Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques 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

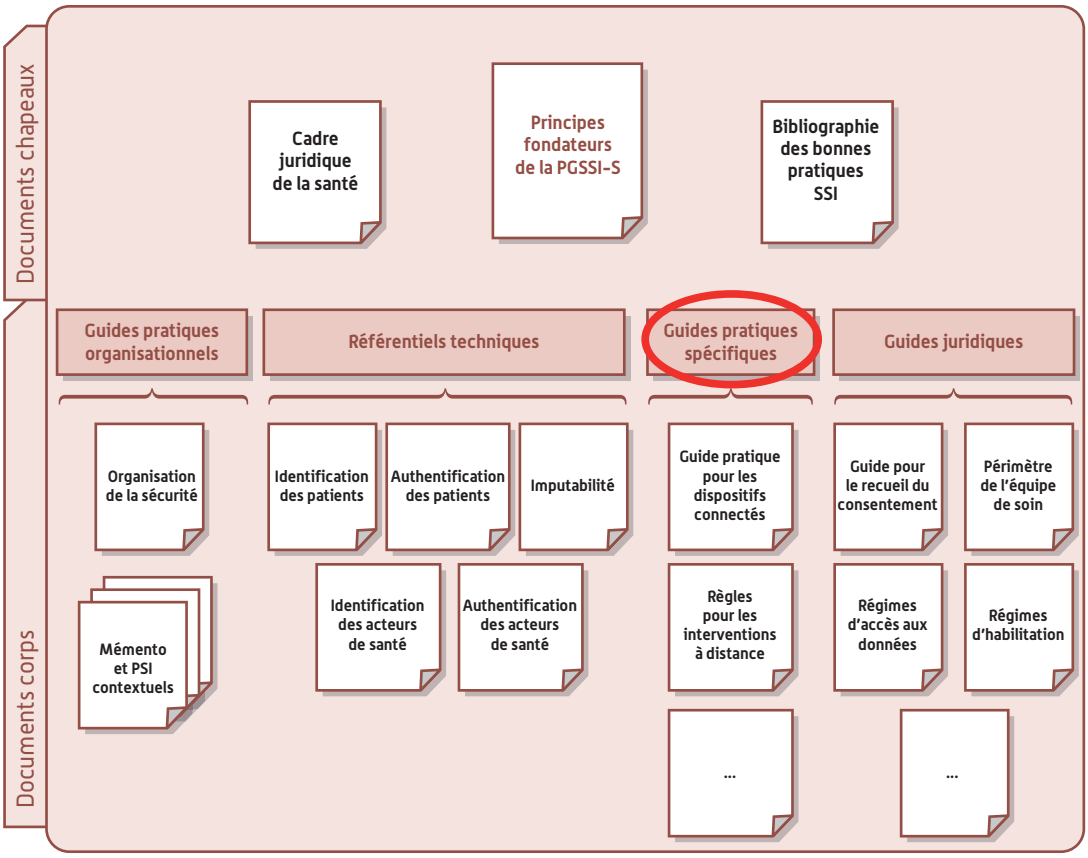
1. INTRODUCTION

1.1. Objet du document

L'objectif du présent document est de définir les règles à appliquer lors de la gestion de tout type de matériels stockant des données sensibles. Ces règles ont pour objectif d'apporter l'assurance que lors du transfert d'un matériel, les données des Systèmes d'Information de Santé (SIS) présentes sur le support de stockage sont détruites de manière à empêcher toute récupération de ces 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 DU CORPUS DOCUMENTAIRE DE LA PGSSI-S



Ce document s'adresse :

- aux responsables de structure utilisatrice de matériel informatique ;
- aux personnes agissant sous leur responsabilité ; en particulier celles impliquées dans :
  - la définition de la politique de sécurité des SIS et sa mise en œuvre au sein de la structure,
  - la maintenance technique des matériels informatiques,
  - l'exploitation des matériels informatiques.

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 Libertés 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, tous les contextes de SIS au sens des « Principes fondateurs de la PGSSI-S » sont concernés quelles que soient les finalités du SIS (production de soin, recherche …), 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 qui permettent d'éviter une divulgation de données sensibles dématérialisées (ex. données de santé, données relevant du secret professionnel…) quand les supports de données sont transférés vers un contexte d'utilisation différent. Il se concentre sur les règles applicables aux processus de gestion des matériels supports de données sensibles lorsque ceux-ci font l'objet de transferts (internes ou externes) qui changent les règles d'accès appliquées ou le périmètre d'utilisateurs susceptibles d'accéder aux données.

On entend par transfert de matériel les cas d'usage suivants :

- **Transfert interne de matériel au sein de la même structure :**
  Ce transfert vise le changement d'utilisateur d'un matériel au sein d'une même structure. Il nécessite la suppression des données pour que le matériel puisse être réutilisé.
- **Transfert externe de matériel en dehors de la structure :**
  Les situations envisageables sont multiples. On citera à titre d'exemple, les cas suivants :
  - la sortie temporaire du matériel (par exemple dans le cadre d'une opération de maintenance ou de garantie) ;
  - la mise au rebut du matériel : destruction de matériel (par exemple en raison d'un dysfonctionnement le rendant désormais impropre à l'usage ou en cas de fin de vie) ;
  - cession du matériel ou retour en fin de location.

Tous les supports de mémoire, intégrés ou non dans des matériels, et susceptibles de conserver durablement des données informatisées (intégrés ou non dans des matériels), sont concernés.

Les équipements suivants (liste non exhaustive) font partie du périmètre d'application du guide :

Catégories	Exemples de ressources informatiques
Poste de travail	Ordinateur fixe, ordinateur portable, tablette, …
Serveur	Serveur de production, de test, de sauvegarde, …
Equipement éditique	Imprimante, photocopieur, scanner, …
Support de stockage externe	Disque dur externe, clé USB, disque optique, support de sauvegarde, …
Equipement téléphonique	Ordiphone[1], téléphone portable[2], …
Equipement biomédical	Appareil d'imagerie médicale, dispositif bio-médical, …
Equipement réseau ou de sécurité	Routeur, firewall, proxy
Dispositif de sécurité	Carte à puce, capacité RFID, dispositif matériel de sécurité, …[3]

1. Le terme anglais smartphone est également largement usité dans le milieu informatique pour désigner un ordiphone.
2. Ces équipements peuvent contenir des données entrant dans le cadre du présent document (photos, notes, contacts, messages, …)
3. Ces équipements peuvent, par exemple, permettre l'accès à des données de santé à caractère personnel.

1.2.1. Limites du champ d'application du guide

1.2.1.1. Contrat de maintenance

Dans certains cas de maintenance, en particulier ceux qui impliquent que l'intervenant remplace des supports amovibles et emporte les supports remplacés, les règles définies dans ce guide ne peuvent pas être appliquées par la structure elle-même. Les mêmes résultats, à savoir la non divulgation des données et/ou la destruction des supports de stockage de données sensibles, doivent être obtenus via un engagement contractuel pris par l'intervenant. En cas de destruction du matériel, le respect de cet engagement doit donner lieu, à l'issue de chaque opération, à la production par l'intervenant d'un document formel qui confirme le respect des exigences pour chaque support emporté. Bien évidemment, il est nécessaire de faire préciser par l'intervenant la procédure qu'il va appliquer et les moyens qu'il va mettre en œuvre pour respecter ses engagements, afin de juger de leur adéquation et de leur crédibilité avant de contractualiser avec lui.

1.2.1.2. Sortie d'archivage

La destruction de données dans le cadre d'un processus de sortie d'archivage fait partie de la gestion de l'archivage. Elle est considérée comme hors périmètre pour ce guide.

1.2.1.3. Effacement fonctionnel

L'effacement de données d'un support matériel dans le cadre d'un processus métier ne modifie ni le contexte, ni le niveau de contrôle d'accès aux données. Ce cas d'usage n'introduit donc pas d'opportunité supplémentaire d'accès non maitrisé aux données. Il est considéré comme hors périmètre pour ce guide.

1.2.1.4. Enquête sur les données

En cas d'enquête portant sur les données présentes sur un support, que celle-ci soit d'origine interne ou externe[4], toute procédure d'effacement sur ce support devra être suspendue jusqu'à conclusion de la dite enquête.

1.3. Enjeux relatifs à la destruction de données

L'activité des SIS conduit à stocker des données sensibles sur différents supports informatiques (ex : disques durs, bandes magnétiques, clés USB, CD, DVD, ...).

Cette opération peut s'effectuer sous le contrôle de l'utilisateur d'un équipement (par exemple copie ou sauvegarde manuelle de données). Mais souvent le stockage est effectué par l'équipement à des fins techniques de manière transparente pour l'utilisateur (stockage dans la mémoire des imprimantes lors de l'impression de documents, sauvegarde technique automatique, ...).

Le cycle de vie des matériels (réaffectation d'un matériel en interne, envoi d'un matériel en maintenance, mise au rebut du matériel, ...) peut conduire un tiers à accéder à ces matériels et aux données qu'il contient. C'est du risque d'accès illégitime d'un tiers aux données contenues dans l'équipement que l'on veut se protéger.

Ce risque pourrait engager la responsabilité pénale du responsable du SIS, en particulier dans le cas de données de santé à caractère personnel et d'utilisation illégitime de ces données. Il appartient donc au responsable de SIS de prendre les mesures nécessaires pour se protéger contre ce risque.

Il est essentiel d'empêcher la fuite et l'exploitation de telles données lorsque l'on perd la maîtrise de l'équipement qui les contient, par exemple en les effaçant de manière sûre ou en détruisant le support de stockage avant que ce dernier ne soit entre les mains d'un tiers.

4. Ordonnance d'un juge par exemple.

2. FONDEMENTS DU GUIDE

Le présent guide propose des dispositions de sécurisation permettant d'encadrer le transfert de matériel informatique.
Ces dispositions de sécurité visent une meilleure maitrise des risques SSI de divulgation de données sensibles liés au transfert de matériel.

Les dispositions préconisées pour ce faire sont issues des bonnes pratiques en matière de SSI notamment celles identifiées dans les documents de référence présentés ci-dessous.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié des recommandations en matière d'effacement de supports de stockage magnétiques (disques durs ou bandes magnétiques) et non-magnétiques (clés USB ou cartes SD par exemple) ayant contenu des informations sensibles (références nº 1 et 2) :

- Recommandation : « Effacement des supports de stockage de masse »[5]
- Guide : « GUIDE TECHNIQUE pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter »[6]

Par ailleurs, différentes organisations de sécurité ont élaboré des référentiels traitant de l'écrasement et de la déclassification des supports d'information électronique.

- Le CST (Centre de la sécurité des télécommunications, Canada) (référence nº 3)
  - Effacement et nettoyage des supports[7]
- La NSA (National Security Agency (USA) (reference nº 4)
  - NSA/CSS STORAGE DEVICE DECLASSIFICATION MANUAL[8]
- Le NIST (National Institute of Standard and Technology) (reference nº 5)
  - Guidelines for Media Sanitization[9]
- Le NISP (National Industrial Security Program) (référence nº 6)
  - Operating Manual (DOD 5220.22-M)[10]

5. http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-medias-amovibles/effacement-des-supports-de-stockage-de-masse.html
6. http://www.ssi.gouv.fr/archive/fr/documentation/Guide_effaceur_V1.12du040517.pdf
7. http://www.cse-cst.gc.ca/documents/services/csg-cspc/csg-cspc08l-fra.pdf, http://www.cse-cst.gc.ca/documents/services/csg-cspc/csg-cspc08g-fra.pdf
8. http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf
9. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf
10. http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

3. PRINCIPES DE SÉCURITÉ DU TRANSFERT DE MATÉRIEL

Les principes de sécurité du transfert de matériel s'articulent autour de la préservation de la confidentialité des données. Tout matériel sur lequel des données sensibles ont pu être stockées doit faire l'objet d'un traitement avant transfert, que ce soit pour réutilisation en interne, cession à un externe ou mise au rebut.

Les traitements du matériel avant son transfert peuvent être de deux types selon la sensibilité des données :

- effacement des données stockées sur le matériel ;
- retrait des supports de stockage de données pour destruction.

Les règles présentées dans la section 5 permettent de mettre en œuvre ces types de traitement.

4. UTILISATION DU GUIDE PRATIQUE

Le guide énonce des règles de sécurité dont l'application est du ressort du responsable du SIS. Elles s'adressent plus spécifiquement au responsable d'exploitation en charge des matériels informatiques.

Ce guide est également applicable aux utilisateurs dans la mesure où ceux-ci utilisent des matériels personnels connectés au SIS (clés USB, ordiphone, ...).

Les responsables identifiés au chapitre 1.1 sont en charge :
- 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 les règles non appliquées.

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 (par exemple en conservant dans les locaux du SIS les disques durs les photocopieurs ou le PC lors d'interventions de maintenance sur ces équipements) ;
- le transférer vers un tiers dans le cadre d'un contrat étant précisé que cela n'exonère pas de sa responsabilité le responsable du SIS.

Il est notamment préconisé de réduire le risque de sécurité par l'utilisation, dans la mesure du possible, de solutions de chiffrement[11] permettant de rendre illisibles les données sans la connaissance de la clé de chiffrement.

Dans le cas d'externalisation de prestations de destruction physique, il est nécessaire de procéder préalablement à un effacement logique : effacement de premier niveau en interne (formatage à zéro ou dégaussage des disques durs) avant destruction physique en externe.

11. L'ANSSI répertorie sur son site internet des solutions certifiées de confiance dans le document de référence n° 1.

5. RÈGLES DE SÉCURITÉ APPLICABLES LORS DU TRANSFERT DE MATÉRIELS

Deux paliers sont définis pour la mise en œuvre des exigences de sécurité applicables à la destruction de données lors du transfert de matériel : un palier 1, porteur des exigences minimales, et un palier 2 qui complète ou, le cas échéant, remplace les exigences minimales afin d'offrir un meilleur niveau de sécurité.

Les règles qui relèvent uniquement du Palier 1 ne doivent pas être utilisées pour les transferts externes au SIS si le support de données est susceptible de contenir des données à caractère personnel ou d'autres données sensibles.

N°	Règle	Niveau exigibilité
Règles d'organisation		
[O1]	La destruction de données doit être réalisée sous la responsabilité du responsable du SIS, soit par le personnel de la structure soit par des prestataires techniques externes dans le cadre de contrats.	**Palier 1 et 2**
[O2]	Afin de définir les responsabilités des acteurs impliqués dans le processus de destruction de données, les règles de ce guide doivent être reprises dans les documents propres à l'organisation du SIS (Politique de Sécurité, Charte informatique, notes d'organisation, fiches de poste, contrats d'externalisation, ...). À titre d'exemple, les utilisateurs de supports de stockage amovibles sont chargés de l'application des règles d'effacement lors du transfert de matériel conformément à la charte informatique de la structure.	**Palier 1 et 2**
Règles techniques		
[R1]	Les interventions techniques doivent être réalisées selon le type de matériel considéré. Dans le cas d'un équipement (ordinateur portable ou fixe, serveur, photocopieur, ordiphone, ...) comportant plusieurs composants (disque dur, clé USB, carte SD, ...), chaque composant devra être traité indépendamment selon les règles applicables.	**Palier 1 et 2**
Règles techniques spécifiques aux disques durs et aux supports flash (disque SSD, clé USB, carte SD, Compact Flash, ...)		
[R2-a]	Un formatage complet doit être réalisé. Ce formatage complet (dit aussi formatage bas niveau ou à zéro[12]) doit être appliqué sur la totalité de la ou des partitions du support considéré. Pour les disques SSD ou support flash, il est recommandé d'utiliser la fonction d'effacement sécurisé fournie par le constructeur lorsqu'elle est disponible.	**Palier 1**
[R2-b]	Il est envisageable, en alternative à la règle [R2-a], de procéder : • à la démagnétisation des disques durs magnétiques, ou à leur destruction physique (broyage, incinération, ...). • à la destruction physique des supports flash (y compris les disques durs SSD ou hybrides) par broyage ou incinération.	**Palier 2**
Règles techniques spécifiques aux disques optiques		
[R3]	Les disques optiques doivent être détruits par destruction physique (broyage, incinération ou meulage).	**Palier 2**
Règles techniques spécifiques aux bandes magnétiques		
[R4]	Les bandes magnétiques doivent être effacées par démagnétisation ou détruites par déchiquetage ou incinération.	**Palier 2**
Règles techniques spécifiques aux cartes à microcircuits		
[R5]	Les cartes à microcircuits (carte SIM, CPS, ...) doivent être détruites par broyage du circuit ou incinération.	**Palier 2**

12. Dans un formatage à zéro, chaque bit de donnée est remplacé par un zéro.
Remarque : la simple réinstallation du système n'est pas suffisante pour assurer la destruction des données.

N°	Règle	Niveau exigibilité
Règles techniques spécifiques aux ordiphones, téléphones portables, tablettes		
[R6-a]	Les données doivent être effacées à l'aide des fonctions d'utilisation puis par application de la procédure prévue par le constructeur pour remise de l'appareil en configuration de sortie d'usine[13].	**Palier 1**
[R6-b]	L'appareil doit être détruit physiquement.	**Palier 2**
Règles techniques spécifiques aux autres matériels		
[R7-a]	Les données des matériels stockant des informations sur des supports autres que ceux-spécifiés ci-dessus (par exemple, dispositifs biomédicaux, ...) doivent être effacées au travers des fonctions d'utilisation puis par application de la procédure prévue par le constructeur pour remise de l'appareil en configuration de sortie d'usine.	**Palier 1**
[R7-b]	L'appareil doit être détruit physiquement.	**Palier 2**
Procédures		
[P1]	Les procédures de destruction de données lors du transfert de matériel doivent être formalisées. En particulier, dans le cas de stockage de matériel en attente de traitement, les procédures doivent prendre en compte la protection physique du lieu de stockage.	**Paliers 1 et 2**
[P2]	Les procédures de gestion du cycle de vie des supports de données numérique doivent être formalisés et intégrer le traitement des données et leur destruction. En particulier, les procédures doivent prendre en compte la possibilité de désosser un matériel (ex. démontage des disques durs d'un poste de travail). Tout élément issu du désossage d'un matériel doit être identifié à part entière dans l'inventaire et rentrer dans la gestion du cycle de vie des supports de données numériques.	**Paliers 1 et 2**
[P3]	Avant toute opération d'effacement ou de destruction, il est préconisé de contrôler, que les supports ne contiennent aucune donnée utile et non sauvegardée par ailleurs. Dans le cas contraire, il convient de procéder à la sauvegarde de ces données nécessaires.	**Paliers 1 et 2**
[P4]	Une fois l'effacement terminé, Il est nécessaire de vérifier que le support ne contient plus de données.	**Paliers 1 et 2**
[P5]	Une fiche d'intervention à destination du responsable de la gestion des matériels, visée par le personnel en charge de l'opération, doit permettre de garder une trace des informations suivantes pour les matériels du SIS : • Identification du matériel (numéro de série, adresse mac, ...) ; • ancien propriétaire (entité, ou à défaut identité personne physique) ; • nouveau propriétaire (entité, identité personne physique) ; • date de transfert de l'équipement ; • date et nature de l'intervention d'effacement ou de destruction effectuée ; • statut des opérations réalisées (opérateur, date, type d'effacement, contrôle de l'effacement, ...).	**Paliers 1 et 2**
[P6]	Les procédures de traitement du matériel en fin de vie doivent prévoir la gestion des supports de données numériques qui peuvent être contenus dans ces matériels.	**Paliers 1 et 2**

13. Il est à noter que cette méthode rend les données inaccessibles à un utilisateur « standard » mais ne garantit pas l'effacement réel des données de l'appareil.

Il est envisageable d'externaliser les prestations de destruction de données. Dans ce cas, les règles suivantes seront inscrites dans le contrat de sous-traitance.

N°	Règle	Niveau exigibilité
Règles relatives aux contrats d'externalisation		
[C1]	Les clauses générales suivantes doivent figurer aux contrats : • 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 réalisées hors Union Européenne[14] ; • Le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative ; • Le fournisseur doit soumettre toute sous-traitance de prestation à l'autorisation du responsable du SIS ; • En cas de recours à la sous-traitance, le fournisseur doit répercuter les exigences qui lui sont applicables vers le sous-traitant.	**Palier 1 et 2**
[C2]	Les clauses de sécurité suivantes doivent figurer aux contrats : • Le fournisseur doit s'engager vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée doit avoir signé un engagement individuel de confidentialité rappelant les dispositions de la loi Informatique&Libertés et les sanctions applicables ; • Le responsable du SIS a la possibilité de faire réaliser des audits de sécurité des dispositions prises par le fournisseur pour la réalisation de sa prestation.	**Palier 1 et 2**
[C3]	Les exigences de sécurité suivantes doivent figurer au contrat : • Le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la confidentialité des données lors de transferts de matériel.	**Palier 1 et 2**

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

Lorsque le responsable du SIS fait appel à des contrats de location de matériel, les règles concernant la destruction des données sont à la charge du fournisseur. Dans ce cas, les règles suivantes sont à intégrer dans le contrat de fourniture.

N°	Règle	Niveau exigibilité
Règles relatives aux contrats de location		
[L1]	clauses générales suivantes doivent figurer aux contrats : • Le fournisseur doit s'engager à respecter les règles du présent guide sur les matériels mis à disposition du SIS; • Le fournisseur est tenu de déclarer tout changement relatif à sa situation administrative ; • Le fournisseur doit soumettre toute sous-traitance de prestation à l'autorisation du responsable du SIS ; • En cas de recours à la sous-traitance, le fournisseur doit répercuter les exigences qui lui sont applicables vers le sous-traitant.	**Palier 1 et 2**
[L2]	Les clauses de sécurité suivantes doivent figurer aux contrats : • Le fournisseur doit s'engager vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée doit avoir signé un engagement individuel de confidentialité rappelant les dispositions de la loi Informatique&Libertés et les sanctions applicables ; • Le responsable du SIS a la possibilité de faire réaliser des audits de sécurité des dispositions prises par le fournisseur pour la réalisation de sa prestation.	**Palier 1 et 2**
[L3]	Les exigences de sécurité suivantes doivent figurer au contrat : • Le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la confidentialité des données lors de transferts de matériel.	**Palier 1 et 2**
[L4]	Les équipements loués doivent présenter des caractéristiques compatibles avec les règles du présent guide. Par exemple, l'établissement doit : • avoir la capacité d'effacement des supports de stockage de dispositifs connectés • pouvoir remettre en configuration d'usine les matériels de type « ordiphone », avec effacement de l'ensemble des données.	**Palier 1 et 2**

ANNEXES

Annexe 1 : Glossaire

Sigle / Acronyme	Signification
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CD	Compact Disc
CST	Centre de la sécurité des télécommunications Canada
ES	Etablissement de Santé
GT	Groupe de Travail
MBR	Master Boot Record
NISP	National Industrial Security Program, États-Unis
NIST	National Institute of Standard and Technology, États-Unis
NSA	National Security Agency, États-Unis
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Personnel de Santé
PTS	Pôle Technique et Sécurité
SD	Secure Digital
SIS	Systèmes d'Information de Santé
USB	Universal Serial Bus

Annexe 2 : Documents de référence

Référence n° 1 : Recommandation sur l'effacement des supports de stockage de masse (ANSSI, 26/05/2010)

Référence n° 2 : Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter (ANSSI, 17/05/2004)

Référence n° 3 : Effacement et nettoyage des supports (CSG-08\G) (CST Canada, 08/2009)

Référence n° 4 : NSA/CSS Storage device declassification manual (NSA, USA, 10/11/2000)

Référence n° 5 : Guidelines for Media Sanitization (NIST, USA, 09/2006)

Référence n° 6 : Operating Manual (DOD 5220.22-M) (NISP, USA, 28/02/2006)

RÉFÉRENTIELS / PGSSI-S - Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé (SIS) – Version V1.0 – Déc. 2014

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