AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Règles de sauvegarde des systèmes d'information de santé

Guide pratique technique
PGSSI-S

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

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. PREAMBULE

1.1. Objet du guide

Le présent document définit les règles en matière de sauvegarde des Systèmes d'Information de Santé (SIS).

L'objet de ces règles est de garantir la pérennité des données en rendant possible la récupération des informations indispensables au fonctionnement opérationnel des SIS à la suite d'un incident ou d'un sinistre et de répondre aux demandes de restauration de données.

Ce document fait partie des guides pratiques spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S].

Il permet aux responsables de traitement de disposer d'un ensemble d'exigences pour définir l'organisation et les mesures de sauvegarde des SIS dont ils ont la responsabilité.

Ce document s'adresse :

- aux responsables de structure et, quand ils sont distincts, aux responsables de traitement ;
- aux personnes agissant sous leur responsabilité, en particulier celles impliquées dans :
  - la direction et l'exploitation du SIS,
  - les prestations d'exploitation et de maintenance des moyens de sauvegardes,
  - la mise en œuvre de la sécurité des SIS,
  - la gestion de la continuité d'activité de la structure.

Pour des raisons de facilité de lecture, dans la suite du document, le terme « responsable du SIS » est utilisé pour désigner toute personne en charge dans la mise en œuvre de tout ou partie des règles, qu'elle soit la personne responsable de la structure ou une personne agissant sous sa responsabilité.

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 applicables à la sauvegarde des données d'un SIS, prises au sens large, à savoir : systèmes d'exploitation, logiciels applicatifs, données de configuration, données techniques, données métiers dont données à caractère personnel et données de santé, documentation. En tant que tel, ce guide participe à l'élaboration des plans de continuité d'activité (PCA) et des plans de reprise d'activité (PRA) associés. Il en constitue la base des règles opérationnelles concernant la préservation des données métiers et techniques en cas d'incident ainsi que leur restauration.

1.3. Limites du périmètre d'application du guide

Ce guide pratique ne traite pas des règles applicables à l'archivage électronique[1].

2. ENJEUX RELATIFS A LA SAUVEGARDE DES SYSTEMES D'INFORMATION DE SANTE (SIS)

La sauvegarde et la capacité de restauration des données d'un SIS constituent un enjeu fort pour **garantir la continuité des activités et la disponibilité des informations non altérées associées**.

Or, ces données sont exposées à différentes menaces susceptibles de porter atteinte à leur disponibilité ou à leur intégrité, menaces pouvant être d'origine :

- Accidentelle :
  - Défaillance de support de stockage de données, incendie, dégât des eaux…
  - Défaut dans un logiciel (*système, application, base de données*…) conduisant à l'altération ou à la suppression imprévue de données,
  - Erreur dans une procédure ou dans une opération effectuée par un exploitant ou un utilisateur du SI, conduisant à l'altération ou à la suppression non souhaitée de données ;
- Malveillante :
  - Infection virale affectant divers fichiers du système ou des utilisateurs,
  - Suppression ou cryptage des données, généralement à fin de chantage (rançongiciel),
  - Ainsi que toute menace d'origine accidentelle mentionnée plus haut, pouvant être provoquée cette fois de façon volontaire.

Face à ces menaces, une organisation et un système de sauvegarde adéquatement planifiés et exploités permettent la restauration de tout ou partie des données du SIS à un état antérieur à l'incident, et une reprise de l'activité avec une perte de données limitée.

Garantir la protection des données de sauvegarde, et plus encore lorsqu'il s'agit de données à caractère personnel, est bien évidemment nécessaire pour :

- **Préserver leur confidentialité** pendant leur conservation (contrôle d'accès, chiffrement selon le cas), et à l'issue de celle-ci (inaccessibilité effective des données sur les supports de sauvegarde) ;
- **Assurer leur disponibilité et leur intégrité**, notamment en garantissant que leur contenant de stockage est pérenne et d'un accès strictement restreint ;
- **Vérifier leur intégrité** de manière régulière et a minima avant leur restauration.

Cette protection doit être assurée tant dans la gestion locale des sauvegardes qu'en cas d'externalisation de tout ou partie du service de sauvegarde (*par exemple sauvegardes externalisées chez un hébergeur de données, stockage des supports de sauvegardes hors des datacenters*…).
Les spécificités et obligations liées aux prestations d'externalisation des sauvegardes de données de santé à caractère personnel sont présentées au chapitre 4.2.

[1] Archivage électronique : Ensemble des actions, outils et méthodes mis en œuvre pour conserver à moyen et à long terme des informations numériques dans le but de les rendre accessibles et exploitables. L'archivage électronique implique d'identifier précisément les responsabilités des différents acteurs (autorité juridique, autorité d'archivage...). (Source : Référentiel General de Gestion des Archives [R2GA])

Le choix d'un système de sauvegarde (*organisation, solutions, architecture, processus…*) présente des enjeux :

- opérationnels d'exploitation du SIS :
  - les capacités de stockage nécessaires à la sauvegarde peuvent varier selon les modes de sauvegarde retenus (*par exemple : sauvegarde totale ou partielle, sauvegarde incrémentale ou différentielle entre deux sauvegardes afin de limiter la quantité de données sauvegardées à chaque fois*),
  - les contraintes opérationnelles sur les applications peuvent être différentes selon que la sauvegarde est réalisée à chaud (applications en fonctionnement pendant le déroulement de la sauvegarde) ou à froid (applications arrêtées lors du déroulement de la sauvegarde). En effet, la cohérence entre les données éventuellement liées entre elles (*index, références…*) doit être garantie dans les sauvegardes, afin que le SIS puisse fonctionner sans erreur due à des incohérences après restauration,
  - les délais acceptables de restauration pour des données à forte volumétrie peuvent justifier des techniques spécifiques de sauvegarde ;
- financiers :
  - le coût de la sauvegarde est fortement dépendant du niveau de service attendu (*fréquence des sauvegardes, durée de rétention…*) et la volumétrie qui dépend en partie du mode de stockage comme vu précédemment ;
- de sécurité au niveau du système de sauvegarde lui-même :
  - les menaces qui peuvent affecter le SIS sont également susceptibles de porter atteinte au système de sauvegarde,
  - le système de sauvegarde rassemble en un point l'ensemble des données essentielles à l'activité, tout en étant souvent le « dernier recours »[2] pour la restauration des données. Il est pour cela particulièrement sensible, et attractif pour les cybercriminels,
  - la parfaite compréhension de différentes menaces prises en compte est essentielle au choix d'un système de sauvegarde. Entre autres choses, le périmètre potentiellement affecté par chaque menace doit être explicité, afin d'éviter que la solution et/ou les données de sauvegarde soient compromises par le même incident que le SIS qu'elles doivent secourir ; s'il est évident que stocker des supports de sauvegarde dans le même bâtiment que le SIS sauvegardé est inefficace face à un risque d'incendie du bâtiment, les impacts négatifs de l'intégration du système de sauvegarde au SIS (*partage des comptes administrateurs, des « disques réseau »… afin de simplifier cette intégration et la réalisation des sauvegardes…*) sont parfois sous-estimés : *par exemple, un pirate informatique usurpant un compte administrateur du SIS pourrait très bien crypter l'ensemble des fichiers, tout en effaçant toutes les sauvegardes antérieures via l'interface de la solution de sauvegarde accessible directement aux administrateurs*.

Il est donc important de choisir les solutions de sauvegarde adaptées et de définir le système de sauvegarde sous tous ses aspects. Ces étapes préalables permettent de répondre aux enjeux de sécurité mais également aux enjeux financiers dans un souci d'efficience économique, en cohérence avec le besoin opérationnel des acteurs de santé.

☞ **Le système de sauvegarde constitue le dernier recours pour rétablir le système d'information dans diverses situations d'incident critique. Pour pouvoir remplir son rôle dans de telles circonstances, il doit être conçu et maintenu avec soin, et faire l'objet d'un haut niveau de protection de façon continue.**

[2] Des solutions alternatives de reconstitution de données sont parfois possibles, mais sont généralement bien plus couteuses et plus lentes, et souvent peu efficaces si elles n'ont pas été pensées et préparées avant le sinistre.

3. DEFINITIONS ET CONCEPTS

Les règles proposées par ce guide sont issues des bonnes pratiques en matière de SSI ainsi que des documents de référence listés en Annexe 1.

Les documents cités en référence sous la forme [REF] sont détaillés en Annexe 2.

3.1. Sauvegarde

- **Sauvegarde** : opération qui consiste à dupliquer et à conserver de manière sécurisée des données contenues dans un système informatique (*ex. données métier, données techniques, paramétrage et réglage du système et des applications…*) et/ou de logiciels présents sur ce système afin d'assurer leur disponibilité sous une forme non altérée (intégrité) et ainsi la possibilité de les réinstaller sur un système informatique après un incident, une erreur de manipulation ou un acte de malveillance portant atteinte à leur disponibilité ou à leur intégrité. Le terme anglais *backup* est largement usité dans le milieu informatique pour désigner une sauvegarde.
- La sauvegarde est asynchrone : elle est distincte des techniques de réplication ou de « clusterisation » qui permettent quant à elles de réaliser des copies en temps réel des données des plateformes de production, et assurent une reprise d'activité, voire l'absence d'interruption, en cas de dysfonctionnement de la plateforme nominale, d'incident dans le datacenter où elle est hébergée ou d'indisponibilité du réseau qui permet de l'atteindre. Il est important de noter qu'en cas de perte d'intégrité de données, les techniques de réplication qui se baseraient sur des données altérées ne permettraient pas à elles seules de récupérer les données non altérées. En effet, les techniques de réplication traitent en priorité la problématique de l'indisponibilité de la plateforme nominale, alors que la sauvegarde répond dans ce contexte particulier à la problématique de perte d'intégrité. La sauvegarde participe également à la restauration d'une plateforme opérationnelle en cas de panne de la plateforme nominale s'il n'y a aucun système redondant disponible.
- La sauvegarde se distingue de la synchronisation de données réalisée à des fins de fonctionnement en mode déconnecté. Dans ce cas, la synchronisation est utilisée pour permettre le fonctionnement d'un système quand il est déconnecté du réseau. On peut citer par exemple la synchronisation des PC nomades, mais aussi des dispositifs tels qu'une station d'anesthésie.
- En termes de finalité, la notion de sauvegarde doit être différenciée des notions fonctionnelles d'archivage d'une part et de gestion de versions qui peut être proposée par une solution de gestion électronique de documents d'autre part, qui l'une comme l'autre n'entrent pas dans le périmètre de ce guide pratique.
- En particulier, la notion de sauvegarde répondant au besoin opérationnel de continuité d'activité et de préservation de données intègres, la durée de conservation des sauvegardes devrait a priori rester limitée, d'un ordre de grandeur correspondant typiquement à celui des évolutions techniques (mises à jour) du SIS. Si un besoin de « retour en arrière » de données sur une plus longue période était exprimé, une solution plus pertinente à ce besoin serait probablement :
  - soit, s'il s'agit d'une problématique métier, la mise en place d'une solution de gestion électronique de documents ou d'archivage électronique ;
  - soit, s'il s'agit d'une problématique technique, la mise en place d'un mécanisme de vérification régulière de l'intégrité des données (voir le Guide des mécanismes de protection de l'intégrité des données stockées [MPIDS]), qui permet d'alerter sur une perte d'intégrité de données et de prendre les actions correctives requises (dont probablement la restauration de sauvegardes).

3.2. Types de sauvegarde

Ce guide distingue les différents types de sauvegarde décrits ci-après.

3.2.1. Sauvegarde centralisée

On désigne par « système de sauvegarde centralisée » tout système de sauvegarde destiné à assurer la sauvegarde et la restauration d'un ensemble d'autres composants du SIS, via un réseau informatique.

3.2.2. Sauvegarde locale

On désigne par « système de sauvegarde locale » tout système de sauvegarde destiné à assurer la sauvegarde et la restauration d'un composant spécifique du SIS. Ce système s'appuie généralement sur un logiciel qui s'exécute intégralement sur le composant à sauvegarder, et qui sauvegarde les données dans un espace de stockage local dédié sur un support de stockage fixe ou amovible.

Les systèmes de sauvegarde locale sont généralement nécessaires aux équipements qui ne sont pas connectés à un réseau et ne peuvent bénéficier des services d'un système de sauvegarde centralisée. Ils sont également utilisés dans d'autres situations d'architecture informatique simple, par exemple quand toutes les données métier sont conservées sur un serveur de fichiers partagé, qui est dès lors le seul composant dont les données métier nécessitent d'être sauvegardées régulièrement.

3.2.3. Sauvegarde (centralisée ou locale) hors ligne

Dans ce guide, on désigne par « système de sauvegarde hors ligne » tout système de sauvegarde centralisée ou locale dans lequel les supports de stockage des sauvegardes sont des supports physiques amovibles, connectés au composant en charge des sauvegardes uniquement pendant la durée des opérations de sauvegarde, de vérification ou de restauration. La connexion des supports de sauvegarde requiert de la part de l'opérateur une action physique locale ne pouvant pas être réalisée par voie uniquement logicielle.

La raison de ce dernier critère est de bien exclure de la définition les solutions de sauvegarde potentiellement vulnérables à une cyberattaque menée à distance, et consistant à altérer, crypter ou effacer l'ensemble des sauvegardes stockées pour interdire tout recours contre une attaque visant l'altération, le cryptage (rançongiciel) ou l'effacement de l'ensemble des données d'un SIS.

Ainsi, une sauvegarde sur un disque dur amovible connecté uniquement pour la sauvegarde et déconnecté ensuite est considéré comme étant une sauvegarde hors ligne. A l'inverse, une sauvegarde effectuée sur une bande dont la manipulation et le stockage sont réalisés par un automate (« bandothèque ») entièrement piloté par logiciel par la solution de sauvegarde n'est pas considérée par le présent guide comme étant une sauvegarde hors ligne.

3.2.4. Sauvegarde (centralisée ou locale) en ligne

Dans ce guide, on désigne par « système de sauvegarde en ligne » tout système de sauvegarde centralisée ou locale qui n'est pas un système de sauvegarde hors ligne.

3.3. Restauration

- **Restauration** : action consistant à utiliser des sauvegardes pour rétablir un système d'information qui a été altéré dans un état antérieur à l'altération.

3.4. Plan de sauvegarde

- **Plan de sauvegarde** : document(s) spécifiant les principes généraux de sauvegarde, les différents périmètres de données devant être sauvegardées et les besoins et contraintes de sauvegarde associés, ainsi que les procédures liées à la sauvegarde et à la restauration pour chaque périmètre identifié.

4. PRINCIPES ESSENTIELS A APPLIQUER

4.1. Principes de sécurité

Les quatre principes de sécurité suivants doivent être appliqués dans la démarche de définition et de mise en œuvre de la sauvegarde :

- identification du besoin ;
- formalisation des procédures ;
- adoption de pratiques conformes à l'état de l'art ;
- restauration et contrôle.

4.1.1. Identification du besoin de sauvegarde et de restauration

Afin de définir les processus et dispositifs de sauvegarde adaptés, il est indispensable de mener une analyse préalable du besoin de sauvegarde incluant notamment :

- la définition du périmètre métier concerné ;
- le niveau de service attendu pour la sauvegarde et la restauration : perte admissible de données non sauvegardées entre deux sauvegardes, délai maximum de restauration des données, durée de conservation des sauvegardes, besoins d'intégrité et de confidentialité des sauvegardes.

Cette analyse du besoin permet de choisir la solution la plus adaptée en termes d'efficacité et de coût.

4.1.2. Formalisation des procédures

Il est nécessaire de définir une méthode permettant d'élaborer et de faire vivre le plan de sauvegarde en :

- identifiant exhaustivement les composants logiciels systèmes et applicatifs, et les données à sauvegarder ;
- formalisant les procédures de sauvegarde, de restauration et de gestion des supports de sauvegarde ;
- intégrant ce processus dans le processus général suivi pour tout nouveau projet de SIS, ou pour toute évolution de SIS.

4.1.3. Adoption de pratiques conformes à l'état de l'art

Le présent document identifie les bonnes pratiques conformes à l'état de l'art. Il met en avant certaines règles applicables spécifiquement à la sauvegarde des serveurs, des postes de travail, ou à l'externalisation de la sauvegarde.

Il reste toutefois important de maintenir une veille continue sur les bonnes pratiques en matière de sauvegarde, et sur les solutions utilisées afin de garantir leur sécurité et leur utilisation optimale.

4.1.4. Restauration et contrôle

Il est essentiel d'avoir l'assurance permanente que le dispositif de sauvegarde et restauration permet de revenir à un état stable antérieur.

A cette fin, le document identifie les règles et les points de contrôle qui permettent de s'assurer que les sauvegardes restent utilisables dans le temps, en particulier par des tests de restauration réguliers.

4.2. Cas de l'externalisation de la sauvegarde

Au vu de la complexité de la mise en œuvre de dispositifs de sauvegardes répondant aux besoins et aux contraintes, et efficaces par rapport aux moyens dont dispose le responsable, le recours à un prestataire peut être une solution adaptée.

Les avantages offerts par une telle solution sont multiples :

- expertise pour la formalisation des procédures de sauvegarde et de restauration ;
- garantie accrue de cohérence et d'exhaustivité du périmètre sauvegardé ;
- conformité aux bonnes pratiques de sauvegardes et de restauration ;
- contractualisation des engagements ;
- coût du service optimisé avec la possibilité de bénéficier de services étendus comme la sauvegarde permanente sous forme de synchronisation de données.

Le recours à une prestation de sauvegarde externalisée doit être réalisé dans des conditions qui permettent au responsable de rester maître des données sauvegardées et de leur protection. Le prestataire doit s'engager sur des contrats de service clairement identifiés en particuliers en termes de périmètre d'intervention, de délai maximal de restauration, de fréquence de sauvegarde, de durée de conservation et de restitution des données.

Enfin, il convient de rappeler qu'en cas d'externalisation des sauvegardes de données de santé à caractère personnel[3] entrant dans le cadre de l'article L1111-8 du code de la santé publique relatives à l'hébergement de données de santé à caractère personnel [CSP-L1111-8], le responsable est tenu de faire appel à un hébergeur de données de santé à caractère personnel certifié à cet effet[4], conformément aux dispositions de ce même article.

Les modalités de certification des hébergeurs de données de santé à caractère personnel sont fixées par l'article R1111-10 du code de la santé publique [CSP].

Les informations relatives à la certification des hébergeurs de données de santé et le Référentiel de certification HDS - Exigences et contrôles [REFHDS] peuvent être consultées sur le site de l'Agence du Numérique en Santé (ANS) (voir [REFHDS]).

[3] Article R1111-9 du [CSP] : « Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes : […] la sauvegarde des données de santé. »

[4] Article R1111-8-8.II du [CSP] : « Les responsables de traitement […] qui confient l'hébergement de données de santé à caractère personnel à un tiers, s'assurent que celui-ci est titulaire du certificat de conformité mentionné au II de l'article L. 1111-8. »

5. REGLES DE SECURITE APPLICABLES A LA SAUVEGARDE

Les règles de sécurité présentées ci-après représentent les exigences prioritaires à respecter dans le cadre des sauvegardes.

Dans certains cas, le responsable du SIS a recours à un hébergeur de données de santé à caractère personnel pour l'exécution de règles inhérentes au service de sauvegarde. Les règles dont l'exécution peut être confiée à un prestataire sont identifiées dans les tableaux ci-après dans la colonne « Délégable à un prestataire ».

5.1. Règles d'organisation

N°	Règle	Délégable à un prestataire
O1	Seul le personnel ou les sociétés désignées par le responsable du SIS doivent intervenir sur les processus de sauvegarde et de restauration des applications et des données. Les données sensibles (à quel titre que ce soit) de la structure dont la sauvegarde est prévue dans le plan sauvegarde doivent être sauvegardées sous le contrôle de ces personnes. La réalisation de ces sauvegardes ne doit pas être confiée à d'autres utilisateurs.	Non
O2	Lorsque cela est permis par la charte utilisateur en vigueur dans l'établissement ou justifié auprès de l'établissement de santé, les utilisateurs du SIS sont autorisés à effectuer, sous leur propre responsabilité, des sauvegardes et restaurations des données de leur poste de travail dans le respect du présent guide, de la PSSI et de la charte utilisateur de la structure responsable du SIS concerné.	Non

5.2. Plan de sauvegarde

N°	Règle	Délégable à un prestataire
P1	Toute mise en production d'un nouveau système, d'une nouvelle application ou d'un nouvel espace de données doit faire l'objet d'une réflexion préalable sur sa sauvegarde et d'un ajout au plan de sauvegarde, validé par le responsable du SIS.	Non
P2	Le plan de sauvegarde doit identifier les besoins opérationnels métiers et d'infrastructure de sauvegarde et de restauration au minimum sur les points suivants : ► définition du périmètre (systèmes, applications, données techniques, données de configuration, données métiers, documentation) à sauvegarder ; ► définition du degré de confidentialité des sauvegardes ; ► définition du degré de garantie d'intégrité des sauvegardes ; ► perte de données maximale admissible (PDMA) qui correspond au laps de temps maximal et admissible entre deux sauvegardes (perte des données modifiées pendant cette durée) ; ► durée maximale admissible de restauration des données (DMARD) qui correspond au temps entre la demande de restauration et la restauration effective des données[5] ; ► durée de conservation maximale des sauvegardes ;	Non

[5] Dans le cadre des plans de continuité et des plans de reprise d'activité, cette notion est intégrée dans la durée maximale d'interruption admissible (DMIA) qui correspond au temps entre le début de l'indisponibilité et la restauration effective, c'est-à-dire la DMARD à laquelle s'ajoute la durée entre le début d'une indisponibilité de données et sa détection ainsi que le délai entre la détection de l'indisponibilité et la demande de restauration des données.

N°	Règle	Délégable à un prestataire
	► autres besoins ou contraintes associées. Remarque : la conservation des sauvegardes sur des longues périodes, au-delà de 2 ans, nécessite des précautions pour permettre une restauration en cas de besoin : régénération des sauvegardes pour s'affranchir de l'obsolescence des supports et du matériel de sauvegarde, et le cas échéant conservation de l'environnement matériel et logiciel. *(Cependant, voir fin du chapitre 3.1 au sujet de la pertinence ou non de l'utilisation de la sauvegarde pour la préservation de données sur de telles durées).*	
P3	Le plan de sauvegarde doit identifier, en conformité avec le périmètre de sauvegarde défini (règle P2), l'ensemble des composants informatiques du SIS à inclure dans les processus de sauvegardes (*ex. : données, bases de données, applications et système d'exploitation des serveurs, des matériels médicotechniques, des équipements réseaux, serveurs, baies de stockage, serveurs de fichiers et postes de travail…*). Le plan de sauvegarde doit prendre en compte les liens entre les composants afin d'assurer la cohérence des données lors des sauvegardes et restaurations. En particulier, lors des montées de versions de logiciel, il est important de sauvegarder la version précédente du logiciel afin de s'assurer de la compatibilité entre les données et le logiciel en cas de restauration. Cette prise en compte peut notamment être réalisée par la sauvegarde conjointe de briques d'infrastructure complètes, éventuellement associée à des plans de virtualisation du SI.	Oui
P4	Pour chaque composant informatique identifié, le plan de sauvegarde doit décrire les procédures de sauvegardes à mettre en œuvre : ► nature (*fichiers, base de données…*) et localisation des données à sauvegarder ; ► type de sauvegarde : sauvegarde complète, sauvegarde partielle, sauvegarde différentielle, sauvegarde incrémentale ; ► outil de sauvegarde utilisé ; ► périodicité de la sauvegarde (*journalière, hebdomadaire, mensuelle…*), périodicité de rotation des sauvegardes (*exemple pour un SIS : sauvegarde différentielle en semaine, sauvegarde complète le weekend…*) ; ► contraintes de sauvegarde : sauvegarde à chaud, sauvegarde à froid, verrouillage éventuel des données, définition de la plage horaire de sauvegarde, ordonnancement des sauvegardes notamment entre les composants ayant des liens entre eux… ► contenant de stockage de sauvegarde utilisé.	Oui
P5	Le plan de sauvegarde doit identifier, pour chaque composant informatique, les procédures et les prérequis à la restauration. Les prérequis doivent inclure les points suivants : ► environnement de restauration (*réseau, matériel de sauvegarde, serveur de restauration...*) ; ► caractéristiques des composants informatiques du matériel cible de la restauration ; ► configurations logicielles (*système d'exploitation, applications…*). Les procédures de restauration doivent formaliser les points suivants : ► diagnostic de la perte de données et détermination des données à récupérer en fonction des données perdues et des sauvegardes disponibles ; ► mode de mise en œuvre de la récupération de données ; ► modalités d'information des utilisateurs.	Oui
P6	Le plan de sauvegarde doit prévoir des tests des dispositions mises en œuvre pour assurer la sauvegarde. En pratique, les règles techniques concernant les sauvegardes, leur fréquence, leurs restaurations et la sécurité associée (règles S1 à S6, T1 à T4, G1 à G8 et R1 à R4) doivent être testées régulièrement. Une fréquence indicative d'une campagne de test annuelle est en général recommandée.	Non

5.3. Exigences techniques de sauvegarde

5.3.1. Règles spécifiques aux serveurs

N°	Règle	Délégable à un prestataire
S1	Une sauvegarde complète doit être effectuée avant chaque modification majeure d'un composant matériel ou logiciel (système ou application) et avant chaque changement majeur de configuration. Une sauvegarde complète doit être également effectuée après la modification si elle n'est pas déjà prévue dans le plan de sauvegarde.	Oui
S2	Pour chaque serveur de production, l'ensemble du paramétrage des systèmes d'exploitation et des applications (*comptes et droits utilisateurs, paramètres métier*…) doit être sauvegardé avec une fréquence minimum déterminée par les besoins et contraintes fixés par les responsables de traitement. A titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'éléments.	Oui
S3	Pour chaque serveur de production, l'ensemble des données des applications métier pour lesquelles des besoins de disponibilité ont été définis par les responsables de traitement doit être sauvegardé avec une fréquence minimum déterminée suivant les besoins et contraintes fixés par ces responsables. A titre indicatif, une sauvegarde quotidienne est en général recommandée pour ce type d'éléments, la périodicité minimale étant déterminée par la PDMA (Perte de données maximale admissible).	Oui
S4	Pour chaque serveur de production, les différentes versions des programmes (systèmes, bases de données et applications) doivent être sauvegardées et les sauvegardes correspondantes conservées, tant que des données de l'application contemporaines de ces versions sont susceptibles d'être restaurées. En effet, il est possible que ces données, une fois restaurées, nécessitent des versions des logiciels et systèmes antérieures aux versions actuelles de production pour pouvoir être exploitées.	Oui
S5	Une vérification systématique des sauvegardes doit être réalisée en fin de procédure. Pour les bases de données, une opération de restauration à blanc peut être planifiée en plus des tests prévus dans le cadre de la règle R2.	Oui
S6	L'ensemble des opérations de sauvegarde doit être journalisé. Les journaux doivent être conservés avec les supports de sauvegarde. Ils doivent comporter au minimum les informations suivantes : ► références du dispositif de sauvegarde ; ► périmètre ou composants concernés ; ► type de sauvegarde ; ► fichiers sauvegardés ; ► date de la sauvegarde ; ► statut de la sauvegarde.	Oui

5.3.2. Règles spécifiques aux postes de travail

N°	Règle	Délégable à un prestataire
T1	Dans le cas d'une utilisation monoposte, une sauvegarde complète doit être effectuée avant chaque modification majeure d'un composant matériel ou logiciel (système ou application) et avant chaque changement majeur de configuration. Une sauvegarde complète doit être également effectuée après la modification si elle n'est pas déjà prévue dans le plan de sauvegarde.	Oui
T2	Dans le cas d'un exercice individuel ou si la charte utilisateur de l'établissement permet le stockage de données métier sur les postes de travail, l'ensemble des données des applications métier doit être sauvegardé selon les besoins de disponibilité définis par les responsables de traitement à une fréquence minimum déterminée selon les besoins et contraintes exprimés. A titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'éléments, la périodicité minimale étant déterminée par la PDMA (Perte de données maximale admissible).	Oui
T3	Une vérification systématique des sauvegardes doit être réalisée en fin de procédure.	Oui
T4	Dans le cas d'un exercice individuel ou d'utilisation de postes de travail déconnectés du réseau, des moyens de sauvegarde locaux doivent être fournis aux utilisateurs[6] (voir chapitre 5.3.4).	Oui

5.3.3. Règles applicables aux systèmes de sauvegarde centralisée

N°	Règle	Délégable à un prestataire
C1	Si le système de sauvegarde centralisée (cf. chap. 3.2.1) est un système de sauvegarde en ligne (cf. chap. 3.2.4), le domaine de gestion des comptes utilisateurs (les gestionnaires des sauvegardes en l'occurrence) et des droits doit être dédié au système de sauvegarde et totalement distinct des domaines de gestion des comptes et de droits utilisés pour le reste du SIS. Ainsi les gestionnaires de sauvegarde et/ou la solution de sauvegarde doit nécessairement disposer de droits sur le SIS sauvegardé pour pouvoir réaliser les opérations liées à la sauvegarde, a contrario, aucun compte ni privilège établi ou potentiel au sein du SIS sauvegardé, y compris les comptes d'administration, ne doit pouvoir disposer de droit sur le système de sauvegarde.	Oui
C2	De manière similaire au réseau d'administration du SIS, le système de sauvegarde centralisée doit faire l'objet d'un cloisonnement logique strict vis-à-vis du reste du SIS, y compris vis-à-vis du réseau d'administration. Les flux réseau entre le système de sauvegarde et le reste du SIS doivent être filtrés, et seuls les flux strictement nécessaires doivent être autorisés. De ce point de vue, le reste du SIS doit être considéré par le système de sauvegarde comme « hostile ».	Oui
C3	Le système de sauvegarde centralisée doit être constitué de matériel dédié à cet usage, et en aucun cas partagé avec d'autres fonctions du SIS.	Oui
C4	Dans le cas de systèmes de sauvegarde centralisée utilisés pour les besoins de centres informatiques, le réseau de stockage des sauvegardes doit reposer sur une architecture dédiée à cet effet.[7]	Oui

[6] Voir règle PDT-SAUV-LOC de la [PSSI-MCAS]

[7] Voir règle ARCHI-STOCKCI de la [PSSI-MCAS]

5.3.4. Règles applicables aux systèmes de sauvegarde locale

N°	Règle	Délégable à un prestataire
L1	Le système de sauvegarde locale (cf. chap. 3.2.2) doit être un système de sauvegarde hors ligne (cf. chap. 3.2.3).	Oui
L2	Une documentation simple et claire des procédures de sauvegarde et de vérification des sauvegardes doit être fournie aux utilisateurs chargés des sauvegardes. Cette documentation doit également intégrer des instructions relatives à la déconnection, au stockage et à la gestion (étiquetage, rotation des supports…) des supports de sauvegarde. Les utilisateurs doivent être formés à ces procédures et pratiques.	Oui
L3	La procédure et les autorisations de restauration peuvent ou non être confiées aux utilisateurs en charge des sauvegardes, en fonction de l'évaluation du risque d'erreur de manipulation pouvant entrainer une restauration involontaire résultant en une perte de données.	Oui

5.3.5. Règles générales

N°	Règle	Délégable à un prestataire
G1	Les dispositifs de sauvegarde doivent faire l'objet d'un contrat de maintenance matérielle et logicielle adapté aux besoins de disponibilité du SIS.	Oui
G2	Chaque support amovible de sauvegarde doit être identifié et étiqueté avec a minima son identifiant, sa date de mise en première circulation et sa date de péremption.	Oui
G3	Un jeu de supports correspondant à une sauvegarde complète doit régulièrement être stocké dans un espace protégé contre les menaces physiques et environnementales (*vols, saccages, incendies, dégâts des eaux, perturbations magnétiques*…) et physiquement éloigné des composants du SIS sauvegardés. Cet éloignement physique doit garantir qu'un même sinistre ne peut affecter à la fois les composants sauvegardés et leur sauvegarde[8]. Selon le type de structure, le lieu de « stockage éloigné » de cette sauvegarde pourra être le domicile du responsable du traitement, un site secondaire de la structure, un coffre de banque… A titre indicatif, une sauvegarde hebdomadaire stockée de façon distante est en général recommandée, la périodicité minimale étant déterminée par la PDMA (Perte de données maximale admissible).	Oui
G4	Lorsque le système de sauvegarde met en œuvre une indexation des sauvegardes et de leur contenu, notamment afin de retrouver les supports et/ou identifiants de sauvegardes nécessaires à la restauration des données souhaitées, ces index doivent eux-mêmes faire l'objet de sauvegardes, avec les mêmes exigences de sécurité que les données sauvegardées, de façon coordonnée avec les sauvegardes des données.	Oui
G5	Le niveau de protection des sauvegardes doit être au moins identique à celui des éléments sauvegardés.[9] En particulier, l'accès aux sauvegardes doit faire l'objet d'un contrôle et d'une restriction d'accès aux seuls intervenants autorisés par le responsable du traitement que ce soit lors de leur	Oui

[8] Voir règle PCA-SAUVE de la [PSSI-MCAS]

[9] Voir règle PCA-PROT de la [PSSI-MCAS]

N°	Règle	Délégable à un prestataire
	manipulation, au cours des sauvegardes-restaurations, sur les lieux de stockage ou pendant les opérations de transport. A cet effet, il est possible de mettre en œuvre des solutions de chiffrement des données afin de réduire les risques d'accès aux données par des personnes non autorisées notamment en cas de perte de supports de stockage. Il est alors essentiel que les clés nécessaires au déchiffrement des sauvegardes soient également sauvegardées et que ces sauvegardes soient protégées et conservées séparément par une personne autorisée. Le lecteur pourra se référer : ► au Référentiel Général de Sécurité [RGS] qui comporte une annexe A1 [RGS-A1] décrivant notamment les exigences relatives à la fonction de sécurité « confidentialité », une annexe B1 [RGS-B1] traitant du choix et du dimensionnement des mécanismes cryptographiques, et une annexe B2 [RGS-B2] traitant de la gestion des clés cryptographiques ; ► au guide des mécanismes cryptographiques [CRYPTO] et au guide de sélection d'algorithmes cryptographiques [CRYPTOSEL] publiés par l'ANSSI.	
G6	Tous les supports de sauvegarde doivent, avant leur réutilisation dans un autre contexte ou leur mise au rebut, faire l'objet d'une campagne systématique d'effacement physique ou, à défaut, être physiquement détruits. Le lecteur pourra se référer au guide pratique spécifique à la destruction des données [GDD] disponible dans l'espace de publication de la PGSSI-S.	Oui
G7	Si la sauvegarde de données sensibles (*données à caractère personnel, paramétrages d'équipements parmi lesquels peuvent se trouver des mots de passe*…) est réalisée via le réseau, ces données ne doivent transiter par le réseau que sous forme chiffrée.	Oui
G8	Quand les besoins métier le nécessitent, un mécanisme de contrôle d'intégrité des données sauvegardées doit être mis en place. Si ce contrôle d'intégrité vise à détecter une éventuelle altération malveillante des données, il est recommandé d'utiliser la fonction de hachage SHA-256 pour réaliser une empreinte des données sauvegardées, voire une signature électronique. Ces empreintes doivent être protégées et conservées séparément des sauvegardes. Le lecteur pourra se référer au guide des mécanismes de protection de l'intégrité des données stockées [MPIDS] disponible dans l'espace de publication de la PGSSI-S.	Oui

5.4. Restauration et contrôle

N°	Règle	Délégable à un prestataire
R1	Tous les supports de sauvegarde doivent faire l'objet d'une surveillance périodique pour garantir leur efficacité physique, que ce soit par échantillonnage et test de restauration à blanc de sauvegardes anciennes, ou par suivi des paramètres techniques de bas niveau (erreurs de lecture, corrigées ou non) à l'occasion d'opérations de restauration. En cas d'incident lié à la qualité du support lors d'une opération de sauvegarde ou de restauration, comme en cas de suspicion de défaut, le support incriminé doit être mis au rebut, tout en respectant la règle G6.	Oui
R2	Des tests de restauration doivent être menés de manière régulière. Une périodicité indicative d'un test annuel est en général recommandée.	Oui

N°	Règle	Délégable à un prestataire
R3	Chaque opération de restauration doit donner lieu à une vérification du bon fonctionnement du composant restauré et de la sécurité. En particulier la gestion des droits d'accès aux éléments restaurés doit être la même que celle mise en œuvre pour les éléments initiaux sauvegardés. Le résultat de cette vérification doit être consigné dans une fiche de restauration qui comporte les informations suivantes : ► opérateur de sauvegarde ; ► demandeur de la restauration ; ► fichiers restaurés ; ► date de la sauvegarde ; ► date de restauration ; ► statut des vérifications effectuées.	Oui
R4	En routine, les exploitants doivent utiliser leur compte nominatif pour effectuer les opérations de restauration ou de contrôle des sauvegardes. Toutefois, il peut exister un compte administrateur du système de sauvegarde. Ce compte ne doit pas être un compte par défaut du système. L'identifiant et le mot de passe durci associés à ce compte doivent être consignés dans un coffre-fort (physique ou électronique) à mots de passe. Il ne sera utilisé qu'en cas de force majeure (indisponibilité des exploitants usuels notamment).	Oui

5.5. Règles relatives aux contrats d'externalisation

N°	Règle	Délégable à un prestataire
E1	Préalablement à la conclusion du contrat d'externalisation, il doit être vérifié que le prestataire est effectivement certifié pour l'hébergement de données de santé, pour ce type de service.	Non
E2	Le contrat d'externalisation doit contenir au minimum les clauses listées à l'article R1111-11 du code de la santé publique. Il convient également de rappeler que : ► l'objet du contrat doit être précis ; ► les rôles et responsabilités des parties doivent être clairement définis ; ► le fournisseur est tenu d'effectuer toutes les activités liées à ce type d'intervention au sein de l'Union Européenne ou conformément aux règles fixées par le [RGPD] pour les interventions hors Union Européenne et rappelées sur le site Internet de la CNIL[10] ; ► le fournisseur doit garantir la disponibilité, l'intégrité, la confidentialité, l'auditabilité, la pérennité des données notamment à travers des contrats de service formalisés en termes de durée maximale de restauration, de fréquence de sauvegarde et de durée de conservation. Ces engagements doivent se traduire par des mesures organisationnelles et techniques internes. Des mesures de contrôle et d'audit réalisées par le responsable du SIS peuvent être prévues dans le contrat.	Non
E3	Pendant toute la durée du contrat d'externalisation, il doit être vérifié que le prestataire est toujours certifié pour l'hébergement de données de santé, pour ce type de service.	Non

[10] Voir https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue

Annexe 1 : Fondements du guide

Le présent guide propose des dispositions permettant d'accompagner la mise en place d'un plan de sauvegarde. Ces dispositions visent une meilleure maitrise des risques SSI pesant sur la pérennité et l'intégrité des données.

Elles sont issues des bonnes pratiques en matière de SSI ainsi que des documents de référence :

- les recommandations publiées par l'ANSSI :
  - « Guide d'hygiène informatique », https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/
  - Guide « Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ? » https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/
  - « Guide des bonnes pratiques de l'informatique » (CPME-ANSSI) https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
- les recommandations publiées par la CNIL :
  - Guide de la sécurité des données personnelles[11] – Fiche 10 : « Sauvegarder et prévoir la continuité d'activité » https://www.cnil.fr/fr/securite-sauvegarder-et-prevoir-la-continuite-dactivite
  - Fiche « Multiplication des attaques par rançongiciel, comment limiter les risques ? https://www.cnil.fr/fr/multiplication-des-attaques-par-rancongiciel-comment-limiter-les-risques
- les bonnes pratiques en matière de sauvegarde identifiées dans :
  - norme NF ISO/IEC 27002 « Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information »,
  - norme ISO 22301 – « Sécurité sociétale - Systèmes de management de la continuité d'activité – Exigences »,
  - « Guide pour réaliser un plan de continuité d'activité » publié par le SGDSN http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

[11] https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Annexe 2 : Documents cités en référence

Réglementation

Renvoi	Document
[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 et Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016
[CSP]	Code de la santé publique
[CSP-L1111-8]	Article L1111-8 du Code de la santé publique, modifié par l'ordonnance n°2017-27 du 12 janvier 2017 - art. 1. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549/
[CSP-L1470]	Articles L1470-1 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
[R2GA]	Référentiel General de Gestion des Archives (R2GA) - octobre 2013 https://francearchives.fr/fr/circulaire/R2GA_2013_10
[REFHDS]	Certification hébergeur de données de santé (HDS) https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante https://esante.gouv.fr/offres-services/hds Référentiel de certification HDS https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification
[RGS]	Référentiel Général de Sécurité - Version 2.0 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[RGS-A1]	RGS A1 - Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[RGS-B1]	RGS B1 - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[RGS-B2]	RGS B2 - Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

[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]	Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS) – version du 1er octobre 2015

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/
[CRYPTOSEL]	Guide de sélection d'algorithmes cryptographiques, version 1.0 du 08/03/2021 ou version ultérieure en vigueur, publié par l'ANSSI https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[GDD]	Guide pratique technique « Destruction des données lors du transfert de matériel informatique », disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[MPIDS]	Guide pratique technique « Mécanismes de protection de l'intégrité des données stockées », disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

Annexe 3 : Glossaire

Sigle / Acronyme	Signification
ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
DMIA	Durée maximale d'interruption admissible
DMARD	Durée Maximale Admissible de Restauration des Données
ES	Etablissements de santé
HDS	Hébergeur de Données de Santé
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PCA	Plan de continuité d'activité
PDMA	Perte de données maximale admissible
PRA	Plan de reprise d'activité
SIS	Système d'information de santé