

Référentiel Force Probante des documents de santé

Mécanismes de sécurité à
mettre en œuvre dans le cadre
de la numérisation

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 1 - Socle commun de principes techniques et organisationnels
3. Référence n° 3 : Référentiel Général de Sécurité V2 - Annexe B1 - Mécanismes cryptographiques (ANSSI)
[\[https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs\]](https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs)
4. Référence n° 4 : Référentiel Force Probante des documents de santé – Annexe 5 – Gestion des métadonnées
5. Référence n° 5 : Référentiel Force Probante des documents de santé – Annexe 6 – Classification des documents de santé

Historique du document

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

SOMMAIRE

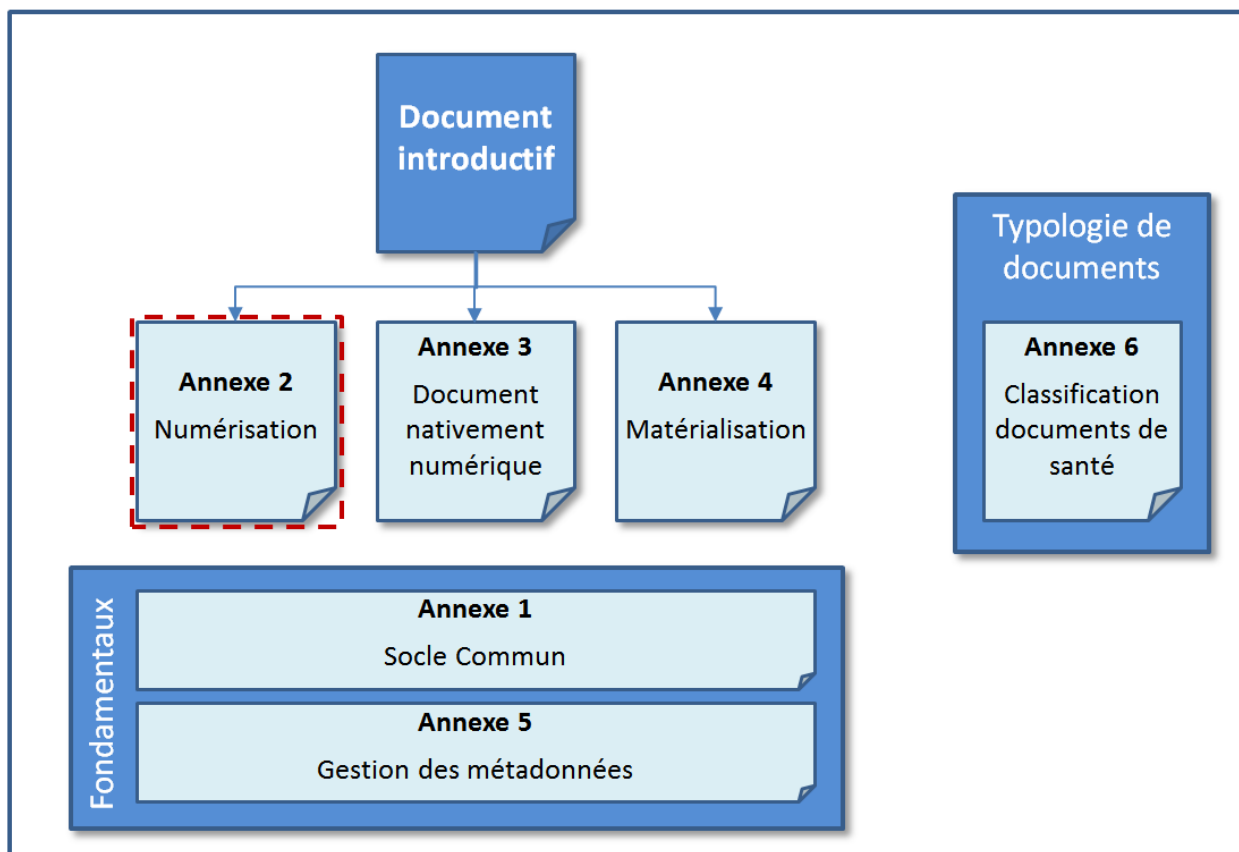
1. INTRODUCTION	4
1.1. Objet du document	4
1.2. Champ d'application	5
1.3. Enjeux et problématiques	5
2. PRINCIPES DE SECURITE DE LA NUMERISATION	6
2.1. Cas d'usage.....	6
2.2. Principes généraux du processus	6
2.3. Paliers associés au processus de numérisation	6
2.4. Choix du palier	7
3. MESURES DE SECURITE A METTRE EN ŒUVRE	9
3.1. Conception et documentation du processus	9
3.1.1. Introduction	9
3.1.2. Conception et documentation pour la copie numérique simple.....	9
3.1.3. Conception et documentation pour la copie numérique sécurisée.....	9
3.1.4. Conception et documentation pour la copie numérique fiable	10
3.2. Numérisation et contrôle	10
3.2.1. Introduction	10
3.2.2. Mesures de sécurité pour la copie numérique simple	11
3.2.3. Mesures de sécurité pour la copie numérique sécurisée	11
3.2.4. Mesures de sécurité pour la copie numérique fiable	13
3.3. Protection de l'intégrité de la copie numérique	14
3.3.1. Introduction	14
3.3.2. Mesures de sécurité pour la copie numérique simple	14
3.3.3. Mesures de sécurité pour la copie numérique sécurisée	14
3.3.4. Mesures de sécurité pour la copie numérique fiable.....	15
3.4. Conservation de la copie numérique.....	15
3.4.1. Introduction	15
3.4.2. Mesures de sécurité pour la copie numérique simple	16
3.4.3. Mesures de sécurité pour la copie numérique sécurisée	16
3.4.4. Mesures de sécurité pour la copie numérique fiable	17
3.5. Traitement du document d'origine	17
3.5.1. Introduction	17
3.5.2. Destruction des documents d'origine	18
4. SYNTHÈSE DES MESURES PAR PALIER	19

1. INTRODUCTION

1.1. Objet du document

Ce document a pour objectif de préciser les mesures de sécurité à appliquer lors de la création de la copie numérique d'un document comportant des données de santé à caractère personnel, processus nommé « numérisation » dans ce document. Vœux

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 (présent document) ;
 - Cas de la production de documents nativement au format numérique ;
 - Cas de la matérialisation (ou impression) de documents ;
- ▶ 2 annexes présentant les principes fondamentaux à appliquer quel que soit le cas d'usage rencontré
 - Socle de principes communs à mettre en œuvre **[document de référence n°2]** ;
 - Explications relatives à la gestion des métadonnées **[document de référence n°4]** ;
- ▶ 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°5]**.

L'objet de la présente annexe du référentiel est de définir des ensembles cohérents de règles de sécurité à appliquer à des processus de numérisation, selon différents paliers clairement identifiés. Le niveau d'exigence des règles est adapté aux enjeux liés à l'objectif de chacun des paliers définis.

Ce document s'adresse aux personnes impliquées dans la mise en œuvre d'un processus de numérisation. Il permet aux responsables de traitement d'identifier les mécanismes de sécurité exigés en fonction du palier requis.

1.2. Champ d'application

Le champ d'application de ce référentiel est précisé dans le document introductif du référentiel **[document de référence n° 1]**.

De façon générale, sont concernés tous les processus de numérisation 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. Enjeux et problématiques

Les enjeux et les problématiques de la numérisation de documents comportant des données de santé à caractère personnel sont rappelés dans le document introductif du référentiel **[document de référence n° 1]**.

2. PRINCIPES DE SECURITE DE LA NUMERISATION

2.1. Cas d'usage

La numérisation de document peut intervenir dans le cadre de besoins très variés (numérisation de courriers, de documents médicaux, de documents fournis ou signés par un patient...). Elle peut porter sur des flux de documents (documents entrants dans une structure de santé ou générés dans le cadre de la prise en charge d'une personne) ou sur des stocks de documents. L'opérateur de numérisation peut être une ressource interne ou externe.

Le responsable d'une opération de numérisation doit donc construire son processus en se basant sur l'objet et l'environnement de réalisation des copies numériques. Le présent document fournit à la fois un ensemble de règles de sécurité et des propositions de mise en œuvre pratique du procédé respectant ces règles.

Une opération de numérisation comprend plusieurs étapes qui sont présentées au paragraphe §2.2.

Afin que le responsable du traitement puisse adapter le niveau de sécurité du processus en fonction de son besoin, des paliers de sécurité sont définis au paragraphe §2.3.

Le choix du palier adéquat est à réaliser par le responsable du traitement selon les indications données au §2.4.

2.2. Principes généraux du processus

La réalisation de la copie numérique d'un document d'origine papier comprend plusieurs étapes successives :

- ▶ Conception et documentation du processus ;
- ▶ Numérisation (« scan ») et contrôle de la copie numérique ;
- ▶ Protection de l'intégrité de la copie numérique ;
- ▶ Conservation de la copie numérique, de la documentation du processus de production et de l'empreinte et des traces liées à la copie numérique ;
- ▶ Traitement (conservation, destruction) du document d'origine.

Toutes ces étapes sont décrites et associées à des exigences de sécurité pour chacun des paliers définis dans ce document.

Quel que soit le palier, l'identitovigilance et la protection des données de santé à caractère personnel doivent être respectées à chaque étape du processus et au-delà pendant toute la durée de vie des copies numériques. En particulier, des mesures de sécurité appropriées doivent traiter les risques portant sur l'identitovigilance dans le cadre de la numérisation en masse de documents. Les copies numériques produites, quel que soit le palier adopté, doivent être diffusées et stockées en respectant les mêmes exigences de sécurité qui s'appliquent aux documents originaux.

2.3. Paliers associés au processus de numérisation

La copie numérique fiable, telle que mentionnée dans l'article L.1111-26 du code de la santé publique qui renvoie vers le code civil (article 1379 alinéa 2) et son décret d'application (décret n° 2016-1673) est la seule copie numérique à bénéficier de la présomption de fiabilité. *Pour plus de détails, consulter le cadre juridique du socle commun du référentiel [document de référence n° 2].*

Les exigences relatives aux conditions de réalisation de cette copie fiable sont fortes et ne seront pas toujours réalisables ou pertinentes pour les cas d'usage recensés. C'est pourquoi ce référentiel définit un ensemble alternatif de mesures de sécurité capables de donner aussi un niveau de force probante acceptable pour la copie numérique et d'autoriser dans certains cas la destruction des originaux papiers dans le respect du cadre propre

aux documents comportant des données de santé (sans bénéficiaire toutefois de la présomption de fiabilité au sens du décret n° 2016-1673).

Ainsi des processus de numérisation sont présentés ci-dessous, avec un niveau de sécurité croissant selon 3 paliers :

- ▶ **Palier 1 : Copie numérique « simple »** : scan simple d'un document respectant au minimum les impératifs de l'identitovigilance et de la protection des données personnelles ;
- ▶ **Palier 2 : Copie numérique « sécurisée »** : numérisation d'un document réalisée dans des conditions maîtrisées, apportant des éléments d'intégrité et de traçabilité suffisants pour autoriser la destruction du document original, sans pour autant imposer la qualification du service de protection de l'intégrité ni la certification du service de conservation afin d'optimiser les coûts ;
- ▶ **Palier 3 : Copie numérique « fiable »** : réalisation d'une copie numérique conforme aux exigences du décret d'application pour la copie fiable stipulées par le code civil, bénéficiant de la présomption de fiabilité et autorisant la destruction de l'original. L'intérêt principal de ce palier est d'offrir toutes les garanties nécessaires sur le plan juridique puisque la copie numérique fiable a, selon la loi, une force probante identique à son original papier (cf. article 1379 du code civil).

Les contraintes associées à ces paliers sont exposées dans le chapitre 3 « Mesures de sécurité à mettre en œuvre » de ce document pour chaque opération. Elles touchent notamment aux aspects suivants :

- ▶ Degré de formalisation du processus ;
- ▶ Intégrité des données ;
- ▶ Confidentialité des documents ;
- ▶ Traçabilité des opérations ;
- ▶ Identitovigilance.

2.4. Choix du palier

L'annexe 6 du référentiel Force Probante traitant de la classification des documents de santé **[document de référence n° 5]** aide à identifier le palier minimum à sélectionner en fonction du type de document à numériser.

Des mesures complémentaires à ce palier peuvent également être mises en œuvre par le responsable de traitement s'il juge que cela est nécessaire. Les critères qu'il est notamment recommandé d'analyser sont les suivants :

- ▶ Contenu du document d'origine, en particulier quand un cadre juridique spécifique au cas d'usage métier s'applique ;
- ▶ Conditions de réalisation de la copie numérique (cf. tableau ci-dessous) :

Usage	Commentaires
Copie réalisée par le producteur du document d'origine	La copie est réalisée dans des conditions maîtrisées et par des personnes disposant aussi du document d'origine. Dans ce cas, et si aucun autre critère ne laisse présager d'un risque important concernant la copie, le palier identifié à l'aide de l'annexe 6 est suffisant.
Copie réalisée par une entité interne mutualisée (exemples : service des archives, secrétariat, etc.)	La gestion de la mise en œuvre de plusieurs processus de copie impose une rigueur accrue.
Copie réalisée par un prestataire externe	La protection de l'empreinte de la copie numérique renforce la confiance dans la copie produite (empreinte générée par le logiciel pilotant la numérisation dans des conditions de production dignes de confiance par exemple, cf. §3.3.2).

- Usage de la copie numérique : Le niveau de sécurité peut être adapté à l'objet de sa création (cf. tableau ci-dessous) ;

Usage	Commentaires
Copie conservée pour une période de temps relativement longue	Pour une copie numérique devant être utilisée sur une longue période (plusieurs mois), il est essentiel d'assurer la traçabilité du document (voir les recommandations de l'annexe 1 du présent référentiel [document de référence n°2]).
Copie intégrée dans le SI	Une copie numérique intégrée au SI doit être accompagnée de métadonnées permettant son classement et sa traçabilité. L'annexe 5 du présent référentiel [document de référence n° 4] et plus globalement le cadre d'interopérabilité des systèmes d'information en santé (CI-SIS) donnent des indications concernant le choix des métadonnées à utiliser.
Copie en vue de détruire le document d'origine papier	L'application du palier 3 doit être privilégiée. Le risque juridique doit bien entendu être considéré.

- Contraintes et risques juridiques attachés au document (cf. tableau ci-dessous) ;

Usage	Commentaires
Document d'origine tamponné par l'organisation réalisant la copie	Le cachet n'ayant pas force d'engagement de l'organisation (en tant que personne morale), on pourra s'en tenir au palier correspondant au type de document numérisé identifié dans l'annexe 6.
Document d'origine signé par un acteur de santé de l'organisation réalisant la copie	La copie numérique sécurisée est à considérer afin de conserver la valeur probante du document une fois sous forme numérique.
Document d'origine signé par un patient	La copie numérique sécurisée est à considérer afin de conserver la valeur probante du document une fois sous forme numérique.
Enjeu financier important	L'application du palier 3 (copie fiable) doit être privilégiée.

La liste ci-dessus n'est pas exhaustive. D'autres contraintes propres à l'environnement de réalisation de la copie ou aux documents de santé concernés peuvent amener à prendre des mesures de sécurité complémentaires. Il appartient donc au responsable du traitement, en coordination avec la direction des systèmes d'information concernée, de procéder à une analyse de risques s'il juge que cela est justifié.

Outre les mesures de sécurité correspondant au palier choisi et celles plus spécifiques au contexte décrites ci-dessus, il est indispensable de veiller au respect des recommandations plus générales citées dans l'annexe 1 du présent référentiel « Socle commun de principes techniques et organisationnels » **[document de référence n° 2]**.

3. MESURES DE SECURITE A METTRE EN ŒUVRE

3.1. Conception et documentation du processus

3.1.1. Introduction

Quel qu'il soit, le processus de numérisation doit être décrit formellement afin de garantir le respect des exigences de sécurité appropriées.

Dans le cadre de la mise en œuvre d'une copie numérique sécurisée ou fiable, le dispositif d'acquisition d'image doit être testé et le processus documenté dans son intégralité puis conservé aussi longtemps que la copie électronique produite.

La description du processus doit traiter :

- ▶ Des aspects techniques : identifier les matériels et logiciels à utiliser pour la numérisation, les tests et contrôles effectués, les solutions de garantie d'intégrité et de conservation des documents ;
- ▶ Des aspects organisationnels : identifier les acteurs du processus (internes et externes), les rôles et leurs prérequis, les relations et interactions entre les acteurs ;
- ▶ De la sécurité : présenter les mesures de sécurité logique et physique concernant chaque phase du processus (contrôle d'accès, mécanisme de garantie de l'intégrité, de conservation...), notamment de la protection des données à caractère personnel ;
- ▶ De l'identitovigilance.

3.1.2. Conception et documentation pour la copie numérique simple

La documentation minimale relative à la numérisation doit rappeler :

- ▶ Le respect de la protection des données à caractère personnel, aussi bien pour le document papier que pour la copie numérique. Le document ne doit être communiqué qu'à des personnes autorisées à prendre connaissance des informations inscrites, puis conservé dans un espace sûr approprié pour le type de données concernées. Le responsable de traitement doit mener une analyse d'impact dans les conditions de l'article 35 du RGPD.
- ▶ Le respect des règles d'identitovigilance. Le responsable du traitement doit être tout particulièrement vigilant à cet aspect pour le cas de la numérisation de stocks de documents (par opposition à une numérisation d'un flux, effectuée au cours du processus métier). Des mesures doivent être prises pour éviter l'inversion ou la répliquation de données entre plusieurs documents traités simultanément ou à la suite.

Ces règles peuvent être par exemple intégrées dans une charte informatique, dans un document de bonnes pratiques générales ou bien dans un document plus approfondi sur la numérisation lorsque d'autres paliers sont mis en œuvre dans la même organisation.

3.1.3. Conception et documentation pour la copie numérique sécurisée

En phase de conception, la qualité des copies numériques produites doit être testée afin d'étalonner et de configurer correctement les dispositifs d'acquisition d'image. En phase d'exploitation, une vérification de la qualité de l'étalonnage doit être menée de façon régulière afin de détecter toute perte de qualité.

Les tests doivent envisager les différentes variations du document d'origine : nombre de pages variable, découpage à faire en plusieurs documents d'un ensemble de feuilles, mentions manuscrites susceptibles de se trouver sur le document, etc.

Les tests devraient prévoir des cas non nominaux (document d'origine incomplet, illisible...) ou des scans successifs d'un même document, afin de vérifier que le processus et les traces se déroulent de façon satisfaisante dans tous les cas.

D'autre part, la documentation du processus doit décrire au minimum :

- ▶ Le déroulement du processus dans son ensemble ;
- ▶ L'architecture technique matérielle (dispositifs d'acquisition d'image) et logicielle ;
- ▶ Les tests initiaux et les résultats de tests d'acquisition d'image ;
- ▶ Les formats et description des copies numériques et des métadonnées associées ;
- ▶ Les contrôles en production de la qualité du processus ;
- ▶ Le mécanisme de calcul et de protection de l'empreinte ;
- ▶ Les conditions de conservation de la copie numérique et des traces associées ;
- ▶ Les traces produites par le processus ;
- ▶ Le traitement ultérieur du document d'origine ;
- ▶ Les mesures de sécurité logique et physique de contrôle d'accès aux dispositifs de reproduction et de conservation.

Lorsque la numérisation est réalisée par une ressource externe, il est conseillé d'établir une convention de numérisation définissant l'objet de la prestation de numérisation, et précisant les différentes tâches, responsabilités et obligations des acteurs concernés (se reporter à la norme NF Z 42-026 dans sa dernière version pour sa rédaction). Lorsque le processus de numérisation est réalisé en interne, il est conseillé de s'inspirer du contenu type de cette convention pour définir les rôles et les responsabilités des différents intervenants.

La documentation doit être conservée aussi longtemps que les copies numériques produites.

3.1.4. Conception et documentation pour la copie numérique fiable

En plus des exigences décrites au §3.1.3, la documentation relative à l'appel d'un service d'horodatage qualifié ou d'un service de signature électronique qualifié doit figurer dans la description du processus de copie numérique fiable.

3.2. Numérisation et contrôle

3.2.1. Introduction

La production du document numérique est la première étape du processus. Au-delà d'une simple génération d'image, cette opération comprend plusieurs tâches :

- ▶ Vérification du document d'origine et préparation du lot pour numérisation ;
- ▶ Acquisition de l'image ;
- ▶ Association de métadonnées à la copie numérique ;
- ▶ Contrôle de la copie numérique produite ;
- ▶ Production de traces des opérations ;
- ▶ Formatage du document numérique.

Dans ce référentiel, la reproduction « à l'identique de la forme et du contenu » est comprise comme étant la production d'une copie numérique **considérée visuellement identique, par une personne physique, au document d'origine**. C'est la définition de la fidélité « formelle » présentée dans la norme NF Z 42-026.

3.2.2. Mesures de sécurité pour la copie numérique simple

L'étape de numérisation pour la production d'une copie numérique simple se limite aux deux premières tâches mentionnées dans l'introduction :

- ▶ Vérification de la qualité et du type de document : Il s'agit de s'assurer que la réalisation d'une copie et surtout de la diffusion de cette copie sont bien autorisées et qu'elles ne présentent pas de risque non traité concernant la confidentialité des données et l'identitovigilance.
- ▶ Acquisition de l'image : le moyen et la configuration d'acquisition de l'image est libre. La personne réalisant cette copie doit s'assurer que l'image produite satisfera aux besoins pour lesquels elle est réalisée. Le format de l'image est aussi laissé à l'appréciation du producteur de la copie, sous réserve d'assurer la lisibilité et la pérennité du document sur la durée prévue de conservation.

Afin de respecter l'identitovigilance, il est conseillé de vérifier que la copie produite porte les informations nécessaires de façon lisible, sans risque d'erreur d'utilisation.

3.2.3. Mesures de sécurité pour la copie numérique sécurisée

L'étape de numérisation pour la production d'une copie numérique sécurisée doit comprendre toutes les tâches mentionnées dans l'introduction.

3.2.3.1. Vérification et préparation du document d'origine

La vérification de la qualité et du type de document a les mêmes objectifs que pour la copie simple.

Il faut de plus veiller à ce que le document d'origine ne soit pas modifié avant sa numérisation par l'ajout d'annotations directement inscrites sur le document ou superposées (type post-it, étiquettes...). L'apposition d'étiquette sur le document d'origine avec des informations d'identification à des fins d'archivage (système d'archivage avec étiquette QR code par exemple), est tolérée avant la numérisation à condition qu'aucune information ne soit masquée par l'étiquette sur le document à numériser.

3.2.3.2. Acquisition de l'image

Afin de produire des copies numériques susceptibles d'avoir la même valeur probante que les documents d'origine, le matériel d'acquisition de l'image doit avoir été validé en amont et doit être configuré selon les préconisations préétablies. En particulier :

- ▶ La résolution conseillée est de 300 dpi au minimum. Ceci permet dans la majorité des cas de reproduire le document en assurant une apparence visuelle identique au document d'origine.
- ▶ Les couleurs du document d'origine ne doivent pas être altérées. Ceci veut dire qu'un document en noir et blanc peut être numérisé en noir et blanc ou préférentiellement en niveau de gris (sur 8 bits par pixel par exemple) pour augmenter la qualité de l'image. Un document d'origine comportant des couleurs (ne serait-ce qu'un logo ou une mention manuscrite ajoutée en couleur) doit être numérisé en mode couleur (24 bits par pixel).

La majorité des scanners ou photocopieurs répondent aux minimas techniques cités ci-dessus. Ils peuvent donc être tous utilisés dans la mesure où ils répondent aussi à des critères de sécurité logique et physique, qui devront être précisés dans la description du processus :

- ▶ Liste ou critères d'identification de modèles admis : Pour assurer la qualité, des tests ont pu être passés sur certains matériels et seuls ceux-là sont autorisés pour garantir la fidélité des numérisations ;
- ▶ Emplacement physique : Pour garantir la confidentialité, des lieux spécifiques ou une liste de matériels peuvent être définis pour réaliser la numérisation ;
- ▶ Diffusion de la copie numérique : Toujours pour la confidentialité, la méthode de mise à disposition de l'image peut être restreinte : envoi par messagerie sécurisée de santé, dépôt dans un espace sécurisé personnel ou à accès restreint.

- Conservation de la copie par le dispositif d'acquisition : Certains scanners ou photocopieurs conservent en mémoire interne tous les documents numérisés. Si tel est le cas, et qu'aucune mesure ne permette de pallier le risque de fuite des données, alors ces dispositifs doivent être exclus des procédés de numérisation.

L'utilisation d'outils de type appareils photos, tablettes ou téléphones portables n'est pas recommandée, la qualité des images produites et la confidentialité des données ne pouvant être suffisamment garanties. Si toutefois l'utilisation de ces dispositifs ne peut être évitée, leur conformité aux recommandations de sécurité de l'ANSSI (« recommandations de sécurité relatives aux ordiphones » DAT-NT-010/ANSSI/SDE/NP notamment) ainsi qu'aux directives RGPD est requise. Les tests effectués ainsi que le processus de numérisation défini (cf. §3.1.3) doivent alors permettre de garantir la qualité des images produites et d'assurer l'absence de risque de fuite des données conservées en mémoire ou transférées.

Suite à l'acquisition d'image, des corrections d'image peuvent être effectuées dans la mesure où elles contribuent à la fidélité du document ou à sa lisibilité : redressement, suppression de points parasites, amélioration du contraste... Dans ce cas, ces traitements doivent impérativement être réalisés avant la protection en intégrité de la copie numérique.

3.2.3.3. Association de métadonnées à la copie numérique

Des métadonnées doivent être associées à une copie numérique, au minimum la date de réalisation de la copie numérique. Certaines valeurs de ces métadonnées peuvent être obtenues par une reconnaissance optique des caractères (ou « océrisation », du terme anglais OCR pour Optical Character Recognition) effectuée sur tout ou partie des documents numérisés. Les informations lues par cette technique, au-delà d'améliorer la traçabilité et de permettre des recherches sur les métadonnées, pourront aussi être reformatées et réimprimées en cas de rematérialisation du document.

Selon le document et le processus, les métadonnées pertinentes peuvent différer mais il est recommandé qu'elles comprennent :

- Métadonnées propres au document d'origine :
 - Type de document ;
 - Titre, date, identifiant unique du document ;
 - Auteur du document d'origine ;
 - Organisation émettrice du document ;
 - Information d'identification du patient ;
- Métadonnées propres à l'opération de copie :
 - Date de numérisation (donnée obligatoire) ;
 - Nom d'un lot ou d'une opération de numérisation ;
 - Lieu de réalisation de la numérisation ;
 - Dispositif de numérisation.

Toutes les informations relatives à la gestion de ces métadonnées (format à utiliser notamment) sont précisées dans l'annexe 5 du présent référentiel **[document de référence n° 4]**. Les métadonnées doivent être intégrées de préférence dans le document au format CDA qui sera le conteneur de la copie numérique.

Bien entendu, le responsable de traitement est libre d'ajouter au document toute autre métadonnée décrite au sein du cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) qu'il jugerait utile de faire figurer au vu du contexte de la numérisation en respectant les contraintes relatives à la réglementation RGPD.

3.2.3.4. Contrôle de copie numérique produite

La qualité des copies numériques doit être garantie par le processus, par des tests préalables du procédé, mais aussi par des contrôles sur les copies produites au cours du temps. Le type de contrôle peut fortement varier selon le cas d'usage et l'environnement de production, par exemple :

- Contrôle visuel d'un échantillon de documents par un opérateur ;
- Contrôle des métadonnées par rapport à des valeurs type attendues.

Les contrôles doivent vérifier en particulier la bonne reproduction des codes-barres, des Datamatrix, des tampons ainsi que des mentions et signatures manuscrites.

3.2.3.5. Production de traces des opérations

La traçabilité des opérations de création d'une copie numérique est un facteur important de la force probante en résultant. De manière générale, chaque étape du processus doit générer des traces indiquant :

- ▶ La désignation de l'opération réalisée ;
- ▶ La date et l'heure de l'opération ;
- ▶ La personne ou le système réalisant l'opération ;
- ▶ Le nom et le format du fichier représentant la copie numérique ;
- ▶ Le résultat (succès / échec) de l'opération ;
- ▶ Des commentaires ou données supplémentaires éventuels sur l'opération.

Les informations qui pourraient être indiquées dans ces traces sont par exemple :

- ▶ Vérification du document d'origine : Type de document reconnu ;
- ▶ Acquisition de l'image : Marque, modèle, identifiant du dispositif d'acquisition, paramètres de configuration ;
- ▶ Association de métadonnées à la copie numérique : Identification des métadonnées ajoutées ;
- ▶ Contrôle de copie numérique produite : Type de contrôles réalisés, résultats obtenus ;
- ▶ Formatage du document numérique : Format produit, nom du fichier...

Pour plus d'informations relatives à la traçabilité des opérations et sa mise en œuvre, se référer au chapitre correspondant de l'annexe 1 de ce référentiel **[document de référence n° 2]**.

3.2.3.6. Formatage de production des copies

Les copies numériques doivent être produites au format PDF/A de préférence, PDF à défaut. Le format PDF/A garantit la lisibilité du document sur le long terme, en incluant dans le fichier lui-même toutes les données nécessaires à sa restitution (polices de caractères par exemple). Ce format est cependant plus lourd et, notamment si la durée de conservation est inférieure à 10 ans, le format PDF peut être employé.

La copie numérique au format PDF ou PDF/A est de préférence encapsulée dans un document au format CDA contenant notamment les métadonnées associées. *Pour plus de détails relatifs à l'usage des métadonnées, se référer à l'annexe 5 du présent référentiel* **[document de référence n° 4]**.

3.2.3.7. Sécurité physique et logique

Les locaux abritant les matériels de numérisation et ceux de stockage temporaire ou de conservation des copies numériques doivent être sécurisés pour éviter toute perte, vol ou détérioration de documents, avant ou après leur numérisation.

Les réseaux informatiques et les machines (postes de travail et serveurs) doivent être protégés contre les risques numériques d'altération, de destruction ou de vol des copies numériques.

Les mesures de sécurité physique et logiques applicables sont décrites dans l'annexe 1 du présent référentiel **[document de référence n° 2]**.

3.2.4. Mesures de sécurité pour la copie numérique fiable

La phase de numérisation d'une copie numérique fiable diffère peu de celle d'une copie sécurisée.

Les contraintes supplémentaires sont :

- ▶ Métadonnées : Toutes les métadonnées proposées pour la copie numérique sécurisée doivent impérativement être ajoutées pour une copie numérique fiable (sauf si non applicable).

- ▶ Traces : Toutes les traces et toutes les informations listées pour la copie numérique sécurisée doivent obligatoirement être produites afin de renforcer le dossier de preuves attaché à une copie numérique. *Pour plus d'informations relatives à la traçabilité des opérations, se référer au socle commun [document de référence n° 2].*
- ▶ Formatage de production des copies : Les copies numériques doivent être produites au format PDF/A pour garantir la stabilité de la copie numérique et la lisibilité sur le long terme. Le document PDF ainsi obtenu doit être intégré dans un document au format CDA qui porte les métadonnées.

3.3. Protection de l'intégrité de la copie numérique

3.3.1. Introduction

L'intégrité de la copie numérique est attestée par le calcul et la conservation d'une empreinte électronique. Cette empreinte doit être produite dans les conditions décrites dans l'annexe 1 du présent référentiel (paragraphe dédié aux mécanismes cryptographiques) [document de référence n° 2]. L'utilisation d'un algorithme compatible avec les recommandations du RGS [document de référence n° 3] est notamment requis.

L'empreinte doit être calculée sur le document PDF constitué par la phase de numérisation et non sur le document au format CDA qui le contient.

3.3.2. Mesures de sécurité pour la copie numérique simple

Pour ce palier, le calcul de l'empreinte est considéré comme optionnel. L'intégrité de la copie numérique ne peut alors pas être démontrée, mais en cas de doute, l'accès à l'original sera toujours possible (la destruction du papier n'est pas permise pour ce palier).

Le calcul et le stockage de l'empreinte par un logiciel pilotant la numérisation peut cependant être un premier élément, permettant notamment le contrôle par le destinataire d'un document transmis.

3.3.3. Mesures de sécurité pour la copie numérique sécurisée

L'empreinte de la copie numérique produite doit être protégée par un cachet électronique de l'organisation. Le cachet, réalisé avec une clé privée cryptographique logicielle appartenant à l'organisation, scelle le document et permet de détecter toute modification ultérieure du document.

Le cachet peut être réalisé sur le document PDF issu de la numérisation en respectant le format PAdES ou être utilisé dans une attestation électronique PDF/A (ou respectivement XML) signée au format PAdES (respectivement XAdES) et comportant l'empreinte de la copie fiable et toutes les autres informations associées (traces, ...). Cette seconde approche permet également d'assurer l'intégrité du dossier de preuve.

Le certificat de cachet doit être demandé par l'organisation auprès de l'ANS. Le certificat à commander correspond à l'offre « Offre certificat logiciel ORG (Personne morale) » de l'IGC Santé, pour l'usage « SIGN ».

Les mesures de sécurité décrites par la politique d'émission de ces certificats de cachet doivent être mises en œuvre et auditées régulièrement. Si possible, le cachet est réalisé selon une politique de cachet validée, propre à la réalisation de la copie numérique sécurisée et indiquée dans le cachet réalisé. De cette façon, la copie numérique est clairement identifiée comme une copie numérique sécurisée, sans nécessiter de mention supplémentaire.

A noter qu'un certificat de personne physique pour l'usage « SIGN » délivré par l'Infrastructure de Gestion de Clés Santé (IGC Santé) peut également être utilisé pour le scellement du document. Cet usage n'est toutefois pas recommandé si la personne à l'origine du scellement n'est pas l'auteur du document.

3.3.4. Mesures de sécurité pour la copie numérique fiable

Le décret n° 2016-1673 impose de garantir l'intégrité de la copie numérique par une empreinte cryptographique, et indique explicitement comme solutions présumées fiables les services qualifiés au sens du règlement eIDAS :

- ▶ Horodatage qualifié ;
- ▶ Ou cachet serveur qualifié ;
- ▶ Ou signature électronique qualifiée.

Cette opération peut être réalisée directement sur la copie numérique ou bien sur une attestation au format PDF ou XML issue du processus de numérisation, en respectant le format standard de la signature avancée (PAdES ou XAdES).

La signature électronique qualifiée désigne une signature électronique réalisée par une personne physique avec un dispositif qualifié, ce qui exclut l'utilisation de la carte CPS. Par ailleurs, le procédé manuel rend difficilement envisageable en pratique la protection de chaque document par une action utilisateur.

La mise en œuvre en interne d'un service qualifié au sens eIDAS requiert à la fois des investissements matériels et humains importants. Il est donc recommandé de faire appel à un prestataire externe proposant ces services en mode SaaS (Software as a Service). Pour identifier ce type de fournisseur, il suffit de consulter la liste des prestataires qualifiés, établie par l'ANSSI et disponible sur son site (www.ssi.gouv.fr).

Contrairement au service d'horodatage, le service de cachet qualifié ne peut pas être qualifié au sens eIDAS. Le service doit utiliser un certificat de cachet qualifié et un dispositif matériel cryptographique qualifié. Lorsque ce service est fourni par un prestataire externe, son niveau de sécurité doit être avéré par un audit de sécurité.

Il est donc conseillé de s'orienter vers un service d'horodatage qualifié eIDAS, moins onéreux, apportant une datation plus sûre, et se trouvant directement présent et identifié dans la liste de confiance de l'ANSSI. Dans le cas où l'horodatage est réalisé directement sur la copie numérique, il a aussi l'avantage de pouvoir être réalisé sans transmettre la copie elle-même au service tiers, mais uniquement son empreinte.

Alternativement aux services qualifiés cités par le décret de copie fiable, d'autres solutions peuvent néanmoins être envisagées pour attester de l'intégrité de la copie numérique, toujours en se basant sur une empreinte cryptographique. Typiquement, l'empreinte (et les données l'associant à la copie numérique source) peut être versée dans un coffre-fort électronique ou un système d'archivage électronique. Toutefois, ces méthodes ne bénéficient pas, comme ci-dessus, de la présomption de fiabilité. Il est donc dans ce cas nécessaire de s'assurer, avec un niveau de confiance équivalent à un service qualifié eIDAS, de la sécurité de la solution employée. La certification de conformité AFNOR d'un SAE vis-à-vis de la norme NF Z 42-013 paraît convenir dès lors qu'une empreinte de la copie est calculée et protégée dès son dépôt.

3.4. Conservation de la copie numérique

3.4.1. Introduction

Une fois générée et protégée par une empreinte le cas échéant, la copie numérique et son dossier de preuve (traces, documentation du processus) doivent être conservés dans le temps dans des conditions aptes à prolonger la garantie d'intégrité qui lui a été donnée à sa création.

La conservation doit de plus protéger la confidentialité des copies numériques, puisqu'il s'agit de données de santé à caractère personnel, ainsi que la disponibilité, en particulier si le document d'origine papier est détruit.

Quel que soit le palier de ce référentiel mis en œuvre, en cas de recours à des prestataires externes pour la conservation des copies numériques (concernant l'hébergement de données de santé et des archives publiques notamment), les mesures correspondantes décrites dans le socle commun du référentiel **[document de référence n° 2]** doivent être appliquées.

3.4.2. Mesures de sécurité pour la copie numérique simple

Les copies numériques simples ne sont pas destinées à être conservées sur une longue période, et n'ont pas de valeur probante à maintenir.

Les mesures de sécurité à respecter concernent le respect de la confidentialité du document, en accord avec les pratiques générales de la politique de sécurité du système d'information et selon les informations contenues sur le document.

3.4.3. Mesures de sécurité pour la copie numérique sécurisée

La conservation d'une copie numérique sécurisée consiste à archiver cette copie dans un espace sécurisé. Cette conservation vise à garantir la force probante du document, ce qui n'interdit pas, en parallèle, d'intégrer la copie au SI ou de la diffuser aux personnes autorisées.

La conservation sécurisée des copies numériques est assurée par la mise en œuvre des mesures de sécurité suivantes :

- ▶ **Disponibilité** : Pour éviter la perte accidentelle de copies numériques, la redondance du stockage des fichiers doit être assurée. Les modalités pratiques de cette redondance doivent prendre en compte la durée de conservation et les risques attachés aux documents (envisager la duplication hors site par exemple).
- ▶ **Contrôles d'accès** : L'accès aux copies numériques archivées doit être strictement restreint à un ensemble minimal d'acteurs. Une archive¹ n'est pas un document vivant, elle n'est consultée que de façon exceptionnelle pour retrouver un document détruit par ailleurs ou à titre de preuve. La modification d'une archive est interdite, sauf pour une opération de conversion nécessaire pour prolonger sa lisibilité dans le temps (voir ci-dessous le maintien de l'intégrité). La destruction d'une archive n'est possible qu'au terme de la durée de conservation fixée pour le document (par exemple une durée légale) et, dans le cas d'archives publiques, sous réserve de l'obtention du visa de l'administration des archives (cf. socle commun du référentiel **[document de référence n° 2]**).
- ▶ **Confidentialité** : Outre le contrôle d'accès, la confidentialité peut être renforcée par le chiffrement des copies numériques avant leur écriture sur les supports de stockage. L'opportunité d'ajout de cette mesure doit être étudiée par l'analyse de risques, cela peut répondre par exemple à un risque lié à l'externalisation de cette conservation.
- ▶ **Traçabilité** : Toutes les opérations concernant les copies numériques conservées doivent être tracées conformément aux exigences décrites dans le socle commun **[document de référence n°2]**.
- ▶ **Intégrité** : L'intégrité du document est garantie par l'empreinte calculée et protégée à l'étape précédente. Cette empreinte ne peut évoluer que dans trois situations :
 - La copie numérique doit être convertie vers un nouveau format (une nouvelle version du format PDF, un autre format standard choisi en remplacement du PDF...) pour assurer la lisibilité de la copie numérique dans le temps ;
 - L'empreinte a été calculée ou protégée avec un algorithme devenu obsolète (ou simplement déprécié) et une nouvelle empreinte doit être calculée sur le document original ;
 - Les moyens cryptographiques (certificat électronique notamment) nécessaires à la vérification de la protection éventuelle de l'empreinte vont bientôt arriver à expiration.

Cette évolution est autorisée, sans perte de valeur probante, dans la mesure où les conditions suivantes sont réunies :

- L'intégrité de la copie numérique et, dans le cas d'une copie sécurisée ou fiable, la validité de l'empreinte protégée, sont vérifiées positivement avant le calcul de sa nouvelle empreinte ;

¹ Le terme « archive » est employé dans ce paragraphe au sens d' « archive intermédiaire » décrit dans le code du patrimoine (voir article R212-11)

- Une nouvelle empreinte est calculée et protégée dans des conditions au moins équivalentes au calcul de la première empreinte ;
- Cette opération est correctement tracée et l'intégrité des traces ne peut être remise en cause.

La preuve d'intégrité peut reposer par exemple sur un mécanisme de signature électronique ou de chaînage d'empreinte, au choix du concepteur. Dans tous les cas, les mécanismes cryptographiques utilisés doivent satisfaire les exigences indiquées dans le socle commun du référentiel **[document de référence n°2]**.

- Veille et maintien en condition de sécurité : S'agissant d'une conservation sur une longue période de temps, les mesures de sécurité adoptées au lancement du processus doivent régulièrement être auditées et remises à l'état de l'art si des faiblesses significatives sont relevées. Cela comprend les algorithmes cryptographiques liés à l'empreinte et au cachet ou à la signature électronique des copies (voir paragraphe « mécanismes cryptographiques » de l'annexe 1 du présent référentiel **[document de référence n° 2]**), mais aussi les autres mesures participant à la disponibilité et à la confidentialité des documents.

La mise en œuvre de ces mesures peut être réalisée par l'emploi d'un Système d'Archivage Electronique (SAE) conforme à la norme NF Z 42-013 dans sa dernière version. Dans ce cas, la vérification de la satisfaction des exigences ci-dessus doit être garantie et tracée par le responsable du traitement de numérisation. Cette solution n'est cependant pas obligatoire, des espaces sécurisés d'archivage (intégrant l'ensemble des fonctions décrites ci-dessus mais pas nécessairement certifiés conformes à la norme) peuvent être mis en place au sein du SI de l'organisation.

Dans le cas où la conservation des copies numériques est réalisée par un prestataire externe, une attention particulière doit être portée sur la contractualisation des mesures et de la veille de sécurité. En plus de la mise en œuvre des mesures propres à l'hébergement chez un prestataire externe décrites dans le document socle commun **[document de référence n° 2]**, la certification de conformité du prestataire à la norme NF Z 42-013 dans sa dernière version est une précaution conseillée.

3.4.4. Mesures de sécurité pour la copie numérique fiable

L'utilisation d'un Système d'Archivage Electronique (SAE) certifié conforme à la norme NF Z 42-013 dans sa dernière version est requise. Cette conformité est en particulier garantie par la certification AFNOR qui délivre la marque NF 461 aux solutions certifiées.

En cas de recours à un prestataire externe, l'ensemble des mesures qui concernent notamment l'hébergement chez un prestataire externe et qui sont décrites dans le document socle commun **[document de référence n° 2]** sont également applicables.

3.5. Traitement du document d'origine

3.5.1. Introduction

Les mesures de sécurité existantes concernant les documents papier d'origine restent applicables à ceux-ci après la numérisation (confidentialité, disponibilité...).

Le responsable du traitement de numérisation peut décider :

- De poursuivre le cycle de vie du document papier tel qu'il préexistait au processus de numérisation ;
- D'archiver le document papier en privilégiant l'usage de la copie numérique intégrée au SI ;
- De détruire le document papier si les conditions requises et décrites dans le chapitre suivant sont réunies.

Dans tous les cas, le traitement du document d'origine doit être tracé et son emplacement doit être connu tant qu'il n'est pas détruit. En particulier, le document d'origine peut être demandé, s'il existe encore, pour le règlement d'un litige par un juge, même en cas de copie numérique sécurisée ou fiable.

3.5.2. Destruction des documents d'origine

Les conditions requises pour autoriser la destruction d'un document d'origine, avant la fin de la durée légale de conservation ou, à défaut, de la durée que le responsable de traitement a déterminée, sont :

- ▶ Une copie numérique fidèle à l'original et correspondant à une copie sécurisée ou une copie fiable (c'est-à-dire conforme au palier 2 ou au palier 3 présentés au §2.3) a été réalisée et archivée conformément aux conditions décrites au sein du présent document ;
- ▶ Une autorisation de destruction a été obtenue auprès de l'administration des archives dans le cas où le document d'origine relève du champ des archives publiques (cf. socle commun « gestion des archives publiques » **[document de référence n°2]**).

Le champ des archives publiques est défini par l'article L. 211-4 du code du patrimoine. L'autorisation de destruction des documents qui en relèvent doit être soumise au visa de l'administration des archives, conformément aux dispositions de l'article L. 212-3 du code du patrimoine.

Le moyen de destruction des documents papier doit lui-même assurer la confidentialité des données, que ce soit durant la collecte ou le stockage temporaire des documents ou après la destruction. La destruction peut être réalisée par un prestataire externe avec lequel toutes les mesures nécessaires ont été contractualisées.

La destruction du document d'origine n'est pas recommandée dans le cas d'une copie simple. Elle peut néanmoins être envisagée à condition que des mesures d'archivage a minima identiques à celles décrites pour une copie sécurisée (cf. §3.4.3) aient été mises en œuvre.

Si la copie réalisée n'est pas une copie fiable, le risque de contentieux impliquant le document concerné doit être considéré et évalué de façon approfondie par le responsable de traitement avant toute prise de décision relative à la destruction de l'original.

4. SYNTHÈSE DES MESURES PAR PALIER

Les différentes mesures propres à chacun des paliers décrits dans ce document sont présentées de façon synthétique dans le tableau suivant.


	Palier 1 : Copie simple	Palier 2 : Copie sécurisée	Palier 3 : Copie fiable
Conception et documentation du processus	<ul style="list-style-type: none"> ▶ Charte informatique ▶ PSSI de l'organisation 	Idem copie simple + <ul style="list-style-type: none"> ▶ Documentation du processus ▶ Dossier de tests 	Idem copie sécurisée
Numérisation et contrôle de la copie numérique	<ul style="list-style-type: none"> ▶ Confidentialité ▶ Identitovigilance 	Idem copie simple + <ul style="list-style-type: none"> ▶ Contrôles de numérisation ▶ Ajout de métadonnées ▶ Production de traces ▶ Format PDF ou PDF/A ▶ Sécurité physique et logique 	Idem copie sécurisée + <ul style="list-style-type: none"> ▶ Métadonnées complètes ▶ Traces complètes ▶ Format PDF/A
Protection de l'intégrité de la copie numérique	<ul style="list-style-type: none"> ▶ Aucune ou stockage d'une empreinte 	<ul style="list-style-type: none"> ▶ Cachet issu de l'IGC Santé 	<ul style="list-style-type: none"> ▶ Horodatage qualifié ou cachet qualifié ou signature qualifiée
Conservation de la copie numérique	<ul style="list-style-type: none"> ▶ Confidentialité 	<ul style="list-style-type: none"> ▶ Archivage sécurisé mais non nécessairement certifié 	<ul style="list-style-type: none"> ▶ SAE certifié conforme à la norme NF Z 42-013 dans sa dernière version
Traitement du document d'origine	<ul style="list-style-type: none"> ▶ Sans impact 	<ul style="list-style-type: none"> ▶ Sans impact ▶ Ou Archive papier ▶ Ou Destruction papier 	Idem copie sécurisée



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)

