Guide Pratique
Règles de sauvegarde des Systèmes d'Information de Santé (SIS)

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

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

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

SOMMAIRE

1. INTRODUCTION

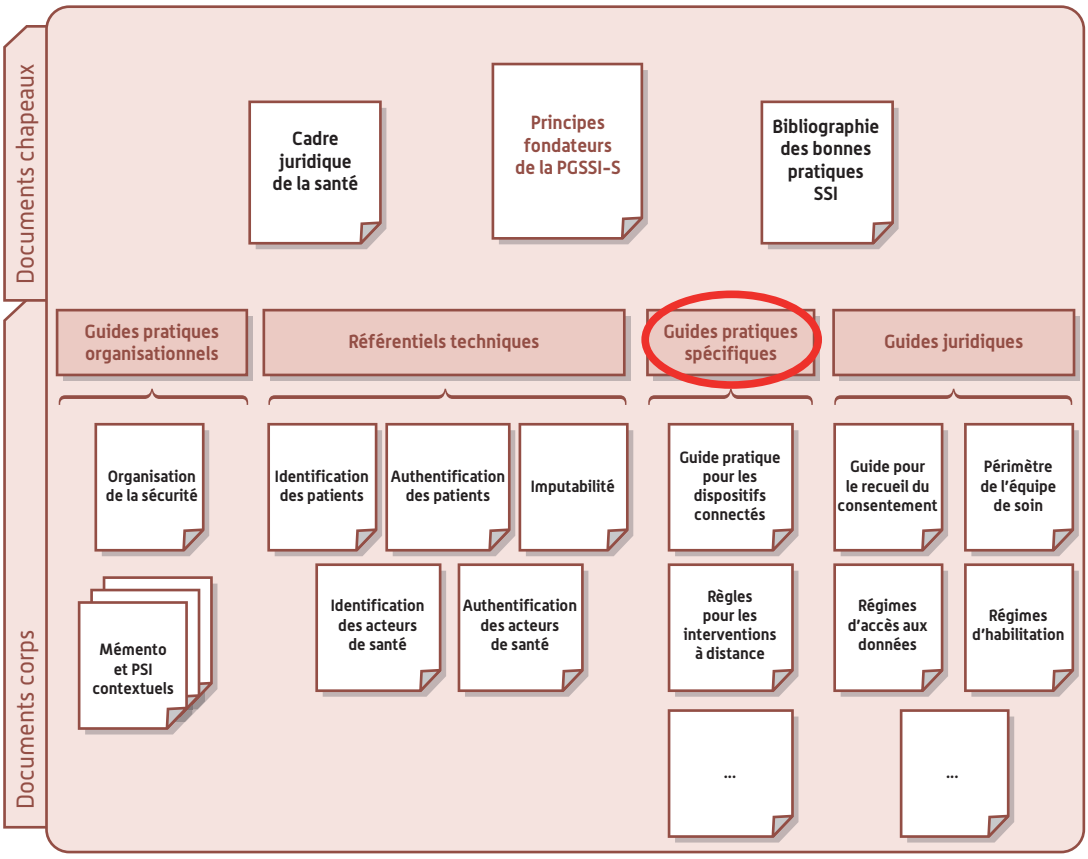
1.1. Objet du document

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

L'objectif 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).

FIGURE 1 : ORGANISATION DES DOCUMENTS DANS LE CORPUS DOCUMENTAIRE DE LA PGSSI-S



Ce document s'adresse :

- aux responsables de structure ;
- 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 identifier une personne impliquée dans la mise en œuvre des règles que celle-ci soit la personne responsable de la structure ou une personne agissant sous sa responsabilité. Le rôle du responsable du SIS est à distinguer de celui de responsable de traitement tel que défini dans la loi « Informatique et Liberté » n° 78-17 du 6 janvier 1978 modifiée, bien que ces rôles puissent être tenus par une même personne.

1.2. Champ d'application du guide pratique

Dans le cadre de ce guide pratique spécifique, tous les contextes de SIS au sens des « Principes fondateurs de la PGSSI-S » sont concernés quels que soient les finalités du SIS (production de soins, recherche clinique, …), le mode d'exercice (PS en exercice libéral, ES, …) et les étapes du cycle de vie de la donnée (conservation, échange/partage, …).

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

Santé						Médico Social
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Pour l'ensemble de ces périmètres, le présent guide décrit les règles applicables aux processus de sauvegarde de données de santé ou relevant du secret professionnel. En tant que tel, il participe aux plans de reprise d'activité (PRA) et aux plans de continuité d'activité (PCA) dont il constitue la base des règles opérationnelles concernant la préservation des données métiers et techniques en cas d'incident ainsi que leur restauration.

Ce guide s'appuie sur les définitions suivantes :

- **Sauvegarde** : opération qui consiste à dupliquer et à conserver de manière sécurisée des systèmes informatiques et/ou des données contenues dans un système informatique (ex. données métier, paramétrage et réglage du système…) afin d'assurer leur disponibilité et leur réutilisabilité même en cas d'incident ou d'erreur de manipulation portant atteinte à leur intégrité. Le terme anglais *backup* est aussi 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 elles permettent de réaliser des copies en temps réel des plateformes de production, et assurent une reprise d'activité 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. 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 de la notion fonctionnelle d'archivage qui n'entre pas dans le périmètre de ce guide pratique.
- **Restauration** : action consistant à utiliser des sauvegardes pour remettre un système d'information qui a été altéré dans un état antérieur à l'altération.
- **Plan de sauvegarde** : principes généraux de sauvegarde et ensemble des procédures liées à la sauvegarde et à la restauration pour un périmètre identifié sur lequel ils doivent être appliqués.

Limites du champ d'application du guide :
Ce guide pratique ne traite pas des règles applicables à l'archivage électronique.

1.3. Enjeux relatifs à la sauvegarde des Systèmes d'information de santé (SIS)

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

La sauvegarde :

- est une composante majeure du processus de continuité et de reprise d'activité du SIS à la suite d'un incident ou d'un sinistre (vol, dégât des eaux, incendie, …) ;
- permet la restauration d'un état antérieur du SIS après une suppression accidentelle de données (par exemple suite à une erreur de saisie d'un utilisateur ou d'un exploitant), une altération de données ou programmes informatiques (par exemple suite à une infection virale, à une panne d'un composant du système de stockage, ou encore à un incident environnemental dans un datacenter).

Garantir la confidentialité des données de sauvegarde, et plus encore lorsqu'il s'agit de données de santé à caractère personnel, est également nécessaire.
Cette confidentialité doit être assurée tant en gestion locale 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 prestations d'externalisation des données de sauvegarde de données de santé à caractère personnel doivent s'inscrire dans le cadre légal de l'hébergement de données de santé (cf. références n° 3 et 4)[1].

Le choix des solutions de sauvegardes présente également :

- des enjeux opérationnels d'exploitation du SIS :
  - les capacités de stockage nécessaires à la sauvegarde peuvent varier selon les modes de sauvegardes retenus (par exemple : sauvegarde totale ou partielle, sauvegarde 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),
  - les délais acceptables de restauration pour des données à forte volumétrie peuvent justifier des techniques spécifiques de sauvegarde ;
- des enjeux financiers :
  - le coût de la sauvegarde est fortement dépendant du niveau de service attendu : fréquence des sauvegardes, durée de rétention, …

Il est donc important de choisir les solutions de sauvegardes adaptées et de définir des processus associés. Ceci afin de répondre aux enjeux de sécurité mais également financiers dans un souci d'efficience économique en cohérence avec le besoin opérationnel des acteurs de santé.

1. L'article L 1111-8 alinéa 1 du code de la santé publique dispose que *« Les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée. »* Les conditions d'obtention de cet agrément, le déroulement de la procédure, ainsi que le contenu du dossier de demande d'agrément sont précisées par le décret 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel.

2. 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 de la fiche technique sur la sauvegarde (référence n° 1) de l'ANSSI : « Fiche technique relative à la sauvegarde »[2] ;
- les bonnes pratiques en matière de sauvegarde identifiées dans :
  - la norme ISO/CEI 27002 - « Code de bonnes pratiques pour la gestion de la sécurité de l'information » (référence n° 2),
  - la norme ISO 22301 – « Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences » (référence n° 5),
  - les bonnes pratiques relatives aux sauvegardes de données à caractère personnel publiées par la CNIL : « Guide Mesures pour traiter les risques sur les libertés et la vie privée »[3] ;
  - le guide pour réaliser un plan de continuité d'activité (référence n° 6) ;
- les formalités sécuritaires, impactant le domaine de la sauvegarde, relatives à l'hébergement de données de santé à caractère personnel :
  - décret n° 2006-6 du 4 janvier 2006 - conditions d'agrément des hébergeurs de données de santé à caractère personnel codifié aux articles R. 1111-9 et suivants du code de la santé publique (référence n° 3)[4],
  - référentiel de constitution des dossiers de demande d'agrément des hébergeurs de données de santé à caractère personnel (ASIP, référence n° 4)[5].

2. http://www.securite-informatique.gouv.fr/gp_article95.html
3. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf#page27
4. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006053120
5. http://esante.gouv.fr/services/referentiels/securite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des

3. PRINCIPES ESSENTIELS DE SAUVEGARDE

3.1. Principes de sécurité de la sauvegarde

Les principes de sécurité de la sauvegarde sont regroupés en 4 thématiques :
- identification du besoin ;
- formalisation des procédures ;
- adoption de pratiques conformes à l'état de l'art ;
- restauration et contrôle.

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

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

3.1.2. Formalisation des procédures de sauvegarde et restauration

Cette étape consiste à adopter une méthodologie permettant d'élaborer 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.

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

Le présent document identifie les bonnes pratiques conformes à l'état de l'art.

Pour tenir compte de la diversité des SIS et identifier rapidement les règles applicables, des éléments de contexte sont fournis (par exemple serveur, poste de travail).

3.1.4. Restauration et contrôles

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

À 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.

3.2. Externalisation de la sauvegarde

Au vu de la complexité de la mise en œuvre de dispositifs de sauvegardes 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 nombreux :
- expertise pour la formalisation des procédures de sauvegarde et de restauration ;
- garantie de cohérence et d'exhaustivité du périmètre sauvegardé accrue ;
- 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, le responsable est tenu de faire appel à un hébergeur de données de santé à caractère personnel agréé à cet effet, conformément aux dispositions du code de la santé publique relatives à l'hébergement de données de santé à caractère personnel.

4. UTILISATION DU GUIDE

Les responsables identifiés au chapitre 1.1 sont en charge :
- d'estimer les risques de sécurité et de prévoir les mesures permettant de les réduire ;
- de mettre en œuvre les règles prescrites ou de les faire appliquer par leurs sous-traitants ;
- d'estimer et de traiter les risques de sécurité induits par la non-application des règles qui ne sont pas respectées, le cas échéant.

Le traitement d'un risque de sécurité peut consister à adopter une ou plusieurs des options suivantes vis-à-vis de ce risque :
- le réduire, par des mesures de protection ou de prévention ;
- l'accepter tel quel notamment si le risque est jugé mineur par le responsable du SIS ;
- l'éviter ;
- le transférer vers un tiers dans le cadre d'un contrat, étant précisé que cela n'exonère pas le responsable du SIS de toute responsabilité.

Le responsable dresse l'inventaire des dispositions de sécurité qui sont applicables au SIS dont il a la charge, au regard de l'analyse des risques réalisée et en s'appuyant sur la liste de règles du chapitre suivant. Il prend ensuite en compte les risques induits par les dispositions qu'il n'est pas en mesure de couvrir.

5. RÈGLES DE SÉCURITÉ APPLICABLES À 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 tableau ci-après par la colonne « recours à un prestataire ».

N°	Règle	Recours à un prestataire
Règles d'organisation		
[O1]	Seul le personnel ou les sociétés désignées par le responsable du SIS peuvent intervenir sur les processus de sauvegarde et de restauration des applications et des données.	
[O2]	Lorsque cela est permis selon la charte utilisateur inhérente à 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 informatique de la structure mettant le SIS à leur disposition.	
Plan de sauvegarde		
[P1]	Toute mise en production d'un nouveau système, d'une nouvelle application ou 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.	
[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 ; • durée maximale admissible de restauration des données (DMARD) qui correspond au temps entre la demande de restauration et la restauration effective des données[6] ; • 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 de conservation maximale des sauvegardes. 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.	

6. Dans le cadre des plans de continuité et des plans de reprise d'activité, cette notion est intégrée dans le délai d'indisponibilité maximale attendu (DIMA) 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	Recours à un prestataire
[P3]	Le plan de sauvegarde doit identifier, en conformité avec le périmètre de sauvegarde défini ([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 synchronisation et la cohérence des données lors des sauvegardes et restaurations, en particulier lors des montées de versions de logiciel à l'occasion desquelles il est important de sauvegarder de la version précédente du logiciel afin de s'assurer du bon accès aux données en cas de restauration. Cette prise en compte peut notamment être réalisée par la sauvegarde de briques d'infrastructure complètes éventuellement associée à des plans de virtualisation du SI.	X
[P4]	Pour chaque composant informatique identifié, le plan de sauvegarde décrit les procédures de sauvegardes à mettre en œuvre : • type de sauvegarde : sauvegarde complète, sauvegarde partielle, sauvegarde différentielle, sauvegarde incrémentale ; • 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, définition de la plage horaire de sauvegarde, ordonnancement des sauvegardes notamment entre les composants ayant des liens entre eux…	X
[P5]	Le plan de sauvegarde doit identifier, pour chaque composant informatique, les procédures et les pré-requis à la restauration. Les pré-requis incluent 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 formalisent 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.	X
[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 [T1] à [T16] et règles [R1] à [R4]) sont à tester régulièrement. Une fréquence indicative d'une campagne de test annuelle est en général recommandée.	

N°	Règle	Recours à un prestataire
Exigences techniques de sauvegarde		
Exigences techniques de sauvegarde : règles spécifiques aux serveurs		
[T1]	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.	**X**
[T2]	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 selon les besoins de disponibilité définis par les responsables de traitement à une fréquence minimum déterminée en fonction des besoins et contraintes. À titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'éléments.	**X**
[T3]	Pour chaque serveur de production, 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 en fonction des besoins et contraintes. À titre indicatif, une sauvegarde quotidienne est en général recommandée pour ce type d'éléments.	**X**
[T4]	Pour chaque serveur de production, les différentes versions des programmes (systèmes, bases de données et applications) doivent être sauvegardées et les supports conservés, tant que les données de l'application sont susceptibles d'être restaurées. En effet, si des données un peu anciennes sont restaurées, il est possible qu'il soit nécessaire de restaurer ces données dans un environnement nécessitant des versions des logiciels et systèmes antérieures aux versions actuelles de production.	**X**
[T5]	Une vérification systématique des sauvegardes est 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].	**X**
[T6]	L'ensemble des opérations de sauvegarde est journalisé. Les journaux sont conservés avec les supports de sauvegardes. Ces derniers comportent 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.	**X**
Exigences techniques de sauvegarde : règles spécifiques aux postes de travail		
[T7]	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.	**X**
[T8]	Dans le cas d'un exercice individuel ou si la charte utilisateur de l'établissement permet le stockage de données métiers 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 en fonction des besoins et contraintes. À titre indicatif, une sauvegarde quotidienne est recommandée pour ce type d'éléments.	**X**
[T9]	Une vérification systématique des sauvegardes est réalisée en fin de procédure.	**X**

N°	Règle	Recours à un prestataire
	Exigences techniques de sauvegarde : autres règles	
[T10]	Les dispositifs de sauvegarde doivent faire l'objet d'un contrat de maintenance matérielle et logicielle adapté aux besoins de disponibilité du SIS.	**X**
[T11]	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.	**X**
[T12]	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. 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 l'organisme, un coffre de banque… À titre indicatif, une sauvegarde hebdomadaire stockée de façon distante est en général recommandée.	**X**
[T13]	Le niveau de protection des sauvegardes doit être au moins identique à celui des éléments sauvegardés. 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 de traitement que ce soit lors de leur manipulation, au cours des sauvegardes-restaurations, sur les lieux de stockage ou pendant les opérations de transport. À 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 décrivant les exigences relatives à la fonction de sécurité « confidentialité »[7].	**X**
[T14]	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.	**X**
[T15]	Si la sauvegarde de données sensibles (données à caractère personnel, paramétrages d'équipement 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.	**X**
[T16]	Quand les besoins métiers le nécessitent, un mécanisme de contrôle d'intégrité des données sauvegardées peut être mis en place. Si ce contrôle d'intégrité vise à détecter une éventuelle falsification 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 devront être protégées et conservées séparément des sauvegardes.	**X**

7. Lien du site de l'ANSSI : http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html

N°	Règle	Recours à un prestataire
Restaurations et contrôles		
[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.	X
[R2]	Des tests de restauration sont menés de manière régulière. Une fréquence indicative d'un test annuel est en général recommandée.	X
[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 est 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.	X
[R4]	En routine, les exploitants doivent utiliser leur compte nominatif pour effectuer des 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).	X
Règles relatives aux contrats d'externalisation		
[E1]	Pré-requis à la conclusion du contrat d'externalisation : • le prestataire doit être agréé pour l'hébergement de données de santé à caractère personnel, pour ce type de service. Le contrat d'externalisation doit contenir au minimum les clauses listées à l'article R 1111-13 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 définies par la CNIL pour les interventions hors Union Européenne[8] ; • le fournisseur garantit 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. Ce qui se traduira par des mesures techniques et d'organisation interne ; • des mesures de contrôle et d'audit réalisées par le responsable du SIS peuvent être prévues dans le contrat.	X

8. http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/

ANNEXES

Annexe 1 : Glossaire

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
DIMA	Durée d'Indisponibilité Maximale Admissible
DMARD	Durée Maximale Admissible de Restauration des Données
ES	Etablissements de santé
GT	Groupe de Travail
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PTS	Pôle Technique et Sécurité
SIS	Système d'Information de Santé
PDMA	Perte de Données Maximale Admissible

Annexe 2 : Documents de référence

Référence n° 1 : Fiche technique relative à la sauvegarde (ANSSI)

Référence n° 2 : Norme ISO/CEI 27002 - *« Code de bonnes pratiques pour la gestion de la sécurité de l'information »*

Référence n° 3 : Décret n° 2006-6 du 4 janvier 2006 - conditions d'agrément des hébergeurs de données de santé à caractère personnel

Référence n° 4 : Référentiel de constitution des dossiers de demande d'agrément des hébergeurs de données de santé à caractère personnel (ASIP)

Référence n° 5 : Norme ISO 22301 – *« Sécurité sociétale -- Systèmes de management de la continuité d'activité – Exigences »*

Référence n° 6 : Guide pour réaliser un plan de continuité d'activité (SGDSN)

Référence n° 7 : Référentiel Général de Sécurité (ANSSI)

Référence n° 8 : Guide d'hygiène informatique (ANSSI)

Référence n° 9 : Corpus documentaire de la PGSSI-S (référentiels et guides pratiques)[9]

Référence n° 10 : Guide des mesures pour traiter les risques sur les libertés et la vie privée (CNIL).

9. Le cas échéant, les évolutions du corpus documentaire de la PGSSI-S seront prises en compte dans des versions ultérieures de ce guide, notamment par référencement de certains guides pratiques sur des sujets spécifiques évoqués dans le chapitre 4 sur les règles.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

asipsanté

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