AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Mécanismes de protection de l'intégrité des données stockées

Guide pratique technique PGSSI-S

Publication : août 2022 | *Classification : Publique* | *Version : v1.1*

SOMMAIRE

1. PREAMBULE

1.1. Objet du guide

Le présent guide définit les mécanismes, règles et recommandations de mise en œuvre relatifs à la protection de l'intégrité des données stockées au sein d'un Système d'Information (SI), et en particulier au sein de Systèmes d'Information de Santé (SIS).

L'objet de ces règles est d'apporter l'assurance que les données stockées bénéficient de mécanismes visant à les protéger de toute modification non légitime, à détecter de telles modifications si elles surviennent, et dans une telle situation, à être en mesure de restaurer les données dans leur état initial. Ces règles sont organisées en paliers de mise en œuvre, qui apportent chacun un niveau de garantie croissante de protection des données stockées.

Ce document fait partie des guides pratiques techniques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

Ce document s'adresse :

- Aux responsables de structure utilisatrice de SI ;
- Aux responsables de traitement de SIS ;
- Aux personnes agissant sous leur responsabilité, et en particulier celles impliquées dans :
  - La définition de la politique de sécurité de ces SIS et sa mise en œuvre au sein de la structure,
  - La définition des exigences et des mécanismes de sécurité dans les cahiers des charges de produits à acquérir ou de développements à réaliser par la structure,
  - L'exploitation et la maintenance de ces SIS ;
- Aux fournisseurs de produits ou de services utilisés dans le cadre de SIS. En effet, il est recommandé que les solutions proposées par ces fournisseurs mettent en œuvre les mécanismes identifiés dans le présent guide.

1.2. Périmètre d'application du guide

Le périmètre d'application de ce guide est celui fixé à l'article L1470-1 du code de la santé publique [CSP-L1470] : est concerné l'ensemble des services numériques en santé, les systèmes d'information (SI) ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités.

Au sein de ce périmètre, le présent guide décrit les règles qui permettent de préserver l'intégrité de données sensibles dématérialisées (*telles que données de santé, données relevant du secret professionnel…*), de détecter d'éventuelles pertes d'intégrité des données, et dans ce cas de restaurer les données dans leur état initial.

1.3. Limites du périmètre d'application du guide

1.3.1. Applicabilité du guide aux données plutôt qu'à l'information elle-même

Le guide s'applique à la protection de l'intégrité des données, c'est-à-dire d'une série d'octets qui représente, au niveau informatique, un ensemble d'informations particulier. Il ne traite pas de l'intégrité des informations elles-mêmes, qui relève d'aspects métiers et sémantiques.

En effet, la représentation informatique sous forme de données d'une information peut être différente selon les conventions de représentation choisies.

Par exemple, si on migre un dossier patient d'un format spécifique vers un format conforme au Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS), l'intégrité des informations du dossier devrait être préservé alors que les données correspondant à ces deux représentations seront différentes.

Des mécanismes techniques génériques de sécurité ne peuvent vérifier l'intégrité de l'information, alors qu'ils peuvent vérifier celle des données.

1.3.2. Applicabilité à l'intégrité des données pendant leur stockage uniquement

Le guide couvre uniquement la protection de l'intégrité des données informatiques pendant leur stockage. Il ne traite pas de la protection de l'intégrité des données au cours de leur acquisition (*saisie au clavier, numérisation*…) ni des traitements, transmissions et restitutions (*affichage, impression*…) dont elles font l'objet dans le cadre des processus informatisés métiers ou support de la structure.

Par exemple, l'habilitation d'un utilisateur du SI à saisir des informations dans un dossier patient informatisé en particulier et à valider ces informations conservées ensuite sous forme de données, participe à l'intégrité dans le processus métier. La traduction de cette habilitation en autorisation d'actions au sein du SI n'entre cependant pas dans le cadre de ce guide.

1.3.3. Confidentialité des données stockées

Le guide ne traite pas des aspects liés à la protection de la confidentialité éventuelle des données stockées.

1.3.4. Types de données

Les données stockées dans le SI considérées sont essentiellement :

- Des fichiers localisés dans des systèmes de fichiers :
  - Fichiers contenant des informations métiers : *fichiers bureautiques, images, vidéos, fichiers de données structurées*…
  - Fichiers contenant des informations nécessaires à l'exploitation technique du SI : *fichiers de configuration, fichiers de traces (« journaux », « logs »)* …

- Fichiers constituant des programmes informatiques : *composant du système d'exploitation, application métier, applications support…*

- Des données dans des bases de données, lesquelles s'appuient parfois elles-mêmes sur des ensembles de fichiers :
  - Base des données métiers,
  - Bases de données techniques du SI : *annuaire de sécurité du SI, « registry » …*

1.3.5. Moyens de stockage de données

Les données peuvent être stockées à l'aide de moyens matériels variés : disques durs individuels, disques SSD, baies de disques, serveurs de stockage en réseau (« NAS »), supports de données amovibles (*CD, DVD, clé USB, disque dur amovible, bande de sauvegarde…*).

Le guide ne traite pas de la protection de l'intégrité des données stockées sur des supports autres que numériques, comme les supports papiers, les microfiches…

1.3.6. Force probante

Le guide ne définit pas de mécanisme qui garantisse la force probante d'une information stockée.

En effet, garantir la force probante d'une information impose des contraintes de protection de l'intégrité des données qui la représentent.

Ces conditions ne sont cependant pas suffisantes à elles seules à la force probante qui s'inscrit dans un cadre plus large que la seule technique informatique : contexte d'élaboration de l'information, authentification de son auteur, de ses signataires éventuels, cadre légal, règlementaire (éventuellement spécifique) et/ou contractuel applicable, éléments d'information connexes (traces d'actions réalisées au cours du processus d'élaboration, autres informations qui corroborent l'information en question…).

Le « Référentiel force probante des documents de santé » [Force Probante] détaille les conditions permettant de garantir la force probante en ce qui concerne les documents de santé.

Le guide propose des mécanismes qui, combinés à des mesures de sauvegarde adéquates, permettent de garantir la préservation de l'intégrité des données stockées correspondant à l'information concernée et qui peuvent participer à fonder la force probante de l'information en tant qu'éléments de preuve.

2. DEFINITIONS ET CONCEPTS

Les documents sur lesquels se base ce guide ou qui sont cités en référence sous la forme [REF] sont listés en Annexe 1 « Documents cités en référence ».

Information

Elément de connaissance susceptible d'être représenté sous une forme adaptée pour être conservé, traité ou communiqué.

Par exemple, le dossier médical d'un patient constitue un ensemble d'informations. Ces informations peuvent indifféremment être représentées sous forme d'un dossier papier, d'un dossier patient informatisé dans un format numérique spécifique à une application de gestion informatisée des dossiers patient, ou encore d'un dossier patient informatisé dans un format numérique conforme au Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS).

Donnée

Représentation formalisée de l'information, adaptée à l'interprétation, au traitement et à la communication. La donnée est donc un conteneur porteur d'une information ou d'un fragment d'information. *(Source : Référentiel General de Gestion des Archives [R2GA])*

Pour l'exemple cité ci-dessus pour « Information », la représentation du dossier médical d'un patient dans un format numérique conforme au Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS) est une donnée. La représentation des mêmes informations dans un format numérique différent sera une donnée différente.

Intégrité

Propriété d'exactitude et de complétude d'une information. *(Source : ISO/CEI 27000:2018 [ISO27000])*

Propriété assurant qu'une information n'a pas été modifiée ou détruite de façon non autorisée. *(Source : Instruction Générale Interministérielle n°1300 [IGI1300])*

Qualité d'un document ou d'une donnée qui n'a pas été altéré. Dans le monde numérique, un document ou une donnée est réputé intègre si son empreinte à un temps t+1 est identique à l'empreinte prise à un temps t. *(Source : Référentiel General de Gestion des Archives [R2GA])*

☞ Dans le cadre de ce guide, les définitions de l'intégrité qui s'appliquent à l'information peuvent être étendues aux données et aux traitements.

Empreinte

Terme de cryptologie désignant un ensemble de bits caractéristique d'un document numérique, obtenu par une fonction de hachage. Toute modification du document numérique entraîne une empreinte différente. La comparaison d'empreintes permet de contrôler l'intégrité d'un fichier. *(Source : Référentiel General de Gestion des Archives [R2GA])*

☞ Dans le cadre de ce guide, cette définition de l'empreinte qui s'applique à l'information peut être étendue aux données.

Disponibilité

Propriété d'être accessible et utilisable à la demande par une entité autorisée. *(Source : ISO/CEI 27000:2018 [ISO27000])*

📖 Les notions d'intégrité et de disponibilité, bien que distinctes, sont néanmoins liées. En effet, l'intégrité de données ne présente un intérêt que si ces données sont disponibles (ou peuvent le redevenir). Réciproquement, garantir la disponibilité de données ne présente un intérêt que si ces données sont bien celles prévues, c'est-à-dire intègres.

📖 Il est important de noter que, même quand l'intégrité de données est préservée, il est généralement nécessaire de disposer du logiciel adéquat pour interpréter ces données et rendre réellement utilisables -et donc disponibles- les informations qu'elles représentent. La disponibilité des logiciels et des environnements, même obsolètes, nécessaires à l'utilisation des données stockées est un point essentiel à intégrer aux réflexions sur la conservation des données.

3. ENJEUX PRINCIPAUX RELATIFS A L'INTEGRITE DES DONNEES STOCKEES

Impacts de l'altération de l'intégrité de données stockées

L'activité des SIS requiert le stockage de types de données extrêmement variés dans leur nature, leurs usages, leur sensibilité.

Une altération de ces données, c'est-à-dire un défaut d'intégrité, peut, **dans les faits**, ne pas avoir d'impact immédiat, voire aucun impact du tout. C'est par exemple le cas des données d'un document administratif qui a été élaboré, lu et pris en compte, et qui ne sera jamais plus consulté. Même si une obligation légale d'intégrité de ces données à fin d'archivage public s'applique peut-être à la structure, l'altération passera probablement inaperçue et restera sans aucun effet opérationnel. Ce constat n'exonère cependant pas les structures de leurs obligations légales et réglementaires éventuelles.

A contrario, pour d'autres données, un défaut d'intégrité peut avoir des conséquences graves, comme dans le cas de données de santé à caractère personnel, qui peuvent être essentielles au traitement d'un patient et dont l'altération peut impacter très significativement la qualité du suivi des soins et des diagnostics.

La modification d'autres types de données présentes dans le SI, comme les programmes des systèmes d'exploitation informatiques ou des applications métiers, ou encore les paramétrages de ces divers programmes ou les traces d'activité du SI, peut entraîner des dysfonctionnements importants du SIS et priver les personnels des outils informatiques nécessaires à leurs activités, ou engager la responsabilité de la structure dans des litiges avec des tiers ou avec l'Etat.

Obligations et contraintes

Le cadre juridique applicable aux secteurs sanitaire, social et médico-social impose, de manière directe ou indirecte, d'assurer l'intégrité des certaines données dans de multiples contextes, tels que ceux de la valeur juridique de l'écrit électronique, de la signature électronique, du traitement de données à caractère personnel, du traitement de données de santé... Parmi les textes qui fixent ces exigences, on peut notamment citer :

- Le règlement général sur la protection des données [RGPD] et la « loi « informatique et libertés » |L78-17] ;
- Le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur [eIDAS] ;
- Les articles 1366 à 1368 et 1379 du code civil relatifs à la preuve par écrit ;
- Les articles L1111-25 à L1111-31 du code de la santé publique [CSP], relatifs aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique […] ;
- Les articles R1111-9 à R1111-11 du [CSP] relatifs à l'hébergement des données de santé à caractère personnel sur support numérique ;
- le référentiel général de sécurité [RGS] ;
- La politique de sécurité des systèmes d'information de l'état [PSSIE] et la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales [PSSI-MCAS] ;
- Les référentiels d'identification électronique des acteurs de santé de la PGSSI-S, pour les personnes morales [IE-ASPM] et pour les personnes physiques [IE-ASPP] ;
- Le référentiel « force probante des documents de santé » de la PGSSI-S [Force Probante] ;
- Le guide pratique technique « Imputabilité » de la PGSSI-S [GIMPU].

De manière générale, les structures des secteurs sanitaire, social et médico-social sont soumises à des obligations légales et règlementaires d'intégrité, comme par exemple pour :

- Les données de santé à caractère personnel ;
- Les autres données à caractère personnel ;
- De multiples données administratives (stocks pharmacie, comptabilité, gestion, actes administratifs…).

En outre, d'autres contraintes ou précautions imposent souvent à la structure, de manière indirecte, d'assurer l'intégrité d'autres types de données, comme par exemple :

- L'intégrité des logiciels et de leur paramétrage, afin de garantir que :
  - La structure est en mesure de remplir ses engagements en termes de services rendus,
  - Le SI assure correctement le contrôle d'accès aux données sensibles et, par exemple, est en mesure de garantir la confidentialité des données de santé à caractère personnel,
  - Les moyens informatiques ne peuvent être détournés de leur usage prévu, la responsabilité de la structure pouvant être engagée quant à des utilisations illicites du SI (ex. : téléchargements illégaux de films, musiques, livres numériques ou logiciels, participation à des activités de commerce illégal telles que l'hébergement pirate de site illicite de vente de médicament en ligne, participation au piratage d'autres systèmes informatiques…) ;
- L'intégrité des traces générées au sein du SI : traces techniques ou fonctionnelles des activités réalisées via son SI, collectées et conservées afin de pouvoir investiguer (ou permettre à la justice d'investiguer) en cas de dysfonctionnement ou d'utilisation malveillante du SI, soupçonnée ou avérée, et de préserver au mieux son activité et sa responsabilité.

Menaces pesant sur l'intégrité des données stockées

La protection de l'intégrité des données stockées doit permettre à la structure de se prémunir contre des menaces variables en fonction de son contexte et des données concernées :

- Les défaillances techniques du SI, ou les erreurs de manipulation commises par les utilisateurs ou les exploitants du SI ;
- Les tentatives de fraudes (de facturation, de paiement…) qui impliquent généralement du personnel interne ;
- Les tentatives de nuisance (vengeance par « sabotages » ou « vandalisme » des données) qui impliquent généralement des personnes ayant ou ayant eu un lien avec la structure (employé, fournisseur…), ou tentatives de déstabilisation des structures de santé par les mêmes moyens (par exemple dans un cadre de piratage) ;
- La délinquance informatique « ordinaires », comme les virus informatiques ;
- La cybercriminalité ciblée, qui vise un gain financier, par exemple en corrompant ou en cryptant des données sensibles et en exigeant une rançon pour fournir le moyen de restaurer les données affectées ;
- Les litiges avec des tiers dans lesquels des données (données médicales à caractère personnel par exemple) peuvent constituer des éléments déterminants dont l'intégrité peut devoir être démontrée dans un cadre juridique.

4. PRINCIPES ESSENTIELS A APPLIQUER

4.1. Principes de protection de l'intégrité des données stockées

Pour répondre aux enjeux relatifs à l'intégrité des données stockées, un ensemble de dispositions organisationnelles et techniques doit être mis en œuvre afin :

- De réduire les risques de modification accidentelle ou non légitime de données stockées ;
- D'être en mesure de détecter les modifications anormales de ces données ;
- D'avoir accès à une copie des « bonnes » données en cas de besoin ;
- Le cas échéant, de pouvoir démontrer à des tiers que les données n'ont pas été modifiées de manière indue.

La protection de l'intégrité apportée par les mécanismes proposés dans ce guide est de nature à augmenter la confiance des personnels traitants dans les données déjà existantes issues du SI et ainsi améliorer et fluidifier la prise en charge des patients (*par exemple : éviter les examens en double, alléger les questions posées aux patients…*).

4.2. Utilisation du guide et paliers d'applicabilité

Quatre paliers de protection de l'intégrité des données stockées sont proposés.

Ces paliers sont numérotés par ordre croissant. Le palier correspondant au niveau le plus élevé définit les mesures permettant la préservation et la vérification de l'intégrité des données stockées avec le niveau de confiance le plus élevé.

Le choix du palier à atteindre et des mécanismes à mettre en œuvre découle de l'analyse de risque du SI et des contraintes règlementaires applicables aux données concernées. Le cas échéant, l'atteinte de ce palier peut suivre une trajectoire croissante fondée sur les paliers de niveau moins élevé.

Des critères de sélection sont indiqués pour chaque palier :

- Des exemples de types de données pour lesquelles le palier peut être pertinent ;
- L'objectif principal poursuivi à ce palier pour la protection de l'intégrité des données stockées. Cet objectif inclut implicitement les objectifs des paliers inférieurs ;
- Les scénarios de menace pris en compte par le palier, c'est-à-dire vis-à-vis desquels les mécanismes de protections doivent apporter une réduction du risque à un niveau acceptable ;
- Les besoins de vérification de l'intégrité des données auxquels le palier vise à répondre, notamment le moment de détection d'un défaut d'intégrité éventuel et la confiance dans la détection effective de défauts d'intégrité.

Palier	Exemples de types de données concernées	Objectifs (Cumulatifs)	Scénarios de menace pris en compte (cumulatifs)	Besoins de vérification de l'intégrité des données pris en compte
1	Tout type de données	Protection limitée à l'usage des mécanismes intégrés en standard aux équipements et aux systèmes d'exploitation	► Défaillances matérielles ou logicielles ponctuelles du SI (*ex. : secteur de disque dur illisible, « plantage » d'une application au cours de la sauvegardes des données mises à jour...*) ► Erreurs d'utilisation (*ex. : extinction brutale du poste de travail sans passer par la procédure d'arrêt prévue par le système*)	► Défaut d'intégrité « détecté » au moment de l'usage des données (*ex. : erreur système de lecture des données, erreur applicative de format de fichier, données incohérentes à leur lecture par l'utilisateur…*)
2	Données sensibles, logiciels, données de configuration de logiciels, données liées à la sécurité du SI, données indispensables au fonctionnement de la structure	Protection contre les modifications accidentelles et contre les modifications malveillantes de faible niveau technique	► Erreur d'exploitation du SI (*ex. : modifications non coordonnées de configurations du système ou d'application, mise à jour intempestive de logiciels, restauration de données plus large que prévue qui écrase des données récentes valides…*) ► Défaut dans un logiciel système ou applicatifs (*ex. : écrasement de données par un script logiciel de maintenance du SI mal conçu*). ► Contamination du SI par un virus informatique générique (i.e. ne ciblant pas spécifiquement la structure) (*ex. : « installation » du virus dans les macros de fichiers bureautique, dans les fichiers de configuration du système et au sein du système de fichiers*) ► Modification malveillante de faible niveau technique de fichiers de configuration ou de données métier (*ex. : modifications manuelles par un personnel interne*). ► Installation de logiciels non autorisée.	► Détection des défauts d'intégrité, qui ne se traduisent pas nécessairement par des dysfonctionnements immédiats, si possible en amont de l'utilisation des données impactées.
3		Protection contre les modifications malveillantes	► Scénarios similaires aux scénarios de malveillance indiqués pour le palier 2, mais exécutés avec un niveau technique supérieur et un objectif ciblé à l'encontre de la structure.	► Détection des défauts d'intégrité au plus vite après leur survenance. ► Résistance renforcée des mécanismes de détection aux actions malveillantes.

Palier	Exemples de types de données concernées	Objectifs (Cumulatifs)	Scénarios de menace pris en compte (cumulatifs)	Besoins de vérification de l'intégrité des données pris en compte
4	Données sensibles pouvant être requises dans la résolution d'un litige	Capacité de production, à l'attention de tiers, d'éléments de preuve sur l'intégrité des données	▶ Déni, par une tierce partie, de la validité des données présentées par la structure dans le cadre d'une procédure en justice.	▶ Palier 3 + Capacité de démonstration à la demande de l'intégrité ou de la non-intégrité des données, avec production des éléments de preuve qui fondent la conclusion.

Il est recommandé que les structures des secteurs sanitaire, médico-social et social appliquent au minimum :

- Le palier 3 des mécanismes de protection de l'intégrité des données aux parties de leur SI qui stockent des données sensibles (données de santé à caractère personnel, autres données à caractères personnel, autres données sensibles ou essentielles à l'activité) ;
- Le palier 1 des mécanismes de protection de l'intégrité des données aux autres parties de leur SI.

Dans tous les cas, la sélection du palier adéquat doit découler des exigences de sécurité identifiées par l'analyse de risque pour le SI et les données concernées.

5. PALIERS DE MISE EN ŒUVRE DES MECANISMES DE PROTECTION DE L'INTEGRITE DES DONNEES STOCKEES

Les paliers 1 à 4 de mise en œuvre des mécanismes de protection de l'intégrité des données stockées apportent un niveau croissant d'assurance sur la vérification de l'intégrité des données et sur la disponibilité de données intègres.

Chaque palier présente les mesures à mettre en place en termes de :

- Prérequis ;
- Mécanismes de protection des données ;
- Mécanismes de vérification de l'intégrité ;
- Mécanismes permettant le retour de données corrompues à un état d'intégrité ;
- Procédures associées.

Les mesures sont cumulatives : sauf indication contraire, chaque palier doit également appliquer les mesures énoncées pour les paliers inférieurs.

Une vue synthétique de l'ensemble des paliers pour les mécanismes de protection de l'intégrité des données stockées est présentée au chapitre 6.

5.1. Palier 1 des mécanismes d'intégrité

5.1.1. Prérequis

N°	Règle
P1-A1	La structure doit définir et mettre en application une politique de sauvegarde afin de pouvoir restaurer les données si elles s'avèrent être corrompues dans les systèmes de stockage nominaux. La politique de sauvegarde doit prévoir les procédures de vérification des sauvegardes réalisées. Le guide pratique « Règles de sauvegarde des Systèmes d'Information de Santé » [Sauvegarde] peut être consulté à cette fin. La politique de sauvegarde doit fixer les durées de conservation en tenant compte du fait que des données corrompues sont susceptibles d'être sauvegardées dans cet état si la corruption n'a pas été remarquée (notamment s'il n'y a pas eu d'accès à ces données depuis leur corruption). Retrouver les données sous forme valide peut alors nécessiter le recours à des sauvegardes anciennes.

5.1.2. Mécanismes de protection des données

La protection des données au palier 1 s'appuie sur les mécanismes de contrôle d'intégrité incorporés aux composants matériels de stockage de données.

Ces mécanismes assurent, de manière transparente pour l'utilisateur, une vérification de l'intégrité et éventuellement une correction d'erreurs matérielles limitées, voire dans certains cas (*disques durs, SSD*…) un remplacement des parties défaillantes du support de données par des parties « de réserve » avant que les données ne soient perdues.

N°	Règle
P1-I1	Quand elles sont disponibles, les fonctions d'autodiagnostic et de supervision matérielle des supports de stockage de données doivent être activées (*ex. : SMART*[1]).
P1-I2	Les données qui sont destinées à ne plus être modifiées qu'exceptionnellement peuvent se voir attribuer la protection « en lecture seule » au sein du système de fichier. Cette protection, qui peut être retirée explicitement quand nécessaire, réduit les risques d'altération des données par de mauvaises manœuvres des utilisateurs.
P1-I3	Sur les supports de données amovibles qui intègrent ce mécanisme (*cartouches de sauvegarde, certaines clé USB…*), la fonction « lecture seule » peut être activée afin d'éviter une suppression ou un écrasement des données par erreur de manipulation.
P1-I4	Seules les personnes en charge de l'administration du SI doivent pouvoir disposer de droits systèmes privilégiés.
P1-I5	Dans la mesure du possible, les droits « administrateur » (ou « root » ou équivalents) ne doivent être activés que pendant la durée où ils sont réellement nécessaires à une opération d'administration du SI. Ainsi, un administrateur du SI doit, l'essentiel du temps, ne disposer que de droits d'utilisateur « normal », et pouvoir activer ses privilèges « administrateur » de façon ponctuelle pour les opérations d'administration qui le nécessitent (*ex : mécanismes « RUNAS », « Run as administator », « sudo » …*).

Les règles P1-I4 et P1-I5 réduisent le risque qu'une erreur de manipulation affecte des quantités importantes de données.

5.1.3. Mécanismes de détection et de vérification

Le Palier 1 ne s'appuie sur aucun mécanisme de vérification spécifique.

Les défauts d'intégrité sont constatés au moment de l'usage des données : erreur système de lecture des données, erreur applicative de format de fichier invalide, données incohérentes à leur lecture par l'utilisateur…

5.1.4. Mécanismes de correction des défauts d'intégrité

N°	Règle
P1-C1	Quand cette méthode est adéquate, la restauration de données dont l'origine est externe à la structure peut être réalisée à partir des supports de données initialement utilisés plutôt que par l'utilisation de sauvegarde. (*ex. : réinstallation du système d'exploitation ou des applications à partir des CD-Rom de distribution de ces logiciels*). Cette méthode requiert toutefois qu'il soit garanti que les éventuelles mises à jour appliquées aux données depuis leur version initiale seront également disponibles pour compléter la restauration, avec des délais de mise en œuvre compatibles avec les exigences de restauration de ces données (*ex : délais de téléchargement et d'application*)

[1] SMART : « Self-Monitoring, Analysis and Reporting Technology », soit « Technique d'Auto-surveillance, d'Analyse et de Rapport ». Système de surveillance du disque dur d'un ordinateur. Il permet de faire un diagnostic selon plusieurs indicateurs de fiabilité dans le but d'anticiper les erreurs sur le disque dur (et les SSD)
(Source Wikipedia - https://fr.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology *)*

5.1.5. Procédures

N°	Règle
P1-F1	Une surveillance régulière et au moins hebdomadaire du bon fonctionnement et de l'état des dispositifs de stockage de données doit être effectuée. Il est recommandé que cette vérification soit automatisée.
P1-F2	Les informations techniques de supervision du matériel (cf. règle P1-I1) doivent exploitées à l'aide de logiciels ad-hoc afin de permettre un remplacement anticipé des supports de données ou des autres composants mis en œuvre (contrôleurs, alimentations…) en cas de symptôme de défaillance prochaine.
P1-F3	Un suivi journalier des traces techniques informatiques doit être effectué afin d'identifier les erreurs survenues au sein des systèmes de fichiers et de prendre les mesures correctives nécessaires.
P1-F4	Une procédure d'alerte par les utilisateurs doit être établie et diffusée, afin qu'un utilisateur constatant une corruption potentielle des données qu'il utilise en informe rapidement ses correspondants informatiques, et puisse le cas échéant demander la restauration d'une version antérieure de ces données.

5.2. Palier 2 des mécanismes d'intégrité

5.2.1. Prérequis

N°	Règle
P2-A1	Une politique de sécurité des systèmes d'information (PSSI) cohérente avec la nature et les enjeux des données et de leurs usages prévus doit être appliquée aux systèmes d'informations qui stockent ces données. Le cas échéant, se reporter au guide « élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée » [Guide PSSI]
P2-A2	Pour les accès effectués par des personnes physiques ou morales, les mécanismes de contrôle d'accès aux données (au niveau des systèmes de fichiers, des bases de données, et/ou des applications) doivent s'appuyer sur une identification et des moyens d'identification électronique qui se conforment aux Référentiels d'identification électronique des acteurs de santé [IE-ASPM] et [IE-ASPP] de la PGSSI-S.

5.2.2. Mécanismes de protection des données

N°	Règle
P2-I1	Les mécanismes de contrôle d'accès aux données (via le système de fichier ou le système de gestion de base de données) doivent être activés afin de limiter aux seules personnes ou programmes autorisés les accès en ajout ou en suppression de données stockées.
P2-I2	Les données destinées à ne plus être modifiées peuvent se voir affecter l'attribut « immuable » (« Immutable ») si le système de fichiers supporte cette fonction, afin d'interdire tout modification du fichier et de ses attributs, sauf application d'une procédure spécifique et d'accès restreint.
P2-I3	Les fichiers de données destinés à recevoir de nouvelles données sous forme cumulative (*ex. : fichier de trace*) peuvent se voir affecter l'attribut « ajout seul » (« Append Only ») si le système de fichiers supporte cette fonction, afin d'interdire tout modification du fichier autre que des ajouts en fin de fichier, sauf application d'une procédure spécifique et d'accès restreint.
P2-I4	En l'absence de son utilisateur, tout support amovible de données (*disque dur externe, clé USB, CD, DVD, bande de sauvegarde*…) dont l'intégrité est requise doit être rangé dans un placard ou un coffre fermé à clé (ou à code). *Ex. : cas d'une clé USB sur laquelle ont été stockés de nouveaux paramétrages d'un équipement biomédical, préparés sur un poste de travail à l'aide d'un logiciel spécifique, et qui doivent être installés à l'aide de cette clé USB sur l'équipement le lendemain, pendant une courte plage durant laquelle l'équipement est disponible pour une mise à jour*. Il est recommandé de ranger de la même manière tout support de ce type dès lors qu'il n'est plus utilisé.
P2-I5	Afin de réduire les risques de corruption, voire de perte, de données pour raison matérielle, tout en bénéficiant d'autres avantages qui sortent du stricte cadre de l'intégrité des données (*remplacement facilité de supports de données, performance d'accès aux données accrues*…), des mécanisme de redondance des systèmes de stockage peuvent être mis en œuvre à l'aide de matériels ou de logiciels dédiés : disques en « miroir » (aussi appelé RAID 1), autre type de groupes de disques redondants (RAID 5, RAID 10…)[2].

[2] Voir https://fr.wikipedia.org/wiki/RAID_(informatique)

5.2.3. Mécanismes de détection et de vérification

N°	Règle
P2-V1	L'opération d'ajout de données au système de stockage doit requérir ou, à défaut, générer un identifiant unique (nom d'un fichier dans le répertoire de stockage, voire chemin d'accès complet au fichier dans le système de fichier, clé primaire de l'enregistrement concerné dans une base de données…) pour chaque donnée ajoutée au stockage.
P2-V2	L'opération d'ajout de données au système de stockage doit être refusée s'il existe déjà des données stockées associées à l'identifiant unique fourni conjointement aux données.
P2-V3	L'opération d'ajout de données au système de stockage doit intégrer une étape de calcul d'empreinte des données avant le stockage effectif des données.
P2-V4	Tout algorithme de calcul d'empreinte défini par un standard peut être utilisé, que sa préconisation d'usage se limite ou non à la détection de corruptions non intentionnelles. ☞ Les algorithmes de calcul d'empreinte qui répondent à l'exigence ci-dessus et qui sont déjà mis en œuvre au sein de la structure peuvent continuer à être utilisés. Il est néanmoins recommandé que pour toute nouvelle mise en œuvre, les mécanismes utilisés soient des fonctions de hachages telles que spécifiées par l'annexe B1 du RGS [RGS-B1] et au chapitre « Fonctions de hachage » du Guide des mécanismes cryptographiques [CRYPTO] publié par l'ANSSI.
P2-V5	L'empreinte calculée doit être stockée conjointement à l'identifiant de la donnée concernée.
P2-V6	Les empreintes et les identifiants de données associés doivent être stockés dans un dispositif de stockage si possible distinct de celui utilisé pour les données elles-mêmes. L'accès à ce dispositif de stockage doit être restreint aux opérations d'ajout, de vérification et de suppression d'empreintes et d'identifiants de données, et de comparaison d'empreintes.
P2-V7	Après l'ajout de données, une opération de vérification des données effectivement stockées, utilisant comme référence l'empreinte calculée avant le stockage, doit être effectuée. Une opération de comparaison d'empreinte entre l'empreinte nouvellement stockée et celle calculée avant le stockage, doit alors être effectuée pour valider l'opération d'ajout. En cas d'échec de l'une ou l'autre de ces vérifications, les données ajoutées doivent se voir appliquer l'opération de suppression et l'opération d'ajout doit être considérée comme invalide.
P2-V8	L'opération de vérification d'intégrité doit permettre de comparer le résultat du calcul d'empreinte de données soumises par le demandeur avec l'empreinte stockée correspondant à l'identifiant de données soumis par le demandeur.
P2-V9	Tout échec de l'opération de vérification d'intégrité doit donner lieu à une trace.
P2-V10	En cas échec de vérification d'intégrité de données déjà stockées, les données potentiellement corrompues doivent rester accessibles afin de permettre, le cas échéant, leur examen, voire leur remplacement (après suppression de la version corrompue) par une version « réparée » par les utilisateurs autorisés.
P2-V11	L'opération de comparaison d'empreinte doit permettre de comparer l'empreinte soumise par le demandeur avec l'empreinte stockée correspondant à l'identifiant de données soumis par le demandeur.
P2-V12	L'opération de suppression de données doit intégrer une étape de suppression de l'empreinte des données concernées préalablement à la suppression effective de ces données.
P2-V13	Dans le cas de stockage de fichiers, pour les systèmes d'exploitation qui la supporte, il est recommandé que la fonctionnalité de notification des actions effectuées au niveau du système de fichiers (*ex. : inotify, change notification*…) soit utilisée pour alerter en cas de changement qui n'aurait pas lieu d'être (*ex. : modification de fichier stocké, puisque les seules opérations réalisées devraient être la création, la lecture et la suppression de fichier*).

N°	Règle
P2-V14	Dans le cas de stockage de données dans une base données, pour les systèmes de gestion de base de données qui la supporte, il est recommandé que la fonctionnalité de déclencheurs (« trigger ») soit utilisée pour alerter en cas de changement qui n'aurait pas lieu d'être (*ex. : modification directe données stockées, puisque les seules opérations réalisées devraient être la création, la lecture et la suppression d'enregistrements*), voire pour bloquer ces opérations anormales.
P2-V15	Les tentatives de modification directe de données stockées qui sont détectée ou bloquées par les mécanismes de contrôle d'accès doivent être tracées. Il est recommandé que ces tentatives déclenchent une alerte.
P2-V16	Les solutions retenues pour fournir les mécanismes de détection et de vérification d'intégrité des données doivent permettre, si l'état de l'art ou l'évolution des besoins d'intégrité le requièrent, de modifier les paramètres des algorithmes cryptographiques utilisés, voire de changer d'algorithmes.

☞ Il n'est pas défini ici d'opération de mise à jour de donnée. En effet, modifier des données dont on veut justement conserver l'intégrité (i.e. qu'elles ne soient pas modifiées) n'a pas de sens. L'opération de « mise à jour des données associées à un identifiant », réalisée du point de vue utilisateur, correspond en fait à la suppression des données précédemment associées à cet identifiant, puis à l'ajout des nouvelles données pour le même identifiant.

📖 Une différence entre l'empreinte calculée lors de la vérification de données et l'empreinte attendue (par exemple celle établie lors de l'ajout des données et conservée depuis) peut traduire le fait que les données ont été corrompues, mais aussi le fait que l'empreinte de référence a elle-même été corrompue. Avec le Palier 3, les mécanismes proposés permettent de limiter cette possible ambigüité.

5.2.4. Mécanismes de correction des défauts d'intégrité

N°	Règle
P2-C1	Les empreintes et leur identifiant de données associé doivent faire partie du périmètre des informations sauvegardées.
P2-C2	Une vérification de l'intégrité des données stockées doit être effectuée avant la réalisation effective de leur sauvegarde.
P2-C3	Une vérification de l'intégrité des données sauvegardées doit être effectuée après la réalisation de la sauvegarde en utilisant comme référence les empreintes des données stockées.
P2-C4	Quand une opération de vérification de données indique que ces données ne correspondent pas à l'empreinte prévue, et qu'elles sont potentiellement corrompues, il peut être nécessaire de recourir à une version sauvegardée des données. Dans cette situation, les étapes suivantes doivent être suivies : ► L'intégrité de la version sauvegardée des données doit être vérifiée vis-à-vis de la version sauvegardée de l'empreinte correspondante ; ► L'opération de suppression de données doit être appliquée aux données potentiellement corrompues ; ► L'opération d'ajout de données au système de stockage doit être appliquée à la version sauvegardée des données ;

N°	Règle
	► L'opération de vérification d'intégrité doit être appliquée aux données nouvellement ajoutées en utilisant comme référence la version sauvegardée de l'empreinte correspondante.

5.2.5. Procédures

N°	Règle
P2-F1	Les procédures : ► D'ajout de données ; ► De vérification de l'intégrité de données ; ► De comparaison d'empreintes de données ; ► De suppression de données ; Dans le système de stockage doivent être formalisées, et doivent constituer le mode d'interaction exclusif avec les données stockées (hors simple consultation des données). Il est recommandé que ces procédures soient intégralement automatisées, c'est-à-dire que ces opérations soient uniquement réalisées à l'aide d'un programme via une interface utilisateur et/ou une interface de programmation.
P2-F2	Une procédure de vérification régulière de l'intégrité de l'ensemble des données stockées concernées par le Palier 2 (ou supérieur) doit être définie et mise en œuvre. Il est recommandé que la vérification soit réalisée avec une périodicité journalière. Il est recommandé que la procédure de vérification soit automatisée et qu'elle donne systématiquement lieu à un rapport positif ou négatif explicite.
P2-F3	Les mécanismes et procédures de protection de l'intégrité des données stockées doivent être documentés. Cette documentation doit être maintenue à jour et gérée selon les principes applicables à la documentation de sécurité fixés par le PSSI de la structure.

5.3. Palier 3 des mécanismes d'intégrité

5.3.1. Prérequis

N°	Règle
P3-A1	Les traces fonctionnelles et techniques générées dans le cadre de l'utilisation et du fonctionnement du système de stockage de données doivent se conformer au moins au Palier 2 du Référentiel d'imputabilité [Imputabilité].

5.3.2. Mécanismes de protection des données

Le Palier 3 n'impose pas de mécanisme de protection supplémentaire à ceux du Palier 2.

5.3.3. Mécanismes de détection et de vérification

N°	Règle
P3-V1	La fonction de génération d'empreinte[3] de données doit être une fonction d'authentification et d'intégrité des messages choisie et mise en œuvre conformément au chapitre « Authentification et intégrité des messages » du Guide des mécanismes cryptographiques [CRYPTO] publié par l'ANSSI. A cette fin, le mécanisme HMAC [HMAC] associé au mécanisme SHA-256 [SHS] peut être utilisé comme fonction de hachage. **(Remplace l'exigence correspondante P2-V4 des paliers inférieurs)**
P3-V2	La taille de clé utilisée par la fonction de génération d'empreinte doit être conforme à l'annexe B1 du RGS [RGS-B1] et au Guide des mécanismes cryptographiques [CRYPTO] publié par l'ANSSI. Il est recommandé d'utiliser une clé symétrique (secrète) de 256 bits pour la mise en œuvre du mécanisme HMAC-SHA256. Le mécanisme HMAC ne doit pas être utilisé avec une clé de taille inférieure à la taille de l'empreinte générée par le mécanisme de hachage retenu, soit 256 bits dans le cas de SHA-256. Cette taille de clé de 256 bits est compatible avec l'exigence, énoncée par l'annexe B1 du RGS, d'une taille minimale de 128 bits pour les clés symétriques devant être utilisées au-delà de 2020, et avec la même recommandation énoncée par [CRYPTO].
P3-V3	La clé utilisée par la fonction de génération d'empreinte doit être exclusivement réservée à cet usage.

[3] Le terme « empreinte » est utilisé ici de manière impropre pour des raisons d'homogénéité entre les paliers, puisqu'il s'agit ici d'une empreinte modifiée à l'aide d'une clé secrète.

N°	Règle
P3-V4	Les traces générées par la fonction de génération d'empreinte doivent inclure l'identifiant de données concerné et l'empreinte générée. Ces traces peuvent être utiles dans le cadre d'audit, d'investigation ou en dernier recours s'il s'avère, par exemple, que les empreintes normalement utilisées ont elles-mêmes été corrompues.
P3-V5	Quand les données stockées intègrent déjà des éléments qui permettent d'en vérifier l'intégrité (ou sont associée à ce type d'éléments) selon des mécanismes cryptographiques conformes aux exigences de ce guide, des dispositions spécifiques et simplifiées peuvent être mises en œuvre : ► En s'appuyant sur le Palier 2 de ce guide pour assurer le stockage des données et les protéger des corruptions non intentionnelles ; ► Et en s'appuyant sur les fonctions de vérification d'intégrité déjà mises en place en amont et en aval du stockage des données pour assurer leur protection contre les modifications malveillantes. *Les données qui entrent dans ce cadre correspondent, par exemple, à des informations qui ont déjà fait l'objet d'un cachet électronique (voir Palier 4), d'un horodatage électronique (voir Palier 4) ou d'une signature électronique réalisés dans le cadre fixé par le « Référentiel force probante des documents de santé » [Force Probante] et selon les modalités qu'il prévoit.*

5.3.4. Mécanismes de correction des défauts d'intégrité

N°	Règle
P3-C1	Les sauvegardes des données stockées et des empreintes associées doivent être conservées de telle sorte que ces données ne puissent être ni modifiées, ni supprimées pendant tout leur durée de conservation prévue. Cette exigence peut être satisfaite soit par une conservation « hors ligne » des données, notamment sur des supports amovibles stockés dans des locaux dédiés et sécurisés, soit par des dispositifs en ligne garantissant avec un haut niveau de confiance l'impossibilité d'accès à ces données en modification ou en suppression.
P3-C2	Il est recommandé que les personnes en charge de la gestion des systèmes de sauvegardes soient spécifiquement habilitées à cette fonction, en nombre restreint, et si possible qu'elles ne disposent pas de fonction d'administration des composants du SI qui stockent les données en question.

5.3.5. Procédures

N°	Règle
P3-F1	La gestion des clés nécessaire au fonctionnement des mécanismes cryptographiques doit être réalisée en conformité avec l'annexe B2 du RGS [RGS-B2] et avec le guide [CRYPTO].
P3-F2	Les procédures doivent inclure la gestion : ► Du changement de la clé secrète utilisée pour la génération (et la vérification) d'empreinte des données : régénération de l'ensemble des empreintes des données stockées après vérification à l'aide de l'ancienne clé, conservation de l'ancienne clé pour vérification du stock de sauvegarde en cas de besoin de restauration de donnée ; ► D'une compromission suspectée ou avérée de cette clé secrète : stratégie adoptée, moyens alternatifs permettant de vérifier si des données ont été modifiées (recours aux données sauvegardées, aux traces...).

5.4. Palier 4 des mécanismes d'intégrité

5.4.1. Prérequis

N°	Règle
P4-A1	Les traces fonctionnelles et techniques générées dans le cadre de l'utilisation et du fonctionnement du système de stockage de données doivent se conformer au moins au Palier 3 du référentiel d'imputabilité [Imputabilité].

5.4.2. Mécanismes de protection des données

Le Palier 4 n'impose pas de mécanisme de protection supplémentaire à ceux du Palier 2.

5.4.3. Mécanismes de détection et de vérification

N°	Règle
P4-V1	La fonction de génération d'empreinte[4] de données doit être : ► Soit une fonction de sécurité « cachet » telle que décrite au chapitre II.4 de l'annexe A1 du RGS [RGS-A1] si aucune information d'horodatage n'est requise dans les éléments de preuve associés aux données protégées ; ► Soit une fonction de sécurité « horodatage » conforme à la Politique d'Horodatage Type spécifiée par l'annexe A5 du RGS [RGS-A5] si une information d'horodatage est requise parmi les éléments de preuve associés aux données protégées. **(Remplace les exigences correspondantes P2-V4 et P3-V1 des paliers inférieurs)**
P4-V2	Si la structure fait appel à un tiers de confiance pour fournir les fonctions de sécurité « cachet » ou « horodatage », ce tiers doit être choisi parmi les prestataires de services de confiance qualifiés au sens du RGS (voir https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/)

5.4.4. Mécanismes de correction des défauts d'intégrité

Le Palier 4 n'impose pas de mécanisme de correction supplémentaire à ceux du Palier 3.

5.4.5. Procédures

N°	Règle
P4-F1	Les procédures doivent inclure la gestion : ► du changement de la bi-clé utilisé pour la génération (et la vérification) d'empreinte des données : régénération de l'ensemble des empreintes des données stockées après vérification à l'aide de l'ancienne clé, conservation de l'ancien certificat pour vérification du stock de sauvegarde en cas de besoin de restauration de donnée, utilisation des traces du dispositif « cachet » ou « horodatage » en cas de besoin de production d'éléments de preuve ;

[4] Le terme « empreinte » est utilisé ici de manière impropre pour des raisons d'homogénéité entre les paliers, puisqu'il s'agit ici d'une empreinte signée, éventuellement complétée par une marque de temps.

N°	Règle
	► D'une compromission suspectée ou avérée de cette bi-clé : stratégie adoptée, moyens alternatifs permettant de vérifier si des données ont été modifiées (recours aux données sauvegardées, aux traces du dispositif « cachet » ou « horodatage »…). **(Remplace l'exigence correspondante des paliers inférieurs)**

6. SYNTHESE DES MECANISMES PAR PALIER

Les différents mécanismes définis pour chaque palier sont présentés 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'intégrité des données stockées apporté par les mesures décrites dans la cellule est important.

Palier	Prérequis	Protection des données	Détection et vérification	Correction des défauts d'intégrité	Procédures
1	► Politique de sauvegarde	► Mécanismes de supervision du matériel ► Protection « lecture seule » ► Limitation des droits Administrateurs	Aucun	► Recours aux sauvegardes	► Supervision et suivi des anomalies
2	► PSSI ► Palier 1 du Référentiel d'identification ► Palier 1 du Référentiel d'authentification	► Mécanismes de contrôle d'accès aux données ► Protection des supports amovibles de données ► Systèmes de stockage redondants	► Empreinte des données par algorithme de hachage standardisé ► Surveillance des modifications directes et anormales des données	► Gestion de l'intégrité des données sauvegardées	► Formalisation et automatisation de procédures de gestion des données stockées ► Vérification régulière de l'intégrité des données stockées ► Documentation
3	► Palier 2 du Référentiel d'imputabilité ► Palier 2 du Référentiel d'authentification		► Empreinte des données par algorithme d'authentification et d'intégrité des messages tel que spécifié par le RGS	► Renforcement de la protection des sauvegardes	► Gestion des clés cryptographiques tel que spécifié par le RGS
4	► Palier 3 du Référentiel d'imputabilité		► Empreinte des données par fonction « cachet » ou « horodatage » tel que spécifié par le RGS		

Annexe 1 : Documents cités en référence

Réglementation

Renvoi	Document
[CSP]	Code de la santé publique
[CSP-L1470]	Articles L. 1470-1 à 1470-5 du code de la santé publique (issus de l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464
[eIDAS]	Règlement (UE) n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE. (« Electronic IDentification Authentication and trust Services » « eIDAS ») https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR et Décision d'exécution (UE) n°2015/1506 de la commission du 8 septembre 2015 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015D1506
[Force Probante]	PGSSI-S - Référentiel Force Probante des documents de santé Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[IGI1300]	Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, approuvée par arrêté du Premier Ministre du 9 août 2021.
[L78-17]	Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et libertés » https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/
[PGSSI-S]	Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s Corpus documentaire de la Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[PSSI-MCAS]	PSSI – MCAS : Politique de Sécurité des Systèmes d'Information pour les Ministère Chargés des Affaires Sociales https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031386468
[PSSIE]	PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat (ANSSI). https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/
[R2GA]	Référentiel General de Gestion des Archives R2GA - octobre 2013 https://francearchives.fr/fr/circulaire/R2GA_2013_10
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« règlement général sur la protection des données »), relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

	https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679 et Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680
[RGS]	Référentiel Général de Sécurité - Version 2.0 https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[RGS-A1]	Référentiel Général de Sécurité - Version 2.0 - Annexe A1 : « Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques » version 3.0 du 27 février 2014 https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[RGS-A5]	RGS v2 - Annexe A5 - Politique d'Horodatage Type https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[RGS-B1]	Référentiel Général de Sécurité - Version 2.0 - Annexe B1 : « Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » version 2.03 du 21 janvier 2014 https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[RGS-B2]	Référentiel Général de Sécurité - Version 2.0 - Annexe B2 : « Gestion des clés cryptographiques - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques » version 2.00 du 8 juin 2012
[IE-ASPM]	Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes morales] Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[IE-ASPP]	Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques] Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

Documents techniques

Renvoi	Document
[CRYPTO]	Guide des mécanismes cryptographiques, version 2.04 du 01/01/2020 ou version ultérieure en vigueur, publié par l'ANSSI https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[Guide PSSI]	Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[HMAC]	RFC 2104 - HMAC: Keyed-Hashing for Message Authentication https://www.ietf.org/rfc/rfc2104.txt
[GIMPU]	Guide pratique technique « Imputabilité » *(Précédemment nommé « Référentiel d'imputabilité »)* Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[ISO27000]	ISO/CEI 27000:2018 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire.
[Sauvegarde]	Guide pratique technique « Règles de sauvegarde des Systèmes d'Information de Santé » Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[SHS]	FIPS 180-4 - Secure Hash Standard https://csrc.nist.gov/publications/detail/fips/180/4/final

Annexe 2 : Glossaire

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANS	Agence du Numérique en Santé
CD	Compact Disc
CD-Rom	Compact Disc Read Only Memory
DVD	Digital Versatile Disc
ES	Etablissement de Santé
FIPS	Federal Information Processing Standards
HMAC	keyed-Hashing for Message Authentication Code
NAS	Network Attached Storage
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Personnel de Santé
PSSI	Politique de Sécurité des Systèmes d'Information
RAID	Redundant Array of Inexpensive Disks
RGS	Référentiel Général de Sécurité
SHA	Secure Hash Algorithm
SI	Systèmes d'Information
SIS	Systèmes d'Information de Santé
SMART	Self-Monitoring, Analysis and Reporting Technology
SSD	Solid-State Drive
USB	Universal Serial Bus