Domaine Infrastructures (« *ITI domain* »)

Livre blanc – Production, gestion et préservation de la valeur neutre et probante de l'information médicale

Identification du document	
Référence	**Livrable**_Complet_20160305_V1-0.Docx
Date de création	26/10/2015
Date de dernière mise à jour	03/05/2016
Etat	En cours / A vérifier / A valider / **Validé**
Version	V 1.0
Nombre de pages	137

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ
Archives de France
Interop'Santé
Pour des systèmes d'information communicants

Documents de référence	
Titre	Auteur
1. Archivage du Dossier Patient : Enjeux et principes de mise en œuvre	ANAP
2. Arrêté du 4 décembre 2009 du ministère de la culture	Ministère de la culture
3. RGI Référentiel Général de l'Interopérabilité, version 1.9.7	Secrétariat Général pour la Modernisation de l'Action Publique
4. Standard SEDA	SIAF
5. Présentation synthétique du règlement eIDAS	SIAF
6. Présentation complète du règlement eIDAS	Didier GOBERT
7. Référentiel Général de gestion des Archives RGA	SIAF
8. Norme OAIS	CCSDS
9. Norme NF Z 44-022 (MEDONA)	AFNOR
10. Norme NF Z 42-013 : archivage électronique	AFNOR
11. Vade-mecum : autoriser la destruction de documents sur papier après leur numérisation	SIAF
12. PGSSI-S, Référentiel d'authentification des acteurs de santé	ASIP
13. PGSSI-S, Référentiel d'imputabilité	ASIP
14. CI SIS cadre d'Interopérabilité des SIS	ASIP
15. XDS-b	IHE
16. DSG Digital Signature	IHE
17. Metadata update	IHE
18. Messagerie de Santé Sécurisée MSS	ASIP
19. Livre blanc « Harmonisation des modes de communications des documents médicaux en intra hospitalier »	Interop'Santé
20. DRPT Displayable Report	IHE
21. Rapport GHT publié en mai 2015	Mission GHT
22. NF EN ISO 15189 : Laboratoires de biologie médicale - Exigences concernant la qualité et la compétence - Laboratoires d'analyses de biologie médicale	AFNOR
23. DSUB : Document Metadata Subscription	IHE

Remerciements

Ce Livre blanc est le fruit des travaux d'un groupe d'IHE ITI France d'InteropSanté, composé des personnes suivantes :

Prénom Nom	Rôle	Organisation
Isabelle GIBAUD	Animateur Rédactrice	InteropSanté/GIP-SIB
Antoine MEISSONNIER	Co-rédacteur	SIAF

Les contributeurs :

Prénom Nom	Rôle	Organisation
Marianne APTEL	Contributeur	XDEMAT
Antony BELIN	Contributeur	Application Projets Infogé-rance. ADULLACT Projet
Olivier BOUSSEKEY	Contributeur	GHPSJ
Jean-Christophe CAUVIN	Contributeur	MEDASYS
Christine COUPE	Contributeur	GIP-SIB
Roger GIMENEZ	Contributeur	XDEMAT
Isabelle GIBAUD	Contributeur	GIP-SIB
Baptiste NICHELE	Contributeur	SIAF
Antoine MEISSONNIER	Contributeur	SIAF
Jean-Marc RIETSCH	Contributeur	EIFISA
Régine TOMASSO	Contributeur	ANTICYCLONE
Manuel METZ	Contributeur	ASIP SANTE

Les participants :

Prénom Nom	Rôle	Organisation
Brice ACHDOU	Participant	DLSANTE
Yves BEAUCHAMP	Participant	ANAP
Léa BENONY	Participant	NAONED
Magali BONAVENT	Participant	GIP CPAGE
Elisabeth BOUILLOT	Participant	MIPIH
Bernard CASSOU-MOUNAT	Participant	Ministère des affaires sociales et de la santé
François DECOURCELLE	Participant	ENOVACOM
Florian FOUCAULT	Participant	GROUPE SAINTE MARGUERITE
Alexis GADENNE	Participant	SILPC

Xavier GAILLARD	Participant	AGFA
Alexandre GUIMOND	Participant	LEXMARK
Cassandre HUC	Participant	MIPIH
Hervé LEMAI	Participant	CIMAIL
Bertrand LE QUELLEC	Participant	HITACHI DATA SYSTEMS
Eric MARCHAND	Participant	MAINCARE
Yohann POIRON	Participant	OPENXTREM
Lucas RAYMOND-PIERRE	Participant	CH VERSAILLES
Philippe RIZAN	Participant	CURIE
Valérie ROUSSEL	Participant	LOGEMED
Olivier THEVENEAU	Participant	APHM
Vuong VU-TIEN	Participant	SECODIF

Sommaire

Préambule et grille de lecture

La constitution du groupe de travail Interop'Santé à l'origine de ce livre blanc fait suite aux travaux réalisés par l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP) au sujet de « L'archivage du dossier patient : enjeux et principes de mise en œuvre », publiés le 10 septembre 2013[1]. Il s'agissait d'un corpus documentaire construit par un groupe multidisciplinaires (constitué d'archivistes, de médecins des départements de l'information médicale (DIM), des associations professionnelles des archivistes, de directeurs des systèmes d'information (DSI), etc.), validé par le Service interministériel des Archives de France (SIAF). Il proposait aux acteurs des établissements hospitaliers des éléments de méthodologie pour construire leur propre démarche d'archivage dans un cadre qui fournissait :

- des fiches de synthèse règlementaire,
- un guide méthodologique et un document type de Politique d'Archivage,
- un guide méthodologique et un plan détaillé type de Déclaration des politiques d'archivage, permettant de formaliser les méthodes et outils de mise en œuvre de la Politique d'Archivage,
- une matrice de l'archivage des données/documents de l'établissement, permettant de construire un référentiel des informations à archiver.

Même si ces travaux étaient fondateurs, ils ne suffisent pas, à ce jour, pour permettre aux établissements de santé de s'engager sereinement dans une démarche de dématérialisation et d'archivage électronique de l'information médicale à valeur neutre et probante.

Pour répondre à ce besoin, l'association Interop'Santé a proposé de créer un groupe de travail dédié à ce sujet. Ce présent document est le résultat des travaux de ce groupe de travail qui a réuni les représentants de l'ANAP, de l'Agence des Systèmes d'information partagés de Santé (ASIP), du Service Interministériel des archives de France (SIAF) et des adhérents de l'association Interop'Santé.

Ce livre blanc s'adresse aux pouvoirs publics, aux directeurs des systèmes d'information (DSI) des établissements hospitaliers, aux chefs de projets, aux archivistes, aux médecins du département d'information médicale (DIM) , aux éditeurs de SIH et aux éditeurs de SAE (Services d'Archivage Electronique). Il traite à la fois d'aspects juridiques, métiers et techniques.

Le chapitre 1 décrit le contexte réglementaire et normatif dans lequel s'inscrit le livre blanc.

Le chapitre 2 liste les objectifs du groupe de travail à l'origine de ce livre blanc.

Le chapitre 3 précise le périmètre du livre blanc et le réduit aux archives courantes et intermédiaires.

Le chapitre 4 présente les caractéristiques de valeur neutre et probante d'une archive.

Ainsi, les chapitres 1, 2, 3 et 4 s'adressent à la fois aux archivistes, aux DSI, aux DIM et aux éditeurs.

[1] ANAP : http://www.anap.fr/publications-et-outils/publications/detail/actualites/larchivage-du-dossier-patient-enjeux-et-principes-de-mise-en-oeuvre/

Le chapitre 5 présente la norme CDA de structuration des documents médicaux et les profils IHE propres au domaine de la santé qui permettent de gérer au plus tôt les caractéristiques d'une archive présentées au chapitre 4. Il est un peu plus technique que les chapitres précédents mais reste suffisamment généraliste pour être consulté par un public diversifié.

Le chapitre 6 décrit des cas d'usage métier décrivant le cycle de vie de l'information médicale dans différents contextes. Pour chaque cas d'usage un ou plusieurs profils IHE présentés au chapitre 5 sont proposés pour permettre de gérer et de conserver au plus tôt la valeur neutre et probante des archives.

Le chapitre 7 s'adresse aux éditeurs de SIH et de SAE. Il effectue la comparaison entre la norme MEDONA (norme d'échange entre le SIH et le SAE) et le profil IHE-XDS implémenté par les éditeurs de SIH dans un contexte de partage de documents médicaux au sein d'une communauté médicale. L'objectif de cette comparaison est de déterminer s'il est possible pour les éditeurs de SIH de réutiliser les concepts XDS pour s'interfacer avec un SAE.

Le chapitre 8 liste les évolutions à prévoir en termes techniques et réglementaires et le chapitre 9 conclue ce livre blanc.

L'annexe 1 donne des repères réglementaires et normatifs au lecteur pour faciliter le choix d'un service d'Archivage Electronique (SAE).

L'annexe 2 établit une comparaison détaillée MEDONA/XDS.

Les commentaires et les interrogations relatives à ce livre blanc pourront être envoyés à l'adresse suivante : info@interopsante.org

1 Le contexte

Les travaux de l'ANAP « L'archivage du dossier patient » se sont accompagnés d'évolutions législatives, réglementaires et normatives importantes. Dans le cadre de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, une disposition (art. 204, 5°, d) habilite le gouvernement à légiférer par ordonnance afin d'atteindre trois objectifs :

- fixer les critères de valeur probante de la copie numérique de documents de santé papier,
- fixer les exigences pour la constitution de données numériques natives à valeur probante,
- fixer les critères de conservation de ces documents et données numériques afin de garantir leur valeur probante et leur lisibilité à long terme.

En parallèle, l'article 1348 (futur article 1379[2]) du Code Civil relatif à la valeur probante de la copie d'un écrit va être modifié à partir du 1er octobre 2016 pour reconnaître pleinement la valeur de la copie numérique fiable, conformément aux dispositions de l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

Dans le cadre d'une réflexion sur la normalisation française en matière d'informatique de santé, le ministère de la Santé s'interroge actuellement sur la nécessité d'une adaptation de la norme d'archivage électronique NF Z42-013 (ISO 14641-1) au secteur de la santé. Il convient de rappeler que l'arrêté du 4 décembre 2009 du ministère de la culture[3] retient les normes NF Z42-013 (ISO 14641-1) et OAIS (ou ISO 14721) pour permettre les prestations en archivage et gestion externalisée des archives publiques sous forme électronique. Le lecteur pourra se référer au chapitre 4 de ce livre blanc concernant ces normes.

Le Référentiel Général d'Interopérabilité (RGI) est en cours de refonte. La version 1.0 du RGI publiée par arrêté du 11 novembre 2009 est remplacée par la version 1.9.7 actuellement en concertation publique.[4]
Le Standard d'Echanges de Données pour l'Archivage (SEDA)[5], maintenu par le SIAF, y figure dans le profil d'archivage électronique. Ce standard SEDA a donné lieu à la publication d'une norme AFNOR, la NF Z44-022 ou MEDONA (Modélisation des Echanges de Données pour l'Archivage).

[2] Cette partie du Code civil sera effectivement modifiée à compter du 1er octobre 2016 par l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

[3] Arrêté du 4 décembre 2009 du ministère de la culture : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021467028

[4] Version 1.9.7 du RGI actuellement en commentaires : http://references.modernisation.gouv.fr/sites/default/files/Referentiel_General_Interoperabilite_V1.9.7-8.pdf

[5] Pour plus de renseignement, voir http://www.archivesdefrance.culture.gouv.fr/seda/

A ce jour, la version 2.0 du SEDA, qui est une spécialisation de MEDONA adaptée à la description et à l'échange d'archives publiques dans le contexte français, a été publiée en décembre 2015[6] et est en cours de normalisation à l'ISO.

Par ailleurs, la réglementation encadrant la signature électronique va être bousculée par l'application au 1er juillet 2016 du règlement « eIDAS » du 23 juillet 2014[7]. Un groupe de travail interministériel piloté par l'ANSSI est en cours afin d'évaluer les évolutions réglementaires nécessaires pour disposer d'un cadre cohérent. Le Référentiel Général de Sécurité (RGS) va connaître des évolutions de ce fait.

C'est dans ce contexte de montée en puissance du cadre juridique de la dématérialisation que s'inscrit la réflexion du groupe de travail Interop'Santé.

2 Objectifs

Ce document vise à poser les bases d'une réflexion portant sur les prérequis nécessaires et suffisants à mettre en œuvre dans les systèmes d'information (SI) de santé pour assurer au plus tôt le caractère neutre et probant des informations médicales, conformément à l'état de l'art existant dans le domaine de l'archivage électronique et de l'interopérabilité des SI de santé.

Ces notions d'archive neutre et à valeur probante sont décrites au chapitre 4 du présent document.

La réflexion au sein du groupe de travail Interop'Santé a eu pour objet :

1. d'obtenir un consensus large de l'ensemble des éditeurs et des utilisateurs sur la définition des prérequis sur les conditions de production et de gestion de l'information médicale au niveau du SIH (archives courantes) permettant d'assurer au mieux la valeur probante de l'information médicale dès sa création et de la préserver.
2. d'obtenir un consensus également sur les solutions techniques d'interopérabilité à mettre en œuvre entre le SIH (archives courantes) et le SAE (Service d'Archivage Electronique – archives intermédiaires).
3. de rédiger des recommandations à destination des acteurs de terrain et des éditeurs pour assurer la valeur probante et d'attirer l'attention des pouvoirs publics sur des points de règlementation ou de normalisation manquants.

Le premier point a été abordé par l'angle de la présentation de cas d'usage de production et de gestion de l'information médicale qui décrivent des situations concrètes de création et de communication de l'information dans des contextes particuliers. Dans chacun de ces cas d'usage, des normes et profils IHE sont recommandés par InteropSanté, ces normes et profils permettant d'assurer au plus tôt la valeur neutre et probante de l'information.

[6] http://www.archivesdefrance.culture.gouv.fr/seda/.

[7] Pour une présentation synthétique du règlement eIDAS, voir ce billet du carnet de recherche du SIAF : https://siaf.hypotheses.org/266
Pour une présentation complète, voir cette note d'un des négociateurs belges du règlement : http://www.droit-technologie.org/upload/dossier/doc/273-1.pdf

Le deuxième point a été abordé par l'angle d'une comparaison entre la norme MEDONA d'un côté et le profil IHE-XDS éventuellement associé à la norme CDA de l'autre. L'objectif de cette deuxième partie du livre blanc est de déterminer comment faire converger les standards et normes précitées pour garantir l'interopérabilité entre SAE et SIH.

Le troisième point résulte de l'analyse des deux premiers points.

Ce livre blanc précise la mise en œuvre du profil IHE-XDS-b, contraint par le CI_SIS pour l'implémentation en France d'une déclinaison des normes OAIS et SEDA 2.0/NF Z44-022 (MEDONA) dans le domaine de la santé.

Dans un second temps les éléments de conclusion de ce livre blanc pourraient être transmis au niveau IHE international pour prise en compte des évolutions éventuelles du profil IHE XDS.

3 Périmètre du livre blanc

Les archives, au sens de l'article L211-1 du Code du patrimoine, constituent « 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 ». Contrairement à l'idée commune, les archives sont donc en droit français autant des données numériques que d'anciens registres papier. Un dossier patient, sous forme papier ou informatisé (DPI) est donc, **dès sa création**, constitué de documents d'archives.

Il convient de distinguer les archives publiques, produites par une personne publique ou une personne privée dans l'exercice d'une mission de service publique (Code du patrimoine, art. L211-4), des archives privées. Les premières sont soumises à un contrôle précis à des fins de transparence et de garantie de la constitution de la mémoire de la Nation[8].

Le DPI est à la fois l'outil de coordination des soins apportés au patient, mais également l'outil de gestion de la preuve en cas de contentieux. En effet, un contentieux peut survenir juste après la sortie du patient de l'établissement ou même pendant la prise en charge, alors même que les informations médicales issues de cette prise en charge n'ont pas encore été communiquées au SAE. Dans ce cas, le juge en charge du contentieux va déléguer des experts qui devront analyser l'ensemble des documents (en version finale, non modifiables) et des traces, stockés dans le DPI, pertinents dans le cadre de l'hospitalisation.

Cette dualité d'usage du DPI confère un caractère d'archive à chaque document médical produit lors de l'épisode de soins et impacte les SIH dans le sens où les systèmes producteurs de ces documents devront d'emblée mettre en œuvre des exigences techniques permettant de garantir les caractéristiques d'un objet d'archive.

Le système d'information doit également intégrer la problématique du cycle de vie de l'information numérique en permettant notamment de gérer les durées d'utilité administra-

[8] Pour une présentation complète de la législation applicable aux archives publiques en France, voir le *Référentiel général de gestion des archives* (octobre 2013) : http://www.gouvernement.fr/referentiel-general-de-gestion-des-archives.

tive (DUA) de l'information définies dans la législation française.

Ainsi que le Code du patrimoine le définit (art. R212-10 à 12), ce cycle de vie de l'information est caractérisé par trois phases principales, représentées sur la figure 3-1, issue des travaux de l'ANAP :

- La création et la gestion des archives courantes. Toute information numérique, dès sa création dans le système d'information, constitue une archive courante. Une des caractéristiques de cette information est qu'elle est utilisée par l'équipe de soins tout au long de la prise en charge du patient, tout en ayant d'emblée un caractère d'archive. Le présent document propose des solutions en termes de normes et d'implémentation de profils IHE qui permettent d'assurer le caractère d'archive neutre et à valeur probante dès la création de l'information.
- La mise en œuvre d'un service d'archivage électronique (SAE) intermédiaire pour permettre la conservation sur le long terme de l'information numérique à valeur probante, quand l'information n'a plus d'usage fréquent (par exemple lorsque l'affaire qu'elle concernait est terminée), mais que le service qui l'a produite peut encore en avoir besoin pour faire face à des recours, à d'éventuels délais de prescription ou encore pour l'instruction d'autres affaires. Le présent document propose des solutions pour interfacer de façon normalisée le SIH au SAE.
- Le versement des archives, après sélection, vers le service public d'archives historiques compétent (pour un établissement de santé exerçant une mission de service public, il s'agit des archives départementales).

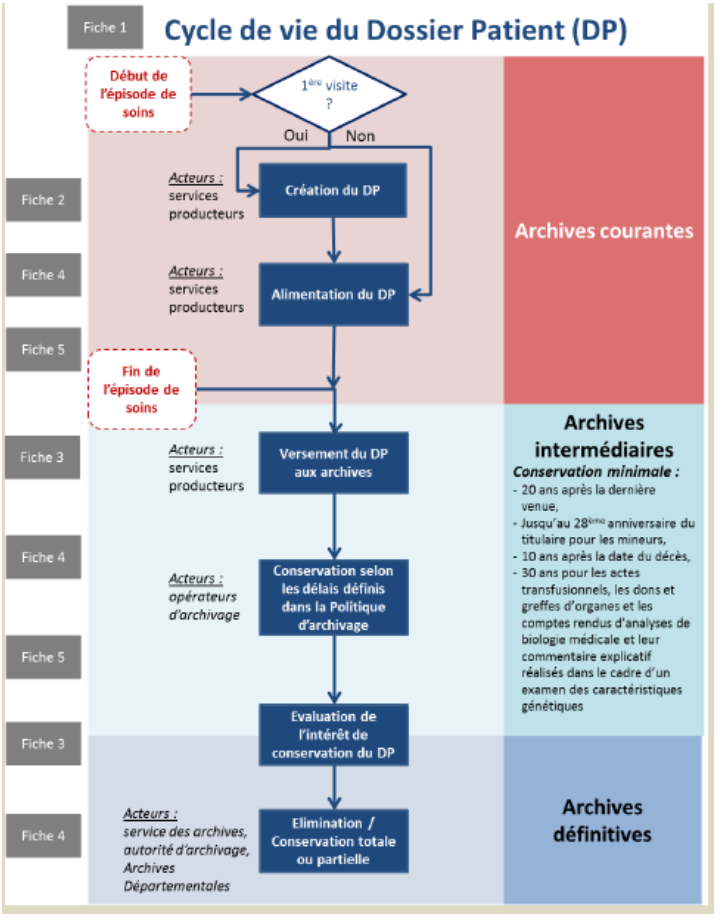


Figure 3-1 : Cycle de vie du DPI *(Extrait ANAP : Fiches règlementaires)*

Le périmètre de l'étude conduite dans le cadre de ce livre blanc correspond à la gestion du cycle de vie de l'information depuis sa création jusqu'à sa conservation, au sens de la norme ISO 15489 « Record management » , c'est à dire du « *champ de l'organisation et de la gestion en charge d'un contrôle efficace et systématique de la création, de la réception, de la conservation, de l'utilisation et du sort final des documents, y compris des méthodes de fixation et de préservation de la preuve et de l'information liée à la forme des documents.* ».

Le périmètre du livre blanc est en conséquence limité aux archives courantes et intermédiaires et ne prend pas en compte les archives définitives ni même l'interopérabilité entre les archives intermédiaires et les archives définitives, même si la mise en œuvre des recommandations contribuerait grandement à faciliter le versement d'archives historiques dans les services d'archives départementales compétentes équipées d'un SAE.

Pour ce qui concerne les archives courantes, ce livre blanc a pris en compte le circuit informatisé des données médicales :

- qui circulent au sein de l'établissement hospitalier,
- qui sont échangées avec les acteurs externes (médecine de ville, laboratoires externes, etc.).

Les données administratives, le processus de numérisation en tant que tel (seul le résultat de la numérisation est pris en compte), ainsi que les images radiologiques et les courriels sont exclus du périmètre de ce livre blanc.

4 Les caractéristiques d'une archive

Les notions de valeur neutre et valeur probante de l'information numérique, lorsqu'elles sont mises en œuvre, garantissent un archivage sécurisé de cette information sur le long terme. Elles sont garanties par l'application de normes de portée internationale ou nationale comme :

- La norme OAIS[9] (Open Archival Information System), qui définit les exigences en termes de structuration de l'information à archiver ainsi que les exigences fonctionnelles d'un service d'archivage électronique. Son objectif est de garantir la pérennité et la lisibilité des informations dans le temps,
- Le standard SEDA 2.0[10] et la norme NF Z 44-022[11] (MEDONA), qui fournissent un cadre normatif pour les différents échanges d'informations (données comme métadonnées) entre le service d'archives et ses partenaires,
- La norme NF Z 42-013[12] (ISO 14 641-1) qui définit les principes de journalisation et de contrôle d'intégrité nécessaires pour attester de la conservation de la valeur probante d'un document numérique dans le temps.

[9] Norme OAIS : http://public.ccsds.org/publications/archive/650x0m2.pdf

[10] SEDA : voir http://www.archivesdefrance.culture.gouv.fr/seda/

[11] NF Z 44-022 (MEDONA) : http://www.boutique.afnor.org/norme/nf-z44-022/medona-modelisation-des-echanges-de-donnees-pour-l-archivage/article/814057/fa179927

[12] NF Z 42-013 : 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 :

4.1 Format neutre de l'archive

Le **caractère neutre** de l'archivage de l'information correspond au fait de conserver cette information associée au patient de façon indépendante du système d'origine qui l'a produite. Cette neutralité de l'archivage implique l'utilisation de normes/standards qui permettent de structurer et de transporter l'information de façon indépendante de tout système d'origine. Le principe de réversibilité des SAE prévu par la norme NF Z 42-013 concourt à cet objectif de neutralité.

La figure 4.1-1 représente les exigences en termes de structuration de l'information archivée conformément à la norme OAIS.

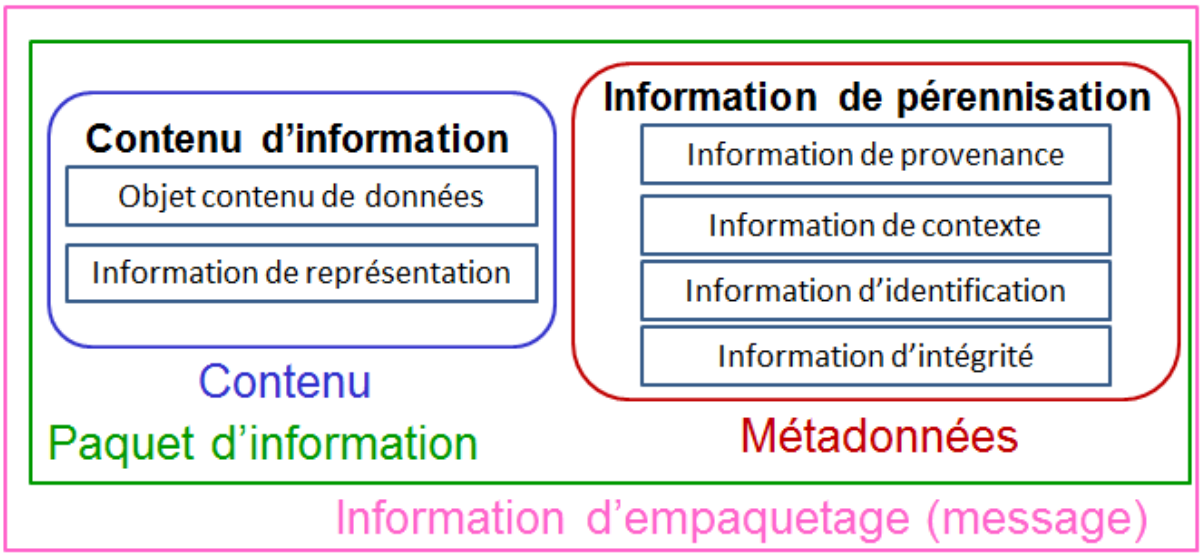


Figure 4.1-1 : Normalisation de la structuration de l'information archivée (norme OAIS)

La norme OAIS spécifie que le contenu d'information (le document associé à ses informations de représentation) doit être associé systématiquement à des métadonnées qui décrivent le contexte dans lequel le document a été produit. Contenu (représenté en bleu sur la figure 4.1-1) et métadonnées (représentées en rouge sur la figure 4.1-1) sont regroupés dans un paquet d'information (représenté en vert sur la figure 4.1-1), lui-même inclus dans un message d'empaquetage (représenté en rose).

L'hypothèse de départ du groupe de travail est la suivante : dans le domaine de la santé, la norme CDA associée aux profils de la famille IHE-XDS (profil IHE XDS-b, IHE XDM, IHE DSUB, IHE DRPT) pourrait répondre aux exigences fixées par la norme OAIS. Cette hypothèse est étudiée et détaillée dans le présent document au chapitre 7.

4.2 La valeur probante de l'archive

La valeur probante d'un écrit électronique est explicitée par l'article 1316-1 (futur article 1366) du Code Civil : « *L'écrit sous forme électronique est admis en preuve au même titre que*

http://www.boutique.afnor.org/norme/nf-z42-013/archivage-electronique-specifications-relatives-a-la-conception-et-a-l-exploitation-de-systemes-informatiques-en-vue-d-assurer/article/773362/fa125098

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 les conditions de nature à en garantir l'intégrité. »

Depuis la loi n°2000-230 du 13 mars 2000, un acte juridique électronique en droit civil dispose de la même force de preuve qu'un document papier sous certaines conditions[13], même si la notion d'archivage légal n'existe pas en droit français. En effet, il n'y a pas à ce jour de certification des conditions de conservation assurant la valeur probante d'un document conformément aux conditions énoncées à l'article 1316-1 (futur article 1366) du Code civil. En cas de litige juridique sur un document électronique, c'est le juge qui décidera de la valeur probante de cette information en fonction des éléments techniques dont il disposera et de leur conformité avec les dispositions du Code civil[14].

En termes techniques, la valeur probante du document archivé est assurée par les caractéristiques suivantes:

- Son authenticité, caractéristique qui intègre la présomption d'intégrité et d'exactitude de l'origine de l'information ainsi que l'horodatage de cette information (au sens Record Management).
    - L'origine de l'information sous-tend la notion d'imputabilité :
        - Possibilité d'identifier de façon non ambigüe l'auteur du document,
        - Impossibilité pour l'auteur de répudier le document par la suite,
    - Son intégrité :
        - Assure le caractère complet et non altéré du document.
    - Son horodatage : sa date de création doit être tracée en conformité avec un temps de référence.
- Son exploitabilité et son intelligibilité
    - Le document peut être localisé, récupéré, communiqué et interprété de façon lisible et compréhensible par le lecteur.

Pour utiliser un écrit à titre de preuve, encore faut-il pouvoir en disposer au moment opportun : c'est pourquoi la pérennité du document est un facteur indirect essentiel de sa valeur probante. Il convient de respecter sa durée de conservation qui va dépendre du type de contenu informationnel et des textes réglementaires.

Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein de l'Europe, abroge la directive Européenne 1999/93/CE relative à la signature électronique. En tant que règlement européen, il s'impose d'emblée au niveau national sans adaptation possible. Il détermine notamment les règles applicables aux services de confiance électronique et instaure un cadre juridique en

[13] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

[14] Cette réflexion juridique est ici simplifiée : il faut savoir que ce principe n'est valable que pour les actes juridiques en droit civil. Pour les faits juridiques comme pour les autres domaines du droit (notamment en droit administratif), la preuve est libre. Aucun texte ne vient donner des dispositions orientant le choix du juge qui est libre de décider d'accepter ou non une preuve. Pour plus de précision sur la validité et la recevabilité de l'écrit électronique devant les tribunaux, voir l'annexe 2 du vade-mecum du Service interministériel des Archives de France intitulé *Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision ?* (version de mars 2014) [en ligne : http://www.archivesdefrance.culture.gouv.fr/static/7429].

particulier pour les services de signatures électroniques, de cachets électroniques (ou scellement) et d'horodatages.

Le règlement précise la notion de service de confiance « qualifié » ou « non qualifié »[15].

Ainsi, « Les notions de service de confiance *qualifié* et de prestataire de services de confiance *qualifié* devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis ». Tous les services qualifiés sont associés à une clause de présomption qui dispense l'établissement d'avoir à faire la preuve de l'efficacité du service en cas de litige.

A contrario, dans le cas d'un service « non qualifié », l'établissement devra apporter, en cas de litige, la preuve devant une juridiction que le service est fiable et qu'il offre les garanties attendues. Néanmoins, le service « non qualifié » ne peut pas être réfuté comme preuve juridique au seul motif qu'il ne correspond pas aux exigences d'un service de confiance « qualifié ».

Le règlement n'impose pas d'usage et laisse le choix du niveau d'exigence des services d'authenticité de l'information mis en œuvre : simple traçabilité sécurisée de ces éléments, utilisation d'une signature électronique, d'un cachet électronique et système d'horodatage participant à l'élaboration de la valeur probante de l'information médicale.
Le choix du niveau d'exigences à mettre en œuvre dépendra de la stratégie juridique et de la politique de gestion des risques définie par l'établissement de santé.

la qualification du service permet de bénéficier des effets de droit prévus dans les différents articles du règlement décrivant ces solutions (art. 25.2 pour les signatures, 34.2 pour les services de conservation de la signature, 35.2 pour les cachets, 41.2 pour l'horodatage électronique).

En France, dans le domaine de la santé, le caractère d'imputabilité/d'intégrité de l'information médicale au sein du SIH est assuré par le choix d'implémentation d'un niveau d'authentification associé à un des paliers décrits dans le référentiel d'authentification des acteurs de santé publié dans le cadre de la PGSSI-S rédigée par l'ASIP santé[16].

Le choix du palier à mettre en œuvre dépendra de la stratégie juridique et de la politique de gestion des risques définie par l'établissement de santé.

Le référentiel d'imputabilité, publié également dans le cadre de la PGSSI-S[17], définit « les prérequis techniques à la mise en œuvre des conditions d'imputabilité de l'information :

[15] Le lecteur pourra se reporter à l'analyse de Didier GOBERT concernant le règlement européen du 23 juillet 2014 : http://www.droit-technologie.org/upload/dossier/doc/273-1.pdf et au résumé disponible sur le carnet de recherche du SIAF : https://siaf.hypotheses.org/266.

[16] Référentiel d'authentification des acteurs de santé : http://esante.gouv.fr/sites/default/files/pgssi_referentiel_authentification_v.2.0.pdf

[17] Référentiel d'imputabilité Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)- Décembre 2014 - V1.0 : http://esante.gouv.fr/sites/default/files/pgssi_referentiel_imputabilite_v1.0_0.pdf

- Les mesures mises en place pour identifier et authentifier les utilisateurs doivent correspondre au moins à celles définies dans le cadre du premier palier de l'authentification de la PGSSI-S (authentification des acteurs par login/mot de passe),
- Une gestion centralisée des identités, des rôles et des contrôles d'accès aux applicatifs et données du système d'information est mise en place,
- Les composants appartenant au même SI doivent disposer d'horloges synchronisées entre elles de manière à ce que les traces générées sur différents composants soient cohérentes. » (Extrait PGSSI-S, référentiel d'imputabilité).

D'autre part, concernant la force probante de l'écrit électronique, le référentiel d'imputabilité précise que « dans le cadre d'une action judiciaire, les traces générées par un système d'information sont susceptibles de constituer un écrit électronique admissible à titre de preuve devant une juridiction civile, pénale ou administrative. Dès lors qu'il est possible de collecter et de conserver des traces dans des conditions garantissant leur intégrité et d'établir un lien entre les actions constatées au sein du système d'information et leur auteur présumé, chacune des traces aura la qualité de preuve ayant la même force probante qu'un écrit sur support papier. » (Extrait PGGSI-S, référentiel d'imputabilité, ASIP). En effet, « les traces contribuent à gérer l'imputabilité dans un SI en permettant la conservation du lien entre les actions réalisées sur le système d'information et leurs auteurs. » Le référentiel d'imputabilité différencie les traces techniques des traces embarquées. Ces dernières correspondent par exemple aux métadonnées associées à un document dématérialisé et identifiant l'auteur et/ou la signature du document dématérialisé.
L'ensemble des traces, techniques et embarquées doivent être horodatées au moyen d'un service d'horodatage homologué RGS.

Le cadre normatif de l'archivage électronique ajoute des exigences permettant de penser la pérennisation de l'intégrité et de la traçabilité ainsi créées. La norme NF Z 42-013 et son guide d'implémentation GA Z 42 019 prévoient ainsi l'édition régulière de journaux, qui deviennent eux-mêmes des objets d'archives intégrés au SAE, et leur chaînage, afin de multiplier les traces garantissant l'intégrité des documents conservés.

Le Dossier Patient Informatisé (DPI) est à la fois l'outil au cœur de la prise en charge médicale du patient et également au cœur de l'expertise lorsque le patient exprime, au travers d'un contentieux, son mécontentement au sujet de sa prise en charge.

Ce contentieux peut intervenir à tout moment du cycle de vie de l'information médicale. Il intervient notamment de plus en plus fréquemment au cours de l'épisode de soins ou immédiatement après cette prise en charge.

Cette dualité d'usage du DPI se traduit par la nécessité, pour les éditeurs des composants du SIH, de faire évoluer leur produits de façon à pouvoir :

- créer, gérer la valeur neutre et probante de l'information médicale (dès sa création) et la conserver au plus tôt,
- assurer la traçabilité des actions réalisées sur ces systèmes.

La mise œuvre d'un mécanisme de traçabilité performant et d'accès sécurisé, associée à une implémentation raisonnable d'authentification et d'imputabilité, permet de garantir le caractère probant des archives courantes.

Le chapitre suivant présente de façon générale la norme CDA (Clinical Document Architecture) ainsi que les différents profils IHE qui permettent de répondre aux caractéristiques énoncées ci-dessus.

5 Présentation générale de la norme CDA et du profil IHE-XDS

5.1 Présentation générale de la norme CDA (Clinical Document Architecture)

En France, les documents médicaux partagés ou échangés doivent se conformer à la norme ***HL7 Clinical Document Architecture, Release 2.0 (CDA R2)*** publiée dans l'***Edition Normative HL7 v3 de Mai 2005*** et référencée dans le Cadre d'Interopérabilité des SIS (CI_SIS) de l'ASIP Santé[18].

Un document CDA est défini comme une entité documentaire complète et autonome (utilisable indépendamment de tout message d'empaquetage).
Il doit pouvoir être consulté via un navigateur du marché sans autre opération que d'utiliser une feuille de style.

Un document CDA est :

- représenté par un flux XML (éventuellement accompagné de pièces jointes et d'une feuille de style),
- toujours constitué d'un entête structuré en XML (ses métadonnées) qui décrit le contexte médical dans lequel le document a été réalisé, et d'un corps qui contient l'information médicale proprement dite.

Il peut inclure du texte, des images, des sons et d'autres types de contenus multimédias.

Les deux parties d'un document CDA, entête et corps du document, sont par essence indissociables. L'information médicale est obligatoirement liée à son contexte.

Le niveau de structuration du document CDA est variable et dépend du degré de sophistication du logiciel producteur de cette information.

En effet, le corps d'un document CDA peut être soit :

- non structuré (NonXMLBody)
    - le contenu médical est alors encodé dans un format autre que le format XML (text, pdf, image, etc.). Le RGI recommande d'utiliser le format PDF/A-1 décrit dans la norme ISO 19005-1 qui répond aux problématiques d'archivage à long terme.
- structuré (StructuredBody)
    - le contenu médical est codé en format XML. Il est composé d'une à plusieurs structures imbriquées (les sections), ces dernières contiennent une zone nar-

[18] Cadre d'Interopérabilité des SIS (CI_SIS) publié par l'ASIP Santé : http://esante.gouv.fr/services/referentiels/referentiels-d-interoperabilite/cadre-d-interoperabilite-des-systemes-d

rative (directement interprétable par l'utilisateur) et peuvent être codifiées (pour un traitement automatisé par la machine). Ces sections peuvent contenir des entrées (codification de tout ou partie de la zone narrative), et des références externes (entre autres possibilités : des pièces jointes structurées ou non).

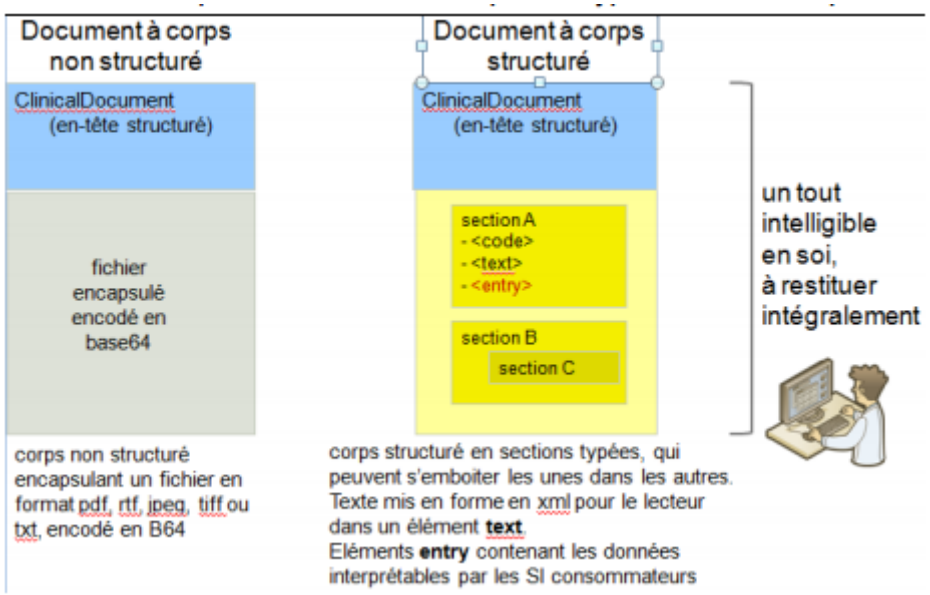


Figure 5.1-1 : les deux formes de documents CDA *(Extrait du CI_SIS de l'ASIP Santé)*

L'entête d'un document CDA est codifié en XML et la structure de cet entête est identique quel que soit le document. Cet entête décrit les métadonnées associées au document médical, c'est-à-dire le contexte dans lequel le document a été produit.

Parmi ces métadonnées, figurent notamment :

- la date de création (effectiveTime),
- l'organisation productrice (custodian)
- le ou les auteur(s) du document (author),
- les approbateurs (authenticator),
- le signataire du document (legalAuthenticator),
- etc.

L'ensemble des métadonnées participent à la qualification de l'origine de l'information et concourent à assurer la « traçabilité embarquée » de l'information médicale élaborée lors de la prise en charge du patient dans l'établissement.

Le lecteur pourra se reporter au document « Volet de structuration minimale de documents de santé » publié dans le CI-SIS de l'ASIP[19] qui présente et détaille le tableau des métadonnées de l'entête CDA.

[19] CI_SIS, Volet de structuration minimale des documents de santé : http://esante.gouv.fr/sites/default/files/asset/document/ci-sis_contenu_volet-structuration-minimale_v1.3.2.1.pdf

Elément XML de niveau 1	Card. CI-SIS	Objet décrit
realmCode	[1..1]	Périmètre d'utilisation : France
typeId	[1..1]	Référence au standard CDA R2
templateId	[3..*]	Déclarations de conformité
id	[1..1]	Identification du document
code	[1..1]	Type de document
title	[1..1]	Titre du document
effectiveTime	[1..1]	Date et heure de création du document
confidentialityCode	[1..1]	Niveau de confidentialité du document
languageCode	[1..1]	Langue principale du document
setId *Non documenté dans ce volet*	*[0..1]*	*Identification d'une série de révisions du document*
versionNumber *Non documenté dans ce volet*	*[0..1]*	*Numéro de version du document*
copyTime *Non documenté dans ce volet*		*Date et heure de remise* *Elément obsolète à ne pas utiliser*
recordTarget	[1..1]	Patient concerné par le document
author	[1..*]	PS, patient ou dispositif auteur(s) du document incluant l'organisation émettrice pour le compte de laquelle le PS ou le dispositif a constitué le document
dataEnterer	[0..1]	Opérateur de saisie
informant	[0..*]	Informateur (informant), ayant fourni des informations utiles aux actes en rapport avec la production du document
custodian	[1..1]	Organisation conservant le document et garantissant son cycle de vie
informationRecipient	[0..*]	Destinataire(s) du document
legalAuthenticator	[1..1]	PS ou patient responsable du document
authenticator	[0..*]	PS attestant la validité du document
participant	[0..*]	Participant, jouant dans l'élaboration du document, un rôle différent de celui d'auteur, de responsable, d'opérateur de saisie, d'informateur ou de destinataire
inFulfillmentOf	[0..1]	Prescription
documentationOf	[1..*]	Acte(s) rapporté(s) par le document Pour l'acte principal, inclusion du PS exécutant, de l'organisation pour laquelle il a exécuté l'acte et de son cadre d'exercice. Pour une expression personnelle du patient, inclusion du patient et de sa démarche.
relatedDocument	[0..1]	Document à remplacer
authorization *Non documenté dans ce volet*	*[0..*]*	*Consentement associé au document*
componentOf	[1..1]	Prise en charge renseignée par le document incluant le type de sortie, le responsable et les personnes impliquées dans la prise en charge ainsi que leur organisation et le lieu de prise en charge

Tableau 1: Eléments de l'en-tête de CDA R2

Figure 5.1-2 : extrait du CI_SIS : Eléments d'entête du CDAr2

En résumé, les caractéristiques d'un document CDA sont les suivantes :

- un document CDA est persistant : il persiste dans un état inaltéré pendant une durée définie par des exigences locales et réglementaires.
- Un document CDA est administrable : il est maintenu par une organisation de confiance chargée de la gestion de ce document.
- Un document CDA est authentifiable : Un document clinique est un assemblage d'informations destiné à être authentifié légalement.
- Un document CDA établit un contexte par défaut pour son contenu médical.
- Un document CDA forme un tout : l'authentification du document s'applique à l'intégralité du document et non pas à des portions du document prises en dehors du contexte dudit document.
- Un document est obligatoirement lisible par un utilisateur.

Ces caractéristiques répondent en grande partie aux exigences de valeur neutre et probante d'un document d'archive présentées au chapitre 4.

En effet, la comparaison entre la structuration d'un document CDA et les exigences portées par la norme OAIS (en termes de structuration de l'information archive), présentée sur la figure 5.1-2, permet de constater :

- Qu'une instance d'un document CDA correspond au Paquet d'information décrit dans la norme OAIS. Elle est constituée :

- D'un entête qui porte les métadonnées (informations de pérennisation décrites dans OAIS et représentées en rouge sur la figure 5.1-3),
- D'un corps qui contient l'information médicale (contenu d'information décrit dans OAIS et représenté en bleu dans la figure 5.1-3).

- Néanmoins, dans la norme CDA les informations de représentation du contenu ne sont pas liées directement à celui-ci mais sont portées par les métadonnées au niveau de l'entête du document CDA.

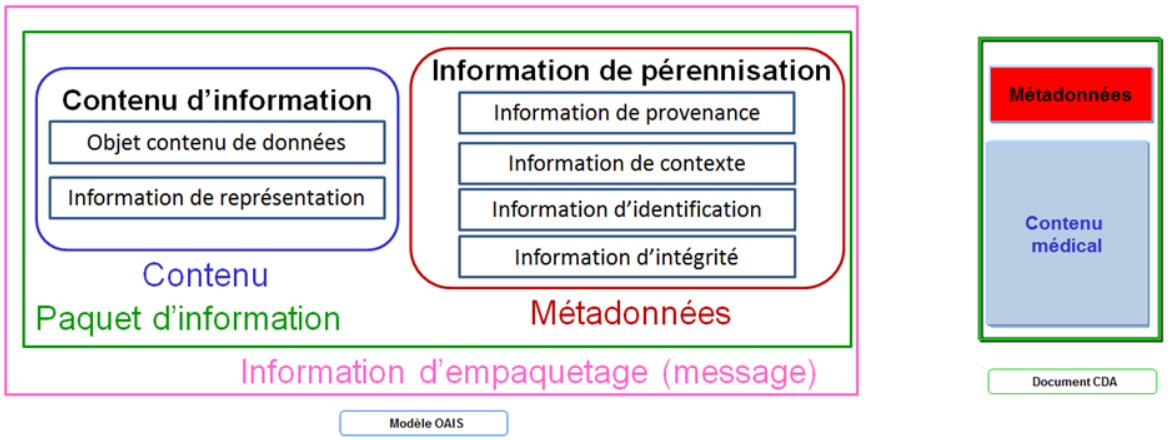


Figure 5.1-3 : Comparaison des normes OAIS/CDA

D'autre part, la norme CDA (en version 2.0) ne décrit pas de mécanisme permettant de faire la preuve du caractère intègre du document. Pour cela, elle doit être associée, tel que c'est décrit dans le CI_SIS, soit à la mise en œuvre d'une signature électronique liée au document (information représentée en noir sur la figure 5.1-4), soit au minimum à un mécanisme d'empaquetage du document par un format de message qui porterait l'empreinte du document CDA (information représentée en rose sur la figure 5.1-4).

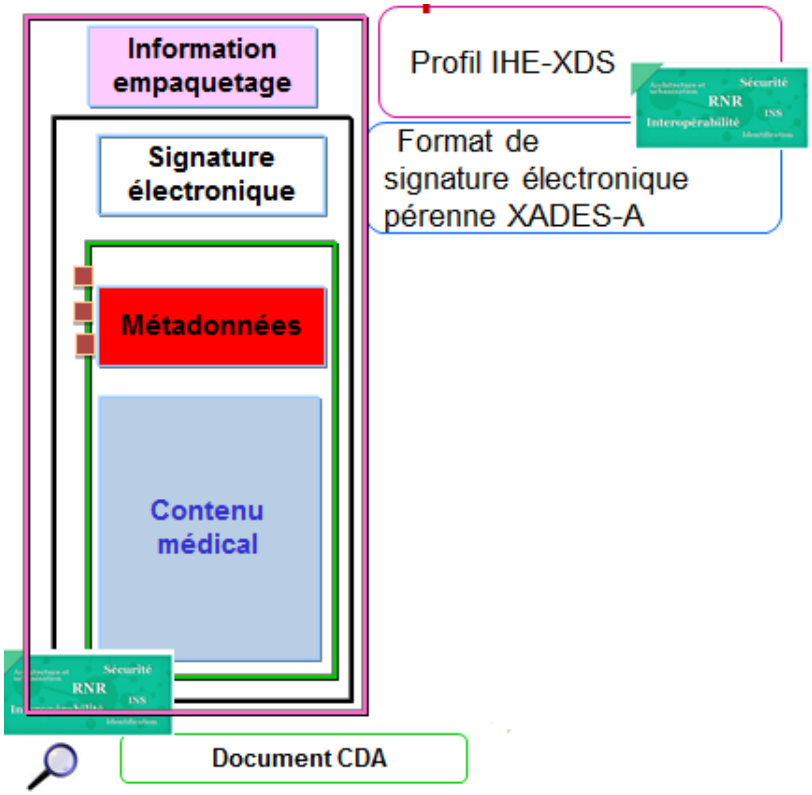


Figure 5.1-4 : Insertion d'un document CDA dans une enveloppe de soumission XDS-b et signature électronique du document

La notion d'empreinte, qui n'existe pas dans CDA, est décrite au niveau des métadonnées du document définies par les profils de partage et d'échange de documents médicaux tels que IHE-XDS (Cross-Enterprise Document Sharing) et IHE-XDM (Cross-Enterprise) présentés au chapitre suivant.

5.2 Présentation générale du profil IHE XDS-b (Cross-Enterprise Document Sharing)

Le profil IHE XDS-b décrit une infrastructure de partage de documents et des métadonnées associées, via un ou plusieurs entrepôt(s) commun(s) piloté(s) par un registre d'index unique.

Cette infrastructure est généralement mise en place dans un contexte de partage des documents médicaux du patient au sein d'une communauté extra hospitalière, d'un Groupement Hospitalier de Territoire (GHT) ou d'un établissement juridique constitué de plusieurs entités géographiques réparties.

Tous les documents gérés et stockés dans l'infrastructure sont obligatoirement rattachés à un patient qui est identifié au sein de la communauté qui gère le partage de l'information.

Le lecteur pourra se reporter au « Volet Partage de documents de santé » publié par l'ASIP dans le CI_SIS[20] et à la lecture du profil international IHE XDS-b[21] pour plus de précisions.

Le profil définit cinq acteurs au sens IHE :

- L'Entrepôt (*Document Repository*) : acteur qui stocke les documents partagés au sein de la communauté de façon sécurisée, fiable et persistante. Il répond également aux demandes de récupération de ces documents. L'infrastructure XDS peut contenir un ou plusieurs entrepôts.
- Le Registre (*Registry*) : acteur qui stocke les informations descriptives associées aux documents (métadonnées) et qui répond aux interrogations des systèmes consommateurs. Les métadonnées servent à classer et à retrouver les documents facilement. L'infrastructure XDS contient toujours un seul et unique Registre qui gère les métadonnées des documents stockés dans un ou plusieurs entrepôts associés.
- Le Producteur (*Document Source*) : acteur qui créé et envoie vers l'infrastructure XDS les documents et métadonnées associées. L'enveloppe contenant les documents associés à leurs métadonnées est réceptionnée par l'acteur Entrepôt qui stocke les documents et transfère les métadonnées au niveau de l'acteur Registre.
- Le Consommateur (*Document Consumer*) : acteur qui interroge le Registre sur des critères déterminés pour récupérer les métadonnées correspondantes à ces critères et qui ensuite récupère les documents correspondants au niveau du ou des Entrepôts qui les détiennent.
- L'Administrateur (*Document Administrator*) : acteur qui gère la mise à jour des métadonnées stockées dans le Registre de l'infrastructure XDS.

Les objets gérés par l'Entrepôt et le Registre sont les suivants :

- Le document (*Document*) lui-même, codé en base64 et inaltérable une fois stocké dans l'Entrepôt.
- La fiche de document (*documentEntry*) : métadonnées associées au document, dont l'identifiant unique du document (uniqueId) et l'identifiant de l'entrepôt (repositoryUniqueId) qui stocke ce document. La fiche de document est stockée au niveau du Registre.
- Le classeur (*Folder*), optionnel, qui permet de regrouper un ensemble de documents du patient selon un critère déterminé. Le classeur est stocké au niveau du Registre où il est lié aux documents qui le constituent et à l'enveloppe de soumission qui le contient. Le classeur est caractérisé par un ensemble de métadonnées stockées au niveau du Registre.
- Le lot de soumission (*Submission Set*) ou enveloppe de soumission correspond au format d'empaquetage de l'ensemble des objets document(s), fiche(s) de document, classeur(s) et associations entre ces objets. Le lot de soumission, une fois stocké au niveau du Registre, est immuable. Il est également caractérisé par un ensemble de métadonnées stockées au niveau du Registre.

[20] Volet Partage de documents de santé : http://esante.gouv.fr/sites/default/files/asset/document/ci-sis_services_volet-partage-documents-sante_v1.3.2.1.pdf

[21] IHE XDS-b : http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf

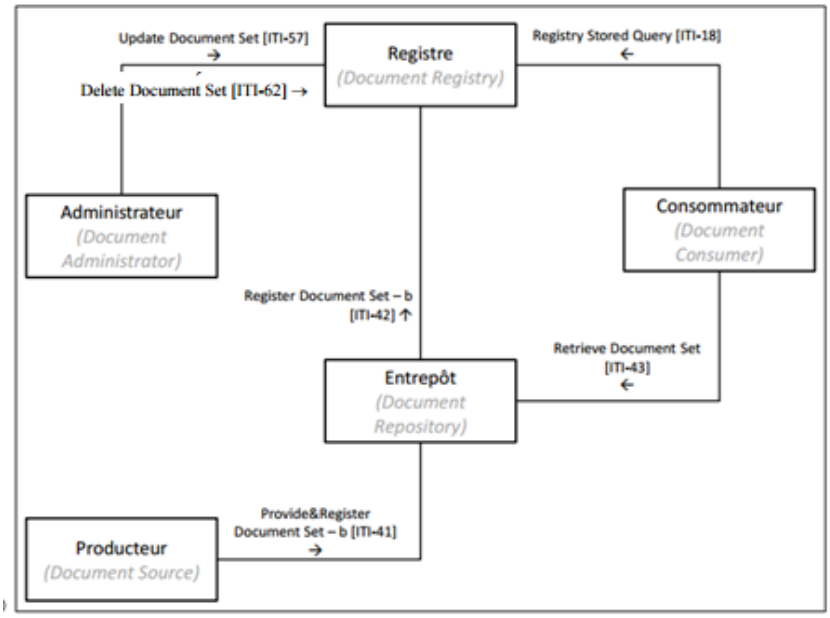
- Les associations (*Association*) créées entre les différents objets et stockées également au niveau du Registre. Ces associations sont typées (hasMember, replace, etc.)

Le lot de soumission (*Submission Set*) correspond au niveau d'empaquetage décrit dans la norme OAIS (représenté en rose sur la figure 5.1-3). Ce lot de soumission, qui contient l'ensemble des documents du patient à publier sur l'infrastructure de partage, est caractérisé par un ensemble de métadonnées définies par le profil XDS-b.

L'ensemble des métadonnées XDS associées au document (*documentEntry*) participe à la qualification de l'origine de l'information et concoure à assurer la traçabilité de l'information médicale élaborée lors de la prise en charge du patient dans l'établissement et gérée par l'infrastructure XDS.

En France, le CI_SIS impose de signer le lot de soumission au moyen d'une signature électronique de type XAdES utilisant un certificat de signature conforme aux spécifications du profil IHE DSG (Document Digital Signature)[22]. Cette signature porte sur l'ensemble des documents contenus dans le lot de soumission.

Les formats acceptés des documents stockés dans l'infrastructure de partage sont définis par la communauté qui gère cette infrastructure. Dans le cas où le document est au format CDA, les métadonnées de l'entête CDA sont dupliquées au niveau de la fiche de document XDS associée à ce document. Dans les autres cas, le RGI recommande d'utiliser le format PDF/A-1 décrit dans la norme ISO 19005-1 et qui répond aux problématiques d'archivage à long terme.
L'ensemble des acteurs de l'infrastructure XDS interagissent entre eux au moyen de transactions IHE qui sont représentées sur la figure 5.2-1 :



(Extrait du CI_SIS : Volet Partage de documents)

Figure 5.2-1 : Diagramme des Acteurs/transactions du profil IHE XDS-b

[22] IHE-DSG: Document Digital Signature http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DSG.pdf

- Provide&Register Document Set-b (ITI-41): transaction d'alimentation de l'infrastructure de partage via le lot de soumission (*Submission Set*) qui contient l'ensemble des documents du patient éventuellement classés. Stockage des documents dans l'Entrepôt.
- Register Document Set-b (ITI-42): transaction de transfert des métadonnées associées au document de l'Entrepôt vers le Registre.
- Registry Stored Query (ITI-18) : interrogation du Registre par un acteur Consommateur sur un ensemble de critères ramenant les fiches de documents (métadonnées, dont l'identifiant du document et l'identifiant de l'Entrepôt qui stocke ce document) correspondant à ces critères.
- Retrieve Document Set (ITI-43) : transaction de récupération des documents correspondants à la sélection de l'utilisateur parmi les éléments renvoyés par la transaction d'interrogation ITI-18.

Le profil IHE-XDS est complété par le profil IHE Metadata Update[23] qui ajoute aux transactions présentées ci-dessus les deux transactions suivantes :

- Update Document Set (ITI-57) : transaction de mise à jour des métadonnées associées au(x) document(s).
- Delete Document set (ITI-62) : transaction de suppression des métadonnées associées au(x) document(s).

5.3 Présentation générale du profil IHE XDM (Cross-Enterprise Document Media Interchange)

Le profil IHE XDM décrit les transactions de transfert de document(s) de santé avec les métadonnées associées via un média : clé USB, CD, pièce jointe d'un e-mail (fichier zip).

Ce profil couvre la notion d'échange d'un ou plusieurs documents concernant un ou plusieurs patient(s). Cette notion d'échange est complémentaire à la notion de partage décrite par le profil IHE XDS-b.

Le profil IHE XDM est implémenté dans la messagerie sécurisée de santé (MSSanté) publiée par l'ASIP santé[24]. Ce système de messagerie sécurisé est réservé à l'ensemble des professionnels de santé et leur permet d'échanger entre eux et par mail des données de santé à caractère personnel.

Le CI_SIS contraint le profil international en retenant uniquement la possibilité d'utiliser la transmission d'un fichier zip (fichier nommé IHE_XDM.ZIP) via une messagerie électronique et en permettant de transmettre un lot de documents pour un seul patient. Les médias autres que le fichier ZIP ne sont pas retenus par le CI_SIS.

Le profil IHE XDM définit deux acteurs au sens IHE :

[23] IHE Metadata Update : http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XDS_Metadata_Update.pdf

[24] MSSanté : http://esante.gouv.fr/services/mssante

- Portable Media Creator : système émetteur d'un lot de documents et des métadonnées associées à déposer sur un média (fichier IHE_XDM.ZIP).
- Portable Media Importer : système récepteur du lot de documents pour import de ces documents dans son système.

Ces deux acteurs interagissent via la transaction Distribute Document Set On Media (ITI-32) :

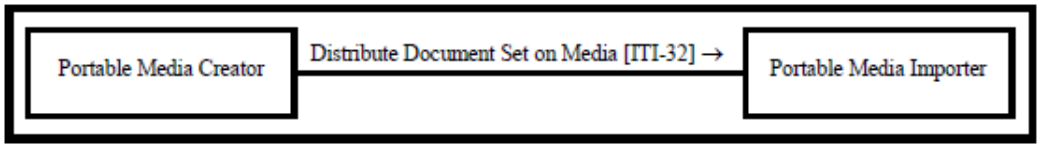


Figure 5.3-1 : diagramme Acteurs/Transactions du profil IHE-XDM

Le profil IHE XDM, via la transaction Distribute Document Set On Media (ITI-32), décrit la structure normalisée du contenu du fichier IHE_XDM.ZIP. Pour plus d'informations, le lecteur se reportera au « Volet Echange de Documents de Santé » du CI_SIS[25].

Ce fichier est constitué :

- D'un répertoire IHE_XDM,
- D'un fichier INDEX.HTM et d'un fichier README.HTM qui sont des fichiers d'aide d'accès au media.

Figure 5.3-2 : Structure générale du media *(Extrait du CI_SIS)*

Le répertoire IHE_XDM contient :

- Un sous répertoire SUBSET01 unique qui contient lui-même :
  - Le(s) document(s) échangés concernant le patient,
  - Eventuellement une ou plusieurs feuille(s) de styles qui accompagne(nt) le(s) document(s),
  - Le document SIGN.XML qui signe le lot de soumission,
  - Le document METADATA.XML qui contient l'ensemble des métadonnées décrivant les documents contenus dans SUBSET01.

[25] Volet Echange des Documents de santé : http://esante.gouv.fr/sites/default/files/asset/document/ci-sis_services_volet-echange-documents-sante_v1.3.2.1.pdf

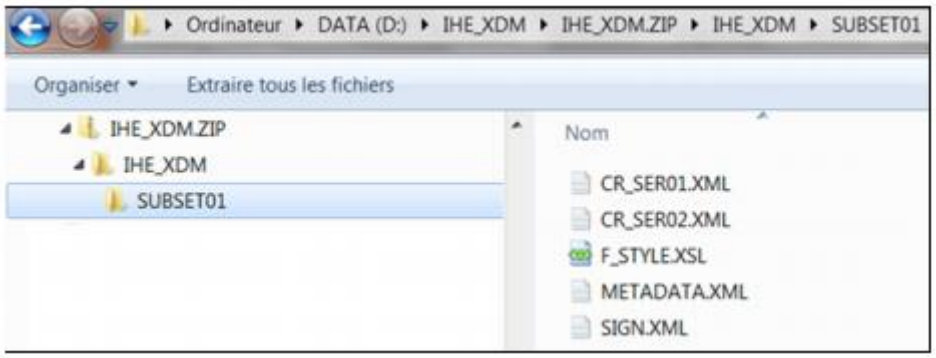


Figure 5.3-3 : Structure d'un lot de soumission *(Extrait du CI_SIS)*

Le document METADATA. XML contient l'ensemble des métadonnées décrivant le lot de soumission ainsi que l'ensemble des objets contenus dans ce lot de soumission. La structuration de ce fichier est identique à la structuration des métadonnées inclues dans la transaction Register Document Set-b (ITI-42) du profil IHE XDS-b décrit précédemment.

L'ensemble des métadonnées associées au(x) document(s) et au lot de soumission participent à la qualification de l'origine de l'information et concourent à assurer la traçabilité de l'information médicale lorsque celle-ci est échangée au moyen de la MSSanté.

5.4 Présentation générale du profil IHE DRPT (Displayable Report)

Le profil international IHE DRPT du domaine IHE-Cardiologie spécifie les transactions supportant la création, la révision, la visualisation et la communication en intra hospitalier ou en extra hospitalier de documents médicaux issus des systèmes d'imagerie (radiologie, oncologie, obstétrique, gynécologie, gastroentérologie, ophtalmologie, orthopédie).

Les formats des documents médicaux supportés par le profil sont les formats PDF/A-1 et CDA (Clinical Document Architecture), permettant ainsi un stockage à long terme de ces documents.

InteropSanté a publié en 2013 un livre blanc intitulé «harmonisation des modalités de communication des documents médicaux »[26] qui étend le périmètre du profil international à l'ensemble des documents médicaux produits par des systèmes autres que ceux d'imagerie (incluant le DPI, les dossiers de spécialités, les systèmes d'information de laboratoire, etc.).
Ce livre blanc se focalise sur trois acteurs IHE en particulier :

- Report Creator : système qui crée et qui communique ensuite le document médical.
- Report Manager : système qui réceptionne le document en provenance du Report Creator, gère le statut du document pour distribution et envoie le document vers un ou plusieurs entrepôts.

[26] Livre blanc « Harmonisation des modes de communication des documents médicaux » : http://www.interopsante.org/412_p_37529/publications.html

- Enterprise Report Repository : système qui réceptionne le document ou la référence au document provenant du Report Manager, qui le stocke sur le long terme et qui le rend disponible en accès intra hospitalier.

Pour plus d'informations concernant les autres acteurs décrits dans le profil international, le lecteur pourra consulter le profil IHE DRPT[27].

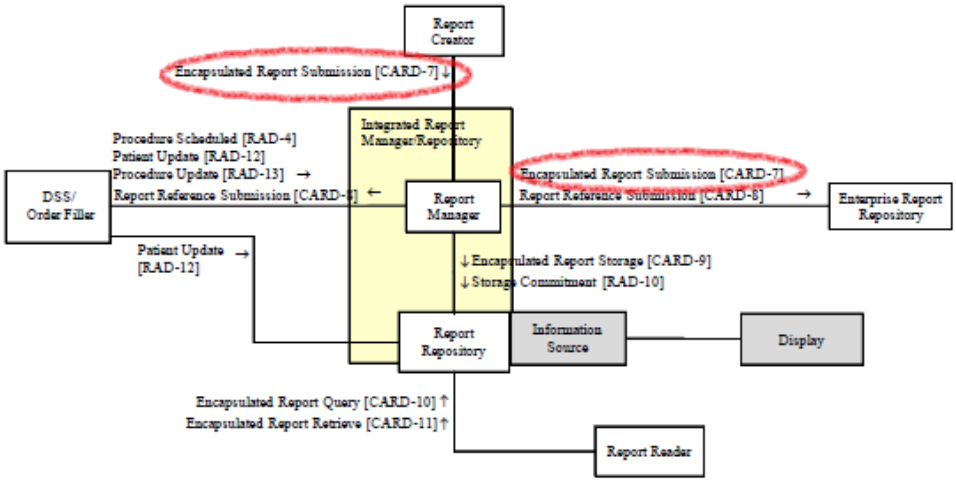


Figure 5.4-1 : diagramme des Acteurs/Transactions du profil IHE DRPT

Le livre blanc d'Interop'Santé met l'accent sur la transaction Encapsulated Report Submission (CARD-7) qui est implémentée entre :

- L'acteur Report Creator et l'acteur Report Manager,
- L'acteur Report Manager et l'acteur Enterprise Report Repository.

Cette transaction CARD-7 implémente le message HL7v2.6 MDM qui permet de véhiculer le document médical (au format pdf/A-1 ou CDA r2), d'un système à un autre en intra hospitalier, en l'associant à un ensemble de métadonnées similaires à celles implémentées par la norme CDA et le profil IHE-XDS et qui décrivent le contexte dans lequel le document a été produit.

Le segment OBX de ce message contient le document lui-même codé en base 64 alors que le segment TXA contient les métadonnées associées au document.

Parmi les métadonnées portées par le segment TXA figurent :

- Le type de document,
- Des informations de présentation du document,
- Date/heure de création du document,
- L'auteur du document,
- Le signataire,
- L'identifiant du document,
- Etc.

Il est à noter que parmi ces métadonnées ne figure pas l'empreinte du document (hash).Cette dernière technologie constitue pourtant une solution technique répandue pour garantir l'intégrité d'un document sans envisager forcément le recours à des solutions plus

[27] Profil IHE DRPT : http://ihe.net/uploadedFiles/Documents/Cardiology/IHE_CARD_Suppl_DRPT.pdf

lourdes come la signature électronique ou le cachet serveur. En effet, les métadonnées décrites dans le profil DRPT ne gèrent pas la notion d'empreinte associée au document. Il est donc impossible pour le système récepteur de vérifier que le document communiqué est intègre et qu'il n'a subi aucune destruction ou modification malveillante.

Il sera nécessaire de faire évoluer le standard HL7 v2.6 ainsi que le profil IHE DRPT international pour prendre en compte cette métadonnée d'empreinte du document, telle qu'elle existe dans les profils IHE XDS-b et IHE XDM.

5.5 Présentation générale du profil IHE ATNA (Audit Trail and Node Authentication)

Le profil IHE ATNA permet à la fois de sécuriser les transactions entre les systèmes (nœuds) appartenant à un domaine sécurisé et d'alimenter un répertoire d'audit centralisé avec les messages d'audits générés de façon normalisée par l'ensemble des systèmes du domaine sécurisé (enregistrement des traces des échanges et des traces d'accès aux données de santé ou d'exportation de ces données).

Le profil IHE XDS-b présenté au chapitre 5.2 est obligatoirement couplé au profil IHE ATNA.

Le profil ATNA définit trois acteurs au sens IHE :

- Time Server : système qui fournit une base de temps commune aux systèmes composant l'infrastructure de partage.
- Secure Node : acteur groupé avec tout autre acteur d'une infrastructure de partage, permettant à chacun des nœuds de s'authentifier mutuellement via un certificat serveur. L'authentification de l'utilisateur reste locale au système qui implémente l'acteur Secure Node.
- Audit Repository : acteur qui réceptionne et stocke les messages d'audit correspondant aux informations échangées, accédées ou exportées.

L'ensemble des acteurs du profil ATNA interagissent entre eux au moyen de transactions IHE qui sont représentées sur la figure 5.5-1 :

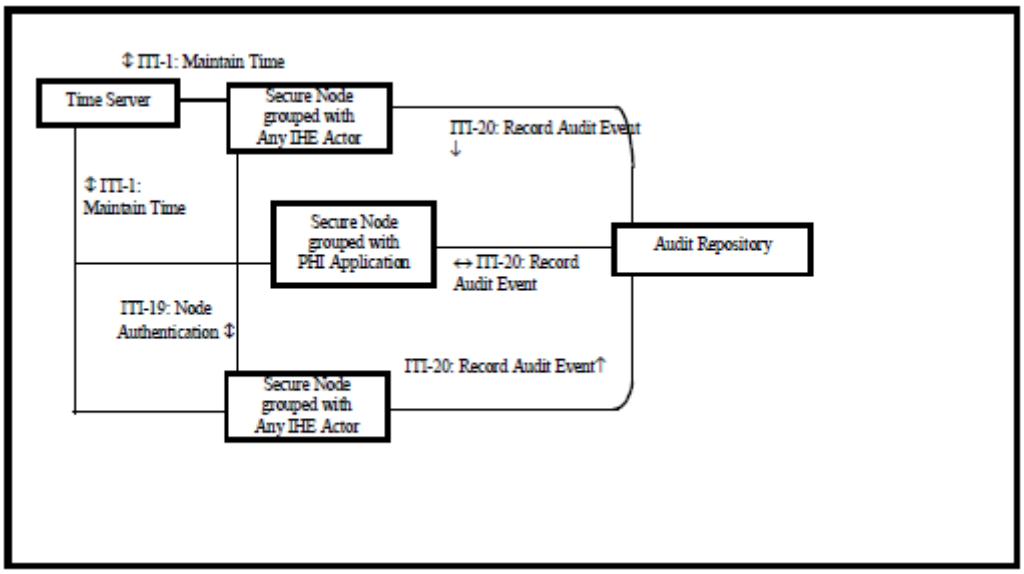


Figure 5.5-1 : Diagramme des Acteurs/Transactions du profil IHE ATNA

- Maintain Time (ITI-1) : transaction de synchronisation du temps entre un système serveur et un système client. L'horodatage contribue à la traçabilité dans la mesure où il permet d'établir la chronologie précise des évènements tracés.
- Node Authentication (ITI-19) : transaction d'authentification mutuelle des nœuds.
- Record Audit Event (ITI-20) : transaction d'enregistrement des traces d'audit au niveau d'un serveur centralisé.

5.6 Conclusion

L'implémentation de la norme CDA, associée ou non aux profils IHE XDS-b, IHE XDM, IHE DRPT permet d'associer des métadonnées aux documents médicaux, c'est-à-dire aux archives courantes, produites au cours de la prise en charge médicale du patient dans l'établissement. Ces métadonnées permettent de faciliter la gestion, l'usage et la préservation du document au sein du SIH. Elles permettent également de préparer le versement des archives courantes (SIH) vers les archives intermédiaires (SAE).

La gestion de la traçabilité, assurée par la mise en œuvre du profil IHE ATNA permet d'apporter les preuves concernant la gestion du cycle de vie des archives courantes et les opérations conduites sur le SIH concernant ces archives courantes.

De ce fait, l'utilisation des profils IHE permet de se rapprocher fortement de la structuration de l'information promue par la norme OAIS. L'implémentation des référentiels d'imputabilité et d'authentification de l'ASIP ainsi que le respect de la norme NF Z 42-013 ajoutent les fonctionnalités garantissant l'authenticité des informations. Cet écosystème normatif permet de créer et maintenir dans le temps la valeur probante des informations.

En outre, la gestion des métadonnées ainsi que la traçabilité permettent aux parties d'envisager l'élaboration d'une convention de preuve pour décider contractuellement de l'acceptation de certains modes de preuve et de reconnaître la valeur probante de l'information électronique échangée.

6 Présentation des cas d'usage

Les cas d'usage décrits dans ce chapitre ne sont pas exhaustifs. Ils ont pour objet de réfléchir aux solutions permettant, dans différents contextes, d'assurer les prérequis à mettre en œuvre au niveau de l'établissement pour créer cette valeur neutre et probante et pour la préserver au plus tôt.

Nous avons cherché, au travers des cas d'usage suivants, à déterminer quels profils IHE pouvaient répondre aux prérequis à mettre en œuvre au niveau du SI pour :

- Gérer de façon rigoureuse le cycle de vie de l'information médicale,
- Créer au plus tôt la valeur neutre et probante de l'information médicale et pour la préserver au plus tôt.

6.1 Prise en charge du patient en intra hospitalier

Ce cas d'usage décrit la prise en charge d'un patient à l'hôpital pour une opération programmée de la hanche. Cette prise en charge se décompose en une préadmission du patient suite à une consultation externe, confirmée en admission hospitalisée par la suite lors de l'arrivée du patient le jour planifié pour l'opération.

Ce cas d'usage est subdivisé en deux sous cas d'usage qui correspondent chacun à des stratégies d'archivage différentes :

- Le premier dans lequel les documents médicaux sont transmis au SAE (Service d'Archivage Electronique) directement par les différents systèmes sources dès leur production et leur validation par l'utilisateur.
- Le deuxième dans lequel les documents médicaux sont transmis au SAE à une date déterminée après la sortie du patient.

Les avantages/inconvénients de chacune de ces stratégies sont présentés au chapitre 6.1.1 (phase 2 : archivage des documents).

6.1.1 Description du cas d'usage

Dans la suite de la description du cas d'usage, l'intitulé « dossier du patient » est utilisé au sens large. Il s'agit, selon l'utilisateur, du DPI (Dossier Patient Informatisé), du logiciel de bloc, du logiciel d'anesthésie, etc. Chacun de ces composants est doté d'un mécanisme d'authentification de l'utilisateur. Ce mécanisme est essentiel par la suite dans la constitution du caractère probant de l'information.

La figure 6.1.1-1 ci-dessous synthétise les étapes de la prise en charge du patient. Ces étapes sont ensuite détaillées dans les figures 6.1.2-1 et 6.1.2-2.

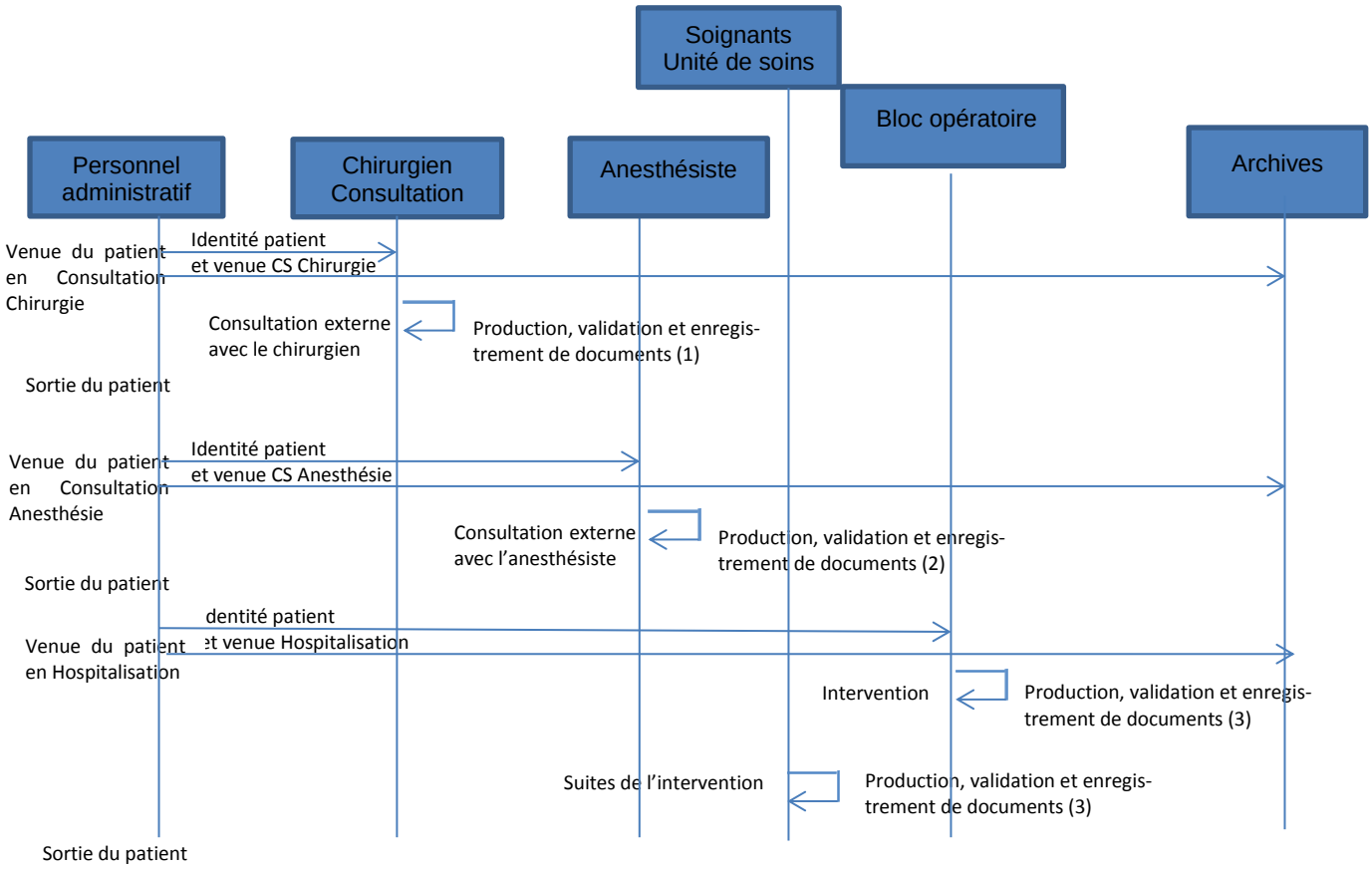


Figure 6.1.1-1 : Synthèse des étapes du scénario

1. *Phase de production des documents médicaux*

- Préadmission d'un patient pour une opération programmée.

Le patient rencontre au cours de deux venues successives, un chirurgien puis un anesthésiste, en prévision d'une opération orthopédique planifiée lors de la pré-hospitalisation.

a) Première venue en consultation externe – rendez-vous avec le chirurgien : Le bureau des entrées identifie le patient, recueille sa couverture sociale (assurances obligatoire et complémentaire), le médecin traitant, et positionne la venue courante par rapport au parcours de soins coordonné. Les données administratives du patient sont enregistrées et la venue de consultation externe est créée. Le patient est aiguillé vers le chirurgien.

b) Le chirurgien reçoit le patient en consultation externe et l'examine. Il enregistre dans le dossier du patient les actes réalisés lors de la consultation externe, le(s) diagnostic(s) posé(s) ainsi que les données cliniques du patient (allergies, antécédents, poids, taille, etc.).

La lettre du médecin traitant adressant son patient est scannée et intégrée au dossier du patient par la secrétaire médicale du service d'orthopédie. Dans l'objectif de pouvoir détruire la version papier de ce courrier, la numérisation du document doit être réalisée con-

formément à un processus de numérisation formellement défini et documenté au sein de la Politique de numérisation de l'établissement en lien avec la Politique d'Archivage.

c) Le chirurgien décide de planifier une intervention :

- Il informe son patient sur la démarche médicale adoptée et lui remet en main propre un document de consentement à lire, signer et ramener lors de la consultation d'anesthésie.
- Il choisit le protocole opératoire pour la future hospitalisation (prothèse totale de hanche).

Cette demande d'intervention est transmise au bloc opératoire, qui dispose de son propre système d'information, où l'intervenant complète la demande d'intervention avec les actes à réaliser, le temps théorique de l'intervention au bloc et les jours prévisionnels pré et post opératoires. La validation de l'intervention au niveau du bloc opératoire engendre la réservation de la prothèse, de médicaments, de produits sanguins et autres consommables liés au protocole opératoire auprès des différents services (pharmacie, dépôt de prothèse, etc.). Elle permet également de confirmer la date de l'intervention.

Le chirurgien rédige le compte-rendu de consultation. Il peut soit valider, soit signer ce compte-rendu de façon électronique. Il prescrit une demande d'examens de laboratoire (ordonnance de sortie) qu'il remet au patient. Le patient ira réaliser ces examens au laboratoire le plus proche de son domicile.

Le compte rendu de la consultation de chirurgie ainsi que l'ordonnance de sortie sont versés au dossier du patient.

d) En fin de consultation, le patient revient au bureau des entrées où la facturation de la consultation est réalisée et la préadmission pour l'opération planifiée est enregistrée par le personnel du bureau des entrées.

e) Seconde venue en consultation externe – rendez-vous avec l'anesthésiste : Le bureau des entrées retrouve le patient, vérifie sa couverture sociale et positionne la venue par rapport au parcours de soins coordonné. La venue de consultation externe est créée. Le patient est aiguillé vers l'anesthésiste.

f) L'anesthésiste reçoit le patient. Il consulte et complète les informations cliniques du patient renseignées par le chirurgien. Il consulte les diagnostics et actes prévisionnels posés par le chirurgien et conduit sa consultation en fonction de ces informations. Il saisit le traitement médicamenteux habituel du patient, le traitement d'entrée du patient et éventuellement des éléments de prémédication pour l'intervention.

Suite à la consultation, l'anesthésiste rédige le compte-rendu d'anesthésie qui récapitule l'ensemble des éléments pertinents de la consultation et qu'il valide ou qu'il signe électroniquement.

Le compte-rendu de la consultation d'anesthésie ainsi que les traitements médicamenteux sont versés au dossier du patient.

- Admission - Le patient entre dans l'établissement à la date prévue (admission en hospitalisation pour réaliser l'intervention).

a) Le bureau des entrées contrôle, via la carte Vitale ou le service en ligne et les attestations papier, les éventuelles évolutions de la couverture AMO (Assurance Maladie Obligatoire) et AMC (Assurance Maladie Complémentaire) du patient. Il confirme la préadmission pour la transformer en admission définitive. Il envoie le patient vers l'unité clinique d'hospitalisation (service d'orthopédie).

b) Le personnel du service d'orthopédie accueille le patient, lui affecte un lit et confirme les responsabilités (hébergement, médical, soin) des unités fonctionnelles concernées.

Les résultats d'examen biologique ainsi que le consentement fournis par le patient sont scannés et intégrés au dossier du patient par la secrétaire médicale du service. La numérisation des documents doit être réalisée conformément à un processus de numérisation formellement défini et documenté au sein de la Politique de numérisation rattachée à la Politique d'Archivage de l'établissement.

Les soignants de l'unité de soins sont informés des prescriptions issues de la consultation d'anesthésie. Les actions correspondantes aux prescriptions sont réalisées par les soignants et enregistrées dans le dossier du patient.

Les professionnels de santé du service d'orthopédie peuvent visualiser le plan de soins qui a été pré-alimenté, suite à la consultation d'anesthésie, avec les éléments de prémédication précédant l'intervention ainsi qu'avec le laps de temps réservé à l'intervention elle-même. Le personnel infirmier administre la prémédication au patient. Cette activité est enregistrée au niveau du dossier du patient.

c) Le patient est ensuite accueilli en salle d'induction pour réalisation de l'anesthésie qui précède l'intervention. L'ensemble des temps opératoires (début d'anesthésie, début d'intervention, etc.) sont enregistrés par l'anesthésiste. L'ensemble de ces informations peuvent apparaître dans le plan de soins, permettant ainsi aux soignants de l'unité de soins, de suivre l'avancement de l'intervention.

d) L'intervention se déroule comme prévu au bloc opératoire. Au cours de cette phase, les traitements prévus par l'anesthésiste sont administrés au patient et le personnel médical suit l'ensemble des constantes médicales du patient. Ces éléments sont enregistrés dans le dossier du patient par les soignants du bloc opératoire.

e) Suite à l'intervention, le patient passe en salle de réveil en soins de suite postopératoires immédiats (SSPI). Au cours de cette phase :

- les traitements administrés au patient, les soins et la surveillance réalisés sur le patient sont enregistrés dans le dossier du patient.
- L'anesthésiste rédige le compte-rendu d'anesthésie et le verse au dossier du patient.
- Les actes (CCAM, NGAP par exemple), les dispositifs médicaux implantables (DMI), les produits sanguins, le document de traçabilité per opératoire et per anesthésie (ou Checklist HAS), le compte-rendu opératoire ainsi que le traitement postopératoire sont enregistrés par le chirurgien et versés au dossier du patient.

La pose de la prothèse oblige à conserver les identifiants de ce produit pour traçabilité, à tarifer le montant exact pour la facturation et induit une commande de réapprovisionnement au laboratoire fournisseur.

f) Suite à l'opération, le patient retourne en unité de soins d'orthopédie, où une surveillance est réalisée par l'équipe soignante. Les éléments de surveillance sont enregistrés dans le plan de soins.

g) Au cours de l'alimentation du dossier par les différents acteurs ou à la fin de la venue du patient, le médecin DIM réalise des contrôles de qualité de la saisie des informations médicales. En fonction du contenu du dossier du patient, il peut changer la typologie des diagnostics (principal, relié, significatif, documentaire). Il peut aussi indiquer à ses collègues les erreurs éventuelles de codification des diagnostics et actes.

Dans tous les cas, un codage PMSI est produit pour l'hospitalisation.

h) A la fin de l'hospitalisation, le médecin responsable du patient donne le feu vert pour la sortie du patient. Il rédige le compte-rendu d'hospitalisation ainsi que la lettre de sortie qui récapitule les éléments pertinents nécessaires à la coordination des soins. Cette lettre de sortie est ensuite envoyée par la secrétaire médicale du service au médecin traitant du patient. Une version est conservée dans le dossier du patient.

Tout au long du scénario, deux variantes sont possibles :

Les différents documents sont simplement validés par l'auteur (validation enregistrée dans le système producteur). Dans ce cas, les traces enregistrées au cours de la prise en charge du patient doivent être suffisamment précises quant à leur contenu. Elles doivent être rattachées aux documents validés et faire l'objet d'un calcul d'empreinte. En effet, le cas échéant, couplées à une authentification forte, elles devraient être assimilables à un processus de signature permettant d'imputer le document à un personnel responsable.

- Les différents documents sont signés électroniquement par le professionnel de santé auteur.

Ces deux variantes sont possibles et permettent d'aboutir au même résultat : le fait que l'auteur endosse sa responsabilité de professionnel de santé et que la traçabilité des soins est assurée.

- la première variante s'appuie à la fois sur l'authentification du professionnel et sur les traces générées par le système qui a produit le document. Il est important de pouvoir prouver que seul le professionnel pouvait agir, qu'il a bien validé le processus et que l'information considérée est toujours celle validée par le professionnel de santé identifié.
- la deuxième variante fait intervenir un processus de signature électronique qui lui-même peut présenter plusieurs variantes :
    - utilisation d'un certificat électronique du médecin, carte CPS,
    - génération d'un certificat à la volée,
    - activation du certificat électronique (clé privée) à distance.

A l'heure actuelle le droit français garantit certains effets de droit pour le niveau de sécurité le plus élevé (signature électronique sécurisée au sens de l'article 1316-4 (futur article 1367)

du Code civil mais ne permet pas de trancher concernant le choix de l'une ou l'autre des alternatives. Il serait souhaitable d'avoir des éléments pour trancher (cf chapitre 8.2).

2. Phase d'archivage des documents

Dans les deux alternatives suivantes, la liste des documents à archiver dans le contexte du cas d'usage décrit ci-dessus (définie dans la Politique d'Archivage) pourrait être par exemple :

- la lettre du médecin traitant qui adresse son patient,
- le consentement du patient,
- le CR de consultation du chirurgien,
- le CR de consultation de l'anesthésiste,
- le CR opératoire,
- la check list HAS,
- le traitement habituel, le traitement en entrée et prémédication, le traitement post-topératoire,
- le compte-rendu d'hospitalisation,
- la lettre de sortie,
- le plan de soins.

1° alternative : archivage des documents au fil de l'eau, dès création par les systèmes sources.

Dans ce contexte, les documents produits lors de la prise en charge du patient sont envoyés automatiquement par le système producteur vers le SAE dès leur production et leur validation par l'auteur (le document est alors dans un état figé).

- Avantages :
  - La valeur probante du document est préservée au plus tôt et sur le long terme par le SAE.
- Inconvénients :
  - Il n'est pas possible de réaliser une analyse de la complétude du dossier avant archivage (ce qui est le cas classique dans un contexte d'archivage du dossier patient papier).
  - Cela nécessite beaucoup plus d'échanges avec le SAE, quasiment à chaque document, ce qui peut poser des problèmes de performances et de disponibilité.

2° alternative : archivage des documents à une date déterminée après la sortie du patient.

Dans ce contexte, l'archivage de l'ensemble des documents produits, pertinents et représentatifs de la prise en charge du patient lors de la sortie de l'établissement à T0 ou à T0+ X mois ou à T0+ X années (en fonction des règles fixées par la Politique d'Archivage et de la complétude du dossier) est réalisé en une seule opération. Dans ce contexte, les documents pertinents pour la prise en charge du patient sont généralement concentrés et communi-

qués au niveau d'un acteur du SI « Entrepôt de documents » avant d'être archivés auprès du SAE.

- Avantages :
    - Il est possible de réaliser une analyse de la complétude du dossier avant archivage, sachant que de toute façon cette analyse est réalisée par les DIM pour permettre l'élaboration du PMSI et la facturation.
    - Limitation des accès au SAE.
- Inconvénients :
    - La gestion de la valeur probante de l'information est dépendante de la capacité du SIH à répondre aux prérequis permettant d'assurer cette valeur probante (précision concernant l'auteur du document, la date de création du document, la validation du document par l'auteur, le calcul d'empreinte, etc.). La création et la gestion de la valeur probante de l'information médicale vont dépendre de la maturité du SIH sur ces sujets, notamment de la capacité du SIH et de l'entrepôt de documents à conserver la valeur probante lorsque l'information est communiquée du système producteur vers l'entrepôt de documents.
    - L'événement déclencheur du versement doit exister quelles que soient les circonstances : il n'est ainsi pas possible de ne considérer que la sortie du patient après l'opération car il est toujours possible que le patient décide de stopper le processus de ce cas d'usage après un des rendez-vous ou alors que, pour certaines pathologies, la date de sortie du patient soit très éloignée de son entrée. Il n'en demeure pas moins que les documents déjà produits sont autant de preuves potentielles de la prise en charge du patient qui doivent être archivés. Il serait donc essentiel dans ces cas problématiques de définir un événement déclencheur alternatif.

Dans les deux alternatives, il est a priori nécessaire de conserver le document archivé dans le système producteur après versement au SAE, de façon à assurer un usage régulier de ce document dans le cadre de la coordination des soins apportée au patient (le SAE n'assurant pas cette gestion quotidienne et opérationnelle des documents médicaux). Cette nécessité a pour conséquence de dupliquer l'information avec l'organisation suivante :

- Le DPI sert à la consultation et à l'usage courant.
- Le SAE sert à la conservation de la preuve sur le long terme.

6.1.2 Description des workflows d'information

1° variante: archivage des informations au fil de l'eau, dès création par les systèmes sources.

Cf diagramme de workflow ci-dessous (figure 6.1.2-1) :

- Etape 1 : consultation externe avec le chirurgien, avec production et enregistrement des documents suivants (1)
    - numérisation de la lettre adressée par le médecin traitant,
    - le compte-rendu de la consultation de chirurgie.

- Etape 2 : consultation avec l'anesthésiste avec production et enregistrement des documents suivants (2)
    - Le consentement du patient (signé)
    - Le compte-rendu de consultation de l'anesthésiste.
    - Le traitement habituel du patient, le traitement prévu à l'entrée en hospitalisation, la prémédication à l'intervention.
- Etape 3 : déroulement de l'intervention avec, suite à l'intervention, production et enregistrement des documents suivants (3)
    - La CheckList HAS (traçabilité per opératoire et per anesthésie),
    - Le compte-rendu opératoire,
    - Le compte-rendu d'anesthésie,
    - Le traitement postopératoire.
- Etape 4 : retour du patient en unité de soins et surveillance médicale, production et enregistrement des éléments suivants (4)
    - Enregistrement des soins apportés au patient dans le plan de soins (administration de médicaments, de soins, surveillance, etc.),
    - Le compte-rendu d'hospitalisation,
    - La lettre de sortie à adresser au médecin traitant du patient,
    - Le codage PMSI du séjour du patient par le DIM en fin de séjour.

2° variante: archivage des informations médicales à la sortie du patient.

Le dossier du patient est vérifié après la sortie du patient de l'hôpital. Les documents le constituant sont versés en une seule fois vers le SAE, à une date donnée après la sortie du patient.

Dans les schémas ci-dessous, les documents numérisés et intégrés au SIH sont indiqués en couleur verte et les documents produits nativement sous forme électronique sont indiqués en orange.

Les flèches en pointillés représentent des flux optionnels.

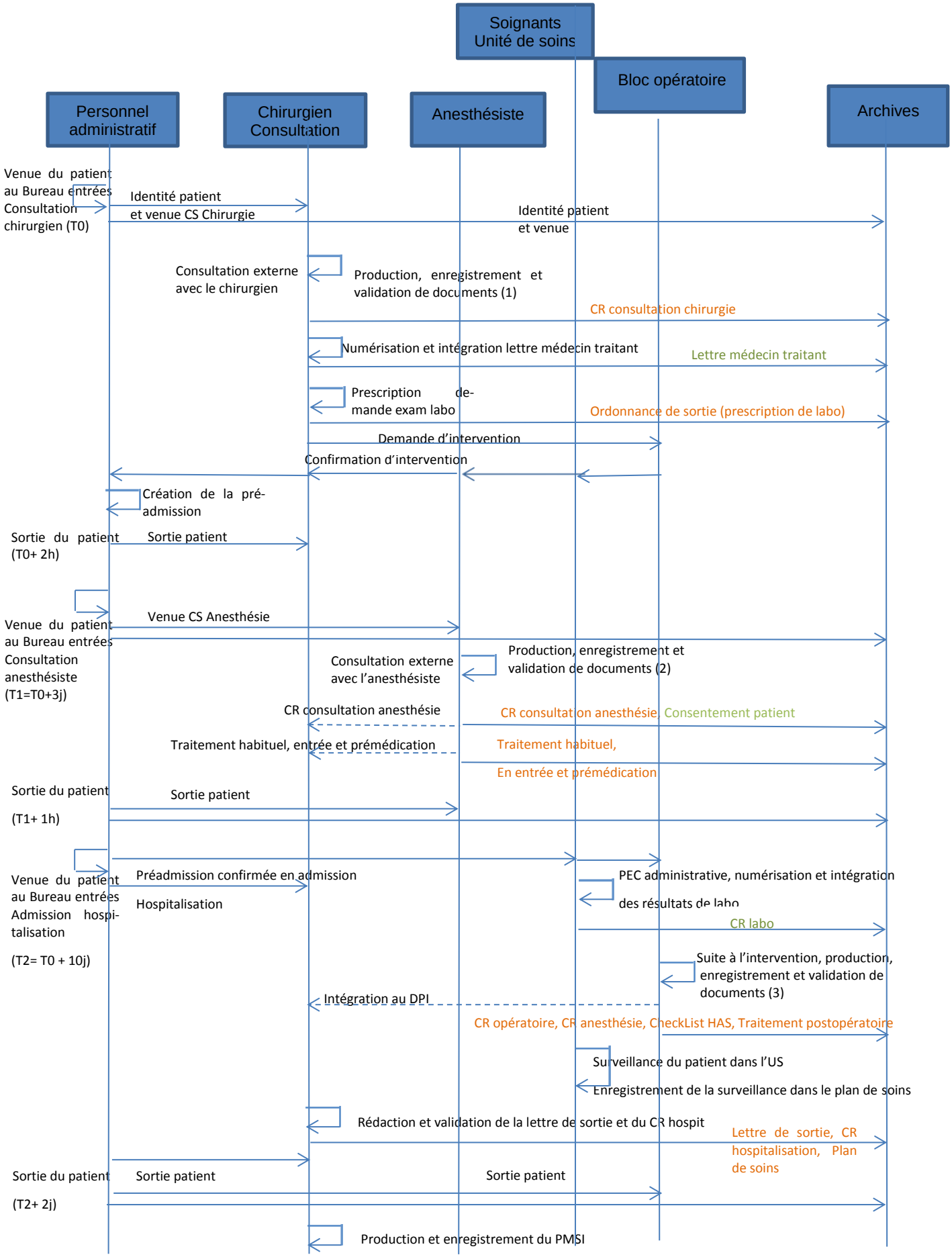


Figure 6.1.2-1 *: archivage des documents du patient dès leur validation dans le système producteur*

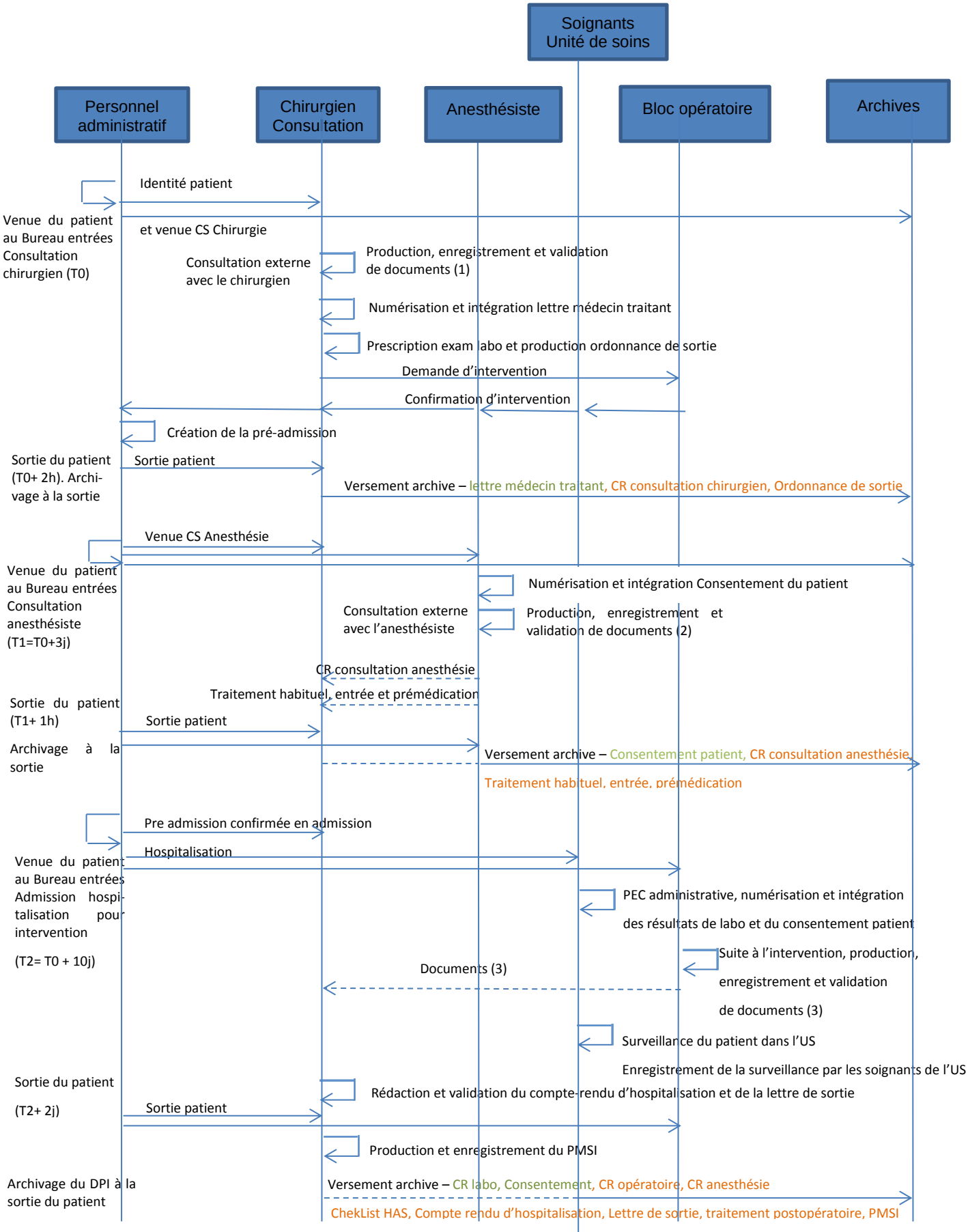


Figure 6.1.2-2 *: archivage des documents à la sortie du patient*

6.1.3 Implémentation des profils IHE et normes internationales répondant au besoin du cas d'usage

Pour ce cas d'usage, les solutions techniques envisagées pour permettre de répondre aux exigences de valeur neutre et probante de l'information médicale peuvent être différentes en fonction de l'alternative choisie.

6.1.3.1 Archivage de l'information dès la validation par le système producteur

Dans ce contexte, le système producteur de l'information en intra hospitalier est directement interconnecté avec le SAE et l'information médicale est directement versée au SAE dès sa validation par le professionnel de santé.

Ce cas d'usage est équivalent à celui décrit au chapitre 6.4. L'hypothèse proposée dans ce présent document consiste à considérer que, tel que décrit dans le chapitre 5, la norme HL7v3 CDAr2 permet de garantir la valeur neutre de l'information et que cette même norme associée au profil IHE-XDS permet d'une part d'assurer la structuration de l'information nécessaire à sa valeur probante dans le SIH et d'autre part d'implémenter les transactions d'inter connexion entre le SIH et le SAE.

6.1.3.2 Archivage de l'information à la sortie du patient

Dans ce contexte, les systèmes producteurs de l'information en intra hospitalier communiquent éventuellement les documents médicaux validés par les professionnels de santé en direction d'un acteur du SIH qui joue le rôle d'entrepôt de documents (implémenté par exemple par un DPI). Ces informations déposées dans l'entrepôt de documents vont ensuite alimenter le SAE après la sortie du patient de l'établissement.

Le profil IHE-DRPT (Displayable Report) décrit dans le chapitre 5.4 de ce présent document ainsi que le livre blanc « Harmonisation de la communication des documents intra hospitaliers » publié par InteropSanté permettent, hormis l'absence actuellement d'empreinte du document, de répondre à l'exigence de préservation de la valeur probante du document lors de sa communication dans un contexte intra hospitalier (par exemple lors de la communication d'un document d'un système source vers un entrepôt de documents).

L'interaction entre l'entrepôt de documents intra hospitalier et le SAE est ensuite équivalente au cas d'usage décrit au chapitre 6.4.

Création, révision, communication et consultation intra et inter entreprise de documents médicaux validés	
Profil IHE :	**« *Displayable Reports* » (DRPT)**
Objet :	Transactions supportant la création, la révision, la communication intra et inter services et la consultation de documents affichables, au format PDF/A et CDAr2
Statut :	Final text : Spécification en test (Trial Implementation)
Résumé :	http://wiki.ihe.net/index.php?title=Displayable_Reports
Extension française	Livre blanc « Harmonisation des modes de communication des documents médicaux en intra hospitalier »
Transactions :	CARD-7 : Communication et mise à disposition du document médical à l'ensemble de l'équipe médicale
Spécifications	CARD Supplement:

Création, révision, communication et consultation intra et inter entreprise de documents médicaux validés	
Profil IHE :	**« *Displayable Reports* » (DRPT)**
générales	http://ihe.net/uploadedFiles/Documents/Cardiology/IHE_CARD_Suppl_DRPT.pdf
Standards	- HL7 Messaging Standard v.2.6, Chapter 9 - ISO 19005-1. Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF (PDF/A) - HL7 v3 Clinical Document Architecture Release 2

L'implémentation du profil DRPT (message HL7v2.6 MDM), associée à un dispositif robuste/sécurisé d'accès à l'information médicale et à un système de traçabilité des actions réalisées sur l'ensemble du SIH (implémentation du profil IHE ATNA) peut permettre d'assurer la valeur probante du document dès sa création et lors de sa communication au sein du SIH.

Les mécanismes d'authentification des professionnels de santé décrits dans le « référentiel d'authentification des acteurs de santé » couplés aux mécanismes d'imputabilité décrits dans le « référentiel d'imputabilité » permettent d'assurer, à différents niveaux, la valeur probante de l'information.

Le lecteur pourra consulter ces deux référentiels pour décider des niveaux d'authentification et d'imputabilité qu'il souhaite implémenter dans son SIH.

La fonctionnalité de traçabilité des actions réalisées sur l'ensemble du SIH est couverte par le profil IHE-ATNA. Ce profil, décrit dans le chapitre 5.5 de ce présent document, permet à la fois de sécuriser les transactions entre les systèmes appartenant à un domaine sécurisé et d'alimenter un répertoire d'audit avec les messages d'audits générés de façon normalisée par l'ensemble des systèmes du domaine sécurisé.

Sécurisation des échanges et traçabilité des actions	
Profil IHE :	**« *Audit Trail Node Authentication* » (ATNA)**
Objet :	*Authentification forte des systèmes impliqués dans les échanges, centralisation des traces des échanges et des traces d'accès aux données de santé ou d'exportation de ces données*
Statut :	Final text : Spécification stable
Résumé :	http://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication
Extension française	N/A
Transactions :	ITI-20 : Alimentation du répertoire d'audit avec les messages d'audit
Spécifications générales	ITI TF : http://ihe.net/Technical_Frameworks/#IT ▪ Vol. 1 - Section 9 ▪ Vol. 2 - Sections 3.19, 3.20

Sécurisation des échanges et traçabilité des actions	
Profil IHE :	**« *Audit Trail Node Authentication* » (ATNA)**
Standards	Audit Log Message - Normative Specification for the Audit Log Message including Schema DICOM PS3.15 A.5

Le profil IHE ATNA doit être associé au profil IHE CT (Consistent Time) qui permet de synchroniser sur une même base de temps, tous les systèmes participant au cycle de vie de l'information médicale au sein d'un domaine sécurisé.

Sécurisation des échanges et traçabilité des actions	
Profil IHE :	**« Consistent Time » (CT)**
Objet :	*Synchronisation des systèmes sur une même base de temps*
Statut :	Final text : Spécification stable
Résumé :	http://wiki.ihe.net/index.php?title=Consistent_Time
Extension française	N/A
Transactions :	ITI-1 : Maintien de la même base de temps
Spécifications générales	ITI TF : http://ihe.net/Technical_Frameworks/#IT • Vol. 1 - Section 7 • Vol. 2 - Sections 3.1
Standards	- NTP Network Time Protocol Version 3. RFC1305 - SNTP Simple Network Time Protocol (SNTP) RFC2030

6.2 Numérisation des documents papier

Ce cas d'usage décrit deux contextes très différents dans lesquels la numérisation des documents médicaux du patient est abordée. Le premier contexte correspond à la numérisation en masse des documents contenus dans les dossiers médicaux papier de l'établissement et le deuxième contexte décrit la numérisation et l'intégration au SIH, au fil de l'eau de documents médicaux provenant de l'extérieur de l'établissement.

L'objectif de la description de ces cas d'usage est d'apporter une réflexion sur les conditions à mettre en œuvre pour permettre à un établissement de passer au tout numérique et de s'affranchir à terme de la conservation des documents papier. Cette stratégie pose la question de la valeur probante de la copie numérique de documents originaux papier. Pour approfondir ce sujet, le lecteur pourra se reporter à l'annexe juridique du vade-mecum du SIAF[28] consacré à la valeur de la copie numérique de documents originaux papier. Ce document stipule qu'il est possible, à droit constant, moyennant une analyse juridique du processus concerné pour écarter les cas les plus risqués (contrats ou décisions de l'administration notamment) de détruire le support papier après numérisation.

Cette destruction ne peut être appliquée que lorsque la numérisation porte sur des documents dont la durée d'utilité administrative (DUA) n'est pas échue[29] et qui sont destinés à alimenter un système d'information (SI).
Dans ces deux cas d'usage, on précisera la composition du SIH en distinguant le DPI à strictement parler d'un logiciel de Gestion Electronique de Documents (GED)[30]. Ce dernier, déployé à l'appui du DPI, est prévu ici pour apporter des fonctionnalités adaptées à la gestion et à la consultation de gros volumes de documents comme les copies numériques issues de la numérisation des documents papier.

Il est possible d'envisager des architectures différentes : le logiciel de DPI peut intégrer des fonctionnalités de GED, rendant la distinction entre ces deux logiciels invisible.

Compte-tenu du fort besoin de garantie de l'intégrité des copies numériques, le SAE peut également jouer le rôle de la GED. Néanmoins, cette configuration est fortement déconseillée car elle nécessiterait de prévoir, depuis le DPI, des accès nombreux et rapides aux documents archivés dans le SAE.

Dans tous les cas, l'ergonomie de l'articulation du DPI et de la GED doit être attentivement pensée pour faciliter le travail des usagers.

6.2.1 Numérisation en masse des dossiers papier

6.2.1.1 Description du cas d'usage

L'objectif principal du projet de numérisation en masse des archives papier de l'établissement est de pourvoir réduire la charge de travail des archivistes et secrétaires,

[28] http://www.archivesdefrance.culture.gouv.fr/static/7429.

[29] Il n'est pas question de pouvoir détruire des archives historiques après leur numérisation à des fins de diffusion patrimoniale.

[30] Le terme de GED ne désigne pas un type de logiciel normé mais une grande variété de logiciels à vocation documentaire. Certaines GED se rapprochent d'un SAE en incorporant des fonctionnalités de garantie de l'intégrité, de gestion de la signature électronique, etc. D'autres sont beaucoup plus basiques ou dédiées au travail collaboratif.

ainsi que le délai d'accès aux informations médicales contenues dans le dossier papier, lors du retour du patient dans l'établissement. Pour atteindre cet objectif, l'établissement décide de numériser les archives papier afin qu'elles soient accessibles en temps réel, sans forcément la volonté de les détruire. La version numérisée n'est finalement qu'une copie d'un original papier qui permet d'éviter la manipulation physique des dossiers.

La procédure de numérisation doit être définie et documentée par l'établissement. Elle doit être réalisée dans les règles de l'art tant du point de vue de son contenu (ajout, suppression de documents) que de son classement. Dans le cas où l'établissement souhaiterait détruire les documents papier originaux après numérisation et qu'il produit des archives publiques, cette procédure de numérisation doit être validée par la personne en charge du contrôle scientifique et technique sur les archives publiques (il s'agit du directeur des archives départementales territorialement compétent).

Dans ce cas d'usage, l'établissement met en place une procédure de numérisation des archives papiers. Cette procédure définit les objectifs de la numérisation, décrit très précisément les différentes étapes du processus, identifie les différents acteurs et leur rôle, ainsi que les paramètres techniques de la chaîne de numérisation (configuration des scanners, résolution et échantillonnage des couleurs, format des copies numériques…[31]. Elle indique aux opérateurs comment réagir face à des cas atypiques (documents hors format, supports spéciaux, présence de couleurs signifiantes, compression, traitements automatisés de l'image…). Un jeu de documents choisis en fonction de leur représentativité des problèmes rencontrés sert à valider les choix techniques et à calibrer les scanners. Une fiche de suivi permet de suivre le processus.

Une fois numérisé, le dossier papier est figé et n'évolue plus (l'établissement a mis en place une organisation pour arrêter de produire du papier en informatisant massivement les services cliniques). Le dossier numérique devient donc le dossier de référence qui va être alimenté par la suite.

Le processus de numérisation décrit dans ce cas d'usage est donné à titre indicatif. Il est appliqué tous les jours pour une liste de patients susceptibles de revenir à l'hôpital dans les 15 jours. Les étapes de ce processus pourraient être les suivantes :

- Sortie du dossier des archives
    - La liste des dossiers papiers à numériser est générée tous les matins par la DSI pour les patients attendus dans les 15 jours. L'agent de régie prélève les dossiers, imprime les bons de numérisation, initialise les fiches de suivi et transporte les dossiers vers le bureau de préparation. Il indique dans le logiciel des archives que le dossier est en cours de numérisation.
- Préparation
    - L'opérateur de préparation vérifie que les bons de numérisation et la fiche de suivi correspondent au dossier papier. L'opérateur prépare les documents du dossier (enlever les agrafes, lisser les feuilles …) et insère les bons de numérisation correspondant à la nature de chaque document. Les tables de prépara-

[31] Pour plus de détails, voir le vade-mecum précité du Service interministériel des Archives de France.

tion sont suffisamment éloignées les unes des autres pour éviter les mélanges. Le dossier préparé est apporté à l'opérateur de numérisation.

- Numérisation
    - L'opérateur de numérisation place les feuilles du dossier dans le scanner et les numérise. Il contrôle la qualité de numérisation des documents (lisibilité, contraste, orientation).
- Indexation
    - Grâce à l'emploi de codes-barres placés sur les bons de numérisation, le système ajoute automatiquement des métadonnées qui identifient les documents numérisés. Ces métadonnées doivent aussi identifier l'opérateur de numérisation et horodater le moment de la numérisation.
    - L'opérateur de numérisation indexe le dossier numérique dans le logiciel des archives papier pour que les utilisateurs aient connaissance de la version numérique du dossier papier.
- Calcul d'empreinte
    - Autant que possible, c'est la chaîne de numérisation qui joint aux copies numériques leur empreinte, afin d'attester ensuite de leur intégrité dans le temps, une fois versées dans la GED. À défaut, la GED doit calculer l'empreinte des copies numériques à leur versement.
- Identification
    - Le contrôleur vérifie la lisibilité, la qualité des documents numérisés. Il vérifie l'identité du patient dans les différents sous dossier et compare le nombre de pages numérisées, sur la fiche de suivi, au nombre de pages dans le système de numérisation. Il ferme le dossier médical à l'aide d'un ruban adhésif et appose le tampon « Numérisé » sur la pochette de façon à identifier que ce dossier a été numérisé. Le dossier est ensuite retourné aux archives. Si une destruction est possible et envisagée, il convient de conserver les documents papier au moins le temps nécessaire pour que l'utilisation de ces documents par le personnel médical laisse une chance supplémentaire de repérer d'éventuelles erreurs de numérisation. Le Service interministériel des Archives de France conseille une durée de conservation de 6 mois.
- Versement dans le système de GED
    - En fin de journée, le responsable de l'atelier compare le nombre de fiches de suivi avec le nombre de dossier scannés. Il procède ensuite au versement des dossiers numérisés de la journée vers la GED (opération de nuit).
- Contrôle
    - Le contrôleur reprend l'ensemble des fiches de suivi de la journée précédente et contrôle sur les documents de la GED l'identité du patient (sur chaque page), compare le nombre de pages indiqué sur la fiche de suivi et le nombre de pages indiquées dans la GED et vérifie également la lisibilité et la qualité des documents de la GED.

Finalement, lorsque le patient revient dans l'établissement,

- Les données médicales produites lors de cette nouvelle prise en charge du patient (archives courantes) sont stockées dans le DPI,
- Les données médicales issues du dossier papier (archives intermédiaires) sont stockées dans la GED.

A la sortie du patient de l'établissement, les documents cliniques de ce patient sont déversés automatiquement du DPI et de la GED dans le SAE.

6.2.1.2 Description du workflow d'information

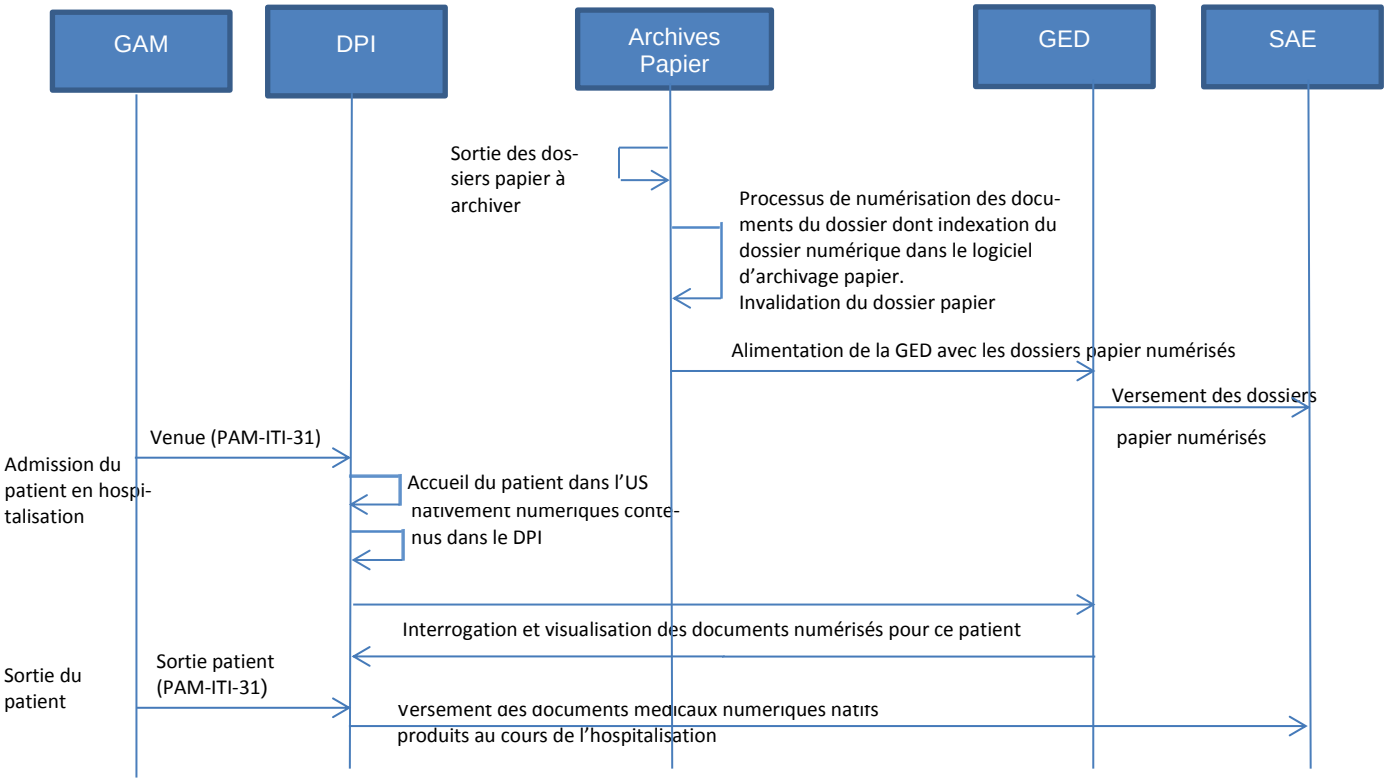


Figure 6.2.1.2-1 : Numérisation en masse du DPI

6.2.2 Numérisation des documents au fil de l'eau

6.2.2.1 Description du cas d'usage

Un patient hospitalisé dans un établissement hospitalier A est adressé, par le médecin responsable de son hospitalisation, vers l'équipe médicale d'un établissement B de soins de suite et de réadaptation (SSR).
Le médecin de l'établissement A rédige un courrier ainsi qu'un volet médical en direction de l'équipe médicale de l'établissement B (SSR).

Deux situations peuvent se présenter:

- Les deux établissements A et B n'ont pas la possibilité d'échanger des informations médicales de façon sécurisée. Le courrier et le volet médical sont imprimés et remis au patient qui les apportera lors de son admission dans l'établissement SSR.
- Les deux établissements A et B ont établi un contrat avec un opérateur de Messagerie de Santé Sécurisée (MSS). Dans ce cas, le courrier, ainsi que le volet médical, sont rédigés et validés par le médecin de l'établissement A et envoyés directement au médecin de l'établissement SSR via la MSS.

6.2.2.1.1 Remise des documents médicaux par le patient

6.2.2.1.1.1 Description du cas d'usage

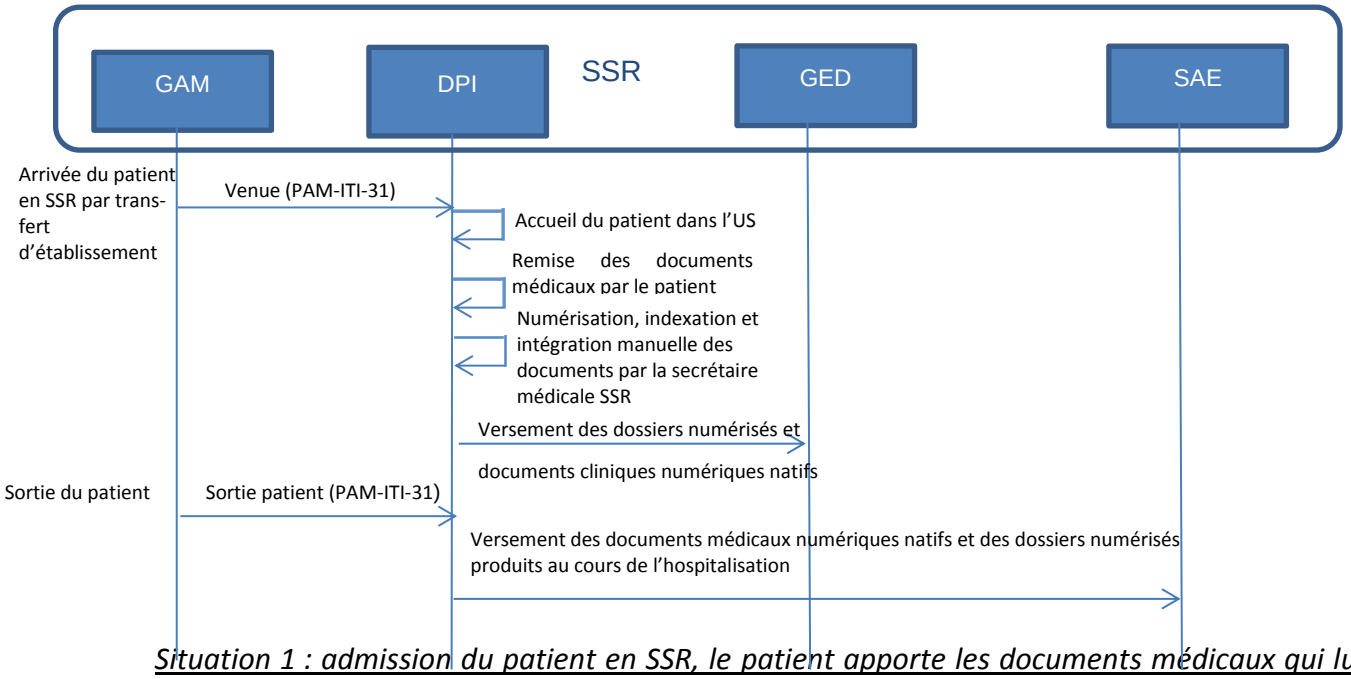
L'établissement SSR est doté d'un DPI et/ou d'une GED. Dans ce cas d'usage, deux choix d'implémentation sont possibles :

- (1) Le DPI est utilisé comme point d'entrée pour numériser les documents remis par le patient lors de son admission. Ces documents numérisés sont ensuite transmis à la GED (en fonction de règles de gestion de l'information définies par l'établissement) qui joue le rôle d'entrepôt de documents intra hospitalier et qui regroupe l'ensemble des documents pertinents dans la prise en charge du patient, provenant de différents systèmes producteurs (dont le DPI).
- (2) La GED est utilisée comme point d'entrée pour numériser les documents remis par le patient lors de son admission. Les documents stockés dans la GED doivent ensuite être rendus accessibles à l'équipe soignante, par un mécanisme d'intégration du DPI à la GED.

C'est le 1° contexte qui est décrit par la suite dans ce cas d'usage.
Lors de l'admission du patient dans l'établissement,

- Le patient est accueilli au niveau du secrétariat, où la secrétaire enregistre le patient et créée le séjour en SSR pour ce patient,
- Elle numérise les documents adressés par l'établissement A, conformément à la procédure de numérisation documentée dans l'établissement SSR, qui devra répondre aux mêmes exigences que dans le cas d'usage vu précédemment,
- Elle associe chaque document manuellement au bon patient et au bon séjour via le logiciel DPI de l'établissement SSR,
- Le système associe automatiquement des métadonnées au document permettant ainsi d'indexer et d'intégrer ce document au DPI du patient. Un calcul d'empreinte est fait dans les conditions évoquées dans le cas d'usage précédent. Certaines métadonnées qui ne peuvent pas être déterminées automatiquement par le système sont ressaisies par la secrétaire médicale. Cette ressaisie doit être limitée de façon à minimiser les erreurs possibles.
  L'opération d'indexation automatique, dans les règles de l'art, devrait au moins définir l'auteur de la numérisation, ainsi que l'horodatage de cette opération.

6.2.2.1.1.2 Description du workflow d'information



Situation 1 : admission du patient en SSR, le patient apporte les documents médicaux qui lui ont été remis lors de sa sortie d'hospitalisation précédente

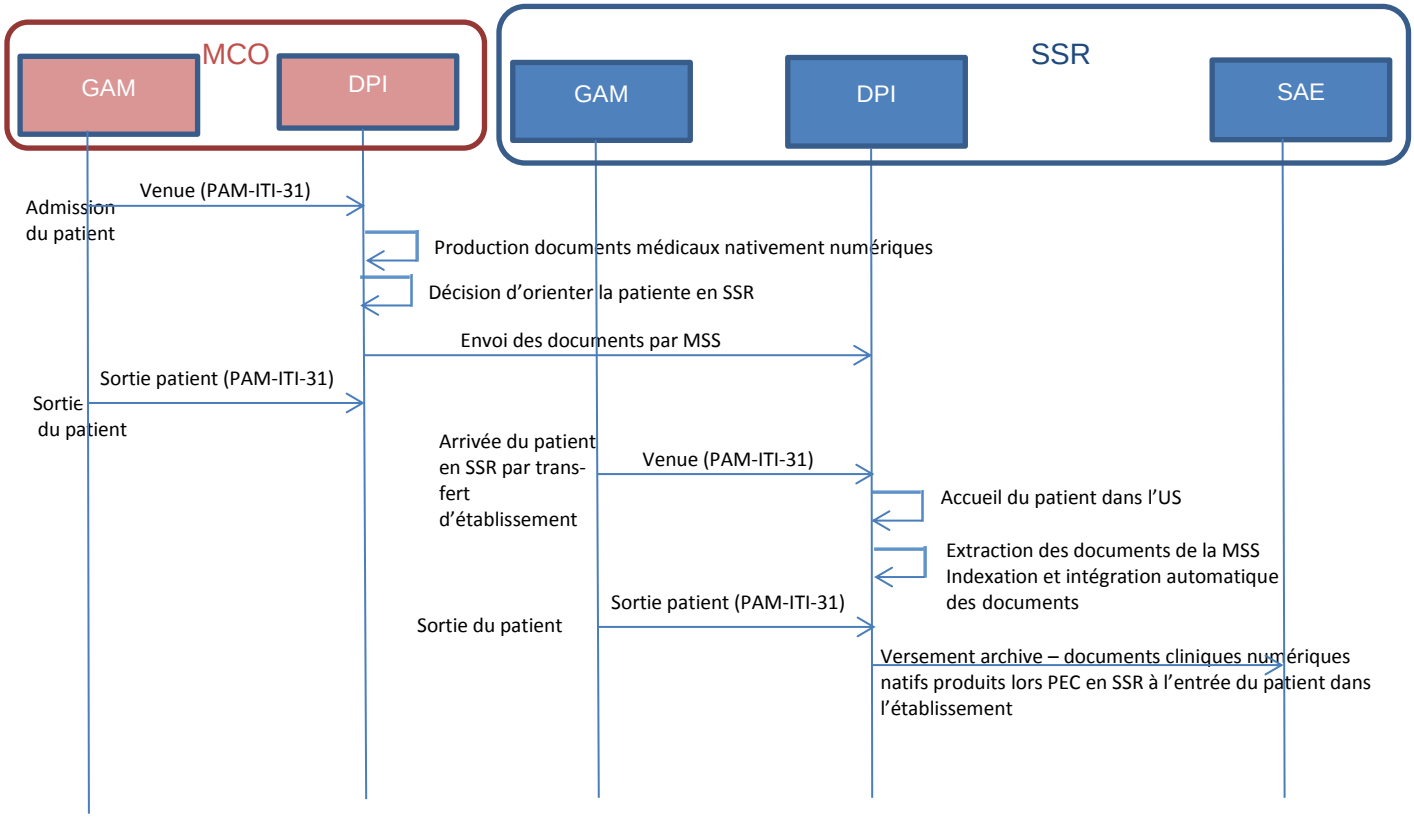
6.2.2.1.2 Transfert automatique des documents via la Messagerie Sécurisée de Santé

6.2.2.1.2.1 Description du cas d'usage

L'établissement SSR est doté d'un DPI et lors de l'admission du patient dans l'établissement,

- Le patient est accueilli au niveau du secrétariat, où la secrétaire enregistre le patient et créé le séjour en SSR pour ce patient,
- Elle réceptionne le courriel envoyé, via la MSS, par le médecin de l'établissement A,
    - Dans le cas où la pièce jointe est au format IHE_XDM, le système destinataire réalise automatiquement l'extraction, l'indexation et le stockage des documents inclus dans cette pièce jointe.
    - Dans le cas où le système destinataire ne serait pas en capacité de traiter la pièce jointe au format IHE_XDM, le système émetteur y adjoint l'ensemble des documents au format pdf/A. La secrétaire médicale devra alors extraire chaque document et associer sur chacun de ces documents un minimum de métadonnées, comme dans le cas précédent.

6.2.2.1.2.2 Description du workflow d'information



Situation 2 : Envoi des documents médicaux via la MSS en préalable à l'admission du patient en SSR

6.2.3 Implémentation des profils IHE et normes internationales répondant au besoin du cas d'usage

6.2.3.1 Numérisation en masse des documents

La valeur probante des documents numérisés en masse est garantie par l'application d'une procédure de numérisation documentée.

Suite à la numérisation en masse des documents, il faut veiller à mettre en œuvre un mécanisme d'intégration entre le DPI et la GED permettant au médecin de visualiser dans le DPI à la fois les documents médicaux produits au cours de la prise en charge du patient en cours et les documents médicaux produits lors des prises en charge antérieures et stockés dans la GED.

Ce mécanisme d'intégration entre le DPI et la GED peut être mis en œuvre par l'implémentation du profil IHE-XDS-b : Cross Enterprise Document Sharing décrit au chapitre 5.2 du présent document :

- Au cours de la procédure de numérisation, les documents numérisés sont indexés par des métadonnées.

- Le document numérisé est stocké dans le composant « Document Repository » implémenté par la GED et les métadonnées associées au document sont stockées dans le composant « Registry » du profil XDS-b.
- Le DPI implémente l'acteur « Document Consumer » qui permet, à partir du DPI, d'interroger le registre d'index et de récupérer ainsi le document numérisé stocké dans la GED.

Production, diffusion, partage de documents médicaux	
Profil IHE :	**« *Cross-enterprise Document Sharing* » (XDS-b)**
Objet :	Partage de documents médicaux au sein d'une communauté médicale
Statut :	Final text : Spécification stable
Résumé :	http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing
Extension française	Volet « *Partage de documents de santé* » du CI-SIS de l'ASIP
Transactions :	ITI-41 : Alimentation de l'infrastructure de partage ITI-42 : Indexation des documents stockés dans l'infrastructure de partage (stockage des métadonnées dans le registre d'index) ITI-18 : Interrogation du registre d'index ITI-43 : Consultation et récupération des documents consultés dans l'infrastructure de partage.
Spécifications générales	ITI TF : http://ihe.net/Technical_Frameworks/#IT Volume 1 – section 10 : Description du profil en termes utilisateur Volume 2b – section 3.41 : alimentation de l'infrastructure de partage Section 3.43 : accès aux documents stockés dans l'infrastructure de partage
Standards	- ebMS OASIS/ebXML Messaging Services Specifications v3.0 - ebRIM OASIS/ebXML Registry Information Model v3.0 - ebRS OASIS/ebXML Registry Services Specifications v3.0 - HTTP HyperText Transfer Protocol HTTP/1.1 (IETF RFC2616) - ISO/IEC 9075 Database Language SQL - HL7 Version 2.5 - HL7 Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration

6.2.3.2 Numérisation des documents au fil de l'eau

6.2.3.2.1 Remise des documents médicaux par le patient

Comme dans le cas d'usage précédent, il est éventuellement nécessaire de mettre en œuvre un mécanisme d'intégration entre le DPI et la GED. Ces mécanismes sont les mêmes quel que soit le point d'entrée choisi pour la numérisation.

- Le document est numérisé lors de l'admission du patient et il est généralement indexé et intégré au DPI. Il peut éventuellement alimenter un entrepôt de données intra hospitalier (une GED par exemple). Il est, dans ce cas, nécessaire de mettre en

œuvre un mécanisme d'intégration entre le DPI et l'entrepôt de documents. Ces mécanismes sont les mêmes quel que soit le point d'entrée choisi pour la numérisation (le DPI ou la GED).

- Le profil IHE-DRPT supporte la création, la révision, la communication inter services et la consultation de documents affichables (au format PDF/A et CDAr2) d'un système producteur vers un système consommateur tout en préservant la valeur probante de l'information lors de la communication.
- Le profil IHE-XDS-b, même s'il est habituellement utilisé pour une communauté extra hospitalière, peut permettre de partager des documents médicaux entre divers systèmes en intra hospitalier.

6.2.3.2.2 Transfert automatique des documents via la MSS

Les modalités d'échange de documents de santé via la messagerie électronique sécurisée, définies dans le volet « Echange de Documents de Santé »[32] du Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS), reposent sur le profil IHE-XDM qui prévoit l'envoi en pièce jointe d'un fichier zip IHE_XDM contenant les documents de santé.
En complément de la pièce jointe IHE_XDM, les documents peuvent être envoyés en pièces jointes au format bureautique (il est recommandé d'utiliser le format PDF/A-1) afin de faciliter la lecture pour les destinataires qui ne seraient pas en capacité d'exploiter le format XDM.
Un message ne doit contenir qu'une seule pièce jointe IHE_XDM, qui peut elle-même contenir plusieurs documents de santé (concept de lot de soumission) concernant le même patient. Chaque document de la pièce jointe IHE_XDM est obligatoirement associé à un ensemble de métadonnées fournies par le système émetteur.

Dans le cas où le système destinataire ne serait pas en capacité d'exploiter la pièce jointe au format IHE_XDM, il pourra récupérer les documents au format PDF/A-1. Dans ce cas, ces documents ne sont pas décrits automatiquement par des métadonnées, ce qui nécessitera une re-saisie de celles-ci

Transfert de documents médicaux et des métadonnées associées via un media	
Profil IHE :	**« *Cross-Enterprise Document Media Interchange* » (XDM), implémenté par la MSS**
Objet :	Transfert de documents médicaux et des métadonnées associées via un media type CR-Rom ou via une pièce jointe d'un e-mail.
Statut :	Final text : Spécification stable
Résumé :	http://wiki.ihe.net/index.php?title=Cross-enterprise_Document_Media_Interchange http://esante.gouv.fr/sites/default/files/asset/document/mss_fon_dst_interfaces_clients_mssante_v1.0.1_150529.pdf
Extension française	Aucune
Transac-	ITI-32 : Distribute Document set on Media

[32] CI_SIS, Volet Echanges de documents de santé : http://esante.gouv.fr/sites/default/files/asset/document/ci-sis_services_volet-echange-documents-sante_v1.3.2.1.pdf

Transfert de documents médicaux et des métadonnées associées via un media	
Profil IHE :	**« *Cross-Enterprise Document Media Interchange* » (XDM), implémenté par la MSS**
tions :	
Spécifications générales	ITI TF : http://ihe.net/Technical_Frameworks/#IT Vol. 1 - Section 16, E, J, K Vol. 2b - Sections 3.32 Vol. 2x - Appendix T Use of e-mail Vol. 3 - Section 4.1 XDS Metadata
Standards	- DICOM PS 3.10 Media Storage and File Format for Data Interchange (DICOM file format). http://dicom.nema.org/ - DICOM PS 3.12 Media Formats and Physical Media for Data Interchange, Annex F - 120mm CD-R media, Annex R - USB Connected Removable Devices, Annex V - ZIP File Over Media, and Annex W - E-mail Media. http://dicom.nema.org/ - XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition). A Reformulation of HTML 4 in XML 1.0. W3C Recommendation 26 January 2000, revised 1 August 2002. http://www.w3.org/TR/xhtml1. - XHTML™ Basic. W3C Recommendation 19 December 2000. http://www.w3.org/TR/xhtm-basic. - MDN: RFC 3798 Message Disposition Notification. http://www.rfc-editor.org/rfc/rfc3798.txt - ebRIM OASIS/ebXML Registry Information Model v3.0 - ZIP format http://www.pkware.com/support/zip-app-note/

6.3 Le cas des Groupements Hospitaliers de Territoire

Ce cas d'usage doit permettre de préciser les échanges d'informations entre professionnels de santé au sein du GHT mais aussi vers les partenaires extérieurs au GHT (système d'information de santé et parcours du patient au sein du territoire de santé) et de réfléchir à l'archivage des données médicales dans ce contexte de fonctionnement.

La création des groupements hospitaliers de territoire (GHT) est prévue à l'article 107 de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, en remplacement des actuelles Communautés hospitalières de territoire.

Extrait du rapport publié en mai 2015 par la Mission Groupements Hospitaliers de Territoire[33] :

« Un GHT constitue un regroupement d'établissements de santé publics (CHU, Centres hospitaliers, établissements psy, EHPAD) définit au niveau d'un territoire.

L'objectif de la mise en œuvre des GHT est de garantir une véritable égalité d'accès à des soins sécurisés et de qualité pour tous en tout point du territoire. Les GHT sont obligatoirement fondés avant tout sur un projet médical commun définit par la communauté médicale au niveau d'un territoire donné. Le 1° objectif du GHT est d'organiser au niveau du territoire une prise en charge graduée des patients de l'hôpital public. De cette approche centrée sur le patient doit découler l'identification des activités à mutualiser entre les différents établissements du GHT.

Le projet médical commun a vocation à définir et à structurer toutes les filières inter-hospitalières de prise en charge de patients, au sein d'un même GHT. Ce projet médical partagé se doit donc d'**intégrer toutes les spécialités**, sans exception. Les établissements participant au GHT devront s'inscrire dans une logique de complémentarité des activités plutôt que dans une logique de compétition. »

Le GHT n'est pas doté de la personnalité morale : il s'agit plus d'un mode d'organisation de la collaboration entre plusieurs établissements de santé. La mise en œuvre d'un GHT va donc consister à construire un projet médical commun entre plusieurs établissements hospitaliers publics d'un territoire et à organiser le parcours de soins du patient au sein de ce GHT en fonction des spécialités et des fonctions supports attribuées à tel ou tel établissement.

Même si le projet de loi préconise d'unifier le SI pour les établissements participant au GHT, il faudra tenir compte sur le terrain des situations transitoires où des SI différents vont cohabiter pendant plusieurs années pour diverses raisons :

- Il semble difficile de déployer un seul type de DPI sur un GHT composé d'établissements hospitaliers très disparates (CHU, CH, établissement de soins de suite et de réadaptation, hôpital psychiatrique, etc..). On peut penser qu'un DPI unique conviendra à des établissements homogènes. A côté du DPI unique subsisteront sans doute des DPI spécialisés.

[33] http://sante.gouv.fr/IMG/pdf/Rapport_intermediaire_Mission_GHT_definitif.pdf

- Certains de ces établissements ont déjà investi dans un DPI, ce qui représente des coûts financiers et un investissement humain important pour maîtriser cet environnement.

Le groupe de travail est donc parti du postulat qu'il devait prendre en compte le caractère hétérogène des SI dans la construction des GHT.

Dans ce contexte, deux questions se posent, exactement comme dans un contexte intra hospitalier :

- Comment assurer le caractère neutre et probant de l'information médicale produite pour le compte du patient pris en charge dans le cadre du GHT ?
- Quels mécanismes envisager pour assurer l'archivage électronique intermédiaire de ces informations médicales ?

6.3.1 Mutualisation d'un plateau technique en biologie spécialisée

6.3.1.1 Description du cas d'usage

On suppose la création d'un GHT constitué de trois établissements hospitaliers CH1, CH2 et CH3.

L'objectif du GHT est de renforcer l'offre de biologie publique vis-à-vis de la concurrence privée, d'assurer la permanence des soins et d'obtenir l'accréditation du laboratoire de biologie spécialisé. Pour cela les trois établissements ont décidé d'engager une coopération forte entre les laboratoires de biologie médicale des différents CH, d'organiser et de mutualiser certaines spécialités de biologie médicale entre les établissements du GHT.

La biologie de routine et d'urgence est maintenue sur chacun des sites du GHT. La mise en œuvre d'une plateforme d'automates de laboratoire mutualisée entre les 3 établissements assurera l'ensemble des examens biologiques spécialisés (biochimie, hématologie, bactériologie, etc.).

D'autre part, ces trois établissements ont décidé également de mutualiser et d'externaliser le Service d'Archivage Electronique des informations médicales.

- Le patient est pris en charge dans son établissement de proximité CH1.
- Au cours de cette prise en charge, les analyses biologiques de routine sont réalisées dans l'établissement par le laboratoire de l'établissement CH1.
- Les demandes d'examens spécialisés sont prescrites par le médecin dans le DPI de l'établissement dans lequel le patient est admis (CH1).
    - Dans le cas d'une prescription connectée, cette demande d'examen spécialisé est transmise par le DPI-1 au système de gestion du laboratoire de l'établissement (SGL1),
    - Le laboratoire de l'établissement CH1 réalise la phase pré analytique de ces examens spécialisés. Un système de transport des contenants est organisé entre chaque établissement de la GHT et le laboratoire mutualisé.
    - La phase analytique est réalisée par le plateau technique mutualisé entre les 3 établissements. La validation technique de ces examens est réalisée au niveau de la plateforme mutualisée et les résultats validés techniquement sont renvoyés vers les sites de proximité via un système de concentrateur accessible à

l'ensemble des biologistes du GHT. Ces résultats ne sont pas communicables au prescripteur en l'état.

- Les résultats validés techniquement sont partagés entre l'ensemble des biologistes, ce qui permet au médecin biologiste du GHT de garde au CH2 (pour les activités du laboratoire spécialisé) de réaliser la validation biologique de ces résultats et d'assurer ainsi la permanence des soins en biologie médicale. Les résultats, une fois validés biologiquement, peuvent être communiqués au prescripteur, via un entrepôt commun de documents, et peuvent être archivés.

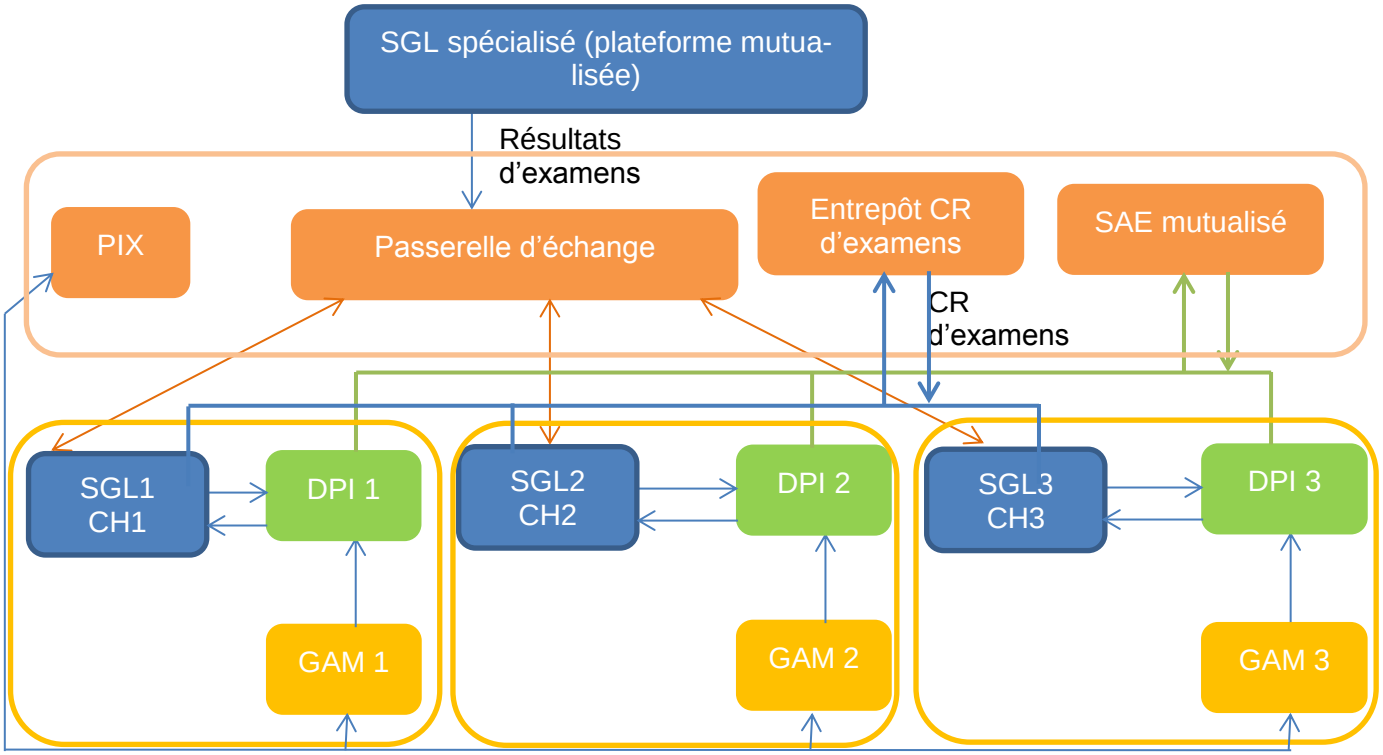


Figure 6.3.1.1-1 : Mutualisation du plateau technique de laboratoire

6.3.1.2 Description du workflow d'information

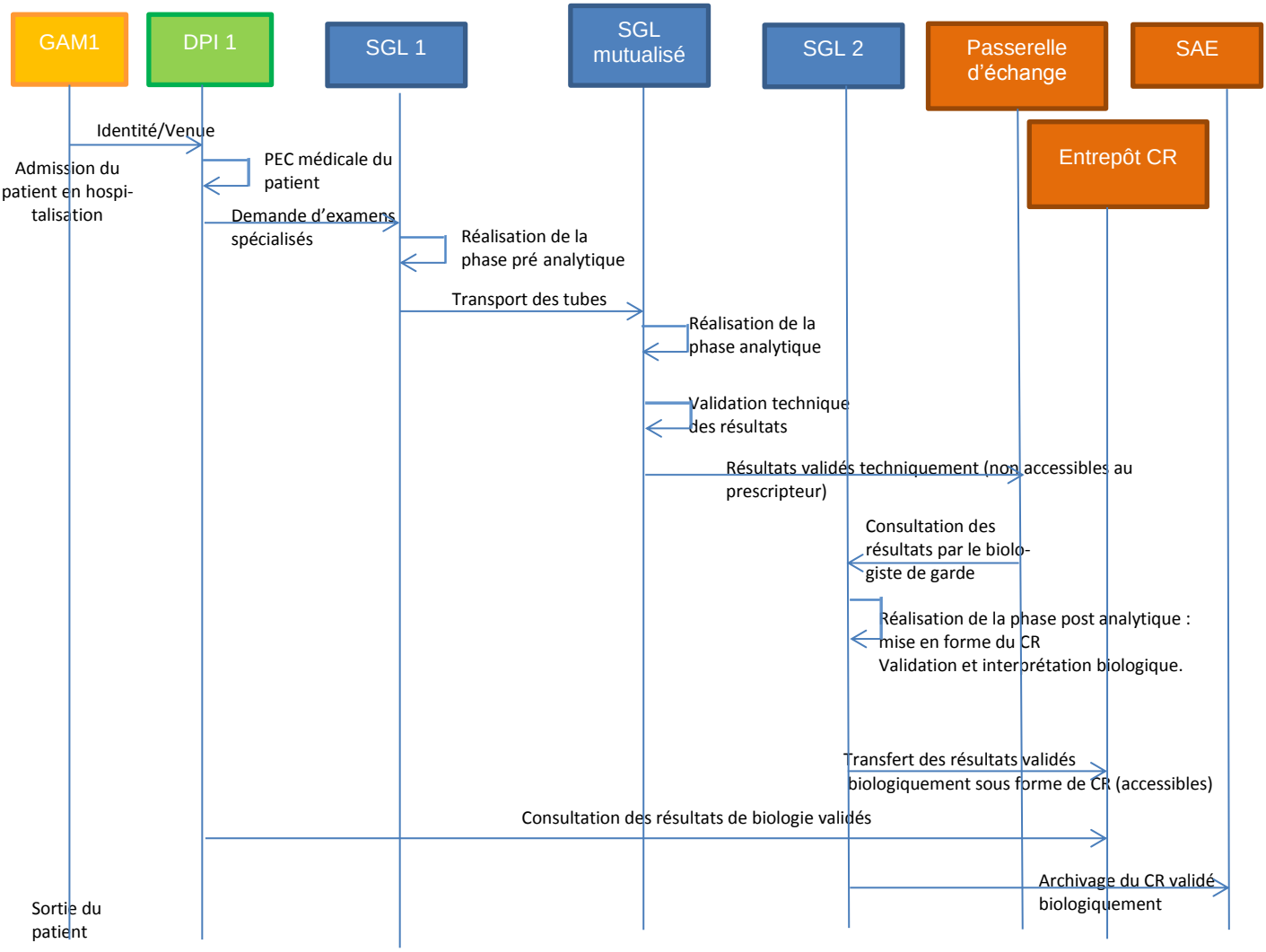


Figure 6.3.1.2-1 : Flux d'informations avec le plateau technique de laboratoire mutualisé

6.3.1.3 Implémentation des profils IHE et normes internationales répondant au besoin du cas d'usage

La norme NF EN ISO 15189[34] définit les exigences particulières concernant la qualité et la compétence, pour les Laboratoires de Biologie Médicale. Le Guide Technique d'Accréditation définit les recommandations relatives à l'application la norme NF EN ISO 15189 en matière de maîtrise des moyens informatiques et de dématérialisation des données au sein des laboratoires de biologie médicale concernés par cette norme.
La diffusion du compte-rendu d'examens validé biologiquement vers l'entrepôt de documents mutualisé utilise :

[34] NF EN ISO http://www.boutique.afnor.org/norme/nf-en-iso-15189/laboratoires-de-biologie-medicale-exigences-concernant-la-qualite-et-la-compe-tence/article/678634/fa157270?gclid=Cj0KEQiA6vS2BRDH8dq06YDHz_IBEiQAzNdBmVT5yuBTwVFTYJ3v1EU1HnV_2vp-I1aTZ73EHbEMzDwaAk0z8P8HAQ

- Le profil IHE-XDS et ses profils associés,
- Le compte-rendu structuré de biologie formaté conformément à la norme CDA, selon le modèle spécifié par le CI-SIS,
- Le compte-rendu PDF encapsulé dans un document CDA non structuré, tel que spécifié par le CI-SIS.

6.3.2 Construction d'une filière de soins

Le GHT est constitué de 3 établissements hospitaliers.

L'organisation en GHT reconnait à chacun de ces établissements une spécialité. Les patients pris en charge par ces établissements sont orientés en cas de besoin vers l'établissement référent pour cette spécialité.

Les patients sont susceptibles d'être admis dans les 3 établissements et d'être suivis par une équipe médicale composée des professionnels de santé rattachés aux trois établissements du GHT.

6.3.2.1 Mise en commun de l'information médicale au niveau d'une plateforme mutualisée

Dans le contexte de ce cas d'usage, les 3 établissements mutualisent des outils de collaboration hébergés chez un tiers : une infrastructure de partage de documents médicaux (XDS), un service de rapprochement d'identités (PIX) et un service d'archivage électronique (SAE).

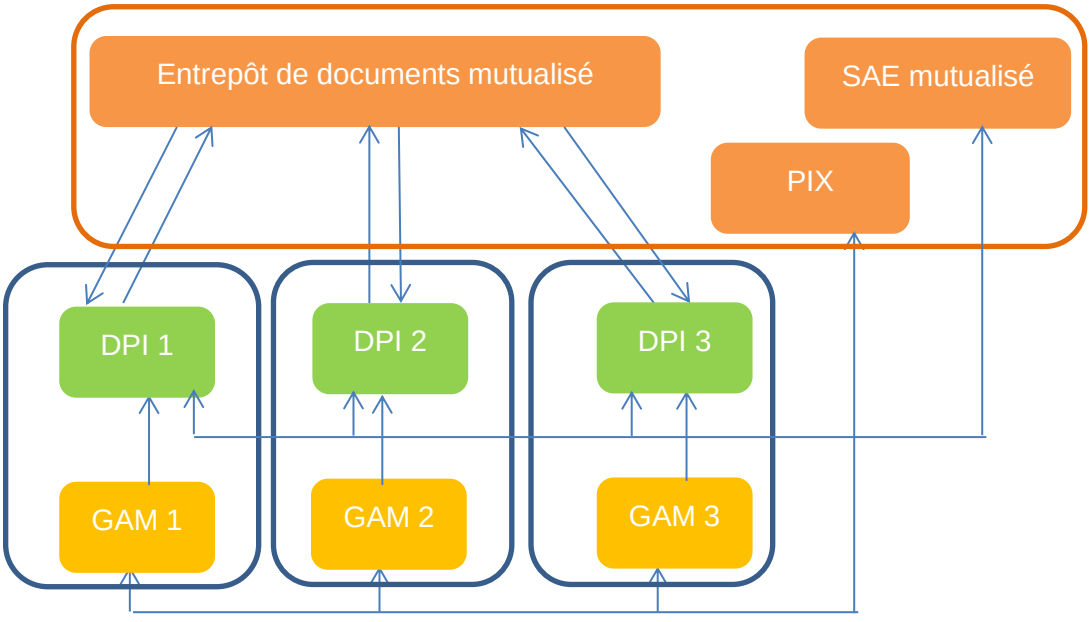


Figure 6.3.2.1-1 : Mutualisation d'outils collaboratifs

6.3.2.1.1 Description du cas d'usage

- Arrivée d'un patient aux urgences du CH1 suite à un problème cardiaque. Le patient est adressé en urgence au CH1 par son médecin généraliste. Le patient est pris en charge pour les soins d'urgence. Son état nécessite une intervention chirurgicale qui

doit être pratiquée par un chirurgien spécialisé de l'établissement CH2. Le résumé urgence est réalisé par l'urgentiste. Il est enregistré dans le DPI1 du CH1 ainsi que d'autres informations médicales résultant de la prise en charge en urgence. L'ensemble de ces documents médicaux sont publiés sur l'entrepôt de données partagé entre les établissements du GHT avec les métadonnées nécessaires à leur consultation par les DPI-2 et 3. Le chirurgien de l'établissement CH2 est averti de l'arrivée du patient et de la mise à disposition des documents médicaux de ce patient.

- Le patient est transféré dans le service de chirurgie cardiaque de l'établissement CH2. Le chirurgien peut visualiser l'ensemble des informations médicales concernant ce patient, y compris les documents issus du passage aux urgences du CH1, pour préparer l'intervention. Suite à l'intervention, l'ensemble des documents médicaux produits, dont le compte-rendu opératoire, sont enregistrés dans le DPI2 du CH2. Ces éléments sont également publiés sur l'entrepôt de données partagé entre les établissements du GHT. Un courrier est adressé au médecin traitant du patient via la MSS.
- Le patient sort de l'établissement CH2 pour être transféré en établissement de soins de suite et de réadaptation CH3. Les professionnels de santé de cette structure peuvent également consulter l'ensemble des documents médicaux partagés produits lors du passage du patient en CH1 et CH2. L'information médicale produite dans le cas de cette prise en charge est enregistrée dans le DPI3 du CH3 et est également publiée sur l'infrastructure de partage.

L'ensemble de l'équipe médicale qui a pris en charge le patient au cours de cet épisode de soins, répartie sur les 3 établissements, doit pouvoir consulter la totalité des documents médicaux stockés dans l'entrepôt de données mutualisé.

A la fin de l'épisode de soins ou au fil de l'eau (en fonction du choix d'organisation du GHT), l'ensemble des documents médicaux produits lors de la prise en charge du patient par les établissements CH1, CH2 et CH3 sont versés au service d'archivage électronique (SAE) mutualisé. Chaque DPI est conservé dans une instance séparée du SAE mutualisé du GHT.

6.3.2.1.2 Description du workflow d'information

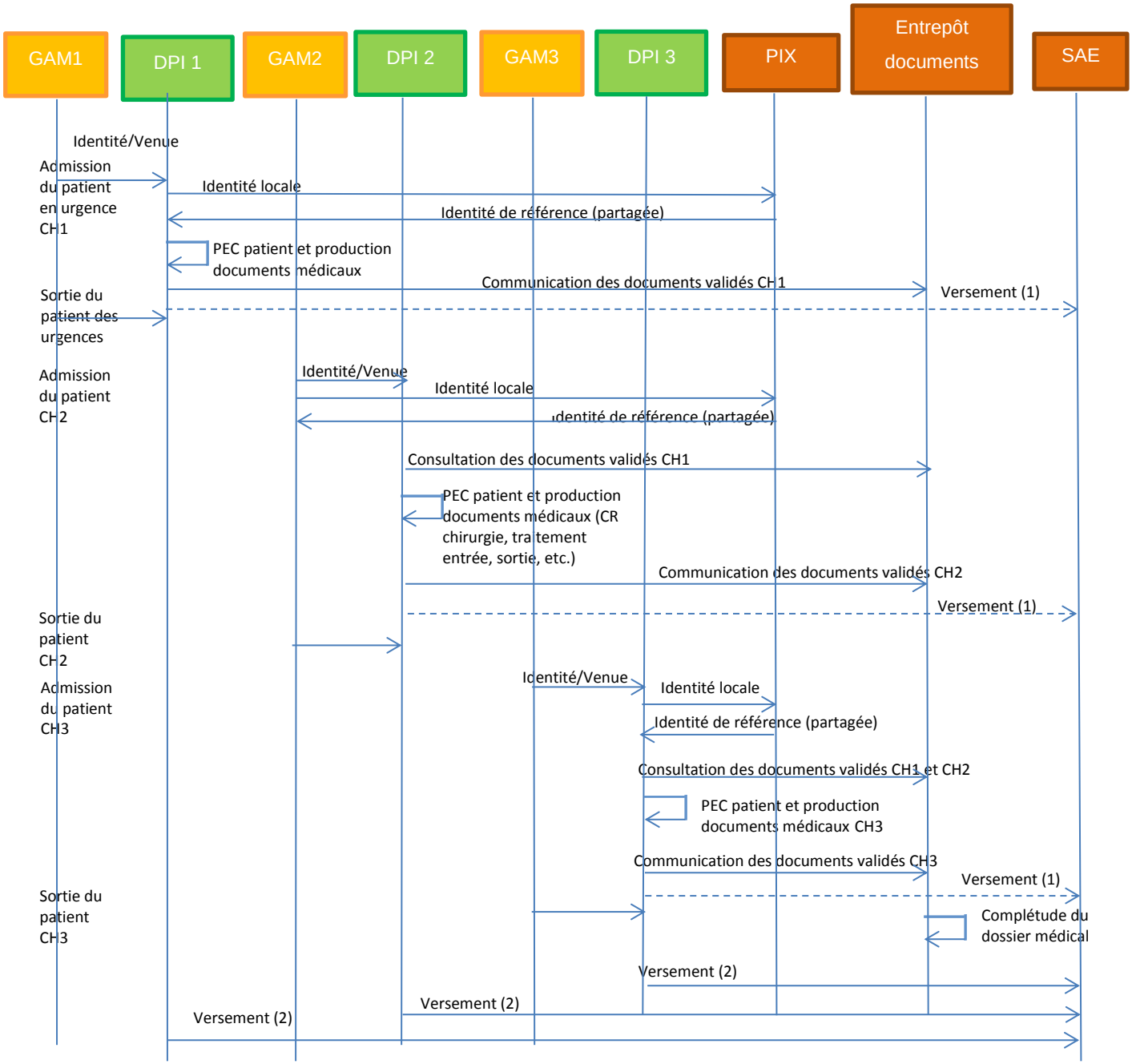


Figure 6.3.2.1.2-1 : Mutualisation d'outils collaboratifs

Versement (1) : versement des documents au fil de l'eau

Versement (2) : versement des documents à la fin de l'épisode de soins

6.3.2.1.3 Implémentation des normes et profils IHE qui répondent au besoin du cas d'usage

Ce cas d'usage met en œuvre les profils IHE-PIX et IHE-XDS-b.

Le profil PIX permet de réaliser le rapprochement des identités locales du patient pris en charge dans les différents établissements,

Le profil IHE-XDS-b permet de partager les documents médicaux du patient nécessaires à la coordination des soins.

Rapprochement d'identifiants patients inter-communautés	
Profil IHE :	**« Patient Identifier Cross Referencing» (PIX)**
Objet :	Rapprochement d'identifiants locaux d'un patient et attribution d'un identifiant commun de référence à un ensemble d'organisations
Statut :	Final text : Spécification stable
Résumé :	http://wiki.ihe.net/index.php?title=Patient_Identifier_Cross-Referencing
Extension française	Aucune
Transactions :	ITI-8 : Alimentation du serveur de rapprochement avec l'identité locale du patient ITI-9 : Interrogation du serveur de rapprochement par un système consommateur ITI-10 : notification du rapprochement d'identités à un système abonné
Spécifications générales	• ITI TF : http://ihe.net/Technical_Frameworks/#IT Vol. 1 - Section 5 • Vol. 2 - Sections 3.8, 3.9, 3.10
Standards	- HL7 Version 2.3.1 - Chapters 2,3 - HL7 Version 2.5 - Chapters 2,3,5

Production, diffusion, partage de documents médicaux	
Profil IHE :	**« *Cross-enterprise Document Sharing* » (XDS-b)**
Objet :	Partage de documents médicaux au sein d'une communauté médicale
Statut :	Final text : Spécification stable
Résumé :	http://wiki.ihe.net/index.php?title=Cross-Enterprise_Document_Sharing
Extension française	Volet « *Partage de documents de santé* » du CI-SIS de l'ASIP
Transactions :	ITI-41 : Alimentation de l'infrastructure de partage ITI-42 : Indexation des documents stockés dans l'infrastructure de partage (stockage des métadonnées dans le registre d'index) ITI-18 : Interrogation du registre d'index ITI-43 : Consultation et récupération des documents consultés dans l'infrastructure de partage.
Spécifications générales	ITI TF : http://ihe.net/Technical_Frameworks/#IT Volume 1 – section 10 : Description du profil en termes utilisateur Volume 2b – section 3.41 : alimentation de l'infrastructure de partage Section 3.43 : accès aux documents stockés dans l'infrastructure de partage
Standards	- ebMS OASIS/ebXML Messaging Services Specifications v3.0 - ebRIM OASIS/ebXML Registry Information Model v3.0 - ebRS OASIS/ebXML Registry Services Specifications v3.0 - HTTP HyperText Transfer Protocol HTTP/1.1 (IETF RFC2616) - ISO/IEC 9075 Database Language SQL - HL7 Version 2.5 - HL7 Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration

6.3.2.2 Mise en commun de l'information médicale au niveau d'un DPI mutualisé

Dans le contexte de ce cas d'usage, les 3 établissements utilisent le même DPI multi juridique mutualisé, un SAE mutualisé et éventuellement un service de rapprochement des identités du patient (PIX) dans le cas où les 3 établissements n'implémentent pas la même solution administrative.

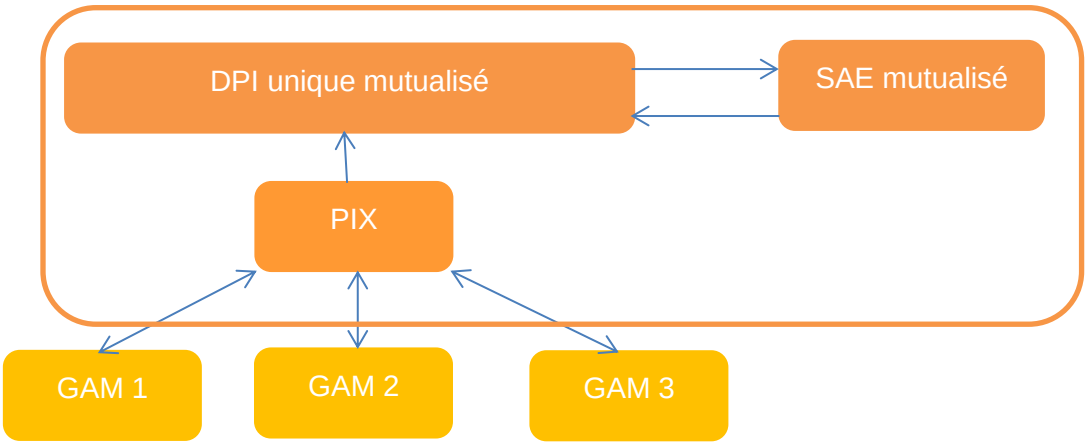


Figure 6.3.2.2-1 : DPI mutualisé

Cette situation n'est pas différente, en termes de flux d'information, de celle qui consiste à interfacer un DPI intra établissement avec un SAE (cf cas d'usage chapitre 6.4 ci-dessous). L'avantage est de résoudre les problèmes d'interopérabilité qui pourraient survenir dans le cas d'usage précédent entre les différents DPI. Le DPI multi-établissements ainsi que le SAE mutualisé doivent supporter une gestion des droits d'accès adaptée au cas d'usage. En particulier, le GHT définit des filières de soins qui font intervenir différents services médicaux appartenant aux différents établissements du GHT. Ainsi l'équipe médicale qui prend en charge le patient au sein de la filière est constituée de professionnels de santé appartenant à l'un ou l'autre des établissements du GHT. Cette notion d'équipe médicale pluri disciplinaire doit être formalisée au niveau du SI et associée à l'information médicale pour permettre en suite de gérer correctement l'accès à l'information.

6.4 Description des échanges entre le SIH et le SAE

L'ensemble des cas d'usage présentés précédemment mettent en jeu des échanges entre un composant du SIH (DPI, GED, entrepôt de données) et le Service d'Archivage Électronique (SAE) interne à l'établissement ou externalisé chez un tiers archiveur.

Recommandé par le Référentiel Général d'Interopérabilité[35], le standard SEDA (Standard d'Echange pour les Données d'Archivage), maintenu par le SIAF, « apporte un cadre normatif pour les différents échanges d'informations (données comme métadonnées) entre le Service d'archives et ses partenaires. Les échanges entre plusieurs services en charge des archives (services intégrés dans les organisations, services publics d'archives, prestataires d'archivage) sont également concernés.

Le standard définit des diagrammes d'activités et des modèles de données selon le formalisme UML. Les échanges se traduisent par des messages formalisés par des schémas XML ».
Seuls les grands principes de ce standard sont présentés ici. Le lecteur pourra consulter directement la spécification pour plus d'informations.[36] Il est à noter que le SEDA décrit des situations d'archivage qui peuvent aller jusqu'au recours à un SAE externalisé ou à vocation historique. Toutes les fonctionnalités ne sont pas forcément utiles dans le cadre d'un SAE implanté à l'intérieur même d'un établissement de santé pour la conservation de ses archives électroniques ayant encore une utilité administrative.

6.4.1 Description des échanges

Ce standard décrit cinq principaux cas d'usage qui interviennent entre le SAE et ses partenaires : Transférer, Communiquer, Modifier, Éliminer et Restituer.

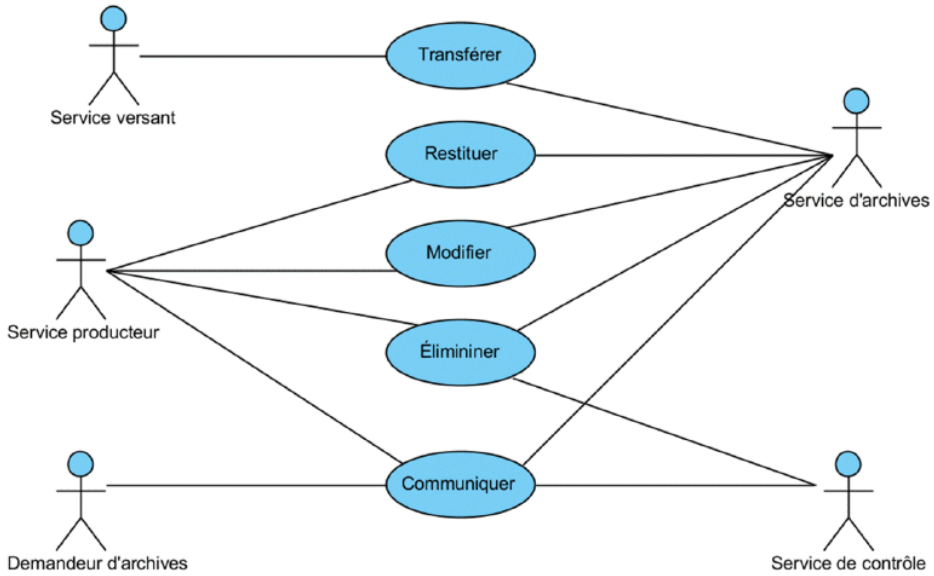


Figure 6.4.1-1 : Les cinq cas d'usage décrits par le standard SEDA

[35] http://references.modernisation.gouv.fr/interoperabilite.

[36] Voir la documentation sur le site spécialisé du Service interministériel des Archives de France : http://www.archivesdefrance.culture.gouv.fr/seda/

6.4.1.1 Transfert d'archives

Le transfert d'archives correspond à la « transmission d'informations par un Service versant à un Service d'archives en vue de lui en confier la conservation. Le Transfert peut être précédé d'une Demande de transfert pour accord. »
La figure 6.4.1.1-1 représente le workflow lié à la fonctionnalité de transfert des pièces d'information.

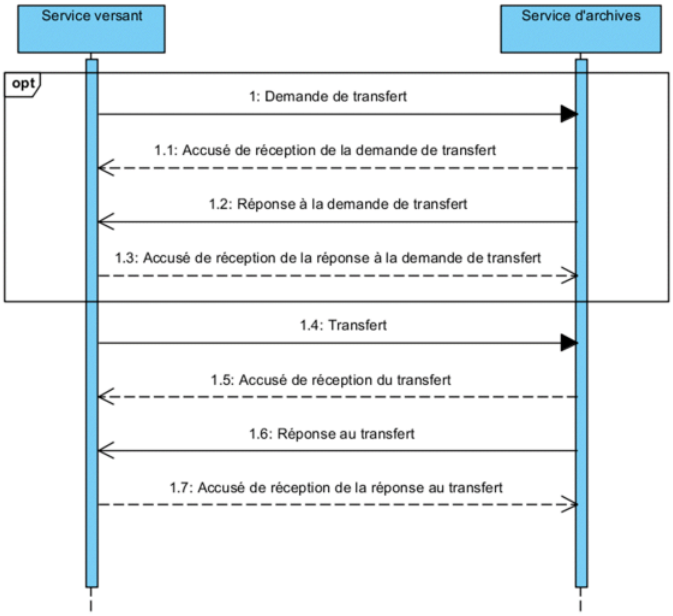


Figure 6.4.1.1-1 : Transfert des paquets d'information

6.4.1.2 Communication d'archives

La communication d'archives correspond à la « transmission d'informations par un Service d'archives à un Demandeur, avec l'autorisation, le cas échéant, du Service producteur et du Service de contrôle compétent». Du point de vue archivistique, on parle de consultation des archives, fonctionnalité complètement différente de la notion de restitution des archives (cf 6.4.1.4).

La communication d'une information (donnée et/ou métadonnée) n'est possible que :

- si l'information est déclarée librement communicable par une règle explicite,
- si l'information est devenue librement communicable en raison du dépassement du délai de la règle de communicabilité,
- si le demandeur est le producteur de l'information, sauf pour les données à caractère personnel au-delà de la durée de conservation pour la finalité initiale (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés),
- dans le cas d'une réquisition judiciaire,
- si le service de contrôle compétent a donné une autorisation de communication (dérogation) de cette information au demandeur.

Ces règles retranscrivent en termes de fonctionnalités techniques les principes juridiques de communication des archives publiques et notamment les principes énoncés aux articles L213-1 à 3 du Code du patrimoine.
La figure 6.4.1.2-1 représente le workflow lié à la fonctionnalité de communication des pièces d'information.

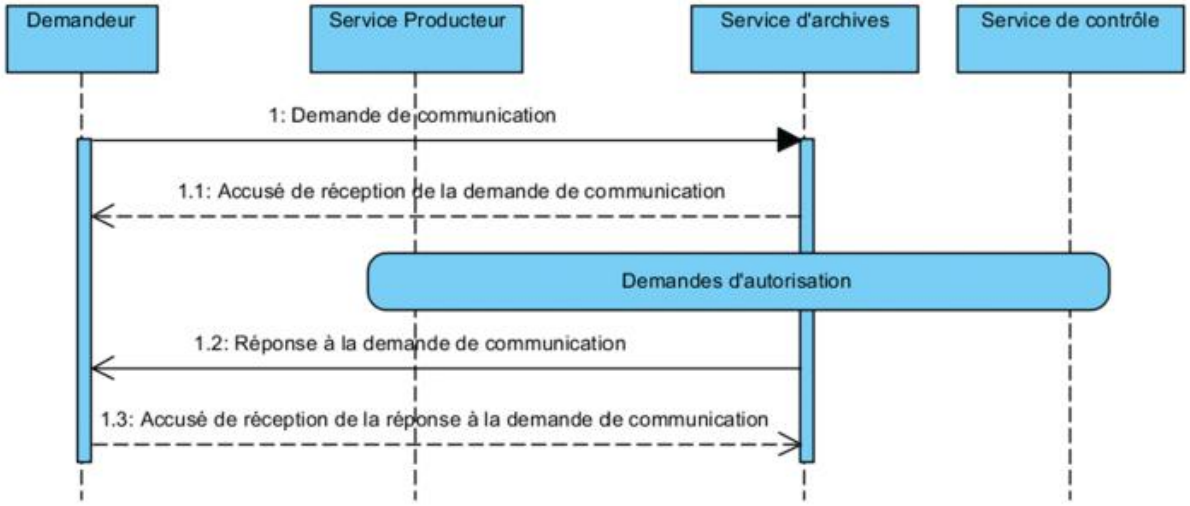


Figure 6.4.1.2-1: Communication d'archives

Pour une consultation immédiate des archives d'un Service producteur, les prérequis sont les suivants :

- être utilisateur du Service producteur correspondant,
- être utilisateur du Service Archives de l'acteur SEDA indiqué dans l'accord de versement référent.

Le cloisonnement des données par services producteurs est assuré sur le Système d'Archivage Electronique par l'accord de service. Celui-ci associe contractuellement, l'Autorité d'archivage (AA) se trouvant modifiée par le transfert d'archives, un Service versant (SV) et un Service Archives (SA), en référence à un profil d'archives décrit dans le cas de flux définis, ou sans profil dans le cas d'un versement ponctuel spécifique. Le Service producteur (SP) est quant à lui relié aux accords de service *via* des contrats de versements et n'aura donc un accès direct qu'à ses propres archives, quand bien même l'accord de service serait mutualisé avec d'autres services producteurs. Le plan de rangement informatique des données pourrait être du type : <…\SA#\Accord-Versement#\SP#\Archive#\...>.

Dans le cas d'un SAE implémenté au sein d'un établissement, il semble complexe et inutile de faire de chaque pôle de soin ou service d'un établissement de santé un service producteur spécifique. Tout membre de l'équipe de soin doit pouvoir consulter l'intégralité des dossiers des patients.

Afin néanmoins de limiter les consultations inutiles motivées par une curiosité qui ne serait pas professionnelle, des contrôles aléatoires des traces de consultation sont recommandés, en parallèle d'une communication adéquate auprès du personnel.

6.4.1.3 Notification de modification d'archives

Il s'agit de la « notification par un Service d'archives à un Service producteur des modifications apportées sur les informations transférées. Ces modifications peuvent être nécessaires afin d'assurer une bonne conservation des informations (par exemple conversion de format ou ajout, correction, mise à jour des métadonnées) ».

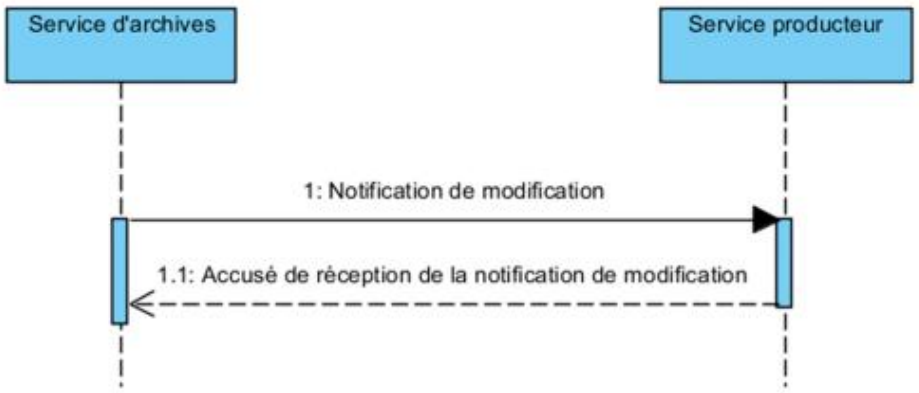


Figure 6.4.1.3-1 : Notification des modifications apportées aux archives

6.4.1.4 Restitution d'archives

La restitution d'archives correspond à la « transmission d'informations par un Service d'Archives à un Service Producteur en vue de lui restituer la responsabilité de la conservation ». Cette restitution peut s'effectuer soit à la demande du Service Producteur, soit à la demande du service de tiers-archivage, par exemple lors de la fin du contrat.

Plusieurs cas peuvent entraîner une procédure de restitution d'archives :

- Restitution intégrale liée à une cessation de contrat, à l'initiative de l'établissement (échéance contractuelle, cessation anticipée…),
- Restitution intégrale liée à une cessation de contrat, à l'initiative du tiers-archiveur (défaut de paiement du client, liquidation du prestataire…),
- Restitution partielle, dans le cadre de contentieux juridiques et de requêtes judiciaires (à ne pas confondre avec la simple communication de pièces à l'institution judiciaire),
- Réactivation d'un dossier archivé,
- Archive mal formée au niveau archivistique et probant, à la responsabilité du Service producteur, indépendamment du parfait fonctionnement du SAE.

Dans tous les cas, il faut restituer toutes les versions des documents. En électronique, cela signifie, avec l'ensemble du contexte (ex. signature, métadonnées, journaux...) :

- le format original,
- le dernier format de conversion,
- le format de conversion précédente (n-1).

A la différence d'une simple communication, le Service Archives, une fois la restitution effectuée, ne conserve pas les données concernées puisque la responsabilité de ces archives est transférée au Service Producteur.

Pour le bon déroulement de l'étape de validation, il faut impérativement la constitution :

- d'un circuit de traitement des demandes de restitution,
- d'un circuit de traitement des accusés de restitution d'archives.

La procédure se déroule en cinq étapes :

- Demande de restitution,

- Validation de la demande de restitution,
- Restitution des archives au Service producteur,
- Acquittement de la restitution par le Service producteur,
- Destruction par le Service Archives des archives restituées au Service Producteur.

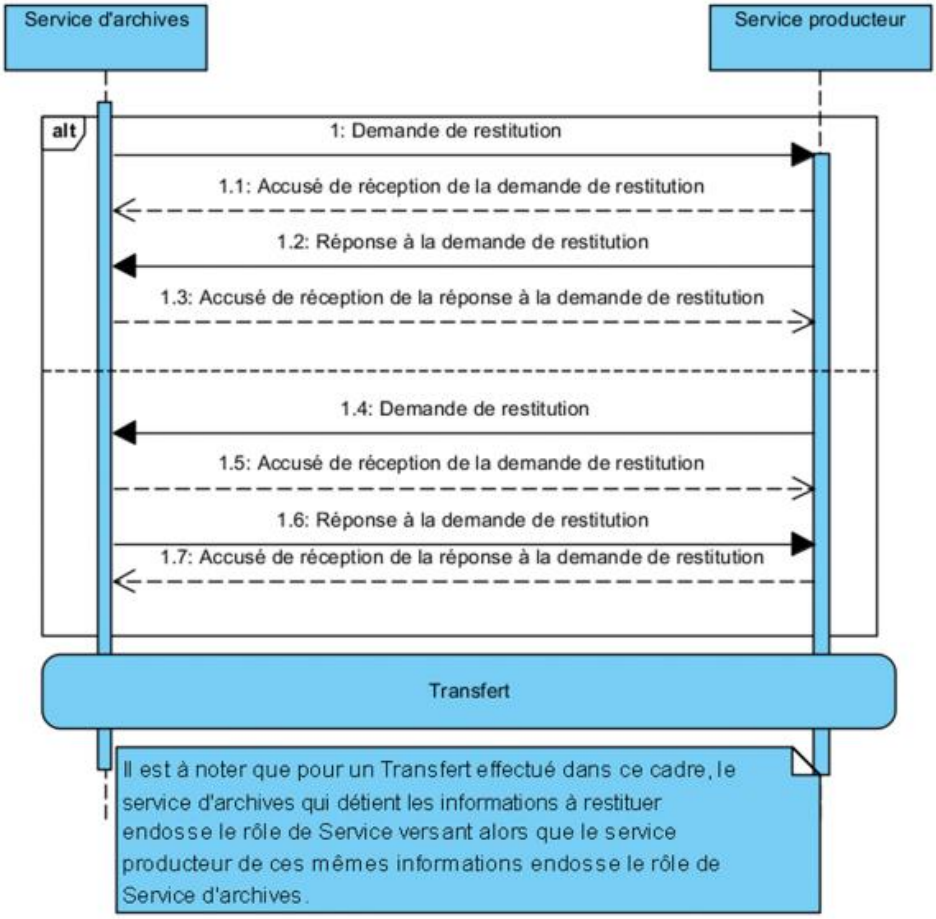


Figure 6.4.1.4-1 : Restitution d'archives

Une fois les archives restituées détruites par le Service Archives, celui-ci se trouve dégagé de toute responsabilité concernant la conservation de ces données, n'étant plus dès lors autorité d'archivage, responsabilité revenue au Service Producteur.

6.4.1.5 Elimination d'archives

L'élimination d'archives correspond à la « notification par un Service d'archives à un Service Producteur de la suppression d'informations. L'élimination peut être précédée, le cas échéant, d'une Demande d'autorisation d'élimination au Service de contrôle et d'une Demande d'autorisation au Service Producteur.

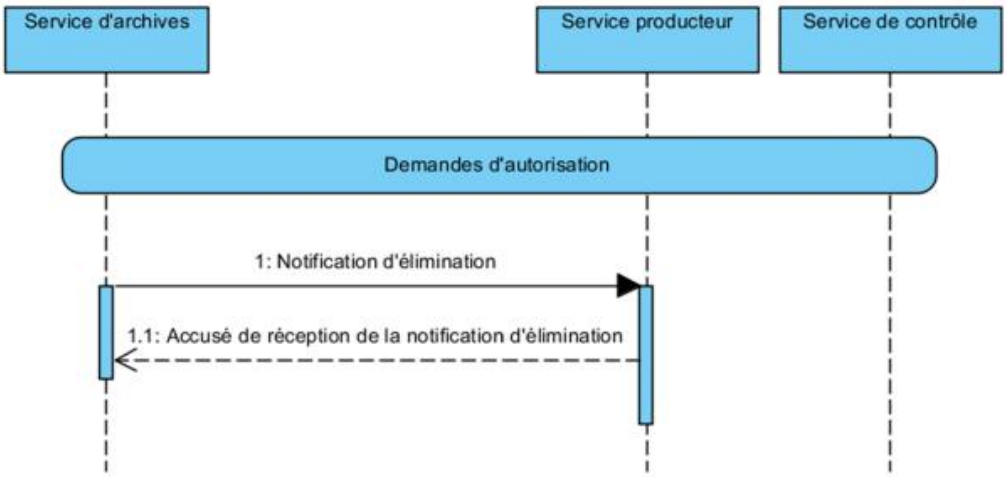


Figure 6.4.1.5-1 : Elimination d'archives

6.4.2 Implémentation des normes qui répondent au cas d'usage

L'ensemble des transactions d'échange entre le SIH et le SAE sont décrites en France par le standard SEDA 2.0 (standard maintenu par le SIAF).

Ce standard décrit à la fois :

- Les acteurs qui interviennent dans les échanges. Un acteur étant défini comme un ensemble cohérent de rôles.
- Les transactions d'échange entre les acteurs,
- Les objets-données échangés dans les transactions, intégrant les métadonnées techniques, et associés aux métadonnées descriptives et de gestion (très orientées archives publiques),
- Les messages échangés.

Les objets échangés sont décrits pour chaque transaction du standard.

La version 2.0 de SEDA, adaptée à la description et à l'échange d'archives publiques dans le contexte français, est une spécialisation de la norme NF Z44-022 (MEDONA). Le périmètre de SEDA 2.0 a été élargi avec la prise en compte de MEDONA.

Contrairement au SEDA 1.0, MEDONA ne définit plus explicitement le modèle de description des paquets d'objets-données et notamment le modèle des métadonnées associées à ces objets échangés. Le modèle de description devient libre et chaque secteur d'intervention peut choisir son propre référentiel.

Nous considérons qu'actuellement la plupart des éditeurs de SAE vont migrer leur solution de SEDA 1 vers SEDA 2.0. En conséquence, ces solutions seront conformes à la norme française MEDONA, étant donné que SEDA 2.0 est une spécialisation de cette dernière.

D'autre part, la norme NF Z44-022 (MEDONA) est en cours de normalisation à l'ISO sous le nom de Data Exchange Protocol for Interoperability and Preservation (DEPIP) et à ce titre deviendra une norme internationale.

Le groupe de travail à l'origine de ce présent document a donc considéré qu'il était utile de faire une étude de comparaison de la norme MEDONA avec la norme CDA et les profils de la

famille IHE XDS associés, de façon à déterminer si ces éléments de comparaison permettaient :

- De répondre aux exigences de structuration de l'information archivée (exigences MEDONA et OAIS),
- D'implémenter les différentes catégories de métadonnées décrites dans MEDONA,
- D'implémenter l'ensemble des transactions décrites dans MEDONA.

Le chapitre 7 fait l'objet de cette étude.

7 Comparaison MEDONA avec XDS/CDA

L'intérêt de comparer la norme MEDONA avec CDA/XDS réside dans le fait de déterminer s'il est possible de réutiliser les métadonnées définies dans CDA et le profil IHE XDS présenté au chapitre 5 de ce présent document, pour formaliser le modèle des métadonnées MEDONA spécifique au domaine de la santé.

7.1 Comparaison des acteurs/transactions

MEDONA définit cinq types d'acteurs :

- Service d'Archives (Archival Agency) : entité destinataire du transfert et assurant la gestion des informations transférées par les Services versants destinées à être communiquées aux Demandeurs dans le respect des conditions légales, règlementaires ou contractuelles.
- Service Versant (Transferring Agency) : entité qui transfère des archives dont il est responsable à un Service d'Archives, qu'il les ait produites ou qu'il les ait héritées d'un Service Producteur dont il a repris les attributions.
- Service Producteur (Originating Agency) : entité qui a produit les informations, c'est-à-dire qui les a créées ou reçues dans le cadre de son activité.
- Service de Contrôle (Control Authority) : entité qui, le cas échéant, autorise ou non la Communication et l'Elimination.
- Demandeur (Requester) : entité qui désigne toute personne physique ou morale qui souhaite consulter les informations conservées par le Service d'archives dans le respect des conditions légales, réglementaires ou contractuelles en vigueur.

A l'ensemble de ces acteurs, le standard SEDA 2.0 ajoute l'acteur Opérateur :

- Opérateur de versement : entité chargée des opérations techniques de transfert des archives demandées par un Service versant, mais qui n'est ni le Service producteur ni le Service versant (par exemple : une DSI ou un tiers-archiveur).

Le tableau suivant présente la correspondance entre les acteurs MEDONA/SEDA et les acteurs définis dans l'infrastructure XDS. Le nom des acteurs XDS est libellé en anglais et le libellé francisé, tel qu'il est défini dans le CI_SIS et présenté au chapitre 5.2 du présent document, est précisé entre parenthèses et en italique. Le tableau fait apparaître un nouvel acteur IHE non défini dans XDS : le « Créateur de contenu » (*Content Creator*) définit dans le profil IHE XDS-MS (Cross Enterprise Sharing Medical Summuries).

Acteur IHE	Profil	Rôle de l'acteur dans XDS	Acteur MEDONA
Content Creator (*Créateur Contenu*)	XDS-MS	Acteur qui a produit l'information (création du ou des documents)	Service Producteur
Patient Identiy Source	XDS	Alimentation de l'infrastructure en identités patient	N/A
Patient Identiy Source	XDS	Idem (techno HL7v3)	N/A
Document Source *(Producteur)*	XDS	Constitution et transfert du paquet d'informations à verser vers l'infrastructure XDS	Service Versant
Document Repository *(Entrepôt)*	XDS	Acteur destinataire du paquet d'information versé par le Document Source	Service d'Archives
		Stockage des documents au niveau de l'Entrepôt et transmission des métadonnées au Registre	
		Communication des documents depuis l'infrastructure vers un acteur consommateur (Document Consumer)	
Document Registry *(Registre d'index)*	XDS	Enregistrement des métadonnées associées aux documents stockés dans l'Entrepôt	Service d'Archives
		Répond aux interrogations du Consommateur, envoi des métadonnées de documents correspondant aux critères de recherche	
Document Consumer *(Consommateur)*	XDS	Interroge le Registre pour obtenir les métadonnées correspondantes aux critères de recherche	Demandeur
		Récupère, à partir des métadonnées obtenues, les documents auprès du ou des Entrepôts qui stockent ces documents	
Document Administrator *(Administrateur)*	XDS	Gère la mise à jour des métadonnées dans le Registre	Service d'Archives
N/A		Entité chargée des opérations techniques de transfert	Opérateur de versement

La figure 7.1-1 représente les acteurs (représentés en jaune) qui échangent avec le service d'archivage, ainsi que les fonctionnalités (notées Fx sur le schéma) d'un service d'Archivage Electronique.

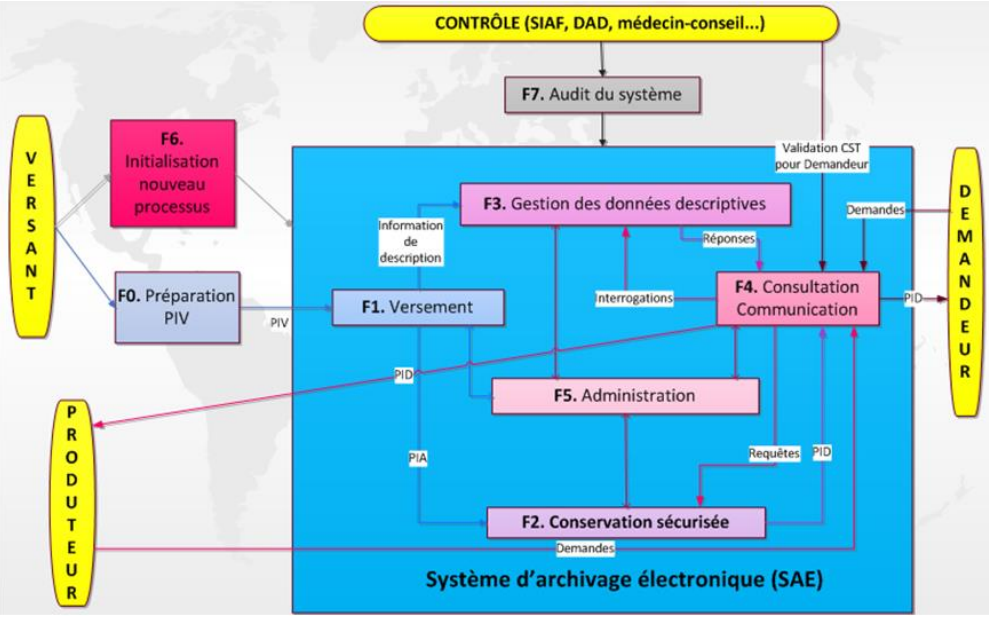


Figure7.1-1: Fonctionnalités d'un SAE et Acteurs qui interagissent avec le SAE.

La même figure ci-dessous présente d'une façon graphique le mapping entre les acteurs ci-dessus et les acteurs IHE XDS.

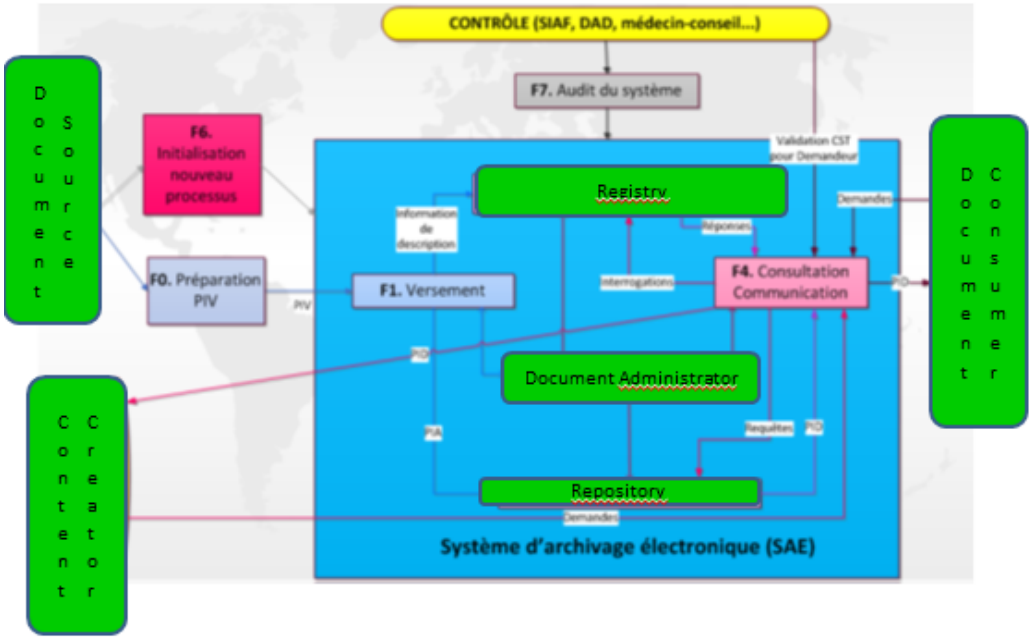


Figure7.1-2: Correspondance avec les acteurs IHE XDS

Le tableau suivant présente la correspondance entre les transactions/messages MEDONA et les transactions/messages décrits dans IHE XDS, IHE DSUB[37].

[37] DSUB (Document Metadata Subscription) : http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DSUB.pdf

Libellé transaction MEDONA	Transaction/message MEDONA	Profil IHE	Transaction/message IHE
Demande de transfert d'archives	ArchiveTransfertRequest	N/A	N/A
Réponse à une demande de transfert d'archives	ArchiveRestitutionRequestReply	N/A	N/A
Transfert d'archives	ArchiveTransfer	XDS	ITI-41 : message Provide&Register Document Set-b Request
Réponse au transfert d'archives	ArchiveTransferReply	XDS	ITI-41 : message Provide&Register Document Set-b Response
Demande de communication d'archives	ArchiveDeliveryRequest	XDS	ITI-43 : message Retrieve Document Set Request
Réponse à la demande de communication d'archives	ArchiveDeliveryRequestReply	XDS	ITI-43 : message Retrieve Document Set Response
Demande de restitution des archives	ArchiveRestitutionRequest	XDS étendu	ITI-43 spécifique : message Retrieve Document Set RequestAndDelete
Réponse à la demande de restitution des archives	ArchiveRestitutionRequestReply	XDS étendu	ITI-43 spécifique : message Retrieve Document Set ResponseAndDelete
Demande d'autorisation au Service Contrôle	AuthorizationControlAuthorityRequest	N/A	N/A
Réponse à la demande d'autorisation au Service Contrôle	AuthorizationControlAuthorityRequestReply	N/A	N/A
Demande d'autorisation au Service Producteur	AuthorizationOriginatingAgencyRequest	N/A	N/A
Réponse à la demande d'autorisation au Service Producteur	AuthorizationOriginationgAgencyRequestReply	N/A	N/A

Notification de modification d'archives	ArchiveModificationNotification	DSUB	ITI-53 : message NotificationMessage
Notification d'élimination d'archives	ArchiveDestructionNotification	DSUB	ITI-53 : message NotificationMessage

7.2 Comparaison de la représentation des objets contenus dans le lot de soumission XDS et les objets manipulés dans un message MEDONA

Une transaction MEDONA donne lieu à l'échange d'un message entre les acteurs concernés par cette transaction. Le message résultant est composé :

- des métadonnées de transport : identification du message, date d'émission, identification des acteurs qui s'échangent le message, etc.
- des paquets d'objets-données, eux-mêmes constitués
    - d'objets-données de type numérique et/ou d'objets-données de type physique. Dans le cas de ce livre blanc, seuls les objets-données de type numérique nous intéressent.
    - Sur chacun de ces objets-données sont attachées des métadonnées techniques (format, empreinte, taille, statut de la signature, éventuellement un lien vers l'objet binaire)
- de métadonnées descriptives des unités d'archives. Les unités d'archives font référence à un objet binaire ou à un objet physique.
- de métadonnées de gestion applicables à la transaction (profil d'archivage, niveau de service, règle d'accessibilité et la règle de calcul du sort final des documents).

La figure 7.2-1 représente graphiquement par exemple la structure du message Archive-Transfer.

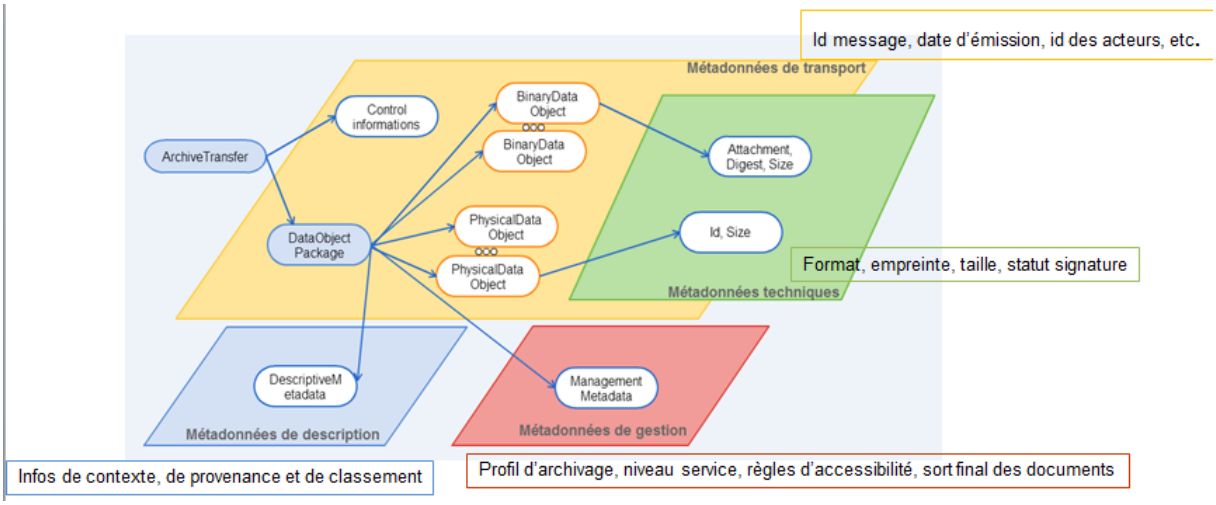


Figure7.2-1: structure du message ArchiveTransfer

Le tableau suivant présente la correspondance entre les objets MEDONA présentés sur la figure 7.2-1 et les objets manipulés dans le profil IHE XDS.

Concept MEDONA	**Commentaire**	**Concept XDS**
DataObjectPackage	Représente un ensemble d'objets-données associé à ses métadonnées (descriptives et de gestion)	Submission Set (lot de soumission)
BinaryDataObject	Un objet-donnée binaire peut contenir des liens avec d'autres objets-données du même package	XDS Document. Les liens entre documents sont décrits par des relations RelationShip typées (RPLC, XRFM, SIGN, etc.). la relation est décrite par les attributs sourceObject, targetObject et associationType.
Métadonnées techniques	format, empreinte, taille, statut de la signature	Informations portées au niveau XDS DocumentEntry (fiche de document)
Métadonnées de gestion	profil d'archivage, niveau de service, règle d'accessibilité et la règle de calcul du sort final des documents	N/A
Métadonnées descriptives	Informations de contexte, de provenance, de classement. Le modèle de description est	Métadonnées associées au lot de soumission

	libre dans MEDONA	
Version des référentiels utilisés	Versions des listes de codes utilisées dans les messages (1)	Listes de codes définis dans le profil IHE XDS
Signature	Peut être ajoutée à tous les messages MEDONA	Signature associée au lot de soumission (document de signature lié au lot de soumission par une association de type SIGN)

(1) liste des codes de sort final, codes de motivation de demandes d'autorisation, codes d'encodage des fichiers, codes de formats de fichiers, codes des algorithmes de calcul d'empreintes, codes des relations entre fichiers, codes retour utilisés dans les messages de réponse.

Il est à noter que les métadonnées de gestion, qui gèrent notamment la règle de calcul du sort final des documents, sont rattachées au DataObjectPackage dans MEDONA (l'équivalent du lot de soumission dans XDS). Dans le domaine de la santé, cette règle ne peut pas être définie au niveau du DataObjectPackage ou du lot de soumission. En effet, la DUA est fixée règlementairement en fonction du type de document, or un lot de soumission XDS peut contenir différents types de documents.

Dans le standard SEDA 2.0, les métadonnées de gestion sont également explicitées au niveau des métadonnées descriptives. C'est dans cette direction que le groupe de travail InteropSanté s'est orienté en se basant sur la possibilité, pour un secteur d'activités donné, de définir son propre modèle de métadonnées descriptives. Nous n'avons pas souhaité réutiliser le bloc de métadonnées descriptives défini dans SEDA 2.0, d'une part car il est très orienté vers le contexte particulier de la gestion des archives publiques définitives et, d'autre part, parce que ce modèle est moins adapté au champ médical que le modèle de métadonnées XDS.

Parmi ces métadonnées XDS lesquelles faut-il garder ? La réponse dépend sans doute de l'usage dont il sera fait de ces métadonnées ensuite. Elles devraient servir notamment:

- à conserver les caractéristiques des documents au niveau des archives intermédiaires permettant par exemple la destruction automatique des documents du SAE qui ont atteint la DUA (par croisement d'information entre le profil d'archivage et le type du document),

- à faire des recherches sur les documents d'archives intermédiaires stockés dans les SAE,
- à sélectionner les informations de santé à archiver de façon définitive (pour raisons patrimoniales et historiques) et à conserver ces métadonnées lors de l'archivage définitif des informations. Par exemple, les archivistes vont avoir envie de sélectionner les archives :
    - par secteur médical. Ex: un CHU est reconnu pour ses compétences en neurologie ou dans les greffes. Dans ce cas, il peut être très intéressant de conserver les dossiers qui en traitent.
    - par médecin. Ex: un chirurgien de renom est affecté dans un service et on voudrait récupérer les dossiers qu'il a suivis.

- par "affaire ou actualité". Ex: il serait intéressant de conserver les dossiers de victimes d'une erreur médicale connue.

Parmi les métadonnées XDS à retenir pour constituer les métadonnées descriptives, la métadonnée patientId est fondamentale puisqu'elle permet de relier les versements successifs de documents médicaux au SAE pour un patient donné.

7.3 Conclusion

La conclusion de la réflexion conduite sur les métadonnées à reporter au niveau des métadonnées descriptives MEDONA nous laisse à penser qu'il faudrait garder l'ensemble des métadonnées décrites dans XDS (métadonnées du lot de soumission, du classeur, du document et des associations entre ces objets).

Une étude est en cours de façon à déterminer si l'ensemble des métadonnées XDS doit être repris au niveau des métadonnées descriptives. Dans ce cas, il serait intéressant de récupérer le schéma complet des métadonnées XDS pour l'intégrer dans le schéma MEDONA.

Une comparaison détaillée des messages MEDONA et des éléments composant ces messages avec les messages et objets XDS est fournie en annexe 2 de ce présent document.

Le lecteur pourra se reporter à cette annexe pour plus de détails.

Cette comparaison permet d'envisager un traducteur des transactions XDS en transactions MEDONA et inversement. Ce traducteur serait a priori positionné du côté du SAE pour deux raisons :

- Le traducteur au niveau du SAE devra vérifier lors du versement l'empreinte du document (BinaryDataObject/SignatureStatus) :
  - Si l'empreinte est vérifiée, le versement est accepté
  - Si l'empreinte n'est pas vérifiée, le versement est refusé.
- Le traducteur devra récupérer la métadonnée TransferringAgency (Service versant) soit
  - via le certificat utilisé par la mise en œuvre du protocole TLS pour la transaction ITI-41 (Provide&Register Document Set-b),
  - ou via l'assertion SAML du message SOAP contenu dans la transaction ITI-41 (Provide&Register Document Set-b).

Du point de vue de l'architecture fonctionnelle, il semble préférable que ce traducteur soit positionné en entrée du SAE intermédiaire. Cette solution permet de disposer dans le SAE intermédiaire d'une version des documents pleinement interopérable avec le SAE définitif, mais également avec d'autres SAE intermédiaires en cas de renouvellement de la solution d'archivage de l'établissement de santé. On crée ainsi pour un SIH, un ensemble de documents vitaux conservés dans un format-pivot favorisant la réversibilité des données entre les SAE intermédiaires.

8 Des évolutions à concrétiser

8.1 Des évolutions techniques

Concernant le profil IHE XDS :

- Les métadonnées de gestion définies dans MEDONA n'ont pas d'équivalent dans XDS :
    - Proposer une évolution des métadonnées du document XDS :
    - AppraisalRule : règle pour le calcul du sort final. Extension XDS à faire avec paramétrage par type de document pour préciser le sort final du document. Cette métadonnée est gérée dans MEDONA au niveau du paquet d'archive, elle devra être gérée au niveau de chaque document dans XDS. Elle est constituée des éléments suivants:
        - AppraisalCode : prévoir un nouveau ebRIM Slot.
        - Duration : prévoir un nouveau ebRIM Slot
            - Startdate : début DUA
            - EndDate : fin DUA
- Etudier la possibilité d'utiliser le nouveau profil IHE Enhanced Patient Privacy Consent pour gérer la métadonnée AccessRule une fois que ce profil est publié.

Concernant le profil IHE DRPT :

- Création d'une nouvelle métadonnée d'empreinte du document.

8.2 Des chantiers réglementaires à mener

L'urbanisation des SIH n'est pas qu'une question organisationnelle et technique. Au cours de ses travaux, le groupe de travail a identifié deux pistes de progrès réglementaires structurants qui nécessiteraient des évolutions pour sécuriser la dématérialisation des processus de soin dans les établissements de santé.

D'une part, dans le contexte de la dématérialisation, l'article R1112-2 du Code de la santé publique (CSP) devrait être revu. Cet article revêt une importance juridique particulière car il est actuellement utilisé par les établissements de santé pour savoir quels documents fournir au patient en cas de demande d'accès à son dossier. Les informations se trouvent en effet aujourd'hui éclatées au sein du SIH, ainsi qu'entre le DPI et le dossier papier.
Le groupe de travail attire l'attention des autorités réglementaires sur le rôle central que pourrait jouer cet article en matière d'urbanisation des systèmes d'information, en lien avec le déploiement de solutions d'archivage électronique dans les établissements de santé. Il pourrait effectivement définir la liste des documents essentiels attestant de chaque étape de la prise en charge du patient. Il permettrait aussi à l'établissement de disposer de toutes les informations nécessaires à sa défense en cas de contentieux, mais aussi au suivi médical du patient sur le long terme et ce malgré les inévitables changements des SI de production. Ce travail reste néanmoins à mener avec des juristes du secteur de la santé et des personnels soignants.
Retranscrite en termes techniques, une telle liste constituerait le noyau des documents à conserver dans un SAE pendant toute la durée de conservation du dossier médical, mentionnée à l'article R1112-7 du CSP.

D'autre part, le CSP est parsemé de diverses mentions de signatures de documents[38]. Dans le contexte papier, la simplicité de la signature manuscrite n'a jamais amené les professionnels à s'interroger sur le sens de cet acte. Il revêt pourtant plusieurs significations : consentement quant à l'engagement inscrit dans l'acte, validation du contenu, simple visa attestant d'un processus…

Dans le monde numérique, les solutions qui permettent d'atteindre ses objectifs sont multiples et ont des coûts différents : adjonction automatique de métadonnées d'identification ou d'authentification forte, empreinte, signature électronique de différents niveaux, horodatage, cachet-serveur… Le CSP ne précise pas à quelle technologie il faut recourir pour remplir la condition de signature de tel ou tel document dans l'univers numérique.

Or la jurisprudence confirme qu'il existe un risque quant aux différents choix faits par les établissements de santé. Dans une décision du 17 juillet 2013, le Conseil d'État, considérant que les comptes rendus d'analyse biologique doivent être signés d'après l'article R6211-21 du CSP, a confirmé une décision d'appel punissant un laboratoire qui avait numérisé ces comptes rendus signés de façon manuscrite avant intégration dans un système d'information. Les juges administratifs suprêmes se sont appuyés sur l'article 1316-4 (futur article 1367) du Code civil pour affirmer que, s'il doit y avoir signature d'un document, celle-ci doit respecter les exigences de cet article dans le contexte électronique[39]. C'est là une vision extensive du champ d'application du Code civil qui mériterait d'être délimité clairement dans le secteur de la santé.

En outre, un problème particulier est posé par le recueil du consentement du patient, source grandissante de contentieux. Compte-tenu de l'absence en France de carte d'identité électronique dotée d'un certificat de signature électronique et compte-tenu de toute façon de la diversité des patients, il est impossible d'exiger de chaque patient de pouvoir signer électroniquement des documents électroniques attestant de son consentement. Diverses solutions pourraient être importées dans le secteur de la santé pour résoudre ce problème (numérisation fiable d'un document papier signé de façon manuscrite, certificat-minute utilisé dans le secteur bancaire, signature numérique sur un terminal sécurisé comme celle utilisée par les forces de l'ordre de la cadre de la chaîne contraventionnelle dématérialisée…). Cependant, toutes ces solutions ne sont pas aujourd'hui universellement reconnues par le droit comme la signature électronique : un choix clair dans le CSP est nécessaire.

La dématérialisation dans le secteur de la santé serait donc grandement facilitée et sécurisée si les autorités réglementaires pouvaient définir les exigences minimales à appliquer pour chaque mention de signature. Sans transiger avec la sécurité de systèmes d'information, un tel travail devrait profiter de l'expérience acquise dans le domaine de la dématérialisation pour définir des solutions réalistes, déployables à grande échelle et correspondant aux usages des professionnels de santé[40].

---

[38] A titre indicatif et non-exhaustif, on peut citer les articles L 1131-1, R 1112-3 et 58, R 1131-19 et 20, R 1211-19, R 1232-3, R 2132-11, R 4127-76, R 4311-8 et 14, R 4312-29, R6211-21 et 44, D5134-9 du Code de la santé publique.

[39] Voir le jugement de la Cour d'appel de Fort-de-France n°12/00311 du 14 décembre 2012 [en ligne : https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000026869735] et la décision du Conseil d'État n° 351931 du 17 juillet 2013 [en ligne : http://legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000027724363].

[40] Un exemple récent montre la voie : le décret n° 2015-1263 du 9 octobre 2015 autorisant la création de traitements de données à caractère personnel pour la mise en œuvre des actes de télémédecine issus des expérimentations fondées sur l'article 36 de la loi n° 2013-1203 du 23 décembre 2013 de financement de la sécurité sociale pour 2014. Son article 7 intro-

9 Conclusion

Par ce livre blanc, le groupe de travail Interop'Santé a permis de présenter les grandes lignes de l'implémentation technique des principes de l'archivage électronique dans le contexte particulier du système d'information hospitalier.

Le groupe de travail est conscient que les cas d'usage décrivent une organisation-cible du SIH qui ne peut être concrétisée en une seule étape. Il s'agit d'un objectif vers lequel tendre sur le long terme.

Néanmoins, le livre blanc montre comment cette organisation peut d'ores et déjà s'appuyer sur un corpus normatif mûr :

1. Les normes et standards IHE permettent une structuration des paquets de documents médicaux conformes au modèle OAIS et l'interopérabilité des échanges.
2. Les référentiels de l'ASIP, notamment ceux d'imputabilité et d'authentification, aident à constituer l'intégrité et l'authenticité des documents électroniques.
3. Les normes d'archivage électronique garantissent, via l'usage d'un SAE conforme à l'état de l'art, la pérennité de ces propriétés.

Avant même la mise en œuvre d'un SAE, ce livre blanc fait ressortir la nécessité impérieuse pour les établissements de santé de commencer

1. par identifier les données indispensables à la traçabilité de leurs activités et à la défense de leurs droits ;
2. par s'assurer de pouvoir rendre ces données facilement exportables hors du SIH pour garantir leur pérennité. Les normes et standards IHE complétées par la norme MEDONA fournissent des règles de structuration des métadonnées à même de rendre cet objectif réalisable.

La comparaison entre les normes XDS et MEDONA montre la proximité des technologies utilisées par les archivistes et les informaticiens hospitaliers. Sur le fondement de l'annexe 2 de ce livre blanc, un travail prometteur reste à mener pour garantir l'exploitation des riches métadonnées du profil IHE-XDS au sein des SAE à vocation historique.

Devant l'importance des chantiers à mener qui découlent de ces conclusions, la mutualisation induite par la mise en œuvre des GHT pourrait être une occasion importante de rationaliser la gestion de l'information au sein des SIH, notamment par le déploiement de systèmes d'archivage électronique mutualisés.

Enfin, compte-tenu de l'intérêt des SAE pour la pérennisation des informations médicales, le groupe de travail tenait à donner aux établissements de santé des repères réglementaires et normatifs pour faciliter le choix de leur SAE. L'annexe 1 au livre blanc contient ces éléments.

duit une dérogation à la signature de la feuille de soins ou du bordereau établi pour la facturation des frais correspondants, quels qu'en soient le support et le mode de transmission.

10 Glossaire des abréviations

ANAP	Agence Nationale d'Appui à la Performance
ANSSI	Agence Nationale de sécurité des Systèmes d'Information *(www.ssi.gouv.fr)*
ARS	Agence Régionale de Santé
ASIP	Agence des Systèmes d'Information Partagés
ATNA	(ou IHE-ATNA) : Audit Trail and Node Authentication *(authentification forte des systèmes impliqués dans les échanges, centralisation des traces des échanges et des traces d'accès aux données de santé ou d'exportation de ces données)*
CCAM	Classification Commune des actes Médicaux publiée par la sécurité sociale
CDA	Clinical Document Architecture : norme HL7 internationale de structuration de documents cliniques persistants
CH	Centre Hospitalier
CHU	Centre Hospitalier Universitaire
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé
CSP	Code de la Santé Publique
CT	(ou IHE-CT) : Consistent Time *(synchronisation des horloges des systèmes impliqués dans les échanges)*
Demandeur	Désigne toute personne physique ou morale qui souhaite consulter les informations conservées par le Service d'archives dans le respect des conditions légales, réglementaires ou contractuelles en vigueur
DEPIP	Data Exchange Protocol for Interoperability and Preservation: normalization à international (ISO) de la norme française MEDONA
DIM	Département d'Information Médicale au sein des établissements
DMP	Dossier Médical Personnel
DPI	Dossier Patient Informatisé dans un établissement de santé.
DSI	Direction des Systèmes d'Information au sein des établissements
DSUB	(ou IHE-DSUB) : Document Metadata Subscription *(définition d'un système de notifications auquel n'importe quelle application peut s'abonner)*
DRPT	(ou IHE-DRPT) : Displayable Report (*spécifie les transactions supportant la création, la révision, la visualisation et la communication en intra hospitalier ou en extra hospitalier de documents cliniques issus des systèmes d'imagerie (radiologie, oncologie, obstétrique, gynécologie, gastroentérologie, ophtalmologie, orthopédie*)).
DSG	(ou IHE-DSG) : Digital Signature *(attachement d'un document Signature à un lot de soumission XDS)*
DUA	Durée d'Utilité Administrative
EHPAD	Etablissement Hospitalier pour Personnes Agées Dépendantes
GED	Gestion Electronique de Documents

GHT	Groupement Hospitalier de Territoire
HAS	Haute Autorité de Santé
HL7	HL7 est une organisation internationale à but non lucratif produisant des standards d'interopérabilité pour les échanges entre applications du domaine de la santé (*www.HL7.org*)
IHE	Integrating the Healthcare Enterprise : Organisation internationale produisant des profils de standards pour les échanges de données électroniques entre systèmes d'information du domaine de la santé (*www.IHE.net*)
MEDONA	Norme française de Modélisation des Echanges de Données pour l'Archivage : NF Z 44-022. Il s'agit d'un cadre normatif pour les différents échanges d'informations (données et métadonnées) entre le Service d'Archivage Electronique et ses partenaires.
MSS	Messagerie Sécurisée de Santé. Nom donné au système mis en place par l'ASIP permettant à tous les professionnels de santé d'échanger entre eux par email, rapidement et en toute sécurité, des données personnelles de santé de leurs patients dans le respect de la réglementation en vigueur.
NGAP	Nomenclature Générale des Actes Professionnels publié par la sécurité sociale.
OAIS	Open Archival Information System : Recommandation publiée par le Comité Consultatif pour les Systèmes de Données Spatiales (CCSDS), qui définit une base commune de termes et de concepts s'appliquant à un Système ouvert d'archivage d'information.
Opérateur de versement	Entité chargée des opérations techniques de transfert des archives demandées par un Service versant.
PGSSI-S	Référentiel de Politique Générale de Sécurité des Systèmes d'Information de Santé publié par l'ASIP-santé
PIX	Patient Identifier Cross Referencing *(rapprochement d'identifiants patrients inter-communautés)*
PMSI	Programme de Médicalisation du Système d'Information de santé
RGI	Référentiel Général d'Interopérabilité
RGS	Référentiel Général de Sécurité
SAE	Service d'Archivage Electronique
SEDA	Standard d'Echange de Données pour l'Archivage : Le standard d'échange de données pour l'archivage vise a faciliter l'interopérabilité entre le système d'information d'un service d'archives public et les systèmes d'informations de ses partenaires (producteurs, utilisateurs...). Il fournit un modelé pour les différentes transactions qui peuvent intervenir : transfert, communication, élimination…
SGL	Système de Gestion de Laboratoire : système d'information propre aux plateaux techniques de laboratoire
SI	Système d'Information
SIH	Système d'Information Hospitalier
SIAF	Service Interministériel des Archives de France
SSPI	Soins de Suite Postopératoires Immédiats

SSR	Soins de Suite et de Réadaptation
SA	Service Archive : entité destinataire du Transfert et assurant la gestion des informations transférées par les Services versants et destinées à être communiquées aux Demandeurs dans le respect des conditions légales, réglementaires ou contractuelles en vigueur
SAML	Security assertion markup language (SAML) est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité.
SC	Service de Contrôle : entité qui, le cas échéant, autorise ou non la Communication et l'Élimination
SOAP	(*Simple Object Access Protocol*), standard du W3C qui décrit la structuration d'un message permettant d'échanger des informations entre des clients et des fournisseurs de services web.
SP	Service Producteur : entité qui a produit les informations, c'est-à-dire qui les a créées ou reçues dans le cadre de son activité
SV	Service Versant : entité qui transfère un ensemble d'informations à un Service d'archives
UF	Unité Fonctionnelle : Structure élémentaire de prise en charge des malades par une équipe soignante ou médico-technique, identifiées par leur fonction et leur organisation (Art. L6146-1) ainsi que les structures médico-techniques qui leur sont associées.C'est la plus petite entité de l'hôpital à partir de laquelle la collecte d'informations peut être réalisée (guide méthodologique de comptabilité analytique).
XDM	(ou IHE-XDM) : Cross-Enterprise Document Media Interchange *(transfert de document de santé avec métadonnées via un média : clé USB, CD, pièce jointe à email)*
XDS-b	(ou IHE-XDS-b) : Cross Enterprise Document Sharing *(partage de documents et métadonnées associées via des entrepôts communs pilotés par un registre d'index)*
XDS-MS	(ou IHE-XDS-MS) : Medical Summaries *(Résumés de sortie et lettres d'entrée ou d'adressage partagés entre organisations de soins et/ou praticiens)*

11 Annexes

Réf.	Annexe
Annexe 1	Repères juridiques et normatifs pour le choix d'un SAE
Annexe 2	Tableau de correspondance XDS/MEDONA

11.1 Annexe 1 : repères juridiques et normatifs pour le choix d'un système d'archivage électronique (SAE)

Cette fiche se propose de présenter les normes et agréments qui organisent aujourd'hui l'offre d'archivage électronique. En revanche, cette fiche ne peut prétendre exposer les critères de choix des orientations stratégiques d'un projet de SAE, comme le fait de savoir s'il est intéressant ou non de recourir à l'externalisation.

1) Des repères réglementaires obligatoires en cas d'externalisation

Dès lors qu'il est décidé de confier la conservation des archives courantes et intermédiaires de l'établissement de santé à un tiers, la loi impose le recours à des services agréés. En matière de données de santé, il convient de distinguer deux agréments :

- l'agrément d'hébergement des données de santé délivré par le ministère de la Santé[41] vérifie les conditions de sécurité des systèmes d'information amenés à recevoir des données de santé.
- l'agrément de conservation externalisée des archives publiques sur support électronique délivré par le ministère de la Culture identifie des prestataires qui proposent des solutions complètes d'archivage à valeur probante, au sens de l'état de l'art fixé par l'arrêté du 4 décembre 2009 (normes ISO 14 721 « OAIS » et norme NF Z 42-013)[42].

Un établissement peut donc externaliser tout ou partie de son système d'information de santé suivant les scénarios suivants[43] :

1) Externalisation uniquement des infrastructures de stockage et/ou de l'infogérance avec installation, maintenance et administration du SAE par services informatiques de l'établissement :
    a. Obligation de recourir à un prestataire agréé « hébergeur de données de santé »,
    b. mais ce prestataire n'a pas à (et ne pourra pas) être agréé par le ministère de la Culture.
2) Externalisation de l'ensemble du SAE (le prestataire maintient et administre la solution logicielle pour le compte de l'établissement) : obligation de recourir à un prestataire agréé par le ministère de la Santé et par le ministère de la Culture lorsqu'il s'agit d'un établissement exerçant une mission de service public.

Ces agréments s'appliquent toujours à des services en production et jamais à des produits. Il n'existe aucun agrément réglementaire d'un logiciel d'archivage électronique.

[41] Il faut souligner que l'article 51-I-5°-c) de la loi n°2016-41 du 26 janvier 2016 relatif à la modernisation de notre système de santé habilite le Gouvernement à prendre par ordonnance des dispositions visant à remplacer cet agrément par une certification réalisé par un organisme accrédité.

[42] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021467028.

[43] La loi n°2016-41 du 26 janvier 2016 relatif à la modernisation de notre système de santé habilite le Gouvernement à légiférer par ordonnance pour améliorer l'articulation entre ces deux agréments. Ces règles sont donc amenées à être actualisée prochainement.

Pour en savoir plus :

- Sur l'agrément du ministère de la Santé : http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees. http://esante.gouv.fr/services/referentiels/securite/hebergement-faq
- Sur l'agrément du ministère de la Culture : http://www.archivesdefrance.culture.gouv.fr/gerer/gestion-externalisee-des-archives/.

2) Des repères facultatifs mais utiles pour cadrer un projet de SAE

Les prestataires et éditeurs de SAE peuvent choisir de se référer à certaines normes techniques d'application volontaire pour améliorer la confiance dans leur produits. Ces normes permettent également aux établissements de santé qui se lancent dans un projet de SAE de cadrer l'expression de leurs besoins pour établir le cahier des charges de la solution à acquérir.

De nombreuses normes existent dans le secteur de l'archivage électronique au niveau tant national qu'international. Pour cadrer un projet d'archivage électronique, les plus pertinentes sont les suivantes :

- Pour les fonctionnalités de conservation de l'intégrité des documents : NF Z 42-013 : *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*, 2009. En mars 2012, elle est devenue une norme internationale publiée sous la référence ISO 14641-1.
- Pour les fonctionnalités de pérennisation : ISO 14 721 : *Space data and information transfer systems - Open archival information system (OAIS) - Reference model*, 2012.
- Pour les fonctionnalités de recherche documentaire et d'accès : ICA-Req : *Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique, modules 1 à 3*, 2008. Ce standard a fait l'objet d'une normalisation en 2011 à l'ISO sous la référence ISO 16 175-2.

Leur application par les prestataires fait souvent l'objet de simples déclarations. Seule une certification par un tiers auditeur permet de prouver leur respect réel. Cependant, de même que pour les agréments, il n'existe pas de certification des logiciels de SAE, mais seulement de services complets d'archivage électronique : un SAE conforme à l'état de l'art n'est pas qu'un logiciel, mais recouvre une offre de service allant des infrastructures de stockage sécurisé au personnel qualifié en passant par les différentes couches logicielles. Ainsi, AFNOR-Certification propose la marque NF461 qui vérifie le respect des exigences de la norme NF Z 42-013 par des services d'archivage électronique.

11.2 Annexe 2 : Comparaison MEDONA/XDS

11.2.1 Tableau de correspondance MEDONA/XDS

Transaction	MEDONA	Obligatoire/facultatif MEDONA	XDS et autres profils IHE
Messages métier			
Demande de transfert d'archives	ArchiveTransferRequest		sans correspondance dans XDS
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	ArchivalAgreement	facultatif	
	CodeListVersions	obligatoire	
	DataObjectPackage	facultatif	
	RelatedTransferReference	facultatif	
	TransferDate	facultatif	
	ArchivalAgency	obligatoire	
	TransferringAgency	obligatoire	
Réponse à la demande de transfert	ArchiveRestitutionRequestReply		sans correspondance dans XDS
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	ArchivalAgreement	facultatif	
	DataObjectPackage	facultatif	
	ReplyCode	facultatif	
	MessageRequestIdentifier	obligatoire	
	TransferDate	facultatif	
	ArchivalAgency	obligatoire	
	TransferringAgency	obligatoire	

Transaction	MEDONA	Obligatoire/facultatif MEDONA	XDS et autres profils IHE
Messages métier			
Transfert archives	ArchiveTransfer		Transaction ITI-41 Provide and Register document Set (ProvideAndRegisterDocumentSet-b)
	Comment	facultatif	SubmissionSet.comments
	Date	obligatoire	SubmissionSet.submissionTime
	CodeListVersions	obligatoire	Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA)
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA en fonction du système versant ou du sourceID du submissionset pour les systèmes versants mutualisés
	DataObjectPackage	facultatif	SubmissionSet
	BinarayDataObject	obligatoire	Métadonnées présentes dans documentEntry : size, formatCode, hash et éventuellement présence d'une association de type sign
	BinaryDataObject@Id	obligatoire	Envelop/Body/ProvideAndRegisterDocumentSetRequest/SubmitObjectsRequest/RegistryObjectList/ExtrinsicObject/ExternalIdentifier[identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"]@value

	BinarayDataObject/Attachment	obligatoire	Document
	BinarayDataObject/Format	obligatoire	FormatCode
	BinarayDataObject/MessageDigest	obligatoire	Hash
	BinarayDataObject/SignatureStatus	obligatoire	Validation du Hash. Pourrait être vérifié par le module de traduction IHE/MEDONA qui indique si le hash est correct ou rejette la traduction si le hash ne correspond pas
	ManagementMetadata	obligatoire	Sans correspondance
	ManagementMetadata/ArchivalProfile	facultatif	Recommandation: un seul profil d'archivage par SIH et renseignement de cette donnée par le module de traduction IHE/MEDONA en fonction du SIH versant
	ManagementMetadata/AccessRule	facultatif	Recommandation: par défaut, les documents ne sont pas communicables (métadonnée à renseigner par le module de traduction IHE/MEDONA). Dans le cas de demande par des chercheurs, il convient de passer par le DIM qui décide si le document demandé est communicable. Le SIH doit demander la communication.

	ManagementMetadata/ServiceLevel	facultatif	Recommandation: à renseigner par le module de traduction IHE/MEDONA en fonction du SIH versant
	Signature	facultatif	Signature détachée. Document de signature associé au SS. Association de type SIGNS. Le document de signature est décrit par des métadonnées XDSDocument.
	RelatedTransferReference	facultatif	La liaison se fait par l'intermédiaire de l'identifiant patient pour les submissionSet et au niveau plus fin par referenceIDList au niveau du document
	TransferRequestReplyIdentifier	facultatif	sans correspondance dans la transaction ITI-41. Mais pas besoin de gérer cette information dans notre cas d'usage
	ArchivalAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	TransferringAgency	obligatoire	Service versant, identifié lors de la connexion au module de traduction IHE/MEDONA, soit par le certificat utilisé pour le TLS, soit dans une assertion SAML
	TransferringAgency	obligatoire	Service versant, identifié lors de la connexion au module de traduction IHE/MEDONA, soit par le certificat utilisé pour le TLS, soit dans une assertion

Réponse au transfert	ArchiveTransferReply		Transaction ITI-41 (ProvideAndRegisterDocumentSet-bResponse)
	Comment	facultatif	SubmissionSet.comments
	Date	obligatoire	SubmissionSet.submissionTime
	CodeListVersions	obligatoire	Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA)
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA en fonction du système versant ou du sourceID du submissionset pour les systèmes versants mutualisés
	DataObjectPackage	facultatif	SubmissionSet
	ReplyCode	facultatif	Liste de valeurs: Success|Failure|PartialSuccess et codes d'erreurs
	MessageRequestIdentifier	obligatoire	Enveloppe SOAP/header/RelatesTo
	GrantDate	facultatif	
	ArchivalAgency	obligatoire	Recommandation: A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	TransferringAgency	obligatoire	Service versant, identifié lors de la connexion au module de traduction IHE/MEDONA, soit par le certificat utilisé pour le TLS, soit dans une assertion SAML

Demande de communication	ArchiveDeliveryRequest		transaction retrieveDocumentSet (ITI-43) (RetrieveDocumentSetRequest)
	Comment	facultatif	Sans correspondance
	Date	obligatoire	soit reprise dans l'header HTTP soit alimentée par le module de traduction IHE/MEDONA
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA
	DataObjectPackage	facultatif	DocumentRequest
	DescriptiveMetadata	facultatif	DocumentRequest / RepositoryUniqueId
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	CodeListVersions	obligatoire	Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA)
	Derogation	obligatoire	Sans correspondance. Valeur "False" par défaut
	UnitIdentifier	obligatoire	DocumentRequest / DocumentUniqueId
	ArchivalAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	Requester	obligatoire	Demandeur identifié lors de la connexion au module de traduction IHE/MEDONA, soit par le certificat utilisé pour le TLS, soit dans une assertion SAML

Réponse à la demande de communication	ArchiveDeliveryRequestReply		transaction retrieveDocumentSet (ITI-43) (RetrieveDocumentSetResponse)
	Comment	facultatif	Sans correspondance
	Date	obligatoire	soit reprise dans l'header HTTP soit alimentée par le module de traduction IHE/MEDONA
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA.
	DataObjectPackage	facultatif	DocumentResponse
	DescriptiveMetadata	facultatif	DocumentResponse / RepositoryUniqueId
	BinaryDataObject/Attachment	facultatif	Document
	BinaryDataObject/Format	facultatif	mimeType
	ReplyCode	facultatif	Liste de valeurs: Success|Failure|PartialSuccess et codes d'erreurs
	MessageRequestIdentifier	obligatoire	Enveloppe SOAP/header/RelatesTo
	AuthorizationrequestReplyIdentifier	facultatif	sans correspondance
	UnitIdentifier	obligatoire	DocumentResponse / DocumentUniqueId
	ArchivalAgency	obligatoire	Recommandation: A renseigner par le module de traduction IHE/MEDONA en fonction du
	Requester	obligatoire	Demandeur identifié lors de la connexion au module de traduction IHE/MEDONA, soit par le certificat utilisé pour le TLS, soit dans une assertion SAML

Demande de restitution des archives	ArchiveRestitutionRequest		Hypothèse de travail: une transaction spécifique RetrieveDocumentSetAndDelete avec la même structure que l'ITI-43 mais un nom et une action soap
	Comment	facultatif	sans correspondance
	Date	obligatoire	soit reprise dans l'header HTTP soit alimentée par le module de traduction IHE/MEDONA
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA.
	DataObjectPackage	facultatif	
	UnitIdentifier	obligatoire	documentuniqueID
	ArchivalAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	Originatingagency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement

Réponse à la demande de restitution	ArchiveRestitutionRequestReply		réponse à la transaction spécifique RetrieveDocumentSetAndDelete
	Comment	facultatif	sans correspondance
	Date	obligatoire	soit reprise dans l'header HTTP soit alimentée par le module de traduction IHE/MEDONA
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA.
	DataObjectPackage	facultatif	
	ReplyCode	facultatif	Liste de valeurs: Success|Failure|PartialSuccess et codes d'erreurs
	MessageRequestIdentifier	obligatoire	Enveloppe SOAP/header/RelatesTo
	UnitIdentifier	obligatoire	documentuniqueID
	ArchivalAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	Originatingagency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement

Demande d'autorisation au service de contrôle	AuthorizationControlAuthorityRequest		sans correspondance
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	ArchivalAgreement	facultatif	
	DataObjectPackage	facultatif	
	AuthorizationRequestContent	obligatoire	
	Requester	obligatoire	
	ArchivalAgency	obligatoire	
	ControlAuthority	obligatoire	
Réponse à la demande d'autorisation du service contrôle	AuthorizationControlAuthorityRequestReply		sans correspondance
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	ArchivalAgreement	facultatif	
	DataObjectPackage	facultatif	
	ReplyCode	facultatif	
	MessageRequestIdentifier	obligatoire	
	ArchivalAgency	obligatoire	
	ControlAuthority	obligatoire	

demande d'autorisation au service producteur	AuthorizationOriginatingAgencyRequest		sans correspondance
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	ArchivalAgreement	facultatif	
	DataObjectPackage	facultatif	
	AuthorizationRequestContent	obligatoire	
	Requester	obligatoire	
	ArchivalAgency	obligatoire	
	OriginatingAgency	obligatoire	
Réponse à la demande d'autorisation au service producteur	AuthorizationOriginatingAgencyRequestReply		sans correspondance
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	ArchivalAgreement	facultatif	
	DataObjectPackage	facultatif	
	ReplyCode	facultatif	
	MessageRequestIdentifier	obligatoire	
	ArchivalAgency	obligatoire	
	OriginatingAgency	obligatoire	

Accusé de réception	Acknowledgement		pas d'accusé de réception dans XDS, on a les messages réponses. Indique que la logique MEDONA est du SOAP asynchrone ce qui est une option dans XDS. Soit utiliser cette option (attention nouveau endpoint ouvert sur internet au niveau du SIH) soit mettre le module de traduction au niveau du SAE et le laisser émuler un comportement synchrone avec le SIH.
	Comment	facultatif	
	Date	obligatoire	
	MessageIdentifier	obligatoire	
	MessageReceiverIdentifier	obligatoire	
	Receiver	obligatoire	
	Sender	obligatoire	

Notification de modification d'archives	ArchiveModificationNotification		Profil DSUB, transaction ITI-53.
	Comment	facultatif	sans correspondance
	Date	obligatoire	soit reprise dans l'header HTTP soit alimentée par le module de traduction IHE/MEDONA
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA.
	CodeListVersions	obligatoire	Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA)
	DataObjectPackage	facultatif	restitution de toutes les métadonnées conservées
	UnitIdentifier	obligatoire	document unique ID
	ArchivalAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	OriginatingAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement

Notification d'élimination d'archives	ArchivedestructionnotificatioNotification		Profil DSUB, transaction ITI-53
	Comment	facultatif	sans correspondance
	Date	obligatoire	soit reprise dans l'header HTTP soit alimentée par le module de traduction IHE/MEDONA
	MessageIdentifier	obligatoire	Enveloppe SOAP/header/MessageID
	ArchivalAgreement	facultatif	Constante à déterminer par le module de traduction IHE/MEDONA.
	CodeListVersions	obligatoire	Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA)
	DataObjectPackage	facultatif	restitution de toutes les métadonnées conservées
	AuthorizationRequestReplyIdentifier	facultatif	sans correspondance
	UnitIdentifier	obligatoire	document unique ID
	ArchivalAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement
	OriginatingAgency	obligatoire	A renseigner par le module de traduction IHE/MEDONA en fonction du ArchivalAgreement

11.2.2 Exemple

Les fichiers XML ci-dessous représentent un exemple de transaction MEDONA de transfert d'archives qui réutilise les métadonnées XDS au niveau des métadonnées descriptives de MEDONA.

Dans l'exemple de la figure 11.2.2-1, les balises Signature et DataObjectPackage sont repliées pour une facilité de lecture

```
<?xml version="1.0" encoding="UTF-8"?>
<ArchiveTransfer xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="org:afnor:medona:v1.0 file:/C:/Documents%20and%20Settings/thomas.bernard/Bureau/Baptiste/schemas/MEDONA.xsd"
    xmlns="org:afnor:medona:v1.0">
    <Comment>Compte rendu test</Comment>
    <Date>20111206110801</Date>
    <MessageIdentifier>T63N6CC3Kogc5g</MessageIdentifier>
    <Signature>
    <CodeListVersions>
        <!-- Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA) -->
    </CodeListVersions>
    <DataObjectPackage>
    <ArchivalAgency>
        <Identifier>00B104155302</Identifier>
    </ArchivalAgency>
    <TransferringAgency>
        <Identifier>00B104155300</Identifier>
    </TransferringAgency>
</ArchiveTransfer>
```

Figure 11.2.2-1 Message ArchiveTransfertRequest de la transaction MEDONA ArchiveTransfer (balises Signature et DataObjectPackage re-pliées)

Dans l'exemple suivant, la balise DataObjectPackage (équivalent du lot de soumission) est dépliée. Elle fait apparaitre la balise DescriptiveMetada qui reprend les métadonnées XDS. La balise Signature est repliée pour des facilités de lecture.

```
<?xml version="1.0" encoding="UTF-8"?>
<ArchiveTransfer xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="org:afnor:medona:v1.0
file:/C:/Documents%20and%20Settings/thomas.bernard/Bureau/Baptiste/schemas/MEDONA.xsd"
   xmlns="org:afnor:medona:v1.0">
   <Comment>Compte rendu test</Comment>
   <Date>20111206110801</Date>
   <MessageIdentifier>T63N6CC3Kogc5g</MessageIdentifier>
   <Signature>  </Signature>

   <CodeListVersions>
      <!-- Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA) -->
   </CodeListVersions>
   <DataObjectPackage>
         <BinaryDataObject xml:id="1.2.250.1.999.1.1.7898.3.333.1">
         <Attachment<!—Document en binaire --></Attachment>
         <Format></Format>
         <MessageDigest algorithm=""></MessageDigest>
         <SignatureStatus></SignatureStatus>
         <Size>6219</Size>
      </BinaryDataObject>
      <DescriptiveMetadata xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:ns4="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0" xmlns:ns5="urn:ihe:iti:xds-b:2007" xmlns:ns6="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0">
         <ns2:RegistryObjectList>
                              <ns2:RegistryPackage id="SubmissionSet01">
                                 <ns2:Slot name="submissionTime">
                                    <ns2:ValueList>
```

```
                                        <ns2:Value>20111206110801</ns2:Value>
                                    </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                    <ns2:LocalizedString charset="UTF8" value="lot du document originel" xml:lang="FR" />
                                </ns2:Name>
                                <ns2:Description>
                                    <ns2:LocalizedString charset="UTF8" value="Compte rendu test" xml:lang="FR" />
                                </ns2:Description>
                                <ns2:Classification classificationScheme="urn:uuid:a7058bb9-b4e4-4307-ba5b-e3f0ab85e12d" classi-
fiedObject="SubmissionSet01" id="cla55" nodeRepresentation="">
                                    <ns2:Slot name="authorPerson">
                                        <ns2:ValueList>
                                            <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;1.2.250.1.71.4.2.1&amp;ISO^D^^^IDNPS</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorSpecialty">
                                        <ns2:ValueList>
                                            <ns2:Value>G15_10/SM26^Médecin - Qualifié en Médecine Générale
(SM)^1.2.250.1.213.1.1.4.5</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorInstitution">
                                        <ns2:ValueList>
                                            <ns2:Value>Cabinet Dr MEDECIN2154-B1
PAUL^^^^^&amp;1.2.250.1.71.4.2.2&amp;ISO^IDNST^^^00B104155300</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500" classi-
fiedObject="SubmissionSet01" id="cla56" nodeRepresentation="04">
```

```
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>1.2.250.1.213.2.2</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Hospitalisation de jour" xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd" classifiedOb-
ject="SubmissionSet01" id="cla57" />
                                <ns2:ExternalIdentifier registryObject="SubmissionSet01" id="ei22" identifica-
tionScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" val-
ue="1164485058822081751070^^^&amp;1.2.250.1.213.1.4.2&amp;ISO^INS-C^^20100522152212">
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="XDSSubmissionSet.patientId" xml:lang="FR"
/>
                                    </ns2:Name>
                                </ns2:ExternalIdentifier>
                                <ns2:ExternalIdentifier registryObject="SubmissionSet01" id="ei23" identifica-
tionScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832" value="1.2.250.1.999.1.1.7898">
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="XDSSubmissionSet.sourceId" xml:lang="FR"
/>
                                    </ns2:Name>
                                </ns2:ExternalIdentifier>
                                <ns2:ExternalIdentifier registryObject="SubmissionSet01" id="ei24" identifica-
tionScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8" value="1.2.250.1.999.1.1.7898.1.20111206120801">
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="XDSSubmissionSet.uniqueId" xml:lang="FR"
/>
                                    </ns2:Name>
```

```
                    </ns2:ExternalIdentifier>
                </ns2:RegistryPackage>
                <ns2:ExtrinsicObject id="document01" mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-
9b2a5b5186c1">
                    <ns2:Slot name="creationTime">
                        <ns2:ValueList>
                            <ns2:Value>20100903114745</ns2:Value>
                        </ns2:ValueList>
                    </ns2:Slot>
                    <ns2:Slot name="languageCode">
                        <ns2:ValueList>
                            <ns2:Value>fr-FR</ns2:Value>
                        </ns2:ValueList>
                    </ns2:Slot>
                    <ns2:Slot name="legalAuthenticator">
                        <ns2:ValueList>
                            <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                        </ns2:ValueList>
                    </ns2:Slot>
                    <ns2:Slot name="serviceStartTime">
                        <ns2:ValueList>
                            <ns2:Value>20100319183244</ns2:Value>
                        </ns2:ValueList>
                    </ns2:Slot>
                    <ns2:Slot
name="serviceStopTime"><ns2:ValueList><ns2:Value>20100319183244</ns2:Value></ns2:ValueList></ns2:Slot>
                    <ns2:Slot name="sourcePatientId">
                        <ns2:ValueList>
                            <ns2:Value>0456789999^^^&amp;amp;1.2.250.1.999.1.1.7898.2&amp;amp;ISO^PI</ns2:Value>
                        </ns2:ValueList>
                    </ns2:Slot>
```

```
                                <ns2:Slot name="sourcePatientInfo">
                                        <ns2:ValueList>
                                                <ns2:Value>PID-5|MARTINQUARANTESIX^Marie^^^^^L</ns2:Value>
                                                <ns2:Value>PID-7|19760414</ns2:Value>
                                                <ns2:Value>PID-8|F</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="hash">
                                        <ns2:ValueList>
                                                <ns2:Value>492E9211C6D56410677CFC3EF914EE634BE88524</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="size">
                                        <ns2:ValueList>
                                                <ns2:Value>6219</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Document 3 (version originale)" xml:lang="FR" />
                                </ns2:Name>
                                <ns2:Description>
                                        <ns2:LocalizedString charset="UTF8" value="commentaire sur document" xml:lang="FR" />
                                </ns2:Description>
                                <ns2:Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d" classi-
fiedObject="document01" id="cla58" nodeRepresentation="">
                                        <ns2:Slot name="authorPerson">
                                                <ns2:ValueList>
                                                        <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                                                </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Slot name="authorSpecialty">
```

```
                                        <ns2:ValueList>
                                            <ns2:Value>G15_10/SM26^Médecin - Qualifié en Médecine Générale
(SM)^1.2.250.1.213.1.1.4.5</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorInstitution">
                                        <ns2:ValueList>
                                            <ns2:Value>Cabinet Dr MEDECIN2154-B1
PAUL^^^^^&amp;amp;1.2.250.1.71.4.2.2&amp;amp;ISO^IDNST^^^00B104155300</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a" classi-
fiedObject="document01" id="cla59" nodeRepresentation="10">
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>1.2.250.1.213.1.1.4.1</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Comptes rendus" xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="document01" id="cla60" nodeRepresentation="N">
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>2.16.840.1.113883.5.25</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Normal" xml:lang="FR" />
```

```
                                        </ns2:Name>
                                    </ns2:Classification>
                                    <ns2:Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classi-
fiedObject="document01" id="cla602" nodeRepresentation="18724-5">
                                        <ns2:Slot name="codingScheme">
                                            <ns2:ValueList>
                                                <ns2:Value>2.16.840.1.113883.6.1</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="HLA" xml:lang="FR" />
                                        </ns2:Name>
                                    </ns2:Classification>
                                    <ns2:Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d" classi-
fiedObject="document01" id="cla61" nodeRepresentation="urn:ihe:iti:xds-sd:text:2008">
                                        <ns2:Slot name="codingScheme">
                                            <ns2:ValueList>
                                                <ns2:Value>1.3.6.1.4.1.19376.1.2.3</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="documents à corps non structuré en texte brut"
xml:lang="FR" />
                                        </ns2:Name>
                                    </ns2:Classification>
                                    <ns2:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1" classifiedOb-
ject="document01" id="cla62" nodeRepresentation="SA01">
                                        <ns2:Slot name="codingScheme">
                                            <ns2:ValueList>
                                                <ns2:Value>1.2.250.1.71.4.2.4</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
```

```
                                        <ns2:Name>
                                                <ns2:LocalizedString charset="UTF8" value="Etablissement Public de santé" xml:lang="FR"
/>
                                        </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead" classifie-
dObject="document01" id="cla63" nodeRepresentation="ETABLISSEMENT">
                                        <ns2:Slot name="codingScheme">
                                                <ns2:ValueList>
                                                        <ns2:Value>1.2.250.1.213.1.1.4.9</ns2:Value>
                                                </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Name>
                                                <ns2:LocalizedString charset="UTF8" value="Etablissement de santé" xml:lang="FR" />
                                        </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983" classifie-
dObject="document01" id="cla64" nodeRepresentation="34874-8">
                                        <ns2:Slot name="codingScheme">
                                                <ns2:ValueList>
                                                        <ns2:Value>2.16.840.1.113883.6.1</ns2:Value>
                                                </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Name>
                                                <ns2:LocalizedString charset="UTF8" value="CR opératoire" xml:lang="FR" />
                                        </ns2:Name>
                                </ns2:Classification>
                                <ns2:ExternalIdentifier registryObject="document01" id="ei25" identificationScheme="urn:uuid:58a6f841-
87b3-4a3e-92fd-a8ffeff98427" value="1164485058822081751070^^^&amp;amp;1.2.250.1.213.1.4.2&amp;amp;ISO^INS-C^^20100522152212">
                                        <ns2:Name>
                                                <ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.patientId"
xml:lang="FR" />
```

```
                                        </ns2:Name>
                                    </ns2:ExternalIdentifier>
                                    <ns2:ExternalIdentifier registryObject="document01" id="ei26" identificationScheme="urn:uuid:2e82c1f6-
a085-4c72-9da3-8640a32e42ab" value="1.2.250.1.999.1.1.7898.3.333.1">
                                        <!-- Envel-
op/Body/ProvideAndRegisterDocumentSetRequest/SubmitObjectsRequest/RegistryObjectList/ExtrinsicObject/ExternalIdentifier@value => Ar-
chiveTransfer/DataObjectPackage/BinaryDataObject@xml:id pour Envel-
op/Body/ProvideAndRegisterDocumentSetRequest/SubmitObjectsRequest/RegistryObjectList/ExtrinsicObject/ExternalIdentifier/Name/Localize
dString@value="XDSDocumentEntry.uniqueId" -->
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.uniqueId"
xml:lang="FR" />
                                        </ns2:Name>
                                    </ns2:ExternalIdentifier>
                                </ns2:ExtrinsicObject>
                                <ns2:ExtrinsicObject id="Signature01" mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-
9b2a5b5186c1">
                                    <ns2:Slot name="creationTime">
                                        <ns2:ValueList>
                                            <ns2:Value>20111206110801</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="languageCode">
                                        <ns2:ValueList>
                                        <ns2:Value>art</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="legalAuthenticator">
                                        <ns2:ValueList>
                                            <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                                        </ns2:ValueList>
```

```
                                    </ns2:Slot>
                                    <ns2:Slot name="serviceStartTime">
                                        <ns2:ValueList>
                                            <ns2:Value>20111206110801</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="serviceStopTime">
                                        <ns2:ValueList>
                                            <ns2:Value>20111206110801</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="sourcePatientId">
                                        <ns2:ValueList>
        <ns2:Value>1164485058822081751070^^^&amp;amp;1.2.250.1.213.1.4.2&amp;amp;ISO^INS-C^^20100522152212</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Source" xml:lang="FR" />
                                    </ns2:Name>
                                    <ns2:Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d" classi-
fiedObject="Signature01" id="cla65" nodeRepresentation="">
                                    <ns2:Slot name="authorPerson">
                                        <ns2:ValueList>
                                            <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorRole">
                                        <ns2:ValueList>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorSpecialty">
```

```
                                        <ns2:ValueList>
                                                <ns2:Value>G15_10/SM26^Médecin - Qualifié en Médecine Générale
(SM)^1.2.250.1.213.1.1.4.5</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="authorInstitution">
                                        <ns2:ValueList>
                                                <ns2:Value>Cabinet Dr MEDECIN2154-B1
PAUL^^^^^&amp;amp;1.2.250.1.71.4.2.2&amp;amp;ISO^IDNST^^^00B104155300</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                        </ns2:Classification>
                        <ns2:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a" classifiedOb-
ject="Signature01" id="cla66" nodeRepresentation="urn:oid:1.3.6.1.4.1.19376.1.2.1.1.1">
                                <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                                <ns2:Value>URN</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Digital Signature" xml:lang="FR" />
                                </ns2:Name>
                        </ns2:Classification>
                        <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="Signature01" id="cla67" nodeRepresentation="N">
                                <ns2:Slot name="codingScheme">
                                        <ns2:ValueList><ns2:Value>2.16.840.1.113883.5.25</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Normal" xml:lang="FR" />
                                </ns2:Name>
                        </ns2:Classification>
```

```
                        <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="Signature01" id="cla671" nodeRepresentation="MASQUE_PS">
                            <ns2:Slot name="codingScheme">
                                <ns2:ValueList><ns2:Value>1.2.250.1.213.1.1.4.13</ns2:Value></ns2:ValueList>
                            </ns2:Slot>
                            <ns2:Name>
                                <ns2:LocalizedString charset="UTF8" value="Document masqué aux professionnels de santé"
xml:lang="FR" />
                            </ns2:Name>
                        </ns2:Classification>
                        <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="Signature01" id="cla672" nodeRepresentation="INVISIBLE_PATIENT">
                            <ns2:Slot name="codingScheme">
                                <ns2:ValueList><ns2:Value>1.2.250.1.213.1.1.4.13</ns2:Value></ns2:ValueList>
                            </ns2:Slot>
                            <ns2:Name>
                                <ns2:LocalizedString charset="UTF8" value="Document non visible par le patient" xml:lang="FR"
/>
                            </ns2:Name>
                        </ns2:Classification>
                        <ns2:Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classifiedOb-
ject="Signature01" id="cla68" nodeRepresentation="1.2.840.10065.1.12.1.14">
                            <ns2:Slot name="codingScheme">
                                <ns2:ValueList><ns2:Value>1.2.840.10065.1.12</ns2:Value></ns2:ValueList>
                            </ns2:Slot>
                            <ns2:Name><ns2:LocalizedString charset="UTF8" value="Source" xml:lang="FR" /></ns2:Name>
                        </ns2:Classification>
                        <ns2:Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d" classifiedOb-
ject="Signature01" id="cla69" nodeRepresentation="http://www.w3.org/2000/09/xmldsig#">
                            <ns2:Slot name="codingScheme">
                                <ns2:ValueList><ns2:Value>URN</ns2:Value></ns2:ValueList>
                            </ns2:Slot>
```

```
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Default Signature Style" xml:lang="FR"
/></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1" classifiedOb-
ject="Signature01" id="cla70" nodeRepresentation="SA01">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>1.2.250.1.71.4.2.4</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Etablissement Public de santé" xml:lang="FR"
/></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead" classifiedOb-
ject="Signature01" id="cla71" nodeRepresentation="ETABLISSEMENT">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>1.2.250.1.213.1.1.4.9</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Etablissement de santé" xml:lang="FR"
/></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983" classifiedOb-
ject="Signature01" id="cla72" nodeRepresentation="E1762">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>ASTM</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Full Document" xml:lang="FR" /></ns2:Name>
                            </ns2:Classification>
                            <ns2:ExternalIdentifier registryObject="Signature01" id="ei27" identificationScheme="urn:uuid:58a6f841-87b3-
4a3e-92fd-a8ffeff98427" value="1164485058822081751070^^^&amp;amp;1.2.250.1.213.1.4.2&amp;amp;ISO^INS-C^^20100522152212">
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.patientId" xml:lang="FR"
/></ns2:Name>
                            </ns2:ExternalIdentifier>
```

```
                        <ns2:ExternalIdentifier registryObject="Signature01" id="ei28" identificationScheme="urn:uuid:2e82c1f6-a085-
4c72-9da3-8640a32e42ab" value="1.2.250.1.999.1.1.7898.3.20111206120801.0">
                            <ns2:Name><ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.uniqueId" xml:lang="FR"
/></ns2:Name>
                        </ns2:ExternalIdentifier>
                    </ns2:ExtrinsicObject>
                    <ns2:Association associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember" id="association1"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Association" sourceObject="SubmissionSet01" tar-
getObject="document01">
                        <ns2:Slot name="SubmissionSetStatus">
                            <ns2:ValueList><ns2:Value>Original</ns2:Value></ns2:ValueList>
                        </ns2:Slot>
                    </ns2:Association>
                    <ns2:Association associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember" id="association2"
      objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Association" sourceObject="SubmissionSet01" tar-
getObject="Signature01">
                        <ns2:Slot name="SubmissionSetStatus">
                            <ns2:ValueList><ns2:Value>Original</ns2:Value></ns2:ValueList>
                        </ns2:Slot>
                    </ns2:Association>
                <ns2:Association associationType="urn:ihe:iti:2007:AssociationType:signs" id="association3" ob-
jectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Association" sourceObject="Signature01" tar-
getObject="SubmissionSet01">
                    <ns2:Slot name="SubmissionSetStatus">
                        <ns2:ValueList><ns2:Value>Original</ns2:Value></ns2:ValueList>
                    </ns2:Slot>
                </ns2:Association>
            </ns2:RegistryObjectList>
        </DescriptiveMetadata>
        <ManagementMetadata/>
    </DataObjectPackage>
    <ArchivalAgency>
```

```
      <Identifier>00B104155302</Identifier>
   </ArchivalAgency>
   <TransferringAgency>
      <Identifier>00B104155300</Identifier>
   </TransferringAgency>
</ArchiveTransfer>
```

Ce dernier exemple présente la structure du message ArchiveTranferRequest avec l'ensemble des balises dépliées, y compris la signature

```
<?xml version="1.0" encoding="UTF-8"?>
<ArchiveTransfer xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="org:afnor:medona:v1.0
file:/C:/Documents%20and%20Settings/thomas.bernard/Bureau/Baptiste/schemas/MEDONA.xsd"
   xmlns="org:afnor:medona:v1.0">
   <Comment>Compte rendu test</Comment>
   <Date>20111206110801</Date>
   <MessageIdentifier>T63N6CC3Kogc5g</MessageIdentifier>
   <Signature>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="1.2.250.1.999.1.1.7898.3.20111206120801.0">
         <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
            <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <Reference Type="http://www.w3.org/2000/09/xmldsig#Manifest" URI="#IHEManifest">
               <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               <DigestValue>qAIDPzlGqLh6MNOHjF4PUNywLiQ=</DigestValue>
            </Reference>
            <Reference Type="http://uri.etsi.org/01903/v1.1.1#SignedProperties" URI="#S0-SignedProperties">
               <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               <DigestValue>Um1r90x3dX5bXRC+Gla1q9Fia7M=</DigestValue>
            </Reference>
         </SignedInfo>
         <SignatureValue>

q0+TK2TBZBcKFXGXNgGW1OwpV4CiYJdpAlK/mWZ8Oc1XenzBq8cLdeSWG0yU7APeclw9PiWyzE304XxNW0LYflhLq8aFWpfSBa0hJ
kYTPZ8QRC+RSrW4Z0kJ0DSBvkd/obwOxLyMj8e651W/fya49+HAK4b2Cw94uJXPBvjHJwP2FBQ3GkmY+iQxGfr36Htf5TCUNbhD7rfkS+
F0DCCGPm+JQrOeAPsqsM7vLb28Z80FbfoGPQIh1LlStn6BRnElQLb6S9tDL3ZsDwYr6J0B56ebBOcWwKOADxpgjRvyXw1cJLLfa/SDYpC
pvsKFlzmNC2iK5CzpALGXhJHoYoCgtA==
         </SignatureValue>
         <KeyInfo>
            <X509Data>
```

```
            <X509Certificate>
               MIIFrTCCBJWgAwIBAgIDTFaC-
MA0GCSqGSIb3DQEBBQUAMFExCzAJBgNVBAYTAkZSMQ0wCwYDVQQKEwRURVNUMRswGQYDVQQLExJURVNUIFBST0ZFU1
NJT05ORUwxFjAUBgNVBAMTDVRFU1QgQ0xBU1NFLTEwHhcNMTEwMzI4MDAwMDAxWhcNMTQwNDMwMjE1OTU5WjBkMQsw
CQYDVQQGEwJGU-
jENMAsGA1UEChMEVEVTVDEQMA4GA1UECxQHTelkZWNpbjE0MBEGA1UEAxMKMDBCMTA0MTU1MzASBgNVBAQUC01FRE
VDSU40MTU1MAsGA1UEKhQEUEFVTDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALIleyZm5NyTzhcKeEHrsXO9C
618wZSXcmg/4HAZIBfSQG90vHt4nTH1Y0eiAzIGNNmVvD41IV7H52OpmBy+nFd/Y0rJESqvRxuS7eZNqPWYb1JUZ/40hupsL0gJRItLRHr
5pbRzBOngC1C6lJ4tiXz0sfrbuTws0u/YpLPygR8DIfbInrLv6wR6I534OgdzhA5spRv0FZLssjx42PzIkIrLJfYil2sieTjaZO1yxVFzzjKPoJtCxjB8
q9Lk4qTrfUdON9ikIuyH8dflloIgOiZwN/zdw5wzG9jDhFDCKfYFl9Qvmb+W4SnTXU3rKZ7YO0If5wYmRB3Sqg8L1d/Nv38CAwEAAaOC
AnkwggJ1MB8GA1UdIwQYMBaAFHYQNUO0i3+MbgC3kqaQgrPBS9LqMB0GA1UdDgQWBBSsSMOz7DcQYT8pKdLAV8liwRb2dTAO
BgNVHQ8BAf8EBAMCBsAwEwYDVR0lBAwwCgYIKwYBBQUHAwQwKwYDVR0QBCQwIoAPMjAxMTAzMjgwMDAwMDFagQ8yM
DE0MDMzMTIzNTk1OVowGQYDVR0gBBIwEDAOBgwqgXoBRwMHCQEBAgEwCQYDVR0TBAIwADCBvgYDVR0fBIG2MIGzMDug
OaA3hjVodHRwOi8vYW5udWFpcmUuZ2lwLWNwcy5mci9jcmwvdGVzdC9URVNUIENMQVNTRS0xLmNybDB0oHKgcIZubGRhcDovL2
Fub-
nVhaXJlLmdpcC1jcHMuZnIvY249dGVzdCBjbGFzc2UtMSxvdT10ZXN0IHByb2Zlc3Npb25uZWwsbz10ZXN0LGM9ZnI/Y2VydGlmaWNhd
GVyZXZvY2F0aW9ubGlzdDtiaW5hcnkweQYDVR0uBHIwcDBuoGygaoZobGRhcDovL2FubnVhaXJlLmdpcC1jcHMuZnIvY249dGVzdCBjb
GFzc2UtMSxvdT10ZXN0IHByb2Zlc3Npb25uZWwsbz10ZXN0LGM9ZnI/ZGVsdGFyZXZvY2F0aW9ubGlzdDtiaW5hcnkwEQYJYIZIAYb4
QgEBBAQDAgUgMCMGCCqBegFHAQIDBBcTFT-
gwMjUwMDAwMDEvMjMwMDA0MjYzMjAPBggqgXoBRwECBQQDBAGAMA8GCCqBegFHAQICBAMCAQAwDwYIKoF6AUcBAgcE
AwIBCjAUBggqgXoBRwQCBQQIMAYMBFNNMjYwDQYJKoZIhvcNAQEFBQADggE-
BALrr21o1Y1W+WWJIF0cSwE8rGicj6zVBBn8D2zYsNzszqVviUBdN27gAHw9aXjLkHbnQrVmbtpOGkH3vUwtCmQYNWALUH/5Q5TNt
k69twvKJg8nRL7vYe6OV5Tn1idPenBlp70PmDJqMfQJ6IMKAk1Gqd6rIs3FUPvYlmefWPDr0q+X5cjedwsw+CeHEFyvQYUJo5bnWbFvchN
qlwqe+JgStmq3xqYJCGCZG+l2sA966odOxbB/UB5Q/Zi4pkjFvnztdJvjqQ4pRFwBZYQjXRsHydjITcrFCuW8QwVnM59Pnk2yOHakjdH3SH0
46ogJlE9++u4e841EvwstfSTNy8h8=
            </X509Certificate>
         </X509Data>
      </KeyInfo>
      <Object>
         <Manifest Id="IHEManifest">
            <Reference URI="urn:oid:1.2.250.1.999.1.1.7898.1.20111206120801">
               <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
            <DigestValue>AA==</DigestValue>
          </Reference>
          <Reference URI="urn:oid:1.2.250.1.999.1.1.7898.3.333.1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>ZE/LGnc62hy16JaNAxjUuVMWMl8=</DigestValue>
          </Reference>
        </Manifest>
      </Object>
      <Object>
        <SignatureProperties>
          <SignatureProperty Id="purposeOfSignature" Tar-
get="#1.2.250.1.999.1.1.7898.3.20111206120801.0">1.2.840.10065.1.12.1.14</SignatureProperty>
        </SignatureProperties>
      </Object>
      <Object>
        <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.1.1#" Target="#1.2.250.1.999.1.1.7898.3.20111206120801.0">
          <SignedProperties Id="S0-SignedProperties" xmlns="http://uri.etsi.org/01903/v1.1.1#">
            <SignedSignatureProperties>
              <SigningTime>2011-12-06T12:08:07.442+01:00</SigningTime>
              <SigningCertificate>
                <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
                  <CertDigest>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue>nxezsT281ZrQ0w+xh41hNxzgt+c=</DigestValue>
                  </CertDigest>
                  <IssuerSerial>
                    <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">CN=TEST CLASSE-1,OU=TEST PROFESSION-
NEL,O=TEST,C=FR</X509IssuerName>
                    <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">5002882</X509SerialNumber>
```

```
                    </IssuerSerial>
                  </Cert>
                  <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
                    <CertDigest>
                      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                      <DigestValue>sDm6ZeMesuvOrs2T6iwjWogcqY0=</DigestValue>
                    </CertDigest>
                    <IssuerSerial>
                      <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">OU=TEST PROFESSION-
NEL,O=TEST,C=FR</X509IssuerName>
                      <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">4368</X509SerialNumber>
                    </IssuerSerial>
                  </Cert>
                  <Cert xmlns="http://uri.etsi.org/01903/v1.1.1#">
                    <CertDigest>
                      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                      <DigestValue>+18e33b11UENgMxtct5FfX2So4Y=</DigestValue>
                    </CertDigest>
                    <IssuerSerial>
                      <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">OU=TEST PROFESSION-
NEL,O=TEST,C=FR</X509IssuerName>
                      <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">4352</X509SerialNumber>
                    </IssuerSerial>
                  </Cert>
                </SigningCertificate>
                <SignaturePolicyIdentifier>
                  <SignaturePolicyImplied/>
                </SignaturePolicyIdentifier>
              </SignedSignatureProperties>
              <SignedDataObjectProperties></SignedDataObjectProperties>
            </SignedProperties>
            <UnsignedProperties>
```

```
                <UnsignedSignatureProperties></UnsignedSignatureProperties>
              </UnsignedProperties>
            </QualifyingProperties>
          </Object>
        </Signature>
      </Signature>
      <CodeListVersions>
        <!-- Constante à déterminer par couple SIH/SAE et à remplir par le module de traduction IHE/MEDONA) -->
      </CodeListVersions>
      <DataObjectPackage>
          <BinaryDataObject xml:id="1.2.250.1.999.1.1.7898.3.333.1">
          <Attachment><!--document en binaire--></Attachment>
          <Format></Format>
          <MessageDigest algorithm=""></MessageDigest>
          <SignatureStatus></SignatureStatus>
          <Size>6219</Size>
        </BinaryDataObject>
        <DescriptiveMetadata xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:ns4="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0" xmlns:ns5="urn:ihe:iti:xds-b:2007" xmlns:ns6="urn:oasis:names:tc:ebxml-
regrep:xsd:lcm:3.0">
          <ns2:RegistryObjectList>
                              <ns2:RegistryPackage id="SubmissionSet01">
                                  <ns2:Slot name="submissionTime">
                                      <ns2:ValueList>
                                          <ns2:Value>20111206110801</ns2:Value>
                                      </ns2:ValueList>
                                  </ns2:Slot>
                                  <ns2:Name>
                                      <ns2:LocalizedString charset="UTF8" value="lot du document originel" xml:lang="FR" />
                                  </ns2:Name>
                                  <ns2:Description>
                                      <ns2:LocalizedString charset="UTF8" value="Compte rendu test" xml:lang="FR" />
```

```
                                    </ns2:Description>
                                    <ns2:Classification classificationScheme="urn:uuid:a7058bb9-b4e4-4307-ba5b-e3f0ab85e12d" classi-
fiedObject="SubmissionSet01" id="cla55" nodeRepresentation="">
                                        <ns2:Slot name="authorPerson">
                                            <ns2:ValueList>
                                                <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Slot name="authorSpecialty">
                                            <ns2:ValueList>
                                                <ns2:Value>G15_10/SM26^Médecin - Qualifié en Médecine Générale
(SM)^1.2.250.1.213.1.1.4.5</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Slot name="authorInstitution">
                                            <ns2:ValueList>
                                                <ns2:Value>Cabinet Dr MEDECIN2154-B1
PAUL^^^^^&amp;amp;1.2.250.1.71.4.2.2&amp;amp;ISO^IDNST^^^00B104155300</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                    </ns2:Classification>
                                    <ns2:Classification classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-df4873be8500" classi-
fiedObject="SubmissionSet01" id="cla56" nodeRepresentation="04">
                                        <ns2:Slot name="codingScheme">
                                            <ns2:ValueList>
                                                <ns2:Value>1.2.250.1.213.2.2</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="Hospitalisation de jour" xml:lang="FR" />
                                        </ns2:Name>
```

```
                                    </ns2:Classification>
                                    <ns2:Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd" classifiedOb-
ject="SubmissionSet01" id="cla57" />
                                    <ns2:ExternalIdentifier registryObject="SubmissionSet01" id="ei22" identifica-
tionScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-96a0a7b38446" val-
ue="1164485058822081751070^^^&amp;1.2.250.1.213.1.4.2&amp;ISO^INS-C^^20100522152212">
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="XDSSubmissionSet.patientId" xml:lang="FR"
/>
                                        </ns2:Name>
                                    </ns2:ExternalIdentifier>
                                    <ns2:ExternalIdentifier registryObject="SubmissionSet01" id="ei23" identifica-
tionScheme="urn:uuid:554ac39e-e3fe-47fe-b233-965d2a147832" value="1.2.250.1.999.1.1.7898">
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="XDSSubmissionSet.sourceId" xml:lang="FR"
/>
                                        </ns2:Name>
                                    </ns2:ExternalIdentifier>
                                    <ns2:ExternalIdentifier registryObject="SubmissionSet01" id="ei24" identifica-
tionScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8" value="1.2.250.1.999.1.1.7898.1.20111206120801">
                                        <ns2:Name>
                                            <ns2:LocalizedString charset="UTF8" value="XDSSubmissionSet.uniqueId" xml:lang="FR"
/>
                                        </ns2:Name>
                                    </ns2:ExternalIdentifier>
                                </ns2:RegistryPackage>
                                <ns2:ExtrinsicObject id="document01" mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-
9b2a5b5186c1">
                                    <ns2:Slot name="creationTime">
                                        <ns2:ValueList>
                                            <ns2:Value>20100903114745</ns2:Value>
                                        </ns2:ValueList>
```

```
                                    </ns2:Slot>
                                    <ns2:Slot name="languageCode">
                                        <ns2:ValueList>
                                            <ns2:Value>fr-FR</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="legalAuthenticator">
                                        <ns2:ValueList>
                                            <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;1.2.250.1.71.4.2.1&amp;ISO^D^^^IDNPS</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="serviceStartTime">
                                        <ns2:ValueList>
                                            <ns2:Value>20100319183244</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot
name="serviceStopTime"><ns2:ValueList><ns2:Value>20100319183244</ns2:Value></ns2:ValueList></ns2:Slot>
                                    <ns2:Slot name="sourcePatientId">
                                        <ns2:ValueList>
                                            <ns2:Value>0456789999^^^&amp;1.2.250.1.999.1.1.7898.2&amp;ISO^PI</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="sourcePatientInfo">
                                        <ns2:ValueList>
                                            <ns2:Value>PID-5|MARTINQUARANTESIX^Marie^^^^^L</ns2:Value>
                                            <ns2:Value>PID-7|19760414</ns2:Value>
                                            <ns2:Value>PID-8|F</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="hash">
```

```
                                        <ns2:ValueList>
                                            <ns2:Value>492E9211C6D56410677CFC3EF914EE634BE88524</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="size">
                                        <ns2:ValueList>
                                            <ns2:Value>6219</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Document 3 (version originale)" xml:lang="FR" />
                                    </ns2:Name>
                                    <ns2:Description>
                                        <ns2:LocalizedString charset="UTF8" value="commentaire sur document" xml:lang="FR" />
                                    </ns2:Description>
                                    <ns2:Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d" classi-
fiedObject="document01" id="cla58" nodeRepresentation="">
                                        <ns2:Slot name="authorPerson">
                                            <ns2:ValueList>
                                                <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Slot name="authorSpecialty">
                                            <ns2:ValueList>
                                                <ns2:Value>G15_10/SM26^Médecin - Qualifié en Médecine Générale
(SM)^1.2.250.1.213.1.1.4.5</ns2:Value>
                                            </ns2:ValueList>
                                        </ns2:Slot>
                                        <ns2:Slot name="authorInstitution">
                                            <ns2:ValueList>
```

```
                                        <ns2:Value>Cabinet Dr MEDECIN2154-B1
PAUL^^^^^&amp;amp;1.2.250.1.71.4.2.2&amp;amp;ISO^IDNST^^^00B104155300</ns2:Value>
                                    </ns2:ValueList>
                                </ns2:Slot>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a" classi-
fiedObject="document01" id="cla59" nodeRepresentation="10">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList>
                                        <ns2:Value>1.2.250.1.213.1.1.4.1</ns2:Value>
                                    </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                    <ns2:LocalizedString charset="UTF8" value="Comptes rendus" xml:lang="FR" />
                                </ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="document01" id="cla60" nodeRepresentation="N">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList>
                                        <ns2:Value>2.16.840.1.113883.5.25</ns2:Value>
                                    </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                    <ns2:LocalizedString charset="UTF8" value="Normal" xml:lang="FR" />
                                </ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classi-
fiedObject="document01" id="cla602" nodeRepresentation="18724-5">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList>
                                        <ns2:Value>2.16.840.1.113883.6.1</ns2:Value>
```

```
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="HLA" xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d" classi-
fiedObject="document01" id="cla61" nodeRepresentation="urn:ihe:iti:xds-sd:text:2008">
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>1.3.6.1.4.1.19376.1.2.3</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="documents à corps non structuré en texte brut"
xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1" classifiedOb-
ject="document01" id="cla62" nodeRepresentation="SA01">
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>1.2.250.1.71.4.2.4</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Etablissement Public de santé" xml:lang="FR"
/>
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead" classifie-
dObject="document01" id="cla63" nodeRepresentation="ETABLISSEMENT">
```

```
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>1.2.250.1.213.1.1.4.9</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Etablissement de santé" xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983" classifie-
dObject="document01" id="cla64" nodeRepresentation="34874-8">
                                    <ns2:Slot name="codingScheme">
                                        <ns2:ValueList>
                                            <ns2:Value>2.16.840.1.113883.6.1</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="CR opératoire" xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:Classification>
                                <ns2:ExternalIdentifier registryObject="document01" id="ei25" identificationScheme="urn:uuid:58a6f841-
87b3-4a3e-92fd-a8ffeff98427" value="1164485058822081751070^^^&amp;1.2.250.1.213.1.4.2&amp;ISO^INS-C^^20100522152212">
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.patientId"
xml:lang="FR" />
                                    </ns2:Name>
                                </ns2:ExternalIdentifier>
                                <ns2:ExternalIdentifier registryObject="document01" id="ei26" identificationScheme="urn:uuid:2e82c1f6-
a085-4c72-9da3-8640a32e42ab" value="1.2.250.1.999.1.1.7898.3.333.1">
                                    <!-- Envel-
op/Body/ProvideAndRegisterDocumentSetRequest/SubmitObjectsRequest/RegistryObjectList/ExtrinsicObject/ExternalIdentifier@value => Ar-
chiveTransfer/DataObjectPackage/BinaryDataObject@xml:id pour Envel-
```

```
op/Body/ProvideAndRegisterDocumentSetRequest/SubmitObjectsRequest/RegistryObjectList/ExtrinsicObject/ExternalIdentifier/Name/LocalizedString@value="XDSDocumentEntry.uniqueId" -->
                                        <ns2:Name>
                                                <ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.uniqueId" xml:lang="FR" />
                                        </ns2:Name>
                                </ns2:ExternalIdentifier>
                        </ns2:ExtrinsicObject>
                        <ns2:ExtrinsicObject id="Signature01" mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
                                <ns2:Slot name="creationTime">
                                        <ns2:ValueList>
                                                <ns2:Value>20111206110801</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="languageCode">
                                        <ns2:ValueList>
                                        <ns2:Value>art</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="legalAuthenticator">
                                        <ns2:ValueList>
                                                <ns2:Value>00B1041553^MEDECIN4155-B1^PAUL^^^^^^&amp;amp;1.2.250.1.71.4.2.1&amp;amp;ISO^D^^^IDNPS</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="serviceStartTime">
                                        <ns2:ValueList>
                                                <ns2:Value>20111206110801</ns2:Value>
                                        </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Slot name="serviceStopTime">
```

```
                                        <ns2:ValueList>
                                            <ns2:Value>20111206110801</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="sourcePatientId">
                                        <ns2:ValueList>
        <ns2:Value>1164485058822081751070^^^&amp;1.2.250.1.213.1.4.2&amp;ISO^INS-C^^20100522152212</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Name>
                                        <ns2:LocalizedString charset="UTF8" value="Source" xml:lang="FR" />
                                    </ns2:Name>
                                    <ns2:Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d" classi-
fiedObject="Signature01" id="cla65" nodeRepresentation="">
                                    <ns2:Slot name="authorPerson">
                                        <ns2:ValueList>
                                            <ns2:Value>00B1041553^MEDECIN4155-
B1^PAUL^^^^^^&amp;1.2.250.1.71.4.2.1&amp;ISO^D^^^IDNPS</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorRole">
                                        <ns2:ValueList>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorSpecialty">
                                        <ns2:ValueList>
                                            <ns2:Value>G15_10/SM26^Médecin - Qualifié en Médecine Générale
(SM)^1.2.250.1.213.1.1.4.5</ns2:Value>
                                        </ns2:ValueList>
                                    </ns2:Slot>
                                    <ns2:Slot name="authorInstitution">
                                        <ns2:ValueList>
```

```
                                        <ns2:Value>Cabinet Dr MEDECIN2154-B1
PAUL^^^^^&amp;amp;1.2.250.1.71.4.2.2&amp;amp;ISO^IDNST^^^00B104155300</ns2:Value>
                                    </ns2:ValueList>
                                </ns2:Slot>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a" classifiedOb-
ject="Signature01" id="cla66" nodeRepresentation="urn:oid:1.3.6.1.4.1.19376.1.2.1.1.1">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList>
                                        <ns2:Value>URN</ns2:Value>
                                    </ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                    <ns2:LocalizedString charset="UTF8" value="Digital Signature" xml:lang="FR" />
                                </ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="Signature01" id="cla67" nodeRepresentation="N">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>2.16.840.1.113883.5.25</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                    <ns2:LocalizedString charset="UTF8" value="Normal" xml:lang="FR" />
                                </ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="Signature01" id="cla671" nodeRepresentation="MASQUE_PS">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>1.2.250.1.213.1.1.4.13</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
```

```
                                    <ns2:LocalizedString charset="UTF8" value="Document masqué aux professionnels de santé"
xml:lang="FR" />
                                </ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f" classifiedOb-
ject="Signature01" id="cla672" nodeRepresentation="INVISIBLE_PATIENT">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>1.2.250.1.213.1.1.4.13</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name>
                                    <ns2:LocalizedString charset="UTF8" value="Document non visible par le patient" xml:lang="FR"
/>
                                </ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classifiedOb-
ject="Signature01" id="cla68" nodeRepresentation="1.2.840.10065.1.12.1.14">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>1.2.840.10065.1.12</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Source" xml:lang="FR" /></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d" classifiedOb-
ject="Signature01" id="cla69" nodeRepresentation="http://www.w3.org/2000/09/xmldsig#">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>URN</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Default Signature Style" xml:lang="FR"
/></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1" classifiedOb-
ject="Signature01" id="cla70" nodeRepresentation="SA01">
                                <ns2:Slot name="codingScheme">
```

```
                                    <ns2:ValueList><ns2:Value>1.2.250.1.71.4.2.4</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Etablissement Public de santé" xml:lang="FR"
/></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead" classifiedOb-
ject="Signature01" id="cla71" nodeRepresentation="ETABLISSEMENT">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>1.2.250.1.213.1.1.4.9</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Etablissement de santé" xml:lang="FR"
/></ns2:Name>
                            </ns2:Classification>
                            <ns2:Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983" classifiedOb-
ject="Signature01" id="cla72" nodeRepresentation="E1762">
                                <ns2:Slot name="codingScheme">
                                    <ns2:ValueList><ns2:Value>ASTM</ns2:Value></ns2:ValueList>
                                </ns2:Slot>
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="Full Document" xml:lang="FR" /></ns2:Name>
                            </ns2:Classification>
                            <ns2:ExternalIdentifier registryObject="Signature01" id="ei27" identificationScheme="urn:uuid:58a6f841-87b3-
4a3e-92fd-a8ffeff98427" value="1164485058822081751070^^^&amp;1.2.250.1.213.1.4.2&amp;ISO^INS-C^^20100522152212">
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.patientId" xml:lang="FR"
/></ns2:Name>
                            </ns2:ExternalIdentifier>
                            <ns2:ExternalIdentifier registryObject="Signature01" id="ei28" identificationScheme="urn:uuid:2e82c1f6-a085-
4c72-9da3-8640a32e42ab" value="1.2.250.1.999.1.1.7898.3.20111206120801.0">
                                <ns2:Name><ns2:LocalizedString charset="UTF8" value="XDSDocumentEntry.uniqueId" xml:lang="FR"
/></ns2:Name>
                            </ns2:ExternalIdentifier>
                        </ns2:ExtrinsicObject>
```

```
                    <ns2:Association associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember" id="association1"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Association" sourceObject="SubmissionSet01" tar-
getObject="document01">
                        <ns2:Slot name="SubmissionSetStatus">
                            <ns2:ValueList><ns2:Value>Original</ns2:Value></ns2:ValueList>
                        </ns2:Slot>
                    </ns2:Association>
                    <ns2:Association associationType="urn:oasis:names:tc:ebxml-regrep:AssociationType:HasMember" id="association2"
      objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Association" sourceObject="SubmissionSet01" tar-
getObject="Signature01">
                        <ns2:Slot name="SubmissionSetStatus">
                            <ns2:ValueList><ns2:Value>Original</ns2:Value></ns2:ValueList>
                        </ns2:Slot>
                    </ns2:Association>
                <ns2:Association associationType="urn:ihe:iti:2007:AssociationType:signs" id="association3" ob-
jectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Association" sourceObject="Signature01" tar-
getObject="SubmissionSet01">
                    <ns2:Slot name="SubmissionSetStatus">
                        <ns2:ValueList><ns2:Value>Original</ns2:Value></ns2:ValueList>
                    </ns2:Slot>
                </ns2:Association>
            </ns2:RegistryObjectList>
        </DescriptiveMetadata>
        <ManagementMetadata/>
    </DataObjectPackage>
    <ArchivalAgency>
        <Identifier>00B104155302</Identifier>
    </ArchivalAgency>
    <TransferringAgency>
        <Identifier>00B104155300</Identifier>
    </TransferringAgency>
</ArchiveTransfer>
```