Référentiel d'imputabilité

Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)- Décembre 2014 - V1.0

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Le présent document a été élaboré dans le cadre d'un processus collaboratif avec les principaux acteurs du secteur (institutionnels, utilisateurs et industriels) et le grand public.

La Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS) et l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) remercient l'ensemble des personnes et organisations qui ont apporté leur contribution à son élaboration et à sa relecture.

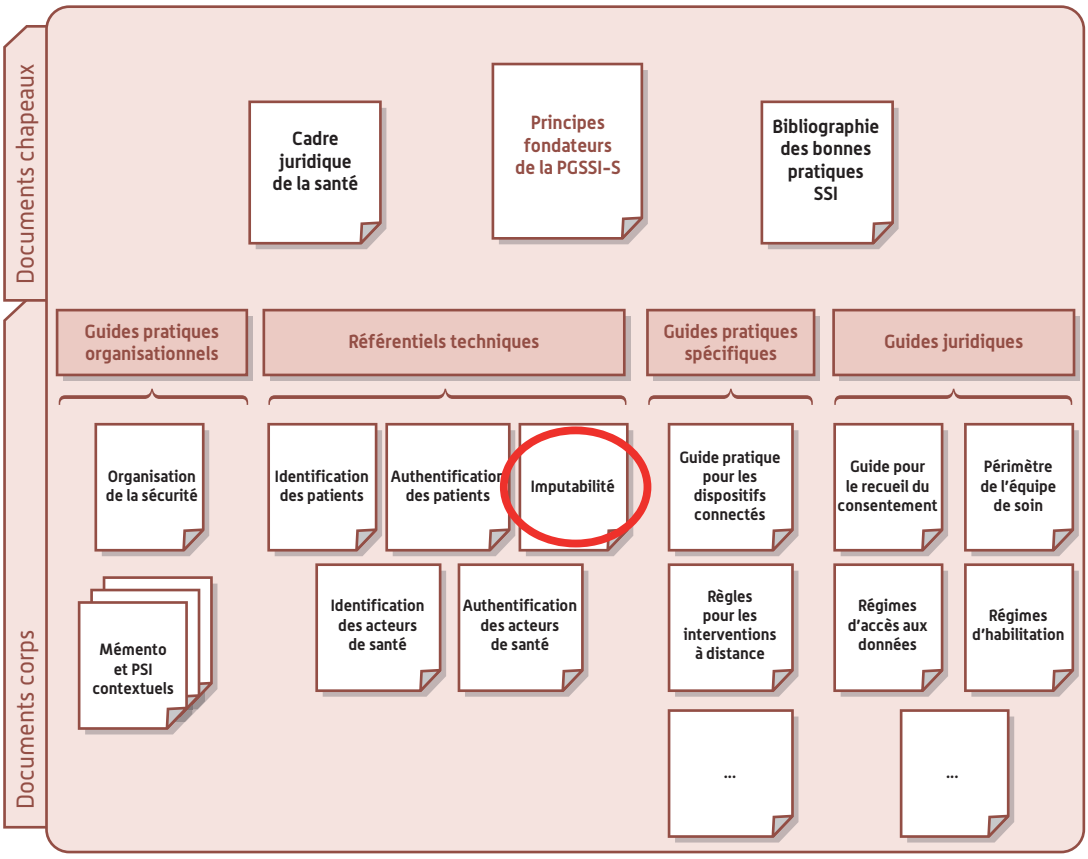
SOMMAIRE

1. OBJET DU DOCUMENT

Le présent document constitue le référentiel d'imputabilité de la Politique Générale de Sécurité des Systèmes d'Information de Santé.

Il fait partie des référentiels techniques de la PGSSI-S (cf. schéma ci-après).

FIGURE 1 : ORGANISATION DU CORPUS DOCUMENTAIRE DE LA PGSSI-S



Le présent référentiel définit les moyens utilisables pour assurer l'imputabilité des actions réalisées vis-à-vis d'un Système d'Information de Santé (SIS) afin de contrôler l'usage fait de ce système d'information.

Ce document s'adresse aux personnes impliquées dans la mise en œuvre de la politique de sécurité de systèmes d'information de santé. Il permet aux responsables de traitement de définir les dispositifs d'imputabilité adaptés aux caractéristiques du SIS dans son contexte, ou de choisir les services mettant en œuvre les dispositifs correspondants.

Il s'adresse également aux fournisseurs de produits ou de services utilisés dans le cadre de systèmes d'information de santé. En effet, ces fournisseurs doivent offrir des solutions qui mettent en œuvre ou permettre la mise en œuvre des dispositifs identifiés dans le présent référentiel.

2. PÉRIMÈTRE D'APPLICATION DU RÉFÉRENTIEL

Le cartouche ci-après présente de manière synthétique le périmètre d'application du référentiel d'imputabilité.

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Vigilance et alertes sanitaires	Recherche clinique	Enseignement et études en santé publique	
✓	✓	✓	✓	✓	✓	✓
Commentaire						
La version actuelle du présent référentiel ne prend en compte que les référentiels d'identification et d'authentification des acteurs de santé. Les éventuelles évolutions nécessaires pour étendre son périmètre aux usagers des SIS seront apportées dans une version ultérieure lorsque les référentiels d'identification et d'authentification des usagers des SIS seront finalisés.						

3. CONTEXTES OPÉRATIONNELS NÉCESSITANT UN BESOIN D'IMPUTABILITÉ

La mise en place d'un dispositif d'imputabilité capable d'établir des traces, de les conserver et de les rendre accessibles à des personnes autorisées répond principalement à deux besoins :

- vérifier l'utilisation du système d'information et augmenter la confiance des utilisateurs (ex. montrer qu'une information n'a été consultée ou modifiée que dans le cadre d'une action légitime, …) ;
- produire des preuves électroniques dans le cadre d'une action en justice.

Par ailleurs, bien que cela corresponde plus à un besoin d'évaluation (ou scoring) qu'à un besoin d'imputabilité, un dispositif d'imputabilité peut également contribuer à la détection de dysfonctionnements ou comportements « anormaux » des utilisateurs, la détermination de leur origine et des éventuels correctifs possibles.

Le besoin d'imputabilité est d'autant plus important que le système d'information est partagé par un nombre important d'utilisateurs disposant de rôles et d'habilitations distinctes augmentant le risque de mésusage.

4. CADRE JURIDIQUE

Tout responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès (Article 34 de la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés).

En outre, dans le cas de systèmes d'information hébergés manipulant des données de santé à caractère personnel, l'article R. 1111-14 2º du code de la santé publique dans sa rédaction issue du décret nº 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel dispose que l'hébergeur de données de santé, au sens de la l'article L. 1111-8 du code de la santé publique, doit notamment décrire dans son dossier de demande d'agrément :

- les moyens mis en œuvre en matière de contrôle des droits d'accès et de traçabilité des accès et des traitements ;
- les conditions de vérification du contenu des traces des accès et des traitements afin de détecter les tentatives d'effraction ou d'accès non autorisées ;
- les modalités de vérification du registre des personnes habilitées à accéder aux données hébergées tenant compte des éventuelles mises à jour.

5. DÉFINITIONS

5.1. Imputabilité

La norme ISO/CEI 27000:2009, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire, définit l'imputabilité comme la « responsabilité d'une entité par rapport à ses actions et ses décisions ».

Au sein d'un système d'information, l'imputabilité vise :
- à attribuer à chaque utilisateur ou à chaque machine l'intégralité des actions qu'il a effectuées sur le système d'information ;
- à s'assurer que chaque action est attribuée de façon univoque à l'utilisateur ou la machine l'ayant effectuée.

Toute action qui peut être imputée à une machine relève in fine de la responsabilité d'une personne physique ou morale.
Afin de couvrir la multiplicité des actions possibles sur les systèmes d'information, deux types d'imputabilité sont distinguées :
- l'imputabilité des modifications[1] ;
- l'imputabilité des consultations[2].

L'imputabilité des modifications[3] contribue à augmenter le niveau d'assurance de l'intégrité des données traitées par le système d'information en démontrant que ces données sont intègres, c'est-à-dire qu'elles n'ont été modifiées que dans le cadre d'une action légitime, par des utilisateurs ou des machines ayant le droit d'effectuer cette action.
L'imputabilité des consultations est en revanche plus complexe à mettre en œuvre. En effet, les informations, qu'un système d'information peut fournir sur une opération de consultation, peuvent permettre d'identifier l'utilisateur ayant effectué l'opération technique de consultation. Mais elles ne peuvent en revanche pas rendre compte des conditions de consultation (éventuels observateurs ayant pu consulter l'information à l'écran, consultation partielle de l'utilisateur qui n'a pas pris connaissance de l'intégralité des informations …).

5.2. Traces

Dans le cadre des systèmes d'information, une trace correspond à un ensemble de données générées pour refléter une action sur le système ainsi que son contexte d'occurrence (ex. type d'action, auteur de l'action, date et heure de l'action, données concernées…). 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.

5.2.1. Traces fonctionnelles

Les traces fonctionnelles rendent compte des actions métiers des utilisateurs ou des machines au sein du système d'information. Le contenu de ces traces est propre à chaque application et doit rendre compte de façon explicite de l'action fonctionnelle ou métier réalisée. Elles sont générées spécifiquement par l'application. Par exemple, les traces générées lors de la connexion à l'application, du dépôt d'un document dématérialisé, de la modification d'un paramètre ou de l'envoi d'un message électronique sont considérées comme des traces fonctionnelles.

1. Quel que soit le type de données modifiées : données métiers, paramétrages, code applicatif…
2. Quel que soit le type de données consultées : données métiers, paramétrages, code applicatif…
3. Dans le cadre de la PGSSI-S, la modification de données est considérée au sens large et recouvre :
   - la création de données ;
   - la mise à jour de données existantes ;
   - la suppression de données.

Exemple de trace fonctionnelle TOM (Téléprocédure Ouverte aux Mandataires)

```
2014-10-24 14:44:35,300 WARN fr.gipcps.tom.ihm.action.demandes.
SaisieServiceAction]
TITULAIRE FAISANT DEJA L'OBJET D'UNE DEMANDE :TitulaireTom
[typeIdentifiant=5, identifiant=Exemple, codeCivilite=31,nom=Dupont,
prenom1=Pierre, nomExercice=TIERS PAYANT, codeLangue1=fr,
codeProfession=*, inscritAuTableauOrdre=null, codeCategorie=null,
codeSpecialite=null, specialisation=null, orientationParticuliere1=null,
codeAttributionCompl1=null]
```

Il est à noter que toutes les fonctions d'un système d'information peuvent générer des traces fonctionnelles. Ainsi, les traces d'utilisation de la fonction de gestion des rôles et des habilitations, pour la définition d'un nouveau rôle par exemple, font partie des traces fonctionnelles.

Les traces fonctionnelles correspondent à des fonctions offertes par le système d'information. Leur interprétation ne doit pas nécessiter de compétence particulière et peut passer si nécessaire par l'utilisation d'un outil de restitution.

D'une manière générale, une action qui génère une trace fonctionnelle produit également plusieurs traces techniques au niveau des composants du système d'information utilisés pour mettre en œuvre cette action.

5.2.2. Traces embarquées

Dans le cadre de la PGSSI-S, par simplification, on appelle traces embarquées les éléments d'imputabilité intégrés aux données métiers qui sont traités par le système d'information comme des données métiers et non comme des traces. Par exemple, les métadonnées associées à un document dématérialisé identifiant l'auteur du document ou la signature d'un document dématérialisé sont considérées comme des traces embarquées.

Par nature, les traces embarquées sont des traces fonctionnelles et font partie de la traçabilité discrète (cf. section 5.3.1 sur la traçabilité discrète).

5.2.3. Traces techniques

Les traces techniques rendent compte de « l'activité » des composants logiciels et matériels utilisés par le système d'information pour assurer la fonctionnalité sollicitée par un utilisateur ou une machine. Une trace est considérée comme technique si l'action à laquelle elle se réfère est une action qui n'est significative qu'au niveau du composant technique sur lequel elle a eu lieu. Par exemple, les traces générées lors de l'établissement d'une session TLS, d'un filtrage de flux au niveau d'un firewall ou du routage d'un message électronique entre deux serveurs sont considérées comme des traces techniques.

En dehors de tout traitement destiné à améliorer leur lisibilité (par exemple, en les restituant au sein d'une piste d'audit via une IHM ergonomique), les traces techniques n'ont généralement pas de signification au niveau métier et nécessitent des compétences techniques pour être interprétées (ex. journaux de systèmes d'exploitations, de pare-feu, de base de données…).

En référence aux dispositifs techniques permettant leur génération, les traces techniques sont par extension parfois appelées journaux ou log.

5.3. Traçabilité

Dans le domaine des systèmes d'information, la traçabilité désigne la situation où l'on dispose de l'information nécessaire et suffisante pour connaitre les actions réalisées sur les données traitées par un système d'information, tout au long de leur cycle de vie.

5.3.1. Traçabilité discrète

On parle de traçabilité discrète[4] lorsque les éléments sur lesquelles repose la traçabilité sont limités et positionnés à des étapes significatives de processus entre lesquelles il est aisé de déduire les événements qui ont menés d'une étape à l'autre. La traçabilité discrète est principalement fondée sur le stockage d'informations propres à la signature électronique de données (ex. signature de jeton d'authentification) ou de documents. Elle est spécialement adaptée à l'authentification applicative ou à l'imputabilité des documents. Elle contribue fortement à prouver l'authenticité des données. Par simplification, une trace qui participe à la traçabilité discrète est appelée « trace discrète ».

5.3.2. Traçabilité continue

On parle de « traçabilité continue » lorsque les éléments sur lesquelles repose la traçabilité sont exhaustifs et produits par l'ensemble des composants du système d'information. La traçabilité continue cherche à rendre compte fidèlement de l'ensemble des actions de l'utilisateur ou de la machine sur le système d'information. Elle contribue à donner une vision exhaustive des actions sur les données. Elle nécessite donc de s'appuyer sur l'ensemble des traces générées par le système d'information.

Par simplification, une trace qui participe à la traçabilité continue est appelée « trace continue ».

5.4. Piste d'audit

Une piste d'audit est un ensemble de traces liées entre elles, afin de suivre l'enchainement des actions réalisées sur un système d'information. Elle est constituée par réconciliation des traces fonctionnelles et techniques (qu'elles soient discrètes ou continues), afin de donner une vision chronologique des différents événements tracés.

Les pistes d'audit sont parfois également appelées « traces d'audit[5] ».

5.5. Signature

La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte (cf. article 1316-4 alinéa 1er du code civil, issu de la loi nº 2000-230 du 13 mars 2000).

La signature peut être manuscrite ou électronique.

5.5.1. Signature électronique

5.5.1.1. Cadre juridique

L'article 1316-4 al.2 du code civil définit la signature électronique : elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

Deux conditions sont posées à l'**équivalence de la signature manuscrite sur support papier et de la signature électronique** (article 1316-1 du code civil) :

4. Dans le cadre de la PGSSI-S, l'adjectif « discret » est à comprendre au sens mathématique du terme, c'est à dire qui désigne quelque chose de non continu.
5. Les deux termes correspondent à la traduction de l'expression anglaise « audit trail ».

- l'identification de la personne dont émane le document ;
- la garantie de l'intégrité du procédé retenu pour l'établissement et la conservation du document.

Lorsqu'elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et la garantie de l'intégrité de l'acte, toutes les signatures électroniques sont recevables en justice.

Sous certaines conditions, la fiabilité de ce procédé est présumée :
« la fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. » (cf. article 1316-4 alinéa 2).

Il existe donc deux niveaux de validité juridique pour les signatures électroniques, dont les caractéristiques sont définies dans le décret n° 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique :
- la signature électronique « simple » ;
- la signature électronique « présumée fiable ».

En synthèse, pour bénéficier de la présomption de fiabilité, le signataire doit mettre en œuvre une signature sécurisée utilisant un dispositif sécurisé de création de signature et un certificat qualifié.

En pratique, la combinaison des rares éléments actuellement disponibles sur le marché pour répondre à l'ensemble des conditions de génération de signature présumée fiable au regard des exigences fixées par la loi n° 2000-230 du 13 mars 2000 et précisée par le décret n° 2001-272 du 30 mars 2001 est trop complexe pour être opérationnelle. Cela ne constitue toutefois pas un obstacle à l'utilisation d'un document signé sous forme électronique en qualité de preuve dans le cadre d'une action en justice : cette preuve ne pourra pas être refusée en justice au prétexte qu'elle ne résulte pas d'une procédure de signature électronique présumé fiable. Seul le niveau de fiabilité du procédé de signature électronique utilisé et sa mise en œuvre pourront éventuellement être contestés. Il appartiendra à celui qui s'en prévaut de prouver la fiabilité du dispositif de signature électronique utilisé et, tout particulièrement, sa capacité à identifier le signataire et à garantir l'intégrité de l'acte.

Concernant la génération de la signature électronique ainsi que les choix de format et d'implémentation, il est recommandé de suivre les dispositions du RGS de l'ANSSI (référence n° 2 en particulier chapitres II.1 et III de l'annexe A1 et chapitre 2.2.3 et 2.3 de l'annexe B1, référence n° 3).

5.5.1.2. Usage de la signature électronique

La mise en œuvre d'une signature électronique, sur un document (ex. signature d'un compte rendu dématérialisé) ou sur un ensemble de données (ex. signature d'éléments d'une base de données), permet à l'aide d'un procédé cryptographique de garantir l'intégrité des données signées et l'identité du signataire.

Elle peut en particulier être utilisée pour assurer l'imputabilité de modifications apportées à des données (dans le cas de la signature d'un document électronique par exemple).

5.5.2. Distinction entre signature utilisateur et scellement

Dans le cadre de la PGSSI-S, deux types de signature sont distingués :
- la signature utilisateur ;
- le scellement.

5.5.2.1. Signature utilisateur

Le terme « signature utilisateur » est utilisé pour désigner la signature électronique de données mise en œuvre avec un certificat de personne physique **dans le cadre d'un acte conscient et volontaire de la personne physique porteuse du certificat.**

La signature utilisateur est une opération dont la signification est à considérer comme équivalente à la signature manuscrite sur support papier en termes d'engagement quant au contenu de ce qui est signé. En revanche, contrairement au papier où la présentation est indissociable de l'élément signé, la présentation des données dématérialisées peut changer en fonction des interfaces et faire évoluer la perception de celles-ci. **Il est en conséquence important de considérer la restitution de l'information par le système d'information comme faisant partie du périmètre de la signature utilisateur**[6] (ex. signature d'un ensemble comprenant le document et la feuille de style de visualisation).

Si la signature utilisateur peut être considérée comme l'équivalent d'une signature manuscrite sur support papier, toute signature papier ne correspond pas forcément à un besoin de signature électronique. Par exemple, dans le cas d'un formulaire de demande de fourniture, la signature papier du formulaire peut, dans certains cas, être remplacée par une case à cocher (ou équivalent) sur un formulaire électronique. Lors de la dématérialisation d'un processus papier, il convient, pour chaque action de paraphe papier, d'évaluer si celle-ci doit se traduire par une signature utilisateur ou par une action de validation fonctionnelle (par exemple un clic sur un bouton « valider »).

5.5.2.2. Scellement

Par opposition à la signature utilisateur, le scellement est une opération de signature électronique d'un document, d'un acte ou d'une donnée technique par une personne physique ou un serveur **sans que cela soit porté à la connaissance de l'utilisateur humain qu'une opération de signature est effectuée** (ex. signature par un certificat serveur sans déverrouillage de la clé privé par une action de l'utilisateur).

5.5.2.2.1. Sursignature

La sursignature apposée sur une signature électronique existante constitue un **scellement particulier**. Elle a pour objectif de pérenniser la validité de la signature initiale et ainsi l'intégrité des documents ou données auxquels elle se rattache pendant la durée de vie du certificat utilisé et également au-delà. La pérennisation d'une signature électronique dans le temps nécessite une suite de sursignature (i.e. une sursignature à chaque fois que le certificat utilisé pour réaliser la précédente arrive en fin de durée de validité).

5.6. Force probante de l'écrit électronique

La notion de preuve par écrit a été redéfinie par la loi du 13 mars 2000 portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique. « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible ». (cf. article 1316 du code civil).

L'article 1316-1 du code civil ajoute que : « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

Ainsi, 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.

La force probante d'un écrit électronique correspond à la capacité d'utiliser cet écrit comme une preuve électronique dans le cadre d'une action judiciaire.

En pratique, la démonstration de la fiabilité de l'écrit électronique dans le cadre d'une action judiciaire dépend également fortement de l'intelligibilité des technologies mises en œuvre par les personnes en charge de caractériser sa force probante. Il est donc essentiel d'accompagner

6. Cette notion est souvent désignée par l'acronyme anglais WYSIWYG pour « What You See Is What You Get » (ce que vous voyez est ce que vous obtenez).

la mise en œuvre de mesures visant à assurer l'imputabilité par de la documentation didactique (cf. section 6.2.3 du présent document relatif à la documentation) sur fonctionnement de ces mesures et de leur apport en termes d'imputabilité ainsi que par la mise en œuvre d'outils ergonomiques d'accès aux preuves générées (ex. outils de visualisation des traces, outils de validation des signatures électroniques…).

5.6.1. La convention de preuve

Afin de reconnaitre une valeur probante à certains éléments de leur relation, les parties[7] peuvent conclure ensemble une convention de preuve.

La convention a pour objet de garantir la force probante des documents et plus généralement des données établies et produites par voie électronique en précisant les éléments techniques et de sécurité pris en compte ainsi que les effets juridiques associés. La loi du 13 avril 2000 a donné une assise juridique à ces conventions de preuve.

Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, il appartient au juge de régler les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. (cf. Article 1316-2 du code civil, créé par Loi nº 2000-230 du 13 mars 2000).

5.7. Auditabilité

Dans le cadre de la sécurisation d'un système d'information et de la couverture des risques de sécurité, il est d'usage d'exprimer le besoin en imputabilité par le critère d'auditabilité. Une fonction du système d'information est dite auditable lorsque le système d'information a la capacité d'établir sans ambigüité les circonstances de l'utilisation de cette fonction. De même, une donnée est dite auditable lorsque le système d'information a la capacité d'établir sans ambiguïté les circonstances de modification de cette donnée.

7. Par exemple les responsables de deux ou plusieurs SI ou encore chaque utilisateur avec le responsable d'un SI accessible sur Internet

6. MÉCANISMES VISANT À ASSURER L'IMPUTABILITÉ

Cette section présente les mécanismes visant à assurer l'imputabilité dans un système d'information. Parmi ces mécanismes, certains constituent des prérequis à la mise en œuvre de tout système de gestion de l'imputabilité

Il appartient au responsable de traitement de mettre en œuvre les mécanismes adaptés aux spécificités de son SI. Du choix de ces mécanismes dépend le niveau de fiabilité du système de gestion de l'imputabilité. On rappelle qu'un système de gestion d'imputabilité est considéré comme fiable 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. Dans ce système, chacune des traces aura la qualité de preuve ayant la même force probante qu'un écrit sur support papier.

Afin d'illustrer la mise en œuvre de ces mécanismes, un exemple de gestion de l'imputabilité dans le cadre du dépôt de document dans le DMP est présenté en annexe.

Les mécanismes présentés dans cette section servent de base aux paliers de l'imputabilité des SIS définis dans la section 7, chaque palier indiquant quels mécanismes mettre en œuvre pour quel périmètre.

Il est entendu que, quels que soient les mécanismes de traçabilité mis en œuvre et leurs périmètres, l'ensemble des informations tracées doit être déclaré aux utilisateurs du SI dans le respect du droit des personnes.

6.1. Prérequis

L'imputabilité d'un système d'information repose principalement sur la « réconciliation » de l'identité des utilisateurs ou des machines avec les actions datées qu'ils réalisent sur le système d'information. Elle ne peut donc être assurée sans la mise en œuvre de l'authentification des utilisateurs ou des machines et la génération automatique d'une trace datée pour les actions des utilisateurs ou des machines présentant un intérêt pour la sécurité des patients ou du SI.

6.1.1. Information des utilisateurs

La mise en œuvre de l'imputabilité constitue un traitement de données à caractère personnel devant faire l'objet de formalités auprès de la Cnil.

À cet égard, les utilisateurs doivent être informés, en application de l'article 32-I de la loi « Informatique et Libertés » :

- de l'identité du responsable de traitement ;
- de la finalité poursuivie par le traitement. Il doit être précisé si les traces peuvent être utilisées pour sanctionner, le cas échéant, les utilisateurs ;
- du caractère obligatoire du traitement ;
- des destinataires ou catégories de destinataires ;
- de ses droits, notamment son droit d'accès ;
- des éventuels transferts de données à destination d'un Etat non membre de la Communauté européenne.

6.1.2. Authentification et habilitation de l'utilisateur

La sécurité du système repose sur l'authentification et l'habilitation des utilisateurs pour :
- accorder un accès au système d'information aux seuls utilisateurs autorisés ;
- différencier les possibilités d'accès aux services du SI et aux données qu'il traite (dont les données de santé), en fonction des droits attachés à chaque catégorie d'utilisateurs ;
- pouvoir imputer les actions à leur auteur.

La qualité de l'authentification d'un acteur de santé conditionne donc la maitrise des accès au SI de santé ainsi que la force probante des preuves électroniques produites, que ce soit sous la forme de traces ou sous la forme de données métiers dématérialisées (ex. documents médicaux signés ou non). En conséquence, les paliers d'imputabilité du présent référentiel s'appuient sur les dispositifs d'authentification présentés dans le document de référence n° 1 – Référentiel d'authentification des acteurs de santé.

6.1.3. Référentiel de temps partagé

La date et l'heure de l'évènement de l'action de l'utilisateur ou de la machine sur le système d'information doivent être enregistrées si possible à la seconde près.

Dans le cas où le système d'information regroupe plusieurs sous-systèmes dont les horloges pourraient ne pas être à la même heure, toutes les machines doivent synchroniser leur horloge sur une même source.

6.2. Mise en œuvre des mécanismes visant à assurer l'imputabilité

La mise en œuvre des mécanismes visant à assurer l'imputabilité **repose sur la génération de traces fonctionnelles et techniques** qui permettent d'attribuer les actions réalisées à leur auteur mais également sur la capacité **à restituer ces traces** au sein d'une piste d'audit intelligible ainsi que sur une **documentation** claire et didactique qui présente les processus de gestion de ces traces.

6.2.1. Constitution, gestion et format des traces

6.2.1.1. Types de traces

Les approches standards pour tracer l'activité d'un utilisateur ou d'une machine sur les données du système d'information amènent à générer deux types de trace :
- Traces continues : traces **fonctionnelles et techniques** permettant de reconstituer les étapes élémentaires de chacune des actions d'un utilisateur ou d'une machine tout au long de leur activité sur le système d'information afin de prouver l'exhaustivité des actions sur les données ;
- Traces discrètes : traces **fonctionnelles** signées à des moments clés de l'activité métier afin de prouver l'authenticité des données.

Ces deux approches sont complémentaires et contribuent directement au niveau de fiabilité du système de gestion de l'imputabilité d'un SI. En effet, il est ainsi capable de reconstituer l'activité d'un utilisateur ou d'une machine sur une donnée dans une piste d'audit réconciliant les éléments de traçabilité discrète et les éléments de traçabilité continue.

Plus une piste d'audit est une combinatoire d'éléments divers et convergents, plus elle est convaincante.

6.2.1.2. Contenu des traces

6.2.1.2.1. Contenu des traces fonctionnelles

Les traces fonctionnelles sont définies lors de la conception des fonctions du système d'information. Elles consignent au minimum :

- le type d'action ;
- la date et l'heure de l'action ;
- l'identité de l'utilisateur ou de la machine ayant effectué l'action[8] ;
- le résultat de l'action (succès, erreur, refus…) ;
- si nécessaire le lien vers les données métiers concernées et d'éventuelles traces embarquées (ex. identifiant du document déposé).

Dans certains cas, ces éléments sont à compléter avec des informations de contexte, par exemple :

- l'historique des données métiers (ex. historique des versions de documents et préservation de l'intégrité de toutes les versions) ;
- le contexte de réalisation de l'action, en particulier les informations fournies à l'utilisateur lui permettant d'évaluer la portée de son action (ex : un message d'avertissement a été présenté à l'utilisateur pour l'avertir de l'effacement irréversible des données).
- Le paramétrage technique de l'application.

6.2.1.2.2. Contenu des traces techniques

Les traces techniques sont directement définies par les composants qui les génèrent et éventuellement enrichies avec l'identification du composant qui les a générées lors de leur chargement dans un outil de gestion de la preuve. En règle générale, elles consignent au minimum :

- le type d'action ;
- la date et l'heure de l'action ;
- l'utilisateur, la machine ou à défaut le composant ayant effectué l'action technique.

6.2.1.3. Conservation des traces

Le système d'information doit être en mesure de conserver l'exhaustivité et l'intégrité des traces. La confiance dans le système d'imputabilité repose sur la capacité du système d'information à protéger dans le temps l'intégrité des traces.

La conservation des traces génère des volumes de données conséquents. Les choix mis en œuvre pour assurer la traçabilité au sein d'un SI doivent tenir compte de cette volumétrie pour le stockage des traces à moyen et long terme.

Ils doivent également tenir compte des exigences relatives à la durée de conservation des traces.

6.2.1.4. Durée de conservation des traces

La traçabilité des accès aux données de santé d'une personne constitue un moyen technique de vérification du respect de ses droits et revêt dans les systèmes d'information partagés de santé, un rôle central.

Les textes relatifs à la protection des données personnelles et en particulier des données de santé ne fixent pas de règles spécifiques relatives à la durée de conservation des traces.

Dans son Guide relatif à la sécurité des données personnelles[9], la CNIL énonce que le responsable de traitement doit donc *« prévoir un système de journalisation (c'est-à-dire un enregistrement dans des «fichiers de logs») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les évènements sur une période glissante* ***ne pouvant excéder six mois*** *(sauf obligation légale, ou demande de la CNIL, de conserver ces informations pour une durée plus longue). […].*
Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que les données consultées par exemple. »

8. L'imputabilité d'un utilisateur ne doit pas être impactée par les délégations fonctionnelles dont il bénéficie au sein du système d'information. Même si la gestion des droits permet une délégation à un groupe fonctionnel, la trace générée doit permettre d'identifier la personne authentifiée et ayant réalisé l'action et non la personne lui ayant délégué les droits ou le groupe auquel elle appartient.
9. Édition 2010

Les traces techniques correspondent aux fichiers de logs identifiés dans le Guide relatif à la sécurité des données personnelles. Sauf exception, elles doivent donc être conservées sur une période dont la durée respecte les directives de la CNIL en la matière.

Les traces fonctionnelles sont inhérentes à la gestion des informations métiers. En fonction des différents enjeux qui viennent d'être rappelés et des caractéristiques du SI, il peut être opportun de conserver les traces fonctionnelles pendant la même durée que les informations métiers auxquelles elles se rapportent. La durée de conservation peut aussi être choisie en fonction du délai de prescription de l'action en responsabilité médicale.

Il est rappelé que les traces de gestion des rôles et habilitation sont des traces fonctionnelles et qu'en tant que telles, si elles font partie du périmètre de traçabilité défini (cf. section 7), elles doivent être conservées pour une durée égale à la durée de conservation des autres traces métiers auxquelles elles se rapportent. Les traces de paramétrage associées doivent suivre les mêmes règles.

En l'absence de règles propres à la durée de conservation des traces, il est de la responsabilité du responsable de traitement, sous le contrôle de la CNIL, de définir la durée de conservation des traces en tenant compte de l'environnement légal et des besoins métiers en traçabilité.

6.2.1.5. Accès aux fichiers de traces

L'accès aux fichiers de traces doit être géré de manière stricte et efficace. Seules les personnes dûment autorisées par le responsable de traitement ou par la loi doivent pouvoir y accéder en consultation. En particulier, si ces traces contiennent des données de santé à caractère personnel, elles ne peuvent être accessibles qu'aux professionnels de santé et aux personnels techniques sous la responsabilité de ces professionnels de santé, l'accès étant également limité à l'exercice strict de leur mission.

Aucune modification des traces ne doit être possible par la personne qui y accède.

6.2.1.6. Horodatage des traces

Chaque action tracée d'un utilisateur ou d'une machine sur le système d'information doit être horodatée.

La confiance que l'on peut avoir dans la mise en œuvre d'une marque temporelle d'un évènement est liée à son caractère non modifiable a posteriori. Pour répondre à cet objectif de sécurité, le système d'information peut faire appel à un service d'horodatage homologué RGS pour obtenir un jeton d'horodatage sur un lot de traces apportant un niveau de garantie élevé de la conservation des traces :

- garantie d'intégrité : le jeton d'horodatage est lié aux données par la mise en œuvre d'un scellement, ainsi toute modification des données horodatées altérerait la correspondance entre elles et le jeton d'horodatage;
- garantie d'antériorité : la datation des données électroniques permet de démontrer qu'elles existaient à partir de la date et heure certifiées ;
- garantie d'exactitude : la date et l'heure attestées par l'autorité sont établies à partir de plusieurs sources de temps fiables, protégées contre des dérive temporelles ;
- garantie de fiabilité : la date et l'heure associées aux données sont validées par la signature d'un tiers de confiance.

6.2.1.7. Format des dates et heures

Afin de permettre une réconciliation des traces, les heures et dates utilisées dans la génération des éléments d'imputabilité doivent être exprimées dans le même format, soit en temps universel coordonné (UTC)[10], soit en heure locale avec spécification du fuseau horaire tel que défini par l'ISO 8601. Le stockage du fuseau horaire est notamment recommandé lorsque les utilisateurs ou les machines sont répartis sur plusieurs fuseaux horaires et que l'heure locale a une signification

10. Anciennement également désigné sous le terme d'heure moyenne de Greenwich (GMT).

métier (ex. l'enregistrement d'identités dans un référentiel d'identité en dehors des horaires d'ouverture des autorités d'enregistrement peut permettre d'identifier comme un comportement anormal). La réconciliation des traces doit néanmoins toujours se faire sur la date et l'heure exprimées pour le même fuseau horaire. Par convention, le temps UTC est utilisé pour réconcilier les traces.

Quel que soit le format de stockage utilisé pour la date et l'heure dans les traces, l'utilisateur de l'outil de gestion de la preuve doit être informé du format des dates et heures qui lui sont présentées (i.e. UTC ou identification du fuseau horaire). Par ailleurs, si l'information est disponible, il doit également être informé du différentiel entre ces dates et heures et les dates et heures locales pour l'utilisateur ou la machine dont les actions sont tracées.

6.2.1.8. Format des traces

Afin de faciliter la réconciliation des traces dans le cadre de la génération et de la « lecture » d'une piste d'audit, il est fortement recommandé de choisir un format pivot de trace et si possible un format standard pour faciliter une lecture indépendante des traces générées.

6.2.1.9. Traçabilité des actions entre systèmes d'information

Dans le cas d'un système d'information offrant des services à d'autres systèmes d'information (ex. des interfaces pour le dépôt, la recherche et la consultation de documents de santé dématérialisé tel que le Dossier Médical Personnel ou des interfaces pour la déclaration d'identité auprès d'un référentiel d'identité), les éléments d'imputabilité sont répartis entre le système de l'utilisateur ou de la machine (ou système initiateur) et le système offrant le service (ou système cible) :

- le système initiateur produit des traces concernant l'authentification locale de l'utilisateur ou de la machine, le service accédé et les opérations réalisées ;
- le cas échéant, le système initiateur produit des traces embarquées (ex. dans le cas d'une signature de document dématérialisé pour alimenter un service de partage de document) ;
- le système cible produit des traces concernant l'authentification de l'utilisateur[11] ou de la machine, la mise en œuvre des droits d'accès et les opérations réalisées ;
- le cas échéant, le système cible stocke les traces embarquées avec les données métiers auxquelles elles sont associées.

Lorsqu'il est nécessaire de constituer une piste d'audit unique regroupant tous les éléments de traçabilité produits (par exemple, dans le cadre d'une enquête sur un incident ou dans le cadre d'une action judiciaire pour mise à disposition d'un expert), il est essentiel de bénéficier de traces interopérables, afin de permettre une réconciliation exploitable des traces. Selon la mise en œuvre des services, cette réconciliation peut être réalisée :

- préalablement à tout besoin dans le cadre d'une gestion commune des traces entre les systèmes initiateurs et le système cible, éventuellement dans le cadre d'une sous-traitance de la gestion des traces ;
- autant que de besoin pour un périmètre bien identifié (période, service, utilisateur ou machine…).

Ces types de réconciliation nécessitent un accord préalable entre les responsables des structures mettant en œuvre les systèmes d'information concernés, ad minima pour s'accorder sur le format des traces à fournir dans le cadre d'une réconciliation.

6.2.1.10. Reconnaissance mutuelle de la fiabilité des traces entre systèmes d'information

En cas d'échanges entre systèmes d'information, il peut être envisagé l'imputabilité des actions mais également l'imputabilité des traces. Chaque trace peut alors être signée par le système l'ayant générée et diffusée :

- soit à l'autre système afin qu'il la vérifie par rapport aux siennes et la conserve;
- soit à un système centralisé de gestion des traces qui vérifie la cohérence des traces qui lui sont diffusées et les conserve.

11. Cette authentification pouvant être directe ou indirecte tel que défini dans le document de référence n° 2 - Référentiel d'authentification des acteurs de santé.

En raison de son impact important sur les performances et de la volumétrie générée, il est recommandé de limiter ce type de dispositif à des cas exceptionnels pour lesquels le besoin d'imputabilité est maximal.

Si le besoin d'imputabilité ne justifie pas une mise en œuvre lourde d'échange de traces, la reconnaissance de la valeur probante des traces entre systèmes d'information peut être mise en œuvre par une convention de preuve instaurant une reconnaissance présumée des traces produites par les systèmes d'information signataires.

Une telle convention doit en particulier indiquer les conditions dans lesquelles les traces sont collectées, traitées, conservées et restituées telles que décrites dans la documentation présentée dans la section 6.2.3
Lorsqu'elles doivent être expressément acceptées par l'utilisateur, les conditions générales d'utilisation d'un service ouvert sur internet peuvent comporter les termes de la convention de preuve.

6.2.1.11. Mise en œuvre de la signature électronique

La signature électronique est un mécanisme particulier dans le cadre de l'imputabilité. Elle permet :
- de générer des « traces embarquées » en liant directement les données et les traces dans le même fichier (ex. signature électronique de documents) ;
- de contribuer à la fiabilité des traces en en garantissant l'intégrité.

6.2.1.11.1. Mise en œuvre de la signature utilisateur

En général, la signature utilisateur est mise en œuvre via l'usage d'une carte à puce et la demande du code PIN à l'utilisateur pour déverrouiller l'usage de la clé privée de signature pour chaque signature utilisateur.

D'autres moyens de signature utilisateur sont envisageables (par exemple, utilisation d'un certificat logiciel de personne physique confié à un service en mode SAAS et déverrouillé par l'échange d'un secret entre l'utilisateur et le service en mode SAAS). Ces moyens alternatifs sont cependant moins fréquents et présentent en général un niveau d'assurance moins fort en termes d'imputabilité de la signature utilisateur à son auteur.

6.2.1.11.2. Mise en œuvre du scellement

Le scellement peut être mis en œuvre au moyen de différents types de certificats électroniques par exemple :
- certificat d'un utilisateur sur support confiné sans mise en œuvre du code PIN à chaque signature ;
- certificat logiciel d'un utilisateur confié à un système d'information (par exemple dans le cadre d'une application en mode SAAS) sans mise en œuvre de mécanisme de déverrouillage par l'utilisateur de la clé privée systématiquement à chaque utilisation de celle-ci ;
- certificat généré à la volée par le système d'information de l'utilisateur (roaming de certificats) ;
- certificat serveur applicatif identifiant une machine effectuant une action ;
- certificat serveur du système d'information cible auquel est confiée la mise en œuvre de l'imputabilité.

6.2.2. Restitution des traces sous forme de piste d'audit

La confiance dans le système d'imputabilité repose non seulement sur la richesse et la pertinence des traces mais également sur la facilité de compréhension de la piste d'audit. Pour être utilisables, les traces présentées doivent être intelligibles. En particulier, leurs copies, imprimées sur papier ou affichées sur un écran doivent être lisibles et compréhensibles par des utilisateurs non spécialistes de la sécurité, notamment dans le cadre d'une action judiciaire. Afin d'en faciliter l'accès et la compréhension, il est recommandé de gérer les traces techniques et fonctionnelles sous la forme d'une piste d'audit liant les traces entre elles et les présentant de manière homogène.

Les pistes d'audit sont idéalement constituées au sein d'un outil de gestion de la preuve[12] respectant les caractéristiques suivantes :

- L'ensemble des traces produites par le système d'information est centralisé et traité au sein de l'outil de gestion de la preuve.
- La restitution des traces doit être fidèle, c'est-à-dire qu'il doit être possible de montrer que l'extraction et la mise en forme des traces conservées et sélectionnées ne sont ni partielles, ni tronquées, ni sujettes à interprétation.
- La restitution des traces sous forme de piste d'audit doit pouvoir se faire selon plusieurs axes ; au minimum par utilisateur ou machine, par type d'action réalisée, par date et heure ainsi que par cible de l'action (ex. dossier de quel patient).
- Les pistes d'audit constituées présentent des liens vers les éléments d'imputabilité intégrés aux données métiers (traçabilité embarquée). L'accès à ces éléments d'imputabilité reste bien évidemment soumis aux droits d'accès définis pour les données métiers dans lesquelles ils sont intégrés.
- La restitution des pistes d'audit doit être ergonomique afin de pouvoir être utilisée par des personnes externes à l'entité responsable du système d'information (expert judiciaire, services du Haut Fonctionnaire de Défense et de Sécurité…).
- Le bon fonctionnement de l'outil de gestion de la preuve doit être maintenu dans le temps notamment en termes de validité des traces et de leur intégrité. Idéalement, l'outil de gestion de la preuve met en œuvre un scellement des traces qui l'alimentent ainsi qu'une fonction de sursignature pour maintenir la validité de ce scellement.
- Si la traçabilité mise en œuvre s'appuie sur de la signature électronique (scellement ou signature utilisateur), l'outil peut intégrer une fonction de validation de signature électronique.

6.2.3. Documentation

L'imputabilité des actions réalisées sur le système d'information doit être documentée afin de définir :

- les éléments de traçabilité recueillis et les conditions de leur collecte ;
- les conditions de conservation et de protection dans le temps des éléments de traçabilité ;
- les modalités de restitution de ces éléments.

Une documentation adaptée du dispositif de gestion des traces permet d'augmenter la confiance dans ce dispositif, notamment en ce qui concerne l'intégrité des traces et l'imputabilité des actions effectuées. La documentation doit répondre à des critères de lisibilité, d'exhaustivité et d'autonomie afin qu'elle puisse être fournie à des non spécialistes habilités, dans le cadre de leur mission, à exploiter les traces (ex. experts judiciaires, auditeurs…).

En outre, afin d'augmenter encore le niveau de confiance dans l'outil de gestion de la preuve, il est recommandé de déposer, chez un notaire ou un huissier, l'ensemble de la documentation technique relative à l'outil de gestion de la preuve (pour chaque version de l'outil : CCTP, spécifications, plans de tests, codes sources, exécutables…). Un auditeur pourra alors vérifier la conformité de l'outil de gestion de la preuve avec la documentation de référence et valider que son fonctionnement correspond à ce qui a été annoncé et, le cas échéant, ce qui a fait l'objet d'une convention de preuve.

12. Plusieurs dénominations sont utilisées pour désigner ce genre d'outil. On parle également d'outil de gestion des traces, d'outil d'administration de la preuve ou d'outil de gestion des pistes d'audit.

7. PALIERS DE MISE EN ŒUVRE DE L'IMPUTABILITÉ DANS UN SIS

Les paliers d'imputabilité 1 à 4 apportent un niveau croissant d'assurance sur la fiabilité des traces générées par le SIS et l'intégrité d'une action légitime de dépôt de donnée par un utilisateur ou une machine.

Chaque palier présente les mesures à mettre en place en termes de prérequis, de traçabilité et de documentation du système d'information en s'appuyant sur les mesures présentées dans la section précédente.

Une vue synthétique de l'ensemble des paliers pour l'imputabilité est présentée en section 8.

7.1. Palier 1 de l'imputabilité

7.1.1. Prérequis

Authentification

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. Ce niveau est présenté dans le document de référence n° 1 - Référentiel d'authentification des acteurs de santé.

Gestion des rôles et des habilitations

Une gestion centralisée des identités, des rôles et des contrôles d'accès aux applicatifs et données du système d'information est mise en place.

La gestion des identités consiste à gérer le cycle de vie des personnes au sein de l'établissement (embauche, mutation, départ, etc..), ainsi que les impacts induits sur le système d'information (création de comptes utilisateurs, attribution de profils utilisateurs, mise en œuvre des habilitations). Cette gestion d'identité doit idéalement être faite d'un point de vue fonctionnel par des non-informaticiens (RH par exemple ou MOA) et d'un point de vue technique par des informaticiens (administrateur par exemple ou MOE). La solution mise en œuvre doit intégrer au minimum une gestion dans le temps :

- du référentiel des utilisateurs ;
- du référentiel des ressources concernées par les droits d'accès ;
- des rôles et des habilitations associées.

Il est entendu que la gestion des rôles et des habilitations est un prérequis nécessaire à la mise en œuvre du palier 1 de l'imputabilité mais qu'elle n'est pas incluse dans le périmètre des traces gérées pour ce palier.

Datation partagée par l'ensemble des composants du SIS

Les composants appartenant au même SIS doivent disposer d'horloges synchronisées entre elles de manière à ce que les traces générées sur différents composant soient cohérentes. Il est recommandé de mettre en place une synchronisation sur une horloge atomique (en passant, par exemple, par un service NTP).

Dans le cas de services mettant en œuvre plusieurs SIS, la source de la synchronisation doit être accessible par tous les SIS initiateurs ainsi que par le SIS cible. Elle peut être externe à tous les SIS impliqués ou fournie par l'un d'eux.

7.1.2. Traçabilité

7.1.2.1. Constitution des traces

Le SIS doit générer des traces fonctionnelles pertinentes au regard des enjeux de l'application ou du dispositif connecté en enregistrant au minimum les actions des utilisateurs ou des machines pour les gestes à risque sur un patient (par exemple toute opération pouvant porter atteinte à la vie ou à la santé d'un patient) ou sur ses données (ex. modification ou destruction d'un document) ainsi que les actions via des comptes privilégiés bénéficiant de droits étendus (ex. compte administrateur).

7.1.2.2. Gestion des traces

Le composant de génération des traces doit permettre l'extraction de celles-ci afin de pouvoir les conserver dans plusieurs endroits et ainsi en réduire le risque de modifications systémiques. Seules les personnes dûment autorisées doivent pouvoir accéder à des traces générées par le SIS. Les traces accessibles par les personnes autorisées peuvent être différentes en fonction de leur profil (ex. traces contenant des données de santé à caractère personnel uniquement accessibles par des professionnels de santé).

Les traces sont restituées à des non spécialistes de la sécurité au sein d'un outil de gestion de la preuve ergonomique et qui ne nécessite pas une formation importante des utilisateurs pour son usage. En particulier, le filtrage des traces doit être aisé en fonction de critères simples (ex. pour séparer les traces concernant les comptes privilégiés des traces des utilisateurs métiers).

L'outil de gestion de la preuve doit mettre en œuvre une gestion des droits d'accès telle que définie dans la section 6.2.1.5. Il doit, en outre, prévoir des mécanismes de conservation des traces en accord avec les durées de conservation de chaque type de trace (cf. section 6.2.1.4).

7.1.2.3. Format des traces

Le format des traces gérées par le SIS est libre.
Dans le cas de services mettant en œuvre plusieurs SIS, le format d'une éventuelle réconciliation entre les traces de plusieurs SIS est à définir par le SIS offrant le service. Ce format peut être différent du format interne de gestion des traces au sein du SIS. S'il y a lieu, il doit être clairement identifié dans les documents définissant la reconnaissance mutuelle de la fiabilité des traces entre les SIS telle que décrit dans la section 6.2.1.10.

7.1.3. Documentation spécifique

La gestion des identités, les mécanismes d'identification et d'authentification ainsi que la politique de gestion des rôles et des habilitations doivent être documentés de façon claire et didactique.

Un guide d'utilisation didactique de l'outil de gestion de la preuve tel que présenté dans la section 6.2.3 doit être élaboré.

7.2. Palier 2 de l'imputabilité

7.2.1. Prérequis

Les pré-requis sont les mêmes que ceux du palier 1.

7.2.2. Traçabilité

7.2.2.1. Constitution des traces

Le SIS doit gérer des traces fonctionnelles telles que définies pour le palier 1 et des traces techniques provenant au moins d'un type de composants du SIS, de préférence lié à la connexion et la déconnexion au SIS (authentification de l'utilisateur ou de la machine).

7.2.2.2. Gestion des traces

Les traces fonctionnelles sont restituées à des non spécialistes de la sécurité au sein d'un outil de gestion de la preuve ergonomique et qui ne nécessite pas une formation importante des utilisateurs pour son usage. En particulier, le filtrage des traces doit être aisé en fonction de critères simples (ex. pour séparer les traces concernant les comptes privilégiés des traces des utilisateurs métiers). L'outil de gestion de la preuve doit mettre en œuvre une gestion des droits d'accès telle que définie dans la section 6.2.1.5.

L'ensemble des traces est constitué en archives journalières regroupant les traces fonctionnelles et les traces techniques. La possibilité de consultation des traces doit être garantie, par exemple directement dans le système d'archivage, ou par réinjection dans les systèmes les ayant produites. Seules les personnes dûment autorisées doivent pouvoir accéder à des traces générées par le SIS. Les traces accessibles par les personnes autorisées peuvent être différentes en fonction de leur profil (ex. traces contenant des données de santé à caractère personnel uniquement accessibles par des professionnels de santé).

L'outil de gestion de la preuve et les archives journalières de traces doivent prévoir des mécanismes de conservation des traces en accord avec les durées de conservation de chaque type de trace (cf. section 6.2.1.4).

7.2.2.3. Format des traces

Même format que pour le palier 1 (format libre).

7.2.3. Documentation spécifique

En plus de la documentation requise pour le palier 1, l'ensemble des traitements opérés par le SIS et liés à la traçabilité doit être documenté :

- liste des composants générant des traces ;
- processus d'alimentation de l'archive journalière.

L'objectif de la documentation est d'apporter l'assurance que l'exhaustivité des actions fonctionnelles est restituée par l'outil de gestion de la preuve. Plus particulièrement, il s'agit d'apporter l'assurance qu'une absence de trace correspond bien à une absence d'action.

7.3. Palier 3 de l'imputabilité

7.3.1. Prérequis

Les pré-requis sont les mêmes que ceux du palier 1.

7.3.2. Traçabilité

7.3.2.1. Constitution des traces

Le SIS doit être en mesure de constituer une piste d'audit des actions réalisées en réconciliant les traces fonctionnelles telles que définies pour le palier 1 et les traces techniques provenant au moins d'un type de composants du SIS, de préférence lié à la connexion et la déconnexion au SIS (authentification de l'utilisateur ou de la machine).

7.3.2.2. Gestion des traces

Les traces sont constituées en archives journalières qui sont scellées. L'accès à la clé de scellement doit être géré de manière stricte et efficace. Seules les personnes dûment autorisées doivent pouvoir accéder à des traces générées par le SIS. Les traces accessibles par les personnes autorisées peuvent être différentes en fonction de leur profil (ex. traces contenant des données de santé à caractère personnel uniquement accessibles par des professionnels de santé).

Les traces doivent pouvoir être réconciliées sous forme de piste d'audit restituée à des non spécialistes de la sécurité au sein d'un outil de gestion de la preuve ergonomique et qui ne nécessite pas une formation importante des utilisateurs pour son usage. À titre d'exemple, une navigation de trace en trace selon des liens intuitifs (ex. chronologie des actions, lien de type hypertexte sur l'identité de l'utilisateur ou de la machine dans une trace fonctionnelle qui renvoie sur la trace technique de l'authentification auprès du SIS…) est une présentation ergonomique qui facilite une prise en main rapide d'un outil de gestion de gestion de la preuve.

L'outil de gestion de la preuve doit mettre en œuvre une gestion des droits d'accès telle que définie dans la section 6.2.1.5. Il doit, en outre, prévoir des mécanismes de conservation des traces en accord avec les durées de conservation de chaque type de trace (cf. section 6.2.1.4).

7.3.2.3. Format des traces

Le format des traces gérées par le SIS est libre. Il peut soit s'appuyer sur un format pivot afin de permettre une intégration aisée dans l'outil de gestion de la preuve ; soit être multiple, charge à l'outil de gestion de la preuve d'en réaliser l'interprétation pour intégration dans la piste d'audit.

Dans le cas de services mettant en œuvre plusieurs SIS, s'il y a utilisation d'un format pivot (ex. ATNA), celui-ci doit clairement être identifié dans les documents définissant la reconnaissance mutuelle de la fiabilité des traces entre les SIS telle que décrit dans la section 6.2.1.10.

7.3.3. Documentation spécifique

En plus de la documentation requise pour le palier 1, l'ensemble des traitements opérés par le SIS et liés à la traçabilité doit être documenté :

- liste des composants générant des traces ;
- processus de collecte des traces par l'outil de gestion de la preuve ;
- processus de constitution des pistes d'audit.

L'objectif de la documentation est d'apporter l'assurance que l'exhaustivité des actions est restituée par l'outil de gestion de la preuve. Plus particulièrement, il s'agit d'apporter l'assurance qu'une absence de trace correspond bien à une absence d'action sur le système.

7.4. Palier 4 de l'imputabilité

7.4.1. Prérequis

Les prérequis sont les mêmes que ceux du palier 1.

7.4.2. Traçabilité

7.4.2.1. Constitution des traces

Le SIS doit être en mesure de constituer une piste d'audit des actions réalisées en réconciliant des traces fonctionnelles et techniques telles que définies pour le palier 3. Chaque piste d'audit correspondant à une action doit au minimum comporter un élément de traçabilité discrète correspondant à la mise en œuvre d'un scellement. Par analogie maritime, on dit alors que la piste s'appuie sur un ilot de traçabilité discrète.

7.4.2.2. Gestion des traces

Les mesures mises en place pour la conservation et la restitution des traces sont identiques à celles demandées pour le palier 3.

7.4.2.3. Format des traces

Le format des traces est identique au format demandé pour le palier 3.

7.4.3. Documentation spécifique

En plus de la documentation requise pour le palier 3, la mise en œuvre du scellement au sein du SIS (création, validation) ainsi que la restitution de ce scellement par l'outil de gestion de la preuve doivent être documentées.

7.5. Palier 5 de l'imputabilité

7.5.1. Prérequis

Les prérequis sont les mêmes que ceux du palier 1 avec l'obligation de proposer la mise en œuvre d'un processus d'authentification générant une signature électronique (ex. signature d'un jeton d'authentification).

7.5.2. Traçabilité

7.5.2.1. Constitution des traces

Le SIS doit être en mesure de constituer une piste d'audit des actions réalisées en réconciliant l'ensemble des traces fonctionnelles et techniques produites par le SIS.

Par ailleurs, chaque piste d'audit correspondant à une action doit comporter un ou plusieurs éléments de traçabilité discrète dont au moins un correspond à la mise en œuvre d'une signature utilisateur.

7.5.2.2. Gestion des traces

Les mesures mises en place pour la restitution des traces sont identiques à celles du palier 4 auxquelles s'ajoute l'obligation d'horodatage du scellement des traces.

Lorsque des éléments de traçabilité discrète correspondent à des traces embarquées, la piste d'audit doit présenter un lien vers celles-ci. L'accès à ces éléments d'imputabilité embarqués reste bien évidemment soumis aux droits d'accès définis pour les données métiers dans lesquelles il est intégré.

7.5.2.3. Format des traces

Le format des traces est le même que pour le palier 4.

7.5.3. Documentation spécifique

En plus de la documentation requise pour le palier 4, la mise en œuvre de la signature utilisateur au sein du SIS (création, validation) ainsi que la restitution de cette signature utilisateur par l'outil de gestion de la preuve doivent être documentées.

8. SYNTHÈSE DES MESURES PAR PALIER

Les différentes mesures présentées pour chacun des paliers sont présentées de façon synthétique dans le tableau suivant. Pour en faciliter la lecture, les cellules ont été colorées en dégradé ; plus la couleur est sombre, plus le niveau d'imputabilité apporté par les mesures décrites dans la cellule est important.

<table>
<tr><th>Paliers</th><th>Prérequis</th><th>Génération de la piste d'audit</th><th>Conservation des traces</th><th>Restitution de la piste d'audit</th><th>Documentation spécifique</th></tr>
<tr><td>1</td><td rowspan="4">• Palier 1 du référentiel d'identification et d'authentification
• Gestion dans le temps des identités, des rôles et des habilitations
• Heure partagée par l'ensemble des composants du SIS</td><td>• Traces fonctionnelles</td><td>• Possibilité d'extraction des traces pour conservation dans des endroits multiples pour réduire le risque de modifications systémiques</td><td rowspan="2">• Outil de gestion permettant la restitution ergonomique des traces utilisable par des non spécialistes de la sécurité</td><td>• Documentation des dispositifs d'authentification, de gestion des identités, des rôles, des habilitations et des traces</td></tr>
<tr><td>2</td><td rowspan="2">• Traces fonctionnelles
• Traces techniques provenant d'au moins un type de composant du SIS</td><td>• Archives journalières regroupant l'ensemble des traces</td><td>• Idem palier 1 +
• Description des sources des traces et des processus mis en œuvre de la génération à la constitution de l'archive journalière</td></tr>
<tr><td>3</td><td rowspan="2">• Scellement quotidien des traces</td><td rowspan="2">• Idem palier 1 +
• L'outil de gestion de la preuve permet de réconcilier les traces autant que de besoin
• L'outil de gestion de la preuve gère un format pivot ou gère de nombreux formats de traces
• Guide didactique d'utilisation de l'outil de gestion de la preuve</td><td>• Idem palier 2 +
• Description des processus mis en œuvre de la génération à la réconciliation</td></tr>
<tr><td>4</td><td>• Idem palier 2 +
• Au moins un élément de traçabilité discrète basé sur un scellement serveur</td><td rowspan="2">• Idem palier 3 +
• Documentation de la mise en œuvre de la signature électronique</td></tr>
<tr><td>5</td><td>• Idem palier 1 +
• Mise en œuvre d'un processus d'authentification générant une signature électronique</td><td>• Continuité totale de la piste d'audit par réconciliation de l'ensemble des traces fonctionnelles et techniques et au moins un élément de traçabilité discrète basé sur une signature utilisateur</td><td>• Mise en œuvre du scellement et de l'horodatage de ce scellement des traces</td></tr>
</table>

9. OFFRE INDUSTRIELLE

Le présent référentiel décrit une trajectoire d'exigences portant sur l'imputabilité des acteurs de santé ayant des impacts sur les solutions techniques (produits commerciaux, produits développés par les acteurs eux-mêmes…) qui les mettent en œuvre. À ce titre, il permet aux industriels de bâtir leur propre feuille de route de développement de leurs produits et d'afficher de façon formelle la conformité de leurs produits aux paliers d'imputabilité exprimés dans le présent référentiel.

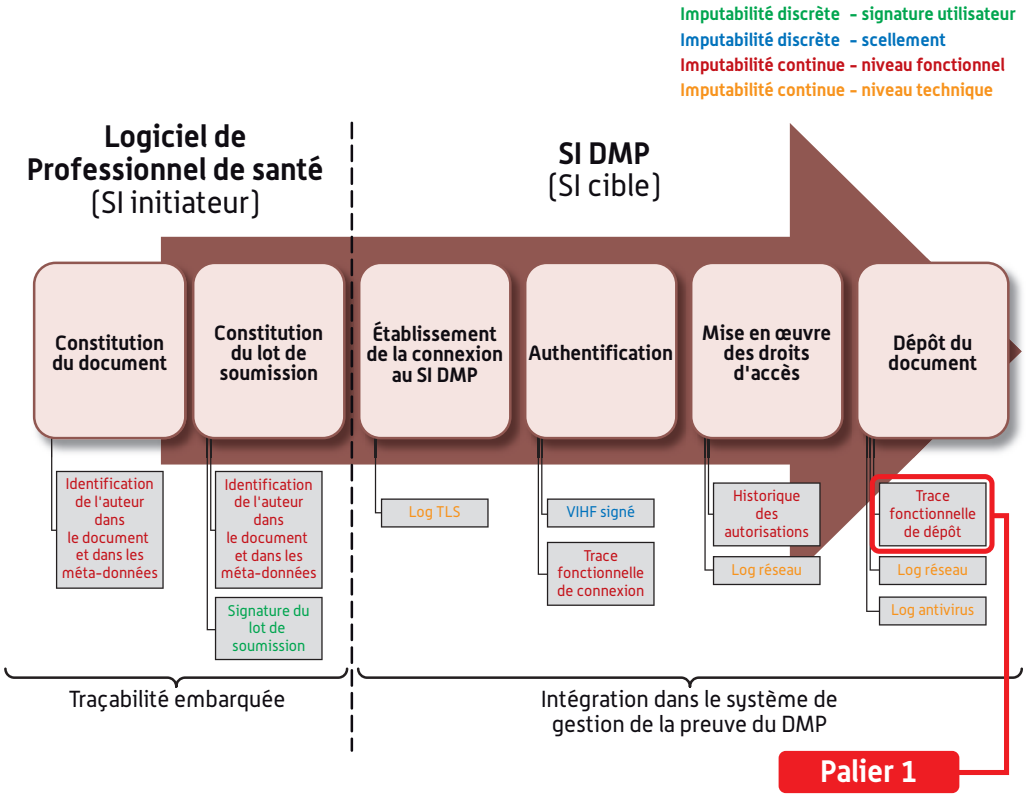
Il est à noter que dans certains cas, les structures mettant en œuvre des SIS peuvent avoir des difficultés pour identifier les traces fonctionnelles pertinentes au regard des enjeux de l'application ou du dispositif connecté (manque de disponibilité, manque de vision globale des processus métier…). Pour ce type de structures, il est recommandé aux industriels d'intégrer l'imputabilité dans leur solution technique sous la forme d'offres packagées ou pré-paramétrées générant automatiquement les traces fonctionnelles pertinentes pour les différents métiers de la santé sans que les utilisateurs n'aient à identifier lors de l'installation de la solution les opérations métiers donnant lieu à des traces fonctionnelles.

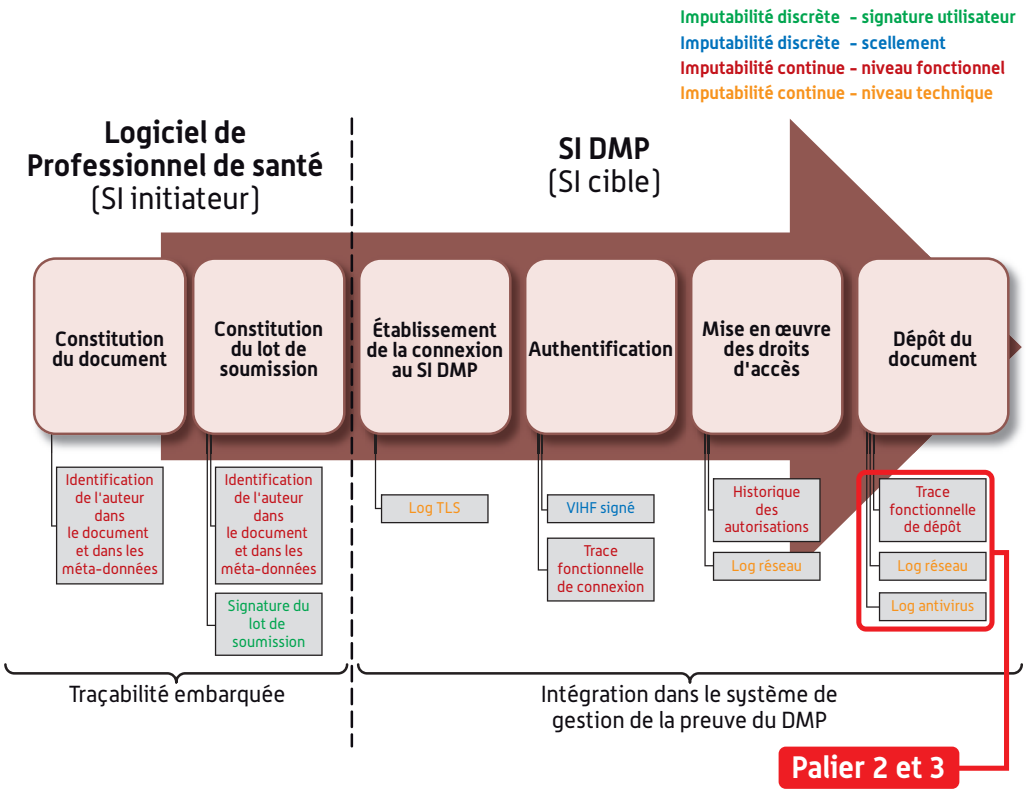
10. IMPACT SUR LES PRATIQUES PROFESSIONNELLES

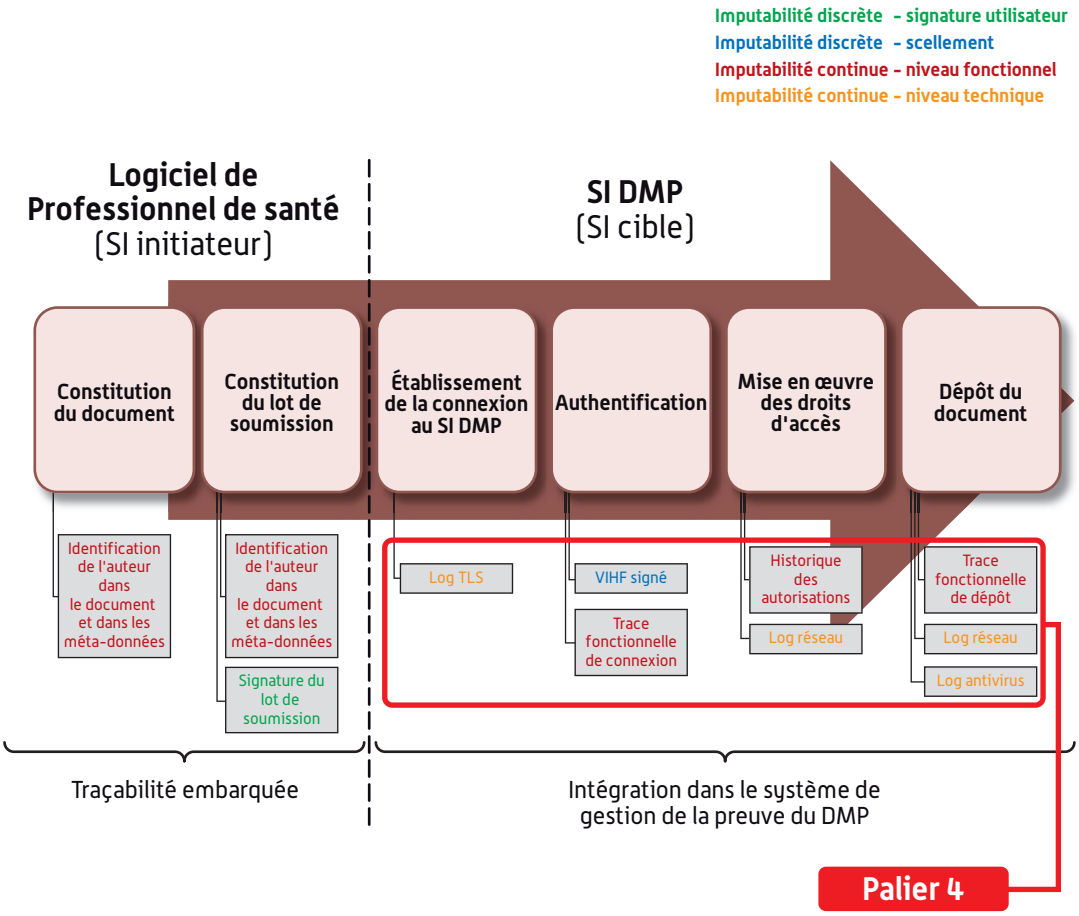
La connaissance des différents paliers, notamment l'introduction de l'usage de la signature utilisateur, permet aux acteurs de santé de préparer l'intégration de l'imputabilité de niveaux 3 et 4 dans la trajectoire d'évolution des pratiques professionnelles induite par la dématérialisation des données de santé.

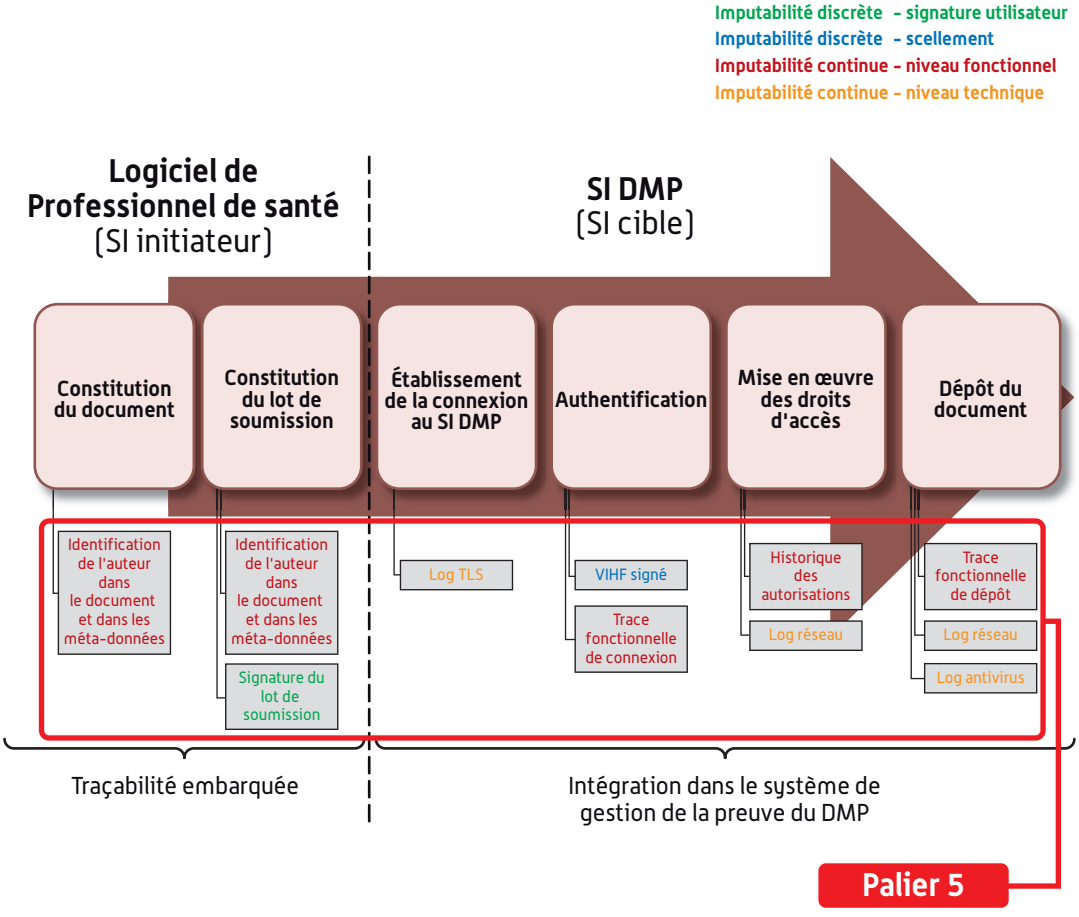
Annexe 1 : Exemple de mise en œuvre de l'imputabilité dans le DMP

L'exemple ci-dessous montre le périmètre de la mise en œuvre des différents paliers d'imputabilité sur le cas d'usage d'un dépôt de document dans le cadre DMP. Il est basé sur une cinématique simplifiée de ce cas d'usage en authentification indirecte et présente les principaux éléments de traçabilité générés lors de cette action.






Imputabilité discrète – signature utilisateur
Imputabilité discrète – scellement
Imputabilité continue – niveau fonctionnel
Imputabilité continue – niveau technique
Logiciel de Professionnel de santé (SI initiateur)
SI DMP (SI cible)
Constitution du document
Constitution du lot de soumission
Établissement de la connexion au SI DMP
Authentification
Mise en œuvre des droits d'accès
Dépôt du document
Identification de l'auteur dans le document et dans les méta-données
Identification de l'auteur dans le document et dans les méta-données
Signature du lot de soumission
Log TLS
VIHF signé
Trace fonctionnelle de connexion
Historique des autorisations
Log réseau
Trace fonctionnelle de dépôt
Log réseau
Log antivirus
Traçabilité embarquée
Intégration dans le système de gestion de la preuve du DMP
Palier 4


Imputabilité discrète – signature utilisateur
Imputabilité discrète – scellement
Imputabilité continue – niveau fonctionnel
Imputabilité continue – niveau technique
Logiciel de Professionnel de santé (SI initiateur)
SI DMP (SI cible)
Constitution du document
Constitution du lot de soumission
Établissement de la connexion au SI DMP
Authentification
Mise en œuvre des droits d'accès
Dépôt du document
Identification de l'auteur dans le document et dans les méta-données
Identification de l'auteur dans le document et dans les méta-données
Signature du lot de soumission
Log TLS
VIHF signé
Trace fonctionnelle de connexion
Historique des autorisations
Log réseau
Trace fonctionnelle de dépôt
Log réseau
Log antivirus
Traçabilité embarquée
Intégration dans le système de gestion de la preuve du DMP
Palier 5

Annexe 2 : Glossaire

Sigle / Acronyme	Signification
ATNA	Audit Trail and Node Authentication (piste d'audit et authentification des systèmes)
DMP	Dossier Médical Personnel
GMT	Greenwich Mean Time (heure moyenne de Greenwich)
IHE	Integrating the Healthcare Enterprise - standard d'interopérabilité international dans le domaine de la santé
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
PIN	Personal Identification Number (numéro d'identification personnel)
SAAS	Software As A Service (logiciel en tant que service)
SIS	Système d'Information de Santé
UTC	temps universel coordonné - l'acronyme ne reflète ni l'expression française ni l'expression anglaise (coordinated universal time) et a été choisi par l'UIT comme acronyme médian entre les deux langues
UIT	Union Internationale des Télécommunications

Annexe 3 : Documents de référence

Référence n° 1 : PGSSI-S – Référentiel d'authentification des acteurs de santé

Référence n° 2 : Référentiel général de sécurité (RGS) et ses annexes

Référence n° 3 : Mémento relatif à la signature électronique de l'ANSSI

Référence n° 4 : Corpus documentaire de la PGSSI-S (autres référentiels et guides pratiques)[13]

13. Le cas échéant, les évolutions du corpus documentaire de la PGSSI-S seront prises en compte dans des versions ultérieures de ce guide.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

RÉFÉRENTIELS / PGSSI-S – Référentiel d'imputabilité – Version V1.0 – Déc. 2014