

LIVRE BLANC

# ARCHIVES DE SANTÉ

Réglementations et bonnes pratiques



**LOCARCHIVES**

# PLAN

---

POURQUOI CE LIVRE BLANC ? .....	3
<b>1. QUEL EST LE CADRE LÉGAL DES ARCHIVES DE SANTÉ ? .....</b>	<b>5</b>
<b>1.1 • Données de santé à caractère personnel.....</b>	<b>6</b>
1.1.1 Le secret médical .....	6
1.1.2 Les données à caractère personnel .....	6
1.1.3 Les données de santé à caractère personnel.....	6
<b>1.2 • Les réglementations principales relatives à la preuve et aux archives .....</b>	<b>7</b>
1.2.1 Le droit de la preuve .....	7
1.2.2 La question de la valeur probante des archives numériques .....	7
1.2.3 La distinction entre archives publiques et archives privées .....	7
<b>1.3 • Obligations relatives aux Archives de Santé .....</b>	<b>9</b>
1.3.1 Les durées de conservation .....	9
1.3.2 L'externalisation des Archives de Santé .....	9
<b>2. ARCHIVAGE ET ARCHIVES DE SANTÉ - DE QUOI PARLONS-NOUS « TECHNIQUEMENT » ? .....</b>	<b>10</b>
<b>2.1 • Les qualifications techniques d'une archive de santé .....</b>	<b>10</b>
2.1.1 Les documents d'archives, dossiers d'archives, unités d'archives.....	10
2.1.2 Les archives physiques, numériques, hybrides.....	10
2.1.3 Les métadonnées de description des archives .....	11
<b>2.2 • Les prestations documentaires .....</b>	<b>12</b>
2.2.1 L'hébergement.....	12
2.2.2 L'archivage .....	12
2.2.3 La sauvegarde .....	12
2.2.4 La numérisation .....	13
<b>2.3 • En synthèse .....</b>	<b>13</b>
<b>3. EXTERNALISATION DES ARCHIVES DE SANTÉ - QUELS AGRÈMENTS ET CERTIFICATIONS EXIGER ? .....</b>	<b>14</b>
<b>3.1 • L'agrément ASIP Santé.....</b>	<b>14</b>
<b>3.2 • Les certifications AFNOR.....</b>	<b>16</b>
<b>3.3 • Les agréments du SIAF .....</b>	<b>17</b>
3.3.1 L'agrément archivage physique .....	17
3.3.2 L'agrément archivage électronique .....	17
<b>3.4 • La Complémentarité des agréments et certifications .....</b>	<b>18</b>
3.4.1 Les principes généraux .....	18
3.4.2 Le cas particulier des métadonnées pour l'archivage physique .....	18
3.4.3 Le cas particulier de la numérisation .....	18
3.4.4 Tableau de synthèse des certifications et agréments.....	19
<b>4. LES 12 BONNES PRATIQUES POUR RÉUSSIR L'EXTERNALISATION DES ARCHIVES DE SANTÉ .....</b>	<b>20</b>
<b>5. L'ÉLABORATION DU LIVRE BLANC .....</b>	<b>22</b>
<b>6. ANNEXE .....</b>	<b>23</b>

# Pourquoi ce livre blanc ?

Ce livre blanc a pour **objectif** d'apporter une vision claire et synthétique de la réglementation et de la gestion des archives dans le milieu médical.

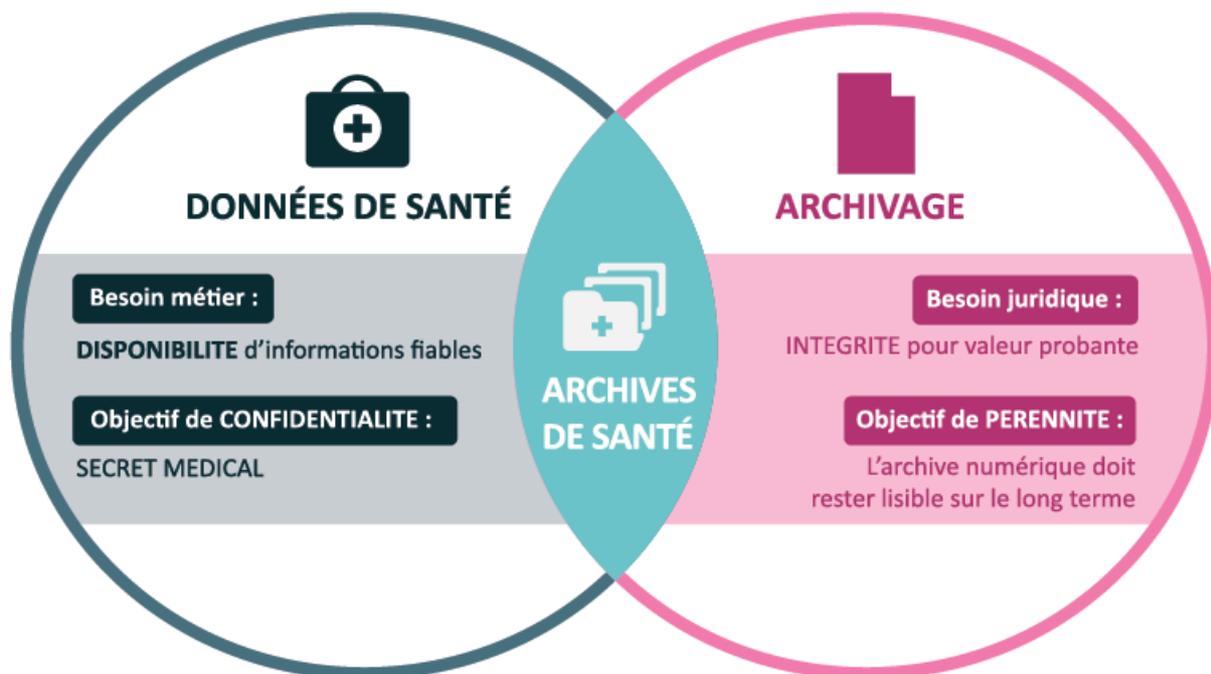
A cet effet, il faut distinguer les archives purement administratives des archives contenant des données de santé à caractère personnel.

Ces dernières, en raison de leur sensibilité particulière, sont soumises à des contraintes réglementaires spécifiques et peuvent désormais faire l'objet d'un « hébergement » auprès d'opérateurs agréés. Ces opérateurs fournissent des services hétérogènes pour l'hébergement de données au sens large (cloud computing, logiciels, imagerie médicale...).

Une confusion est souvent faite entre hébergement et **archivage**, ce dernier ayant pour finalité l' « *Organisation et le contrôle de la constitution, de la sélection, de la conservation et de la destination finale des documents d'une administration, d'une entreprise ou d'un organisme* »<sup>1</sup>.

L'archivage est donc un cas particulier d'hébergement complexe qui couvre **deux besoins** principaux :

- **un besoin métier** : l'accès à des archives fiables et intègres est indispensable pour les professionnels de santé dans leur **pratique des soins**,
- **un besoin juridique** : les archives couvrent un **risque juridique** pour l'établissement de santé en cas de réclamation ou de contentieux.



La gestion des « Archives de Santé » doit répondre à deux problématiques :

- un contexte réglementaire plus étendu que l'hébergement des données de santé pour assurer la **valeur probante** des documents d'archives,
- une temporalité différente des systèmes informatiques qui assurent l'hébergement : les archives doivent être **pérennes**.

<sup>1</sup> [Commission générale de terminologie.](#)

### **1) Quel est le cadre légal des Archives de Santé ?**

Nous verrons que la réglementation applicable aux Archives de Santé émane de différentes sources, telles que le droit commun, le Code de la Santé Publique, le Code du Patrimoine... Ces textes ont pour objectif la protection des données personnelles du patient (à travers la préservation de la confidentialité de ses données) et des droits de l'établissement de santé par une maîtrise des archives.

### **2) Archivage et Archives de Santé - De quoi parlons-nous « techniquement » ?**

Les archives sont des agrégats de données matérialisés sur un support physique ou numérique. Les archives sont accompagnées de métadonnées stockées sous différentes formes (index de moteur de recherche, bases de données...). Ce livre blanc précise les différentes composantes d'un objet d'archives en vue de définir les traitements qui seront réalisés sur les Archives de Santé.

### **3) Externalisation des Archives de Santé - Quels agréments et certifications exiger ?**

Selon qu'il s'agisse d'archives publiques ou privées, et selon le support de l'archive (physique ou numérique), un prescripteur doit spécifier des exigences de certification ou d'agrément. Cette partie du livre précise les moyens pour s'assurer de la conformité d'un tiers archiveur.

Après avoir répondu à ces 3 questions, le livre propose **12 bonnes pratiques pour l'externalisation des Archives de Santé**.

Ces informations peuvent être utilisées par un prescripteur lors de l'élaboration d'un cahier des charges d'externalisation.

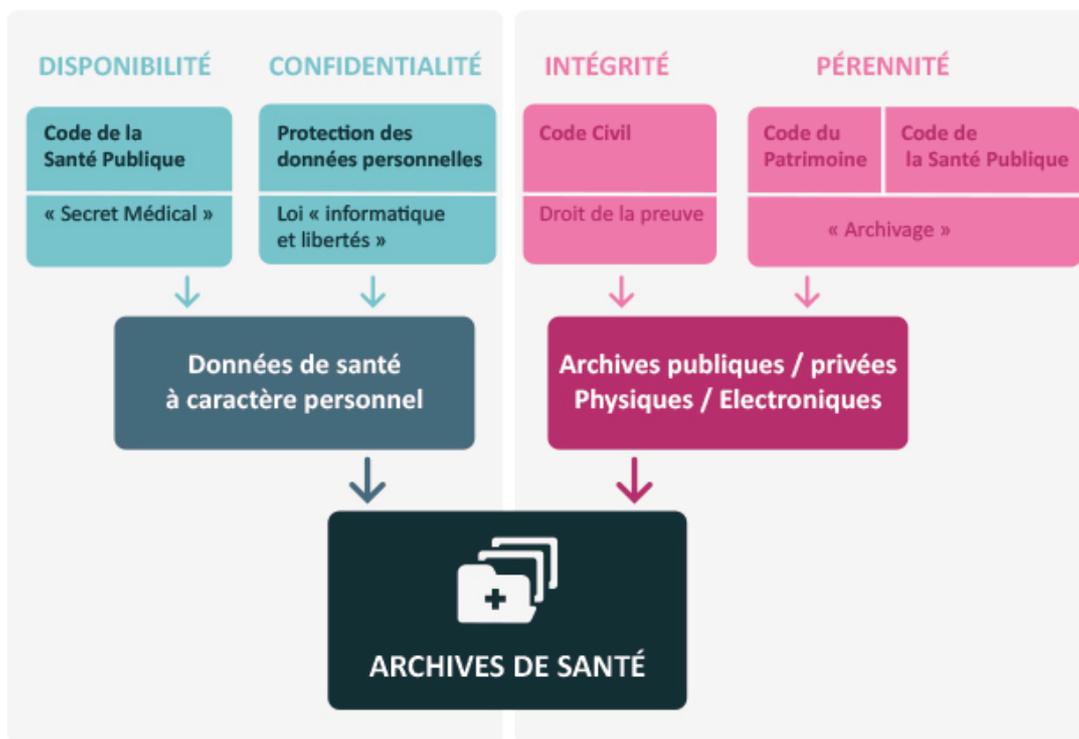
# 1. Quel est le cadre légal des Archives de Santé ?

L'**objectif** de la réglementation est d'**assurer le respect de la confidentialité** des données de santé à caractère personnel afin de **protéger le patient** de tout risque lié à la divulgation et l'exploitation des données, qui pourraient lui être préjudiciables.

La **réglementation** du Code de la Santé Publique s'appuie notamment sur les dispositions de la Loi « Informatique et Libertés »<sup>2</sup> en matière d'exigences de confidentialité et de sécurité des données.

Lorsqu'il s'agit d'**Archives de Santé**, un professionnel de santé doit également respecter les dispositions du Code Civil et du Code du Patrimoine en matière de **preuve** et de vocation probatoire des documents d'archives.

L'intégrité de la preuve, et donc de l'Archive de Santé, doit être démontrable et exploitable sur des durées longues. Cette **problématique de pérennité et d'intégrité** peut s'avérer assez simple à gérer s'agissant d'une archive sur support physique. Pour autant, nous le verrons, des précautions particulières sont nécessaires pour les archives sur support électronique.



Ce guide est rédigé en l'état de la réglementation en vigueur au mois de janvier 2016. Un projet de loi présenté en annexe identifie les évolutions potentielles à moyen terme.

Cette première partie synthétise les exigences des différents textes pour le traitement des « Archives de Santé ».

<sup>2</sup> Loi n° 78-17 du 6 janvier 1978.

## 1.1 • Données de santé à caractère personnel

Les données de santé à caractère personnel cumulent les exigences de protection du secret médical et des données personnelles.

### 1.1.1 Le secret médical

Le respect de la vie privée<sup>3</sup> et le secret médical sont deux droits fondamentaux du patient.

Le terme « secret médical » est utilisé dans le langage courant, cependant il convient mieux de parler de « secret professionnel ». En effet, le Code de la Santé Publique en donne une définition précise :

*« Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris »<sup>4</sup>.*

L'ensemble du corps médical constitue un cercle de confiance qui vient améliorer le suivi médical des patients et la circulation de l'information.

### 1.1.2 Les données à caractère personnel

Dès 1978, le législateur est intervenu pour définir et encadrer les données personnelles avant d'être suivi par le Conseil Européen. Aujourd'hui, l'arsenal législatif est abouti. Dès lors qu'une information rend possible l'identification d'une personne physique, il s'agit d'une donnée personnelle, quel que soit ce moyen d'identification.

Juridiquement, les **données à caractère personnel** sont définies à l'article 2 de la loi dite « Informatique et Libertés »<sup>5</sup> selon les termes suivants « [...] Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres [...] ».

### 1.1.3 Les données de santé à caractère personnel

Les données de santé à caractère personnel sont des données qui bénéficient de protections particulières. Ces données comprennent tous types de documents produits par les établissements de santé publics ou privés participant au service public « hospitalier ».

La gestion et le traitement des données de santé à caractère personnel (ci-après « données de santé ») font l'objet d'une **protection renforcée** par la loi Informatique et Libertés, le Code de la Santé Publique, la CNIL<sup>6</sup> et une directive européenne<sup>7</sup>.

Non seulement le praticien doit respecter le secret médical auquel il est tenu, mais il doit aussi veiller à la **conservation** et à l'**hébergement** des données de santé dans des conditions de nature à **conserver** leur **confidentialité**, leur **sécurité**, leur **intégrité** et leur **pérennité**<sup>8</sup>.

La loi précise également que les données de santé à caractère personnel sont des données sensibles<sup>9</sup>. Elles recouvrent les informations relatives à la santé d'une personne physique.

---

<sup>3</sup> [Article L1110-4 alinéa 1er du Code de la Santé Publique](#)

<sup>4</sup> [Article R.4127-4 du Code de la Santé Publique](#)

<sup>5</sup> [Loi du 6 janvier 1978 n°78-17](#)

<sup>6</sup> Commission nationale Informatique et Liberté.

<sup>7</sup> [Directive n° 95/46 du 24 octobre 1995](#)

<sup>8</sup> [Article 1110-4, 1111-8 du Code de la Santé Publique et décret du 4 janvier 2006 n° 2006-6](#)

<sup>9</sup> [Article 8 de la loi du 6 janvier 1978 n°78-17](#)

## 1.2 • Les réglementations principales relatives à la preuve et aux archives

Les archives de Santé sont également un moyen de preuve. Du droit de la preuve découle la notion de **valeur probante**, très importante dans le monde juridique, dont la matière première est le document d'archives.

### 1.2.1 Le droit de la preuve

De manière générale, l'administration de la **preuve** est régie par les articles 1315 à 1369 du Code Civil. Celle-ci peut se définir comme la **démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation**.

Selon l'article 1315 du Code Civil alinéa 1<sup>er</sup>, la charge de la preuve repose en principe sur le demandeur<sup>10</sup>, toutefois le droit de la responsabilité médicale et hospitalière s'oriente vers une protection accrue des victimes, et donc vers une tendance au renversement de la charge de la preuve contre les professions médicales et établissements de santé.

Le droit français tend à privilégier la **preuve écrite**. L'article 1316 du Code Civil définit la preuve littérale ou preuve par écrit comme résultant « [...] *d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission* ».

Les archives physiques peuvent constituer des preuves par écrit : par exemple, le dossier médical d'un patient, contenant des résultats d'examen, des prescriptions médicales, un résumé de consultations ou encore les échanges entre professionnels, servira de preuve en cas de litige<sup>11</sup>.

Mais quid des dossiers médicaux dématérialisés ?

### 1.2.2 La question de la valeur probante des archives numériques

Depuis la loi du 13 mars 2000, l'écrit sous forme électronique **peut avoir valeur probante** au même titre que l'écrit sur support papier, sous réserve que puisse être dûment **identifiée la personne dont il émane**, et qu'il soit établi et **conservé dans des conditions de nature à en garantir l'intégrité**<sup>12</sup>.

Toutefois, dans la sphère électronique, comme dans l'univers du papier, la preuve est toujours un concept relatif : un document détient une valeur probante **tant qu'il n'est pas contesté**.

Lorsque la loi ne prévoit rien, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support<sup>13</sup>.

### 1.2.3 La distinction entre archives publiques et archives privées

Les archives sont définies à l'article L. 211-1 du Code du Patrimoine qui dispose que « *les archives sont l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité* ».

Ce même code opère une distinction entre deux catégories d'archives : les archives publiques<sup>14</sup> et les archives privées<sup>15</sup>.

---

<sup>10</sup> Principe : *actori incombis donatio*

<sup>11</sup> Il incombe au médecin d'assurer la bonne tenue et la complétude du dossier médical. Il a été jugé par Cour de Cassation (arrêt 1<sup>ère</sup> chambre civile du 9 avril 2014, pourvoi n° 13-14.964) que le fait d'omettre de remplir le dossier médical d'un patient est désormais constitutif d'une faute pour un médecin, ce qui retournerait la charge de la preuve contre lui.

<sup>12</sup> [Article 1316-1 du Code Civil](#)

<sup>13</sup> [Article 1316-2 du Code Civil](#)

<sup>14</sup> [Article L.211-4 du Code du Patrimoine](#)

A la lecture de la définition de l'article L.211-4 Code du Patrimoine, sont considérés comme documents d'archives publiques tous les documents d'archives produits par : les établissements publics de santé, les établissements de santé privés d'intérêt collectif (ESPIC) ainsi que les établissements médico-sociaux publics dans le cadre de leur mission de service public. A contrario, les documents d'archives, qu'ils soient de santé ou non, produits par les autres structures, sont des archives privées.



## FOCUS :

### L'obligation de conservation des archives sur le territoire national

C'est le principe de provenance territoriale. Il stipule que « les archives doivent être conservées dans les services d'archives du territoire sur lequel elles ont été produites, (...) »<sup>16</sup>. Il faut cependant distinguer selon la nature publique ou privée de la structure. S'il s'agit d'une structure publique, alors la conservation devra se faire sur le territoire national. En effet, le Code du Patrimoine oblige à conserver sur le territoire national les archives qui sont confiées à une personne physique ou morale souhaitant assurer la conservation d'archives publiques<sup>17</sup>. En revanche, lorsqu'il s'agit d'une structure privée, cela dépendra de la nature des données à conserver.

Par exemple en matière d'hébergement de données de santé à caractère personnel : si celles-ci n'ont pas le caractère d'archives publiques, rien ne s'oppose à ce que les données de santé à caractère personnel soient hébergées en dehors du territoire français, tant qu'il s'agit de les héberger au sein de l'Union Européenne<sup>18</sup> (exemple : le dossier médical personnel peut être conservé dans tous les pays de l'Union Européenne). En revanche, le transfert de données de santé à caractère personnel vers un pays tiers à l'Union Européenne est en principe interdit<sup>19</sup>.

Il faut noter que même si la loi autorise la conservation de certaines données en dehors du territoire national, cette solution n'est pas à préconiser pour plusieurs raisons :

- l'état de l'art du métier n'est pas forcément le même d'un pays à l'autre, notamment sur les exigences relatives au respect de la confidentialité<sup>20</sup>,
- les éventuels contentieux pourraient entraîner des difficultés supplémentaires comme des conflits de loi et de juridiction<sup>21</sup>.

Nous recommandons la lecture du guide pour la confidentialité des archives numériques publié par la Fédération Nationale des Tiers de Confiance (FNTC), qui présente une analyse juridique plus détaillée de la problématique de localisation des données et des risques associés<sup>22</sup>.

<sup>15</sup> [Article L. 211-5 du Code du Patrimoine](#)

<sup>16</sup> [Dictionnaire de terminologie archivistique](#) (voir aussi principes du respect des fonds et de la pertinence territoriale)

<sup>17</sup> Article R. 212-23 du Code du Patrimoine

<sup>18</sup> La directive communautaire 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données du Parlement européen et du Conseil établit un cadre de protection des données à caractère personnel équivalent à l'ensemble des pays membres de l'Union européenne. Cette directive a été transposée en France par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

<sup>19</sup> Cependant les articles 68 et 69 de la loi du 6 janvier 1978 rendent ce transfert possible au travers de mécanismes permettant de s'assurer du niveau de protection adéquat des données : la Commission Européenne a reconnu comme présentant un niveau de protection adéquat, les pays suivants : Canada, Suisse, Argentine, territoires de Guernesey, de Jersey et de l'Isle de Man.

<sup>20</sup> [Guide pour la Confidentialité des archives numériques de la FNTC](#)

<sup>21</sup> [Pour plus d'information voir cours sur le Droit International Privé](#)

<sup>22</sup> Guide FNTC sur la confidentialité : <https://www.fntc.org/fr/publications/func-startdown/475/>

## 1.3 • Obligations relatives aux Archives de Santé

Une définition d' « Archives de Santé » est proposée dans ce livre. D'un point de vue juridique, il s'agit de données de santé à caractère personnel, matérialisées dans un document d'archives et dont la nature peut révéler un caractère de preuve pour un usage juridique.

### 1.3.1 Les durées de conservation

La loi impose une conservation longue des données personnelles à caractère médical<sup>23</sup>. La problématique de l'archivage de ces données est par conséquent très importante. Ces données sensibles font l'objet d'une législation qui encadre les modalités d'archivage, physique et électronique. Il conviendra d'identifier les différentes natures d'archives existantes pour déterminer les durées de conservation appropriées.

### 1.3.2 L'externalisation des Archives de Santé

Le législateur est venu préciser les règles applicables à la **conservation externalisée** d'Archives de Santé. Le cadre n'est pas le même selon s'il s'agisse d'Archives de Santé physiques ou électroniques.



#### FOCUS INFO :

#### Principales durées de conservation des Archives de Santé

**Pour les établissements publics ou privés** la durée réglementaire de conservation des dossiers médicaux<sup>1</sup> est de 20 ans minimum à compter du dernier passage du patient dans l'établissement<sup>1</sup>.

**Pour les praticiens libéraux**, la durée réglementaire de conservation est de 10 ans à compter de la stabilisation de la santé du patient (consolidation du dommage)<sup>1</sup>.

**NB : Délai de communication du dossier médical au patient<sup>1</sup>** : huit jours à compter de la demande pour les dossiers récents et deux mois pour les dossiers anciens, c'est-à-dire :

- dont la dernière pièce remonte à plus de 5 ans,
- s'il y a eu admission en psychiatrie.

En matière d'archivage physique, les règles applicables concernant les Archives de Santé, quel que soit l'organisme émetteur, figurent dans le Code du Patrimoine<sup>24</sup>. Ainsi les archives ne peuvent être confiées qu'à un tiers archiveur agréé pour l'externalisation d'archives publiques physiques. Le Code de la Santé Publique<sup>25</sup> a étendu la portée de cet agrément à l'archive de santé sur support physique. Cet agrément est attribué par le Service Interministériel des Archives de France (SIAF)<sup>26</sup>.

Pour l'archive de santé électronique, un décret<sup>27</sup> a posé des exigences spécifiques qui doivent être respectées en cas d'externalisation. Un agrément spécifique est délivré par le Ministère de la Santé, après avis de la CNIL, pour une durée de trois ans<sup>28</sup>.

Les différents agréments relatifs à l'externalisation des Archives de Santé sont détaillés dans le chapitre 3 du présent livre, consacré aux normes et agréments.

<sup>23</sup> [Article R1112-7 du Code de la Santé Publique](#)

<sup>24</sup> [Articles L212-4 et R212-19 à R.212-31 du Code du Patrimoine](#)

<sup>25</sup> [Article R.1111-16 du Code de la Santé Publique](#)

<sup>26</sup> <http://www.archivesdefrance.culture.gouv.fr/gerer/gestion-externalisee-des-archives/>

<sup>27</sup> [Décret n°2006-6 du 4 janvier 2006](#)

<sup>28</sup> <http://esante.gouv.fr/services/referentiels/securite/hebergement-faq>

## 2. Archivage et Archives de Santé - De quoi parlons-nous « techniquement » ?

---

Les Archives de Santé sont des données de santé à caractère personnel sur support physique ou numérique (document d'archives).

Ce chapitre propose une **qualification technique des Archives de Santé** pour ensuite définir les différents **traitements d'archivage**. C'est sur ces traitements que portent les exigences de sécurité pour la protection des données de santé.

### 2.1 • Les qualifications techniques d'une archive de santé

#### 2.1.1 Les documents d'archives, dossiers d'archives, unités d'archives

Les Archives de France définissent le document d'archives comme un « *ensemble constitué d'un support et de l'information qu'il porte, utilisable comme preuve ou à des fins de consultation.* »

Elles définissent le dossier comme un « *Ensemble de documents constitué soit organiquement par le producteur d'archives pour la conduite ou le traitement d'une affaire, soit par regroupement logique lors du classement dans le service d'archives.* »<sup>29</sup>

Dans le contexte d'un établissement de santé, l'Archive de Santé est par exemple un dossier patient constitué organiquement par le producteur (les services de l'établissement de santé).

Le dossier patient est généralement évolutif (intégration ou élimination de pièces) mais chaque document d'archives contenu dans le dossier doit rester intègre.

#### 2.1.2 Les archives physiques, numériques, hybrides

Si le dossier est sur un support physique, il sera classé selon un ordre déterminé ou regroupé en unité d'archives (boîte ou conteneur) selon le mode de stockage choisi.

Si le dossier est sur support numérique, il sera classé et structuré « virtuellement » par l'application de gestion de dossier métier.

Le dossier peut également avoir une forme hybride et être composé de pièces sous forme physique et numérique.

L'hybridation des fonds d'archives est une conséquence directe de la transition numérique qu'opère notre société. La capacité à gérer des fonds hybrides est un enjeu important car cette situation transitoire sera pérenne du fait des durées de conservation très longues des Archives de Santé et des contraintes économiques, organisationnelles et techniques de reprendre l'ensemble de fonds d'archives physiques pour tendre vers le tout numérique.

***La donnée de santé restera à la fois sur des archives physiques et électroniques  
sur de longues périodes.***

---

<sup>29</sup> [Dictionnaire de terminologies archivistique](#)

### 2.1.3 Les métadonnées de description des archives

Les archives sont consultées par l'intermédiaire d'**outils de recherche**.

Historiquement, il s'agissait de registres papiers qui sont aujourd'hui informatisés dans des systèmes de gestion des archives physiques ou des systèmes d'information métiers.

L'outil de recherche est un ensemble structuré de **métadonnées** techniques de gestion et de description, attaché à une archive et servant à en décrire les caractéristiques en vue de faciliter son repérage, sa gestion, son usage et sa préservation tout au long de son cycle de vie.

Les métadonnées descriptives servent donc à l'indexation des documents numériques. Elles sont généralement complétées par la possibilité d'indexer l'intégralité des contenus informationnels des documents d'archives (**index plein texte**) afin de permettre leur exploitation par un moteur de recherche. Il s'agit là d'une fonctionnalité à très forte valeur ajoutée apportée par le numérique pour exploiter un fonds d'archives. C'est en effet sur cette innovation que Google a forgé sa réussite en indexant le plus gros fonds documentaire mondial constitué par le web.

Ainsi l'ensemble des contenus d'archives de santé peuvent également être intégrés dans des bases d'**index plein texte** d'un moteur de recherche. A la différence du Web, les fonds d'archives sont strictement confidentiels et nécessitent des moteurs de recherches évolués permettant une gestion des accès fine et une protection renforcée des index.

Pour des raisons de pérennité, le modèle OAIS (ISO 14 721)<sup>30</sup> préconise que les objets d'archives soient indépendants de tout système informatisé, car le cycle de vie d'une application informatique est inférieur aux durées de conservation des archives.

A ce titre, l'usage, dans un système d'archivage électronique professionnel, est d'associer les métadonnées au document d'archives avec un **fichier de description** connexe lié au document d'archives. L'objet d'archives stocké est, dans ce cas, un « paquet » composé d'un ou plusieurs documents d'archives et d'un fichier de description contenant les métadonnées structurées dans un format ouvert et interopérable.

Les métadonnées d'archivage peuvent donc coexister sous plusieurs formes :

- dans les instruments de recherche,
- dans les index plein texte,
- dans les fichiers de descriptions de l'objet d'archives.

Si ces métadonnées contiennent des données de santé à caractère personnel, il conviendra de s'assurer que les systèmes ou opérateurs qui les exploitent répondent aux exigences de sécurité réglementaires<sup>31</sup>.

*La sécurité des métadonnées est aussi importante que la sécurité du document d'archives lui-même.*

<sup>30</sup> [Plus d'informations sur la norme OAIS \(ISO 14721\) sur le site des archives de France](#)

<sup>31</sup> [Référentiel Général de Sécurité et décret de 2006-6 du 4 janvier 2006](#)

## 2.2 • Les prestations documentaires

Les traitements d'archivage peuvent être opérés sur les données contenues dans les Archives de Santé ainsi que sur les métadonnées d'exploitation de ces archives.

A chaque traitement correspondent des prestations dont la définition peut varier selon la pratique du prescripteur ou de l'opérateur du traitement. Ainsi l'archivage peut parfois être qualifié de sauvegarde, de stockage ou d'hébergement.

Nous proposons ici une définition des traitements les plus courants opérables sur les Archives de Santé.

### 2.2.1 L'hébergement

L'hébergement recouvre une réalité complexe car il existe de nombreux types d'hébergeurs pouvant répondre aux critères du décret du 4 janvier 2006<sup>32</sup> (cloud computing, éditeurs, opérateurs téléphoniques ...).

Toutefois, le décret ne donne pas une définition précise de ce qu'est « l'hébergement ».

Dans le cadre du présent livre blanc, la notion d'hébergement est entendue comme le stockage d'un objet numérique dans une infrastructure informatique pour des usages variés (traitement, consultation, ...) et pouvant permettre la modification d'objets hébergés.

### 2.2.2 L'archivage

Il s'agit de la conservation d'un document ou dossier d'archives dans un système d'archivage électronique à vocation probatoire disposant de fonctionnalités définies dans la norme NF Z 42-013 et notamment :

- la capacité à démontrer la préservation de l'intégrité dans la durée avec des mécanismes cryptographiques (empreinte numérique, horodatage) et une traçabilité avancée (journalisation),
- la mise à disposition de fonctions de recherche,
- la gestion des habilitations d'accès à la donnée,
- la gestion du cycle de vie des archives,
- ...

*La norme NF Z 42-013 fournit des spécifications concernant les mesures à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques, afin d'assurer leur conservation et leur intégrité.*

Afin de préserver l'intégrité, un traitement d'archivage comprend donc l'hébergement des documents d'archives sans possibilité de modifier ces derniers.

Les métadonnées associées sont également hébergées et peuvent évoluer dans le temps.

### 2.2.3 La sauvegarde

Il s'agit d'une copie de sécurité d'objets numériques et/ou de données numériques sur un support physique ou numérique. Ce dispositif est étroitement lié à la continuité d'activité et aux plans de secours informatiques.

Les Archives de Santé ainsi que les métadonnées sont sauvegardées pour des raisons de sécurité, et répliquées sur un site distant pour assurer la disponibilité des systèmes d'information qui les exploitent.

---

<sup>32</sup> Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel

## 2.2.4 La numérisation

Il s'agit de constituer une copie numérique d'un document physique.

S'il est nécessaire de conférer une vocation probatoire à la copie numérique, voire de la substituer à l'original papier, il est nécessaire de démontrer qu'il s'agit bien d'une copie fidèle et durable<sup>33</sup>, c'est-à-dire que le contenu de la copie numérique ne peut pas être interprété différemment du contenu du document original.

Cette exigence du droit, respectée par l'application de la norme NF Z 42-013, précise les modalités de **numérisation fidèle** et de **conservation durable** dans un système d'archivage électronique (cf. 2.2.2).

Le cas échéant, il est possible de réaliser une numérisation non probatoire (l'original physique portera la vocation probatoire) et d'héberger les documents produits (cf. 2.1.1).

## 2.3 • En synthèse

Un document électronique est soit archivé, soit hébergé, selon qu'il est nécessaire de **conserver sa vocation probatoire** ou non. Dans les deux cas, la donnée de santé contenue dans le document doit être protégée.

**Les métadonnées** physiques ou électroniques permettant d'exploiter les documents d'archives **sont hébergées** dans un système d'information. Selon qu'elles contiennent des données de santé ou non, les niveaux de protection et d'engagements juridiques seront différents.

Les documents d'archives et les métadonnées sont répliqués ou sauvegardés pour des raisons de sécurité. Les supports de réplication et de sauvegarde doivent intégrer le dispositif de protection de la donnée de santé.



### FOCUS : LES TRAITEMENTS DE SAUVEGARDE DES SYSTÈMES D'INFORMATION DES ÉTABLISSEMENTS DE SANTÉ

La sauvegarde régulière des données contenues dans les systèmes d'information de santé (par exemple le logiciel de gestion hospitalière) n'est pas considérée comme une archive mais comme une copie de sécurité.

S'il s'agit de « purger » les données d'un système et de les conserver sur un autre support, il s'agit bien d'archives de données numériques (sous forme de documents, de bases de données, de fichiers techniques, ...).

Dans les deux cas il s'agit de données de santé numériques hébergées (au sens du traitement) qu'il convient de sécuriser au même titre qu'une donnée hébergée « online » dans un entrepôt de données.

<sup>33</sup> Article 1348 alinéa 2 du Code Civil

### 3. Externalisation des Archives de Santé - Quels agréments et certifications exiger ?

L'ensemble du corps médical constitue un cercle de confiance qui vient améliorer le suivi médical des patients et la circulation de l'information. La protection du secret médical est une obligation essentielle d'un établissement de santé, qu'il doit faire respecter à l'intérieur de ses murs.

L'externalisation des données de santé suppose cependant de faire respecter les obligations de confidentialité à l'extérieur des murs, chez des opérateurs qui ne sont pas des professionnels de santé.

Le législateur a donc élaboré un ensemble de dispositifs d'agrément permettant l'externalisation de données de santé, en assurant la protection des données dans un environnement externalisé.

Concernant les Archives de Santé, les agréments nécessaires dépendent de la nature du support (physique et électronique), de la nature de la donnée (personnelle de santé ou non) et de la nature de l'archive (privée ou publique).

Ce chapitre présente les différents agréments ainsi qu'un tableau d'aide à la détermination des exigences d'agrément ou de certification pour le choix d'un tiers-archiviste physique et électronique.



#### FOCUS : Le médecin de l'hébergeur<sup>1</sup>

L'une des exigences du décret de 2006 est la présence d'un médecin dans l'entreprise candidate à l'agrément. Le médecin sélectionné doit être inscrit au Tableau de l'Ordre des Médecins. Il doit conserver son indépendance de jugement, de décision et sa capacité à agir, et l'Ordre des Médecins s'en assure.

Le médecin est le garant de la confidentialité des données personnelles de santé déposées chez l'hébergeur à toutes les étapes de leur traitement. Il veille au respect des conditions d'accès aux données personnelles de santé, conformément à la loi n°78-12 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et au Code de la Santé Publique.

Le médecin du tiers-archiviste de santé est l'interlocuteur privilégié du médecin en charge de la protection des données de l'établissement de santé pendant la prestation d'archivage.

#### 3.1 • L'agrément ASIP Santé

L'hébergement de données de santé à caractère personnel sous forme électronique relève d'une **réglementation** très **exigeante**. La politique de **confidentialité** et de sécurité est particulièrement rigoureuse concernant le respect des droits des personnes concernées par les données hébergées, la sécurité de l'accès aux informations, la pérennité des données hébergées, l'organisation et les procédures de contrôle interne. L'hébergeur de données de santé relève d'un agrément du Ministère de la Santé. Les établissements de santé qui souhaitent externaliser des Archives de Santé électroniques doivent impérativement faire appel à un prestataire agréé.

Le référentiel de constitution des dossiers de demande d'agrément des hébergeurs de données de santé à caractère personnel comprend plus de **73 impératifs**, parmi lesquels **l'inviolabilité**, la **sécurité**, la **qualité de service**...<sup>34</sup>. Le respect de ces exigences est soumis à un contrôle qui prend la forme d'un **agrément** remis pour 3 ans par le Ministère de la Santé. La procédure d'agrément des hébergeurs de données de santé à caractère personnel<sup>35</sup> représente une des conditions essentielles au développement des systèmes d'information de santé.

<sup>34</sup> [http://esante.gouv.fr/sites/default/files/Guide\\_constitution\\_dossiers\\_demandes\\_agrement\\_hebergeurs\\_v1.1.4.pdf](http://esante.gouv.fr/sites/default/files/Guide_constitution_dossiers_demandes_agrement_hebergeurs_v1.1.4.pdf)

<sup>35</sup> [Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé et décrite par le décret du 4 janvier 2006](#)

Un agrément correspond à une solution ou une prestation proposée par un opérateur. Ainsi un opérateur peut disposer de plusieurs agréments correspondant à différents périmètres d'application. Au moment de la rédaction du présent livre blanc, l'ASIP Santé<sup>36</sup> avait rendu 78 décisions d'agrément pour l'hébergement de données de santé à caractère personnel, réparties entre des opérateurs cloud computing, des éditeurs, des établissements de santé ou encore des opérateurs téléphoniques. Les tiers-archivistes sont encore peu représentés dans ce panel.

**Lors de la sélection d'un hébergeur de données de santé, il est donc important de bien analyser sur quel périmètre repose son agrément, et qu'il correspond à la prestation souhaitée par l'établissement de santé.** La compréhension des différences entre une prestation d'archivage et d'hébergement (cf. §2.2) est essentielle si la composante juridique du projet d'externalisation est importante.



## FOCUS :

### Le contrat de dépôt d'Archives de Santé

Le droit français encadre le **contrat de dépôt** dans le Code Civil. La loi<sup>1</sup> dispose que « le dépôt, en général, est un acte par lequel on reçoit la chose d'autrui, à la charge de la garder et de la restituer en nature ». L'**obligation de garde** est fondamentale et ne peut être supprimée. Ce contrat se distingue des autres contrats car le **dépositaire n'a pas le droit d'utiliser le bien**. Le contrat de dépôt induit des objectifs qui doivent être clairement spécifiés par le dépositaire.

Concernant les **Archives de Santé**, la loi précise que l'hébergement de données de santé à caractère personnel « [...] ne peut avoir lieu qu'avec le **consentement** exprès de la personne concernée, [...] », notamment lorsque les contractants d'un service d'hébergement sont des professionnels de santé ou des établissements. Dans le cadre d'un contrat de dépôt chez un tiers-archiviste, ce dernier n'assume pas la relation directe avec le patient et n'est pas en mesure de recueillir son consentement. Cette responsabilité est reportée sur l'établissement de santé, qui devra mettre en œuvre les mesures nécessaires pour informer le patient des modalités d'hébergement de ses données et obtenir son consentement.

Le patient dispose également d'un **droit d'opposition et de rectification**<sup>1</sup>.

Ce droit ne peut être exercé par le patient directement auprès du dépositaire (le tiers-archiviste), car il entre en opposition avec les principes régissant le contrat de dépôt (notamment les articles 1933 et 1937 du Code Civil), en vertu desquels le donneur d'ordre est le déposant et non le patient. Ce dernier ne pourra donc exercer ses droits que par l'intermédiaire de l'établissement ou du professionnel de santé (les déposants).

Un tiers archiviste ne peut prendre la responsabilité de modifier ou détruire un document d'archives sans accord du déposant dans le cadre d'une prestation particulière.

Par ailleurs, concernant les archives publiques, ni le déposant, ni le dépositaire ne peuvent détruire une archive sans l'accord préalable de la personne chargée du contrôle scientifique et technique de l'Etat.

Afin de sécuriser la consultation des archives, leur accès est protégé au moyen des identifiants d'accès fournis à une ou plusieurs personnes habilitées. Pour plus de sécurité, une **authentification forte** est requise par l'agrément. Cela se fait par exemple par un mot de passe à usage unique généré par un dispositif en possession de l'utilisateur (token physique, soft token sur smartphone...).

Dans le cadre de son agrément, le tiers-archiviste propose un modèle de contrat spécifique à l'archivage de santé à ASIP Santé. Ce modèle est systématiquement proposé aux professionnels et aux établissements de santé pour assurer un cadre de conformité juridique de la prestation.

<sup>36</sup> [http://esante.gouv.fr/sites/default/files/PAHDS\\_Presentation\\_generale\\_v1.0.1.pdf](http://esante.gouv.fr/sites/default/files/PAHDS_Presentation_generale_v1.0.1.pdf)

## 3.2 • Les certifications AFNOR

AFNOR Normalisation a édité des normes concernant l'archivage physique et numérique sur lesquelles reposent les agréments du SIAF.

AFNOR Certification propose des certifications de conformité à ces normes pour les tiers archiveur. Ces certifications apportent une confiance supplémentaire dans la capacité à respecter les engagements de qualité et de sécurité du tiers archiveur.

	NORMES	CERTIFICATION	POINTS AUDITÉS ET CERTIFIÉS
Archivage électronique	<p><b>NF Z 42-013</b> : Archivage électronique - 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</p> <p><b>ISO 14641-1</b> est une traduction de NF Z 42-013 pour une application internationale</p>	<p><b>Règle NF 461</b> : Organisme de certification AFNOR</p>	<ul style="list-style-type: none"> <li>• <b>Conformité</b> : dossier de description technique du système permettant d'assurer la conformité du système d'archivage électronique lors des versements</li> <li>• <b>Intégrité</b> des documents : empreinte, métadonnées, traçabilité de l'ensemble des événements, journalisation...</li> <li>• <b>Sécurité du data center</b> : sécurité physique, cloisonnement des espaces clients, continuité d'activité</li> <li>• <b>Fidélité</b> des copies numériques : qualité de la chaîne de numérisation de documents, contrôles d'exhaustivité, journal des événements...</li> <li>• <b>Professionalisme et pérennité</b> de l'entreprise : gouvernance, rôle de conseil, accompagnement des projets clients...</li> </ul>
Archivage physique	<p><b>NF Z 40-350</b> : Prestations d'archivage et de gestion externalisée de documents</p>	<p><b>Règle NF 342</b> : Organisme de certification AFNOR</p>	<ul style="list-style-type: none"> <li>• <b>Sécurité</b> : protection des documents contre les risques d'incendie, le vol, les dégâts des eaux, les parasites (rongeurs).</li> <li>• <b>Contrôle</b> : contrôle des accès au lieu de conservation</li> <li>• <b>Confidentialité</b> : stockage aléatoire des documents d'archives, anonymat des boîtes, caisses, conteneurs, protection des données</li> </ul>

Notons que la certification NF Z 42-013 peut intégrer deux périmètres :

- Système d'Archivage Electronique à usage interne (pour un établissement de santé par exemple) ou pour un usage externe (tiers archiveur numérique),
- avec ou sans le périmètre de numérisation fidèle. Il n'est actuellement pas possible d'obtenir une certification NF Z 42-013 pour la numérisation uniquement.

### 3.3 • Les agréments du SIAF

Le SIAF<sup>37</sup> gère les attributions spécifiques aux archives de la Direction Générale des Patrimoines. Afin d'encadrer l'archivage des archives publiques, le SIAF a mis en place, pour garantir le respect de la loi<sup>38</sup>, des agréments qui autorisent l'externalisation d'archives publiques courantes ou intermédiaires sur supports physiques et/ou électroniques<sup>39</sup>. L'archivage définitif d'Archives de Santé reste, quant à lui, de la prérogative de l'organisme public compétent.

Le SIAF a mis en œuvre un dispositif d'agrément pour les périmètres d'archivage physique, et un autre pour l'archivage électronique sur la base d'un référentiel d'évaluation spécifique.

#### 3.3.1 L'agrément archivage physique

L'agrément du SIAF repose sur la norme AFNOR NF Z 40-350, renforcée d'exigences propres aux archives publiques, notamment :

- l'obligation de sprinklage des entrepôts de conservation au-delà d'un seuil de 3 000 m<sup>2</sup>,
- la nécessité de vérifier la validation par la personne chargée du contrôle scientifique et technique de l'Etat préalablement à toute opération de destruction. Cette procédure vise à éviter toute destruction non appropriée et à sélectionner les archives éligibles en tant qu'archives définitives qui devront être conservées dans un dépôt d'archives relevant du contrôle scientifique et technique.

Le SIAF n'impose pas de certification NF Z 40-350 pour les tiers archiveur. Cependant la certification est un gage de confiance supplémentaire, car les contrôles des sites de conservation réalisés par les conservateurs du patrimoine sont complétés par les audits réguliers d'AFNOR Certification.

#### 3.3.2 L'agrément archivage électronique

L'agrément du SIAF repose sur la norme AFNOR NF Z 42-013, renforcée d'exigences propres aux archives électroniques publiques, notamment :

- la référence au Référentiel Général de Sécurité de l'ANSSI (RGS) conférant lui-même à la série des normes ISO 2700X pour la sécurité des systèmes d'information,
- la référence au Référentiel Général d'interopérabilité (RGI) non spécifique à l'archivage ainsi qu'une préconisation de format d'interopérabilité SEDA<sup>40</sup>,
- la même exigence concernant les modalités de destruction que pour les archives physiques.

Les moyens nécessaires à l'audit d'un système d'archivage électronique étant importants, le SIAF a impulsé la création d'un référentiel de certification, NF 461, afin de certifier la conformité d'un SAE à NF Z 42-013.

La certification n'est pas imposée pour l'agrément mais amène une confiance supplémentaire dans la capacité d'un tiers archiveur à respecter l'état de l'art par des moyens d'audit considérablement élargis. En effet, l'agrément du SIAF nécessite, en plus d'une analyse de dossier, une journée d'audit tous les trois ans. Quant à lui, l'audit AFNOR nécessite un audit initial de 7 jours tous les trois ans ainsi qu'un audit de suivi par an.

---

<sup>37</sup> Service Interministériel des Archives de France (SIAF)

<sup>38</sup> [Articles L212-4 et R212-19 à R.212-31 du Code du Patrimoine](#)

<sup>39</sup> [Article L. 212-4 II du Code du Patrimoine](#)

<sup>40</sup> Standard d'échange de données pour l'archivage.

## 3.4 • La Complémentarité des agréments et certifications

### 3.4.1 Les principes généraux

Les prestataires agréés par le Ministère de la Culture (via le SIAF) pour les archives physiques le sont également pour l'hébergement de données de santé à caractère personnel sur support papier<sup>41</sup>. Cet agrément est applicable pour l'externalisation d'archives publiques mais également pour les archives de santé privées.

Toutefois il ne faut pas oublier que si l'agrément SIAF emporte ipso facto le droit de procéder à l'archivage de dossiers patients sur support physique, ce n'est pas le cas pour l'hébergement de dossiers patient sous forme électronique, soumis à l'agrément ASIP Santé (Décret n°2006-6 du 4 janvier 2006).

### 3.4.2 Le cas particulier des métadonnées pour l'archivage physique

Il faudra être particulièrement attentif aux métadonnées choisies pour décrire les archives physiques de santé externalisées. Lorsqu'elles contiennent des données personnelles à caractère médical, il est légitime de supposer qu'un agrément supplémentaire d'ASIP Santé puisse être nécessaire, si le système d'archivage physique contient des métadonnées de santé à caractère personnel sous forme numérique.

### 3.4.3 Le cas particulier de la numérisation

L'agrément du SIAF ne prend pas en compte le périmètre de la numérisation d'archives. Cependant, si le besoin est d'obtenir une copie numérique fidèle, une certification NF Z 42-013 intégrant le périmètre de numérisation peut être exigée.

Le SIAF a défini un cadre pour la numérisation d'archives publiques en vue de la destruction des originaux physiques<sup>42</sup>.

Ces dispositions peuvent être pertinentes pour les archives à faible valeur probatoire dont la durée de conservation est relativement courte, mais présentent un risque particulier pour les établissements de santé sur la reprise de fonds importants pour une durée de conservation longue (dossiers patients par exemple).

Une analyse de risque intégrant les considérations juridiques, économiques et archivistiques doit être réalisée dans le cadre de ce type de projet. Une « autorisation » préalable à la numérisation doit également être accordée par la personne chargée du contrôle scientifique et technique de l'Etat.



#### CONFORME, CERTIFIÉ, AGRÉÉ Quelles différences ?

Chacun peut déclarer un produit ou une prestation conforme. La confiance en la conformité ainsi déclarée dépend de la confiance accordée en celui qui la déclare, sans autre élément objectif.

La certification implique la réalisation des essais, examens et évaluations permettant de prouver le respect à l'ensemble des exigences, directives ou réglementations d'une norme.

Dans ce cas, un organisme indépendant et accrédité par le COFRAC procède à toutes les vérifications nécessaires. Si la satisfaction aux exigences de la norme visée est avérée, l'organisme de certification délivre un certificat. Un audit de contrôle est réalisé tous les ans afin de vérifier le maintien en conformité.

Autant une certification est d'application volontaire, autant un agrément est un « droit régalien » obligatoirement délivré par une autorité mandatée. Un agrément peut reposer sur les moyens de contrôle d'un tiers certificateur ou agréé pour réaliser le contrôle.

<sup>41</sup> [Article R. 1111-16 du Code de la Santé Publique](#)

<sup>42</sup> [Vade-mecum pour la destruction des archives publiques après numérisation](#)

### 3.4.4 Tableau de synthèse des certifications et agréments

Le tableau suivant synthétise les agréments et certifications à spécifier dans un cahier des charges pour l'externalisation des archives de santé chez un tiers archiveur.

 **Obligatoire**     **Préconisé**

SUPPORT DE LA DONNÉE	DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL	ARCHIVES PRIVÉES	ARCHIVES PUBLIQUES
Archives physiques	Sans	Certification NF Z 40-350	Agrément SIAF physique Certification NF Z 40-350
	Avec	Agrément SIAF physique Certification NF Z 40-350	
Métadonnées d'archives physiques	Sans	Certification NF Z 40-350	Agrément SIAF physique Certification NF Z 40-350
	Avec	Agrément ASIP Santé	Agrément ASIP Santé Agrément SIAF physique Certification NF Z 40-350
Archives électroniques + métadonnées de description	Sans	Certification NF Z 42-013	Agrément SIAF électronique Certification NF Z 42-013
	Avec	Agrément ASIP Santé Certification NF Z 42-013	Agrément SIAF électronique Agrément ASIP Santé Certification NF Z 42-013

Les principes à retenir :

- les archives publiques nécessitent un agrément du SIAF quel qu'en soit le support (physique ou électronique),
- dès qu'il existe une donnée de santé sous forme électronique, et quel qu'en soit son support (archives ou métadonnées), un agrément ASIP Santé est nécessaire,
- privilégier les tiers-archiveurs certifiés, même si aucun agrément n'est exigé.

Il convient d'être vigilant sur le périmètre d'application des certifications et agréments :

- les agréments SIAF concernent **des sites de conservation** pour les archives physiques et électroniques et non une personne morale dans sa globalité,
- l'agrément ASIP Santé concerne **une solution**. S'il s'agit d'une prestation d'archivage à vocation probatoire, il doit s'agir d'une solution d'archivage désignée en tant que telle,
- les certifications AFNOR concernent **des sites et des prestations**. Au même titre que les agréments, les périmètres de certification doivent coïncider avec les périmètres du besoin client.

## 4. Les 12 bonnes pratiques pour réussir l'externalisation des archives de santé

### AVANT D'EXTERNALISER

1	<p><b>Faire un état des lieux sur la nature et la constitution des fonds d'archives</b></p> <ul style="list-style-type: none"><li>• Identifier la nature et la forme des données à externaliser :<ul style="list-style-type: none"><li>▪ Données personnelles,</li><li>▪ Données de santé,</li><li>▪ De nature privée ou publique,</li><li>▪ Sous forme d'archives physiques, électroniques ou hybrides,</li><li>▪ Associées à des métadonnées.</li></ul></li></ul>
2	<p><b>Définir les prestations attendues</b></p> <ul style="list-style-type: none"><li>• Opération de mise en conformité des fonds d'archives physiques et électroniques (exemple : tri, description, dépollution...)</li><li>• Hébergement,</li><li>• Archivage à vocation probatoire,</li><li>• Numérisation (avec ou sans vocation probatoire),</li><li>• Sauvegarde.</li></ul>
3	<p><b>Spécifier les exigences en termes d'agrément et certifications</b></p> <ul style="list-style-type: none"><li>• Certifications NF Z 40-350 (physique) ou NF Z 42-013 (électronique et numérisation),</li><li>• Agrément SIAF (physique et / ou électronique),</li><li>• Agrément ASIP Santé.</li></ul>
4	<p><b>Vérifier les périmètres des agréments et certifications</b></p> <ul style="list-style-type: none"><li>• Le périmètre doit couvrir les prestations attendues par la solution proposée et les sites mentionnés sur les certificats.</li></ul>
5	<p><b>Identifier où seront localisées les données stockées</b></p> <ul style="list-style-type: none"><li>• Exiger une conservation sur le territoire national,</li><li>• Analyser pour chaque forme de données (archives, métadonnées, sauvegarde...) quel système assure l'hébergement et par qui il est opéré (contractant ou sous-contractant),</li><li>• Privilégier les solutions qui contiennent le moins d'intermédiaires possibles.</li></ul>
6	<p><b>Vérifier la conformité du contrat de dépôt</b></p> <ul style="list-style-type: none"><li>• Le tiers archiveur doit proposer un contrat de dépôt conforme aux prescriptions d'ASIP Santé spécifique aux établissements de santé,</li><li>• Les contrats de dépôt pour les archives publiques doivent être pré-validés par les services de contrôle scientifique et technique de l'Etat</li></ul>

## AU MOMENT D'EXTERNALISER

7	<b>Définir les métadonnées descriptives et les instruments de recherche</b> <ul style="list-style-type: none"><li>Le tiers archiveur doit apporter des conseils dans la définition des méthodes de description des archives afin de permettre la bonne gestion du cycle de vie des données et afin de constituer des moyens de recherches efficaces pour les utilisateurs</li></ul>
8	<b>Définir les modalités d'accès</b> <ul style="list-style-type: none"><li>Le système d'archivage électronique doit être paramétré pour permettre de gérer les habilitations d'accès des utilisateurs conformément aux spécifications du client,</li><li>Les administrateurs client du système doivent être responsabilisés et formés à l'administration des utilisateurs,</li><li>Un moyen d'authentification forte est imposé pour l'accès aux données de santé à caractère personnel.</li></ul>
9	<b>Valider l'adéquation au besoin avec les utilisateurs</b> <ul style="list-style-type: none"><li>Réaliser un test avec un échantillon d'archives et quelques utilisateurs clés avant le déploiement de la solution.</li></ul>

## APRÈS L'EXTERNALISATION

10	<b>Gérer le cycle de vie des archives</b> <ul style="list-style-type: none"><li>Identifier annuellement les archives éligibles à l'élimination,</li><li>Dans le cadre d'archives publiques, l'élimination doit être préalablement validée par les services exerçant le contrôle scientifique et technique de l'Etat,</li><li>Lorsque les dates d'élimination ne sont pas connues au moment du versement, procéder à l'identification des archives à détruire sous la responsabilité des établissements de santé et dans le respect de la législation applicable.</li></ul>
11	<b>Administrer « proprement » les utilisateurs</b> <ul style="list-style-type: none"><li>Mettre en œuvre une procédure d'information des administrateurs en cas de départ ou mutation d'un utilisateur afin de désactiver ses accès aux archives de santé,</li><li>Prévoir régulièrement des campagnes de vérification des bases utilisateurs et de révocation des mots de passe.</li></ul>
12	<b>Contrôler le tiers archiveur</b> <ul style="list-style-type: none"><li>Demander annuellement la mise à jour des certificats et agréments,</li><li>Vérifier la localisation des archives par sondage, assorti de visites,</li><li>Si le tiers archiveur n'est pas certifié, l'auditer selon les modalités contractuelles convenues et sur tous les sites de conservations déclarés.</li></ul>

## 5. L'élaboration du Livre Blanc

Ce livre blanc a été rédigé par les experts de LOCARCHIVES en charge des systèmes d'archivage, des certifications et agréments, avec l'appui d'un étudiant du Master 2 Droit des Affaires et de l'Entreprise, parcours Tiers de Confiance et Sécurité Numérique (promotion Louis Pouzin 2014-2015). Ce master de l'Université de La Rochelle a été créé en 2014 par la Fédération des Tiers de Confiance et la Faculté de Droit de La Rochelle avec le soutien de la Chambre Nationale des Huissiers de Justice.

### Comité de rédaction

- Xavier BERLOTY – Directeur Général
- Emeric SZPYRKA – Juriste
- Hervé STREIFF – Responsable Conformité et Sécurité de l'Information
- Séverine DENYS – Responsable Archivage Electronique
- Monica LELIEVRE – Juriste
- Marie BRUNELLO – Directeur Juridique
- Emmanuel FAURE – Directeur Stratégie et Marketing
- Alban VERCHERE – Responsable Développement Activités Numériques
- Samuel LE BIDEAU – Consultant

# LOCARCHIVES

Avec un chiffre d'affaires de 44,5 M€ en 2015, LOCARCHIVES se positionne comme le second prestataire de services en France, spécialiste de l'externalisation d'archives et de l'ingénierie documentaire. L'expertise en Records Management, en gestion documentaire et gestion de l'information permet de concevoir et de mettre en œuvre des solutions performantes, globales et évolutives de gestion – forme papier et électronique – pour plus de 4 500 clients professionnels.

**LES CHIFFRES 2015 : 450 SALARIÉS - 9 SITES DE CONSERVATION - 4 000 KM LINÉAIRES DE RAYONNAGES - CAPACITÉ DE STOCKAGE ÉLECTRONIQUE DE 1 PO. LOCARCHIVES EST MEMBRE DE L'AFNOR ET DE LA FNTC. AGRÉÉE HÉBERGEUR DE DONNÉES DE SANTÉ, LOCARCHIVES EST ÉGALEMENT CERTIFIÉE ISO 9001, NF Z 40-350 ET NF Z 42-013 - LABELLISÉE FNTC-TA - AGRÉÉE POUR LA GESTION ET LA CONSERVATION D'ARCHIVES PUBLIQUES SUR SUPPORTS PAPIER ET ÉLECTRONIQUES.**



Le master Droit du numérique, parcours Tiers de confiance et sécurité numérique, couvre, en complément de l'étude du droit applicable, les aspects technologiques mais également stratégiques, organisationnels et économiques de la confiance et de la sécurité numérique. A cette fin, l'équipe pédagogique associe universitaires, juristes et informaticiens, praticiens et experts de la dématérialisation.



Créé en 2001 en France par un ensemble d'acteurs institutionnels et de prestataires de services suite à la loi du 13 mars 2000 et afin de structurer les échanges numériques naissants, elle a pour vocation désormais à étendre son action au niveau international avec l'ensemble des acteurs qui souhaitent développer la confiance dans le numérique, que ce soit en Europe, dans les pays Francophones ou ailleurs.

## 6. Annexe

---

Changements à venir avec la « loi de modernisation de notre système de santé »<sup>43</sup> : ce texte adopté en nouvelle lecture par l'Assemblée nationale le 1er décembre 2015, a été promulgué le 21 janvier 2016.

Cette « loi santé » portée par Marisol Touraine donne un aperçu de ce qui va changer pour l'hébergement des données de santé :

### 1° Sur le consentement de la personne :

Actuellement, le consentement exprès et préalable de la personne concernée est nécessaire pour l'hébergement externalisé, sauf exception prévue par le Code de la Santé Publique. La nouvelle rédaction modifie cela. A l'avenir il s'agira simplement d'informer la personne concernée de l'hébergement de ses données de santé. Par conséquent, le consentement exprès ne sera plus nécessaire. Cependant, la personne concernée conservera le droit de s'opposer à l'hébergement de ses données de santé pour un motif légitime.

### 2° Le projet de loi autorise le gouvernement à prendre par voie d'ordonnance des dispositions pour « simplifier la législation en matière de traitement des données personnelles de santé ».

Cela impliquera :

- a) d'harmoniser les dispositions relatives aux procédures d'agrément des hébergeurs de données de santé,
- b) de remplacer l'agrément actuel de l'ASIP Santé par une accréditation donnée par l'instance nationale d'accréditation<sup>44</sup>,
- c) d'encadrer les conditions de destruction des dossiers médicaux conservés sous une autre forme que numérique, lorsqu'ils ont fait l'objet d'une numérisation.

Concernant les points a) et b), et d'après le projet de loi, l'ordonnance entraînera les changements suivants :

Il s'agira de **transformer la procédure d'agrément en procédure de certification placée sous la responsabilité du COFRAC**. Le dispositif d'agrément des hébergeurs repose actuellement sur un double examen des demandes d'agrément par la CNIL et par une instance ad-hoc, le « *comité d'agrément des hébergeurs de données de santé* », dont le secrétariat est assuré par l'ASIP Santé. La spécificité nationale et la lourdeur de ce dispositif constituent un obstacle à sa transposition au niveau européen ou international. **Il est donc proposé d'évoluer vers une démarche de certification en transférant la compétence d'agrément des hébergeurs à des opérateurs économiques certifiés par le COFRAC**, instance nationale d'accréditation créée par le décret du 19 décembre 2008. Au-delà de la possibilité d'extension de ce dispositif au niveau international, cette évolution libèrerait les pouvoirs publics d'une charge de travail et de coûts non négligeables, ces derniers reposant sur les prestataires souhaitant être certifiés.

Concernant le point c) : il s'agira, dès lors qu'un établissement ou professionnel de santé dispose d'un dossier patient informatisé, de procéder à la **destruction des dossiers papier après leur numérisation** dans des conditions définies par un décret en Conseil d'État, et garantissant l'authenticité, l'intégrité et la pérennité de leurs copies numériques.

**3° Le projet de loi supprime la référence aux PS, ES<sup>45</sup> et aux autres personnes concernées**, de sorte que tout responsable de traitement de données de santé à caractère personnel doit respecter l'obligation de recourir à un tiers agréé pour l'hébergement de données de santé.

Après adoption, **la loi sera a priori d'application immédiate**, et l'ordonnance modifiant le décret de 2006<sup>46</sup> sera prise rapidement.

---

<sup>43</sup> Pour plus d'infos, suivre le lien : <http://www.assemblee-nationale.fr/14/projets/pl2302.asp>

<sup>44</sup> Mentionnée à l'article 135 de la loi n° 2008- 776 du 4 août 2008 de modernisation de l'économie

<sup>45</sup> Professionnels de Santé et Etablissements de Santé

<sup>46</sup> [Décret n°2006-6 du 4 janvier 2006](#)

POUR PLUS D'INFORMATIONS

**LOCARCHIVES**

Tiers Archiveur de Confiance

Solutions globales d'Archivage  
& de gestion documentaire

[contact@locarchives.fr](mailto:contact@locarchives.fr)

01.49.33.78.81

LOCARCHIVES est agréée HADS depuis décembre 2015.

