Agence du Numérique en Santé (ANS), définissant les règles et les bonnes pratiques (confidentialité, intégrité et disponibilité des données) pour assurer la sécurité des systèmes d'information de santé.

PSSI-MCAS : Politique de Sécurité des Systèmes d'Information des ministères sociaux
Cadre de référence visant à garantir la sécurité des échanges et du stockage des informations de santé (messagerie sécurisée de santé).