AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Destruction des données lors du transfert de matériel informatique

Guide pratique technique PGSSI-S

Publication : août 2022 | *Classification : Publique* | *Version : v2.0*

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 guide propose un ensemble de règles à appliquer lors de la gestion de tout type de matériel stockant des données sensibles.

L'objet de ces règles est d'apporter l'assurance que, lors du transfert d'un matériel vers un contexte d'utilisation différent, les données des Systèmes d'Information de Santé (SIS) présentes sur le(s) support(s) de stockage que comporte ce matériel sont détruites de manière à empêcher toute récupération de ces données. Ces règles sont établies sur la base d'un ensemble de documents de référence présentés en Annexe 1 « Fondements du guide ».

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

Ce document s'adresse :

- Aux responsables de structure utilisatrice de matériel informatique ;
- Aux personnes agissant sous leur responsabilité, et 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 désigner toute personne en charge de 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 qui permettent d'éviter une divulgation de données sensibles dématérialisées (*telles que données de santé, données à caractère personnel, données relevant du secret professionnel…*) quand des 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 type de transfert vise le changement d'utilisateur d'un matériel au sein d'une même structure. Il nécessite la suppression des données avant que le matériel puisse être réutilisé.
- **Transfert externe de matériel en dehors de la structure** :
  Les situations envisageables sont multiples. On peut citer 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*) ;
  - Le retour du matériel à son propriétaire en fin de location ;
  - La cession du matériel à un tiers (*par exemple don à une association pour réemploi du matériel, vente*…).

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

Les équipements suivants, qui sont des matériels de stockage de données ou qui sont susceptibles d'intégrer des supports de stockage de données, font partie du périmètre d'application du guide (liste non exhaustive) :

Catégorie	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 biomédical…
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 pour désigner un ordiphone.

[2] Ces équipements peuvent contenir des données entrant dans le cadre du présent document (par exemple *photos, notes, contacts, messages*…).

3 Ces équipements peuvent, par exemple, permettre l'accès à des données de santé à caractère personnel.

1.3. Limites du périmètre d'application du guide

Données « matérialisées »

Ce guide concerne uniquement la destruction de données dématérialisées présentes sur un support de stockage numérique.

La destruction d'informations « matérialisées » sur des supports papier (*impressions*…) ou des films plastiques (*microfilms*…), que ces informations soient lisibles directement (*texte, image*…) ou via un codage numérique visuel (*QRCode*…), n'est pas traitée dans le présent guide. La destruction d'informations rémanentes éventuellement présentes sur certaines parties de matériel d'impression (*tambour, tonner*…) n'est pas non plus traitée dans le présent guide.

Stockage de données « dans le cloud »

Le recours à un prestaire de service, ou plus généralement à un tiers, pour assurer le stockage de données est hors du périmètre de ce guide. Le contrat établi avec le tiers doit toutefois permettre, directement ou via une certification HDS, d'obtenir les mêmes garanties de destruction des données lors du changement de contexte d'usage des supports de stockage mis en œuvre que celles poursuivies par ce guide.

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.

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.

Enquête sur les données

En cas d'enquête portant sur les données présentes sur un support, qu'elle soit d'origine interne ou externe[4], toute procédure d'effacement impliquant ce support doit être suspendue jusqu'à conclusion de ladite enquête.

Destruction des données à distance

Il est recommandé que tout terminal nomade, s'il stocke des données sensibles, dispose de fonctionnalités d'effacement des données activable à distance en cas de perte ou de vol du terminal. Ce type de destruction de données ne fait pas partie du périmètre couvert par le présent guide.

[4] Ordonnance d'un juge par exemple

2. ENJEUX RELATIFS A LA DESTRUCTION DE DONNEES

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

Ces opérations s'effectuent parfois sous le contrôle direct de l'utilisateur d'un équipement (*par exemple copie ou sauvegarde manuelle de données vers un disque dur externe*). 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 ou la numérisation de documents, sauvegarde technique automatique…*).

Le cycle de vie des équipements (*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 équipements et aux données qu'ils contiennent. C'est du risque d'accès illégitime d'un tiers aux données contenues dans l'équipement dont on veut se protéger.

Ce risque pourrait engager la responsabilité pénale du responsable de traitement concerné, ou 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 à ce responsable de prendre les mesures nécessaires pour se protéger contre ce risque.

C'est pourquoi il est essentiel de s'assurer, lorsqu'on perd la maîtrise d'un équipement qui contient des données sensibles, de mettre en œuvre un processus qui garantit l'inaccessibilité définitive de ces données, afin d'en empêcher la fuite et l'exploitation illicite.

3. PRINCIPES ESSENTIELS A APPLIQUER

3.1. 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 sont susceptibles d'avoir été stockées doit faire l'objet d'un traitement spécifique avant son transfert, que ce soit pour sa réutilisation en interne, sa remise à un tiers externe ou sa mise au rebut.

Les traitements du matériel avant son transfert peuvent être de deux types selon la sensibilité des données qu'il est susceptible d'avoir stocké d'une part, et selon la nature du matériel d'autre part :

- Effacement des données stockées sur le matériel ;
- Retrait des supports de stockage de données du matériel (le cas échéant) pour procéder ensuite à leur destruction physique.

Les principes suivants sont appliqués dans ce guide :

- La « suppression logique » de fichiers ou d'autres formes de stockage de données à l'aide de fonction accessibles de manière simple à l'utilisateur est insuffisante pour assurer la suppression effective des données concernées ;
- L' « écrasement logique » des données par remplissage de l'ensemble du support de stockage par des données nulles, aléatoires ou par d'autres motifs est suffisante pour rendre inaccessibles les données uniquement face à des tentatives d'accès illicite à ces données ne s'appuyant que sur des moyens limités ;
- La mise en œuvre de procédures garantissant l'inaccessibilité définitive des données est requise pour la suppression effective des données face à des tentatives d'accès illicite à ces données s'appuyant sur des moyens importants. Ces procédures peuvent s'appuyer :
  - Sur des mécanismes de chiffrement permettant de rendre les données définitivement inaccessibles avec un niveau de confiance élevé dès lors que les clés chiffrement/déchiffrement sont effacées de manière fiable. Ce niveau de confiance élevé nécessite au minimum la mise en œuvre à l'état de l'art de processus et moyens cryptographiques cohérents avec les enjeux liés aux données concernées ou la mise en œuvre de fonctions d'effacement intégrées aux matériels de stockage conformes à des normes ou standards industriels fiables qui garantissent leur efficacité totale ;
  - Ou à défaut, sur la destruction physique du support de données par des méthodes appropriées à sa nature.

☞ Afin de satisfaire aux exigences légales et règlementaire relatives au traitement des déchets d'équipements électriques et électroniques [DEEE], il est généralement nécessaire de recourir aux services d'une entreprise spécialisée de ce secteur afin d'assurer la destruction physique des matériels de stockage selon des modalités permettant leur recyclage et/ou leur traitement comme déchet.

Le contrat de service correspondant doit alors apporter des garanties quant à la préservation de la confidentialité des données stockées sur les supports confiés pour destruction (voir chapitre 4.4.2).

Pour rappel, les responsables du SIS 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, au vu de l'analyse de risques.

3.2. Utilisation du guide et paliers d'applicabilité

Le guide énonce au chapitre 4 des règles de sécurité dont l'application est du ressort du responsable du SIS. Ces règles 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 qui leur sont attribués individuellement, qui sont sous leur contrôle et qui sont connectés au SIS (*clés USB, ordiphone…*).

Deux paliers sont définis pour la mise en œuvre des règles de sécurité applicables à la destruction de données lors du transfert de matériel :

- Le palier 1, porteur des règles minimales qui s'appliquent au palier 1 dans tous les cas, ainsi qu'au palier 2 quand aucune règle spécifique au palier 2 ne s'y substitue ;
- Le palier 2, porteur des règles qui complètent ou, le cas échéant, remplacent les règles minimales du palier 1 afin d'offrir un niveau de sécurité renforcé.

Le chapitre 4 rappelle à quel(s) palier(s) chaque règle doit être appliquée.

Les critères de sélection du palier à appliquer sont les suivants :

Palier 1

- **Règles visant à protéger contre des tentatives d'accès aux données s'appuyant sur des moyens limités :**
  - Tentatives d'accès basiques (*ex : simple branchement et consultation du support de stockage…*) ;
  - Tentatives d'accès avec compétences (*ex : accès logique « bas niveau » au support de stockage, usage d'outils logiciels de récupération de données effacées disponibles sur le marché…*) ;
  - Généralement réalisées de manière opportuniste.
- **Palier pouvant être sélectionné :**
  - S'il est certain que le matériel considéré n'a jamais stocké de données à caractère personnel ni d'autres données sensibles depuis sa mise en service (i.e. y compris durant ses usages avant éventuelle réaffectation interne) ;
  - **Ou** si le transfert du matériel reste interne à la structure.

Palier 2

- **Règles visant à protéger contre des tentatives d'accès aux données s'appuyant sur des moyens importants :**
  - Tentatives d'accès expertes (*ex : analyse des composants du support de stockage en laboratoire…*) ;
  - Généralement réalisées de manière ciblée, avec des objectifs de récupération de données bien définis.
- **Palier à sélectionner si le matériel considéré :**
  - Est susceptible de contenir des données à caractère personnel ou d'autres données sensibles ;
  - **Et** est transféré à un tiers externe à la structure (hors cas du transfert à un prestataire spécialisé pour la destruction de ce matériel).
- **Palier à sélectionner également dans le cas où le matériel considéré ne fonctionne plus normalement.**

3.3. Cas des données stockées sous forme chiffrée

Les données peuvent se trouver être stockées sur le support de données sous forme chiffrée selon trois types de modalités (non exclusives les unes des autres) :

- Elles peuvent avoir été chiffrées spécifiquement au niveau applicatif ;
- Elles peuvent avoir été chiffrées par un dispositif générique (i.e. non spécifique à l'application) au niveau du système d'exploitation ;
- Elles peuvent avoir été chiffrées par un dispositif générique intégré au dispositif de stockage ; C'est typiquement le cas des disques qualifiés de « Self-Encrypting Drive » ou « SED », c'est-à-dire de « disque auto-chiffrant ».

Quand ces différentes solutions de chiffrement des données sont conçues et mises en œuvre en conformité avec la réglementation et l'état de l'art en matière de cryptographie, il peut être considéré que la destruction des données concernées se réduit à la destruction de clés cryptographique nécessaires à leur déchiffrement.

Dès lors, l'opération de destruction des données est fortement facilitée, puisque qu'il suffit d'assurer l'écrasement sûr (conforme au palier 2) de quelques kilo-octets de données (les clés cryptographiques) là où il aurait fallu procéder à l'écrasement sûr de giga-octets, de téraoctets, voire de pétaoctets, écrasement potentiellement irréaliste du point de vue de leur durée, voire irréalisable de manière effective selon la technologie de stockage utilisée (*cas de disques SSD par exemple*).

Dans les cas de « Self-Encrypting Drive », la capacité d'écrasement de la clé de chiffrement/déchiffrement confinée dans le disque est généralement désignée sous le nom de « cryptographic erase » ou « effacement cryptographique ».

☞ **Règlementation et état de l'art en matière de cryptographie auxquels les solutions de chiffrement de données doivent se conformer pour que la destruction des données puisse bénéficier de la simplification exposée ci-dessus :**

- Référentiel Général de Sécurité - Version 2.0 [RGS],
  - Annexe B1 : « Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » [RGS-B1],
  - Annexe B2 : « Gestion des clés cryptographiques - Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques [RGS-B2]
- Guide des mécanismes cryptographiques [CRYPTO], publié par l'ANSSI ;
- Guide de sélection d'algorithmes cryptographiques [CRYPTOSEL], publié par l'ANSSI.

4. REGLES DE SECURITE APPLICABLES LORS DU TRANSFERT DE MATERIELS

4.1. Règles organisationnelles

N°	Règle	Paliers d'applicabilité
[O1]	La destruction de données doit être réalisée sous la responsabilité du responsable du SIS, par le personnel de la structure et/ou par des prestataires techniques externes exclusivement dans le cadre de contrats de prestation de service.	Paliers 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*…). *A titre d'exemple, la charte informatique de la structure peut prévoir que les utilisateurs de supports de stockage amovibles sont chargés de l'application des règles d'effacement lors du transfert de ces matériels.*	Paliers 1 et 2
[O3]	Afin de satisfaire aux exigences légales et règlementaire relative au traitement des déchets d'équipements électriques et électroniques [DEEE], il est généralement nécessaire de recourir aux services d'une entreprise spécialisée de ce secteur afin de d'assurer la destruction physique des matériels qui stockent des données selon des modalités permettant le recyclage et/ou le traitement des déchets. Ces prestations de service doivent prendre en compte les règles énoncées au chapitre 4.4.	Palier 2
[O4]	Les contrats de prestation de service qui incluent une maintenance ou une location de matériel informatique ou informatisé doivent prendre en compte les règles énoncées respectivement aux chapitres 4.4.3 et 5.	Paliers 1 et 2

4.2. Règles techniques

4.2.1. Règles communes à l'ensemble des supports de stockage

N°	Règle	Paliers d'applicabilité
[R1-a]	Toute réutilisation dans un contexte de sécurité différent ou transfert à un tiers d'un matériel susceptible d'avoir stocké des données à caractère personnel, des éléments secrets (*mot de passe, clé privée, clé symétrique*…) ou d'autres données sensibles doit donner lieu à une opération d'effacement, appliquée à chaque support de stockage de données du matériel, préalablement à la réutilisation ou au transfert.	Paliers 1 et 2

N°	Règle	Paliers d'applicabilité
[R1-b]	Toute transfert à un tiers, y compris envoi en maintenance ou fin de location, d'un matériel susceptible d'avoir stocké de données à caractère personnel, des éléments secrets (*mot de passe, clé privée, clé symétrique*…) ou d'autres données sensibles depuis sa mise en service, doit donner lieu à une opération garantissant l'inaccessibilité définitive des données, appliquée à chaque support de stockage de données du matériel, préalablement au transfert.	Palier 2
[R1-c]	Quand il est fait appel à un prestataire de service pour assurer la destruction physique de supports de données, chaque support de données concerné doit faire l'objet de l'effacement prévu par la règle [R1-a] préalablement à sa remise au prestataire de service, sauf à ce qu'il soit porteur d'une défaillance technique interdisant cette opération.	Palier 2
[R1-d]	Les opérations techniques de destruction de données doivent être réalisées en fonction du 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 qui stocke de données devra être traité indépendamment selon les règles applicables. Il convient de s'assurer de ne pas oublier les supports de stockage qui seraient directement connectés à la carte mère (*comme par exemple un disque SSD connecté sur un port NVMe, PCIe, mSATA, M.2, U.2…)*.	Paliers 1 et 2
[R1-e]	L'effacement des données d'un support de stockage doit garantir qu'aucune donnée n'est plus accessibles par aucun moyen logiciel accessible via un système d'exploitation standard. *Par exemple, l'écriture d'un motif quelconque (tous les bits à zéro ou à un, valeur aléatoire, …) sur l'ensemble de l'espace adressable de bas niveau du support de stockage répond à cette exigence.* Bien évidemment, la simple réinstallation du système d'un équipement n'est de façon générale pas suffisante pour assurer l'effacement des données précédemment stockées.	Paliers 1 et 2
[R1-f]	Après les opérations d'effacement, et avant le transfert du matériel à un tiers ou au prestataire en charge de la destruction du matériel, toute batterie du matériel doit être retirée, et l'alimentation électrique du matériel doit être débranchée pendant au minimum 10 minutes, afin d'assurer l'effacement de toute information présente en mémoire RAM. Si possible, les connexion internes de l'alimentation au reste de l'équipement doivent être débranchée pendant cette durée. Batteries et connexions peuvent ensuite être rebranchées si le matériel est destiné à être réemployé et que les modalités de destruction de données mise en œuvre l'y autorisent.	Palier 2
[R1-g]	Les équipements utilisés pour réaliser la destruction physique de matériel ayant stocké des données doivent être conformes aux standards en vigueur [ISO27040] pour la destruction du type de matériel considéré.	Palier 2

4.2.2. Règles techniques spécifiques aux disques durs

Le terme « disque dur » couvre ici aussi les disques durs « classiques » qui s'appuient sur des disques magnétiques, les « disques » SSD qui s'appuient sur de la mémoire flash et les disques hybrides qui combinent un disque dur « classique » et un SSD.

Des règles spécifiques à certains types de disques sont proposées en complément de celles applicables à tous types de disques durs.

N°	Règle	Paliers d'applicabilité
[R2-a]	Un effacement complet des données présentes sur le support doit être effectué. Cet effacement peut être réalisée par l'une des méthodes suivantes, selon leur disponibilité pour le matériel considéré, leur facilité de mise en œuvre ou la durée nécessaire à leur d'exécution : ► Utilisation d'un logiciel spécialisé dans l'effacement des données, qui sélectionne généralement la méthode d'effacement optimale en fonction des capacités fonctionnelles du disque ; ► Suppression de l'ensemble des partitions, recréation d'une partition occupant l'ensemble de l'espace de stockage du support, puis formatage « à zéro » du support (i.e. sans l'option « formatage rapide », avec réécriture de valeur zéro sur l'ensemble de l'espace disponible) ; ► Ecriture d'un motif quelconque (tous les bits à zéro ou à un, valeur aléatoire, …) sur l'ensemble de l'espace adressable du support de stockage, une seule passe étant suffisante, puis recréation d'une table de partitions ; ► Utilisation d'une fonction de remise en « configuration de sortie d'usine » ou d'« effacement sécurisé » du matériel, généralement à l'aide d'un logiciel mis à disposition par le constructeur, à condition que le constructeur spécifie expressément que l'usage de cette fonction réinitialise à zéro ou rend inaccessibles les données précédemment stockées.	Paliers 1 et 2
[R2-b]	**Cette règle est spécifique aux « self-encrypting drives (SED) »** (voir chapitre 3.3) ► La capacité d' « effacement cryptographique » (« cryptographic erase ») d'un SED peut être utilisée pour assurer l'équivalent d'un écrasement logique des données stockées sur le disque. ► La fonction du disque utilisée à cette fin doit être documentée par le constructeur comme réalisant cet « effacement cryptographique ». Elle est généralement accessible via les outils mis à disposition par le constructeur. ► Quand elle est disponible, cette méthode devrait être préférée aux autres.	Paliers 1 et 2
[R2-c]	► Les commandes « de bas niveau » standard d'effacement parfois disponibles pour certains supports de stockage (*comme par exemple les instruction ATA « Erase Unit » ou « Security Erase Unit » de certains disques durs*) ne peuvent pas être, de façon générale, considérées comme des solutions fiables pour garantir l'écrasement logique des données stockées dans un disque dur magnétique, un SSD [5] ou un disque hybride, et ne sont donc pas utilisables dans ce contexte, sauf garantie forte d'efficacité apportée par le constructeur du disque *(par exemple attestée par une certification, un rapport d'audit...*) ► Les commandes « de bas niveau » standard ATA d'effacement appartenant au groupe « SANITIZE feature set » (notamment SANITIZE BLOCK ERASE ou SANITIZE CRYPTOGRAPHIC SCRAMBLE), quand elles sont supportées, peuvent néanmoins être utilisées pour réaliser l'écrasement logique des données stockées dans un disque dur.	Paliers 1 et 2

[5] En effet, des tests en laboratoire ont montré que l'efficacité de ces commandes était extrêmement variable d'un constructeur et d'un modèle de support de stockage à l'autre, et que les mises en œuvre réellement efficaces étaient minoritaires dans le cas des disques SSD (voir [Wei]).

N°	Règle	Paliers d'applicabilité
[R2-d]	Le « disque dur » support des données doit être : ► Soit soumis à un processus de purge de données effectué par un logiciel spécialisé ; ► Soit détruit physiquement par broyage ou incinération, sauf si d'autres options spécifiques au type de disque considéré sont permises par les règles qui suivent, et qu'elles sont effectivement applicables au matériel considéré.	Palier 2
[R2-e]	Les logiciels spécialisés dans l'effacement des données, utilisables dans le cadre du palier 2, doivent, outre les opérations de purge des données : ► Assurer la vérification du bon effacement des données ; ► Produire un rapport des opérations d'effacement et de vérification ; ► Disposer d'une certification de sécurité attestant son efficacité pour le type de disque considéré (magnétique, SSD, hybride, les types supportés devant être explicitement mentionnés), délivrée sous le contrôle soit d'une agence étatique, soit d'un organisme de certification reconnu par l'état en référence à un standard international établi portant sur l'effacement des données. ► Le site Internet de l'ANSSI référence les solutions d'effacement de données (voir [Produits]) auxquelles elle a attribué une certification de sécurité de premier niveau (CSPN).	Palier 2
[R2-f]	**Règle spécifique aux « self-encrypting drives (SED) »** (voir chapitre 3.3) **conformes aux spécifications « Opal » SCC ou « Enterprise » SCC du Trusted Computing Group** ► La capacité d' « effacement cryptographique » (« cryptographic erase ») d'un SED dont le constructeur atteste la conformité aux spécifications « Opal » SCC [Opal] ou « Enterprise » SCC du Trusted Computing Group peut être utilisée pour rendre définitivement inaccessibles les données stockées sur le disque. ► La fonction du disque utilisée à cette fin doit être assurer l'effacement sûr de l'ensembles des clés permettant de déchiffrer les données stockées, et leur remplacement par des valeurs issues d'une source d'aléa cryptographiquement sûre. Elle est généralement accessible via les outils mis à disposition par le constructeur. ► La fonction de réinitialisation du disque à son état de "sortie d'usine" prévue par [Opal] permet notamment cet effacement et réinitialisation des clés de chiffrement internes du disque, et ne requiert pour son activation (via le logiciel ad hoc) que la valeur « PSID » de 32 caractères imprimés physiquement sur l'étiquette apposée sur le disque par son constructeur. ► Il est recommandé de procéder à la réinitialisation du disque à son état de "sortie d'usine" au moment de sa mise première en service.	Palier 2

☞ Il est fortement recommandé de ne pas utiliser directement de commande bas niveau ATA pour lancer des opérations d'effacement de données sur un disque dur externe connecté via USB. Les possibles incompatibilités entre l'interface USB/ATA avec ces commandes et les potentiels dépassement de délai des communications USB peuvent provoquer des dysfonctionnements allant éventuellement jusqu'au blocage définitif du disque.

L'usage de l'utilitaire de gestion de disque mis à disposition par le constructeur est préconisé pour effectuer les opérations d'effacement.

4.2.3. Règles spécifiques aux autres supports de stockage utilisant de la mémoire flash : clé USB, carte SD, Compact Flash…

N°	Règle	Paliers d'applicabilité
[R3-a]	Un effacement complet des données présentes sur le support doit être effectué. Cet effacement peut être réalisée par l'une des méthodes suivantes, selon leur disponibilité pour le matériel considéré, leur facilité de mise en œuvre ou la durée nécessaire à leur d'exécution : ► Utilisation d'un logiciel spécialisé dans l'effacement des données, qui sélectionne généralement la méthode d'effacement optimale en fonction des capacités fonctionnelles du disque ; ► Suppression de l'ensemble des partitions, recréation d'une partition occupant l'ensemble de l'espace de stockage du support, puis formatage « à zéro » du support (i.e. sans l'option « formatage rapide », avec réécriture de valeur zéro sur l'ensemble de l'espace disponible) ; ► Ecriture d'un motif quelconque (tous les bits à zéro ou à un, valeur aléatoire, …) sur l'ensemble de l'espace adressable du support de stockage, une seule passe étant suffisante, puis recréation d'une table de partitions ; ► Utilisation d'une fonction de remise en « configuration de sortie d'usine » ou d'« effacement sécurisé » du matériel, généralement à l'aide d'un logiciel mis à disposition par le constructeur, à condition que le constructeur spécifie expressément que l'usage de cette fonction réinitialise à zéro ou rend inaccessibles les données précédemment stockées.	Paliers 1 et 2
[R3-b]	Le support de données utilisant de la mémoire flash doit être détruit physiquement par broyage ou incinération.	Palier 2

4.2.4. Règles spécifiques aux disques optiques (CD-Rom, DVD…)

N°	Règle	Paliers d'applicabilité
[R4-a]	Le palier 1 n'est pas applicable aux disques optiques : qu'ils soient à écriture unique ou réinscriptibles, les supports de stockage de type disques optiques ne doivent pas être transférés.	Palier 1 non applicable
[R4-b]	Les disques optiques doivent être détruits physiquement par broyage, incinération ou meulage.	Palier 2

4.2.5. Règles spécifiques aux bandes magnétiques (dont cartouches DDS, DLT…)

N°	Règle	Paliers d'applicabilité
[R5-a]	Un effacement complet, appliqué à la totalité de la bande magnétique, doit être réalisé : ► Soit à l'aide du logiciel de sauvegarde ; ► Soit à l'aide des commandes système adéquates ; ► Soit en remplissant l'ensemble de l'espace adressable du support de stockage par un motif quelconque (*tous les bits à zéro ou à un, valeur aléatoire*…), une seule passe étant suffisante.	Paliers 1 et 2
[R5-b]	Les bandes magnétiques doivent être détruites physiquement par broyage ou incinération.	Palier 2

4.2.6. Règles spécifiques aux cartes à microcircuits ou « cartes à puce »

N°	Règle	Paliers d'applicabilité
[R6-a]	Le palier 1 n'est pas applicable aux cartes à microcircuits (*cartes SIM, CPS*…) car les informations qu'elles comportent ne peuvent généralement pas être effacées. Les supports de type cartes à microcircuits ou « cartes à puce » ne doivent pas être transférés.	Palier 1 non applicable
[R6-b]	Les cartes à microcircuits (*cartes SIM, CPS*…) doivent être détruites physiquement par broyage du circuit ou incinération.	Palier 2

4.2.7. Règles applicables aux ordiphones, téléphones portables, tablettes et aux autres matériels

N°	Règle	Paliers d'applicabilité
[R7-a]	Les données des ordiphones (ou « smartphones »), tablettes et téléphones portables, ainsi que celles des matériels stockant des informations sur des supports autres que ceux spécifiés jusqu'ici (*par exemple, des équipements participants à un dispositif médical…*), doivent être effacées à l'aide des fonctions correspondantes des diverse applications utilisées, puis par application de la procédure prévue par le constructeur pour remise de l'appareil en configuration de sortie d'usine[6].	Paliers 1 et 2
[R7-b]	Les données des cartes mémoire et des autres supports de stockage additionnels éventuels doivent être effacées soit dans la cadre de la procédure mise en œuvre conformément à la règle [R7-a], soit séparément à l'aide des techniques applicables à ces types de supports.	Paliers 1 et 2
[R7-c]	Les cartes mémoire additionnelles et autres supports de stockage additionnels éventuels doivent être retirés et détruits séparément à l'aide des techniques applicables à ce type de support.	Palier 2
[R7-d]	Les parties « informatiques » de l'appareil, comprenant processeurs informatiques, mémoires intégrées, etc. doivent être détruites physiquement par broyage ou incinération.	Palier 2

4.3. Procédures

N°	Règle	Paliers d'applicabilité
[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.	Paliers 1 et 2
[P3]	Les procédures de gestion du cycle de vie de tout matériel informatisé doivent prendre en compte la possibilité de désassembler le matériel (ex. démontage des disques durs d'un poste de travail). Tout élément de stockage de données issu du désassemblage 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
[P4]	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 (*par exemple, en consultant une attestation établie par le dernier utilisateur de l'équipement, confirmant que toute*	Paliers 1 et 2

[6] 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.

N°	Règle	Paliers d'applicabilité
	donnée utile a bien été copiée ailleurs ou sauvegardée). Dans le cas contraire, il convient de procéder à la sauvegarde de ces données.	
[P5]	Une fois l'effacement terminé, Il est nécessaire de vérifier que le support ne contient plus de donnée qui soit accessible par les moyens correspondant au palier retenu. Un contrôle par échantillonnage, c'est-à-dire uniquement de certains emplacements du support de stockage et non pas de l'ensemble du support, est suffisant pour assurer cette vérification (*voir [ISO27040] chapitre 6.8.1.5 pour un exemple de modalités de vérification*). Un effacement ne peut être considéré comme réalisé qu'à la condition que cette vérification confirme le bon effacement des données.	Paliers 1 et 2
[P6]	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*…) ; ► Nature du matériel (*ex : ordinateur, disque dur, SSD, clé USB*…) ; ► Ancien propriétaire ou responsable (entité, ou à défaut personne physique) ; ► Nouveau propriétaire ou responsable (entité, ou à défaut personne physique) ; ► Date de transfert effectif de l'équipement au nouveau propriétaire ou responsable ; ► Date et nature de l'opération d'effacement ou de destruction effectuée (*identité et visa de l'opérateur, type d'effacement ou de destruction, résultat de vérification de l'effacement*…) ; ► Si cette opération a été confiée à un prestataire, procès-verbal (ou référence du procès-verbal disponible par ailleurs) de l'opération d'effacement ou de destruction effectuée par le prestataire.	Paliers 1 et 2

4.4. Règles relatives aux contrats de service portant sur le matériel

4.4.1. Règles communes à tous les types de contrats de service portant sur le matériel

N°	Règle	Paliers d'applicabilité
[G1]	Les clauses générales suivantes doivent figurer aux contrats : ► Le prestataire de service 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] et la loi « informatique et libertés » [L78-17] pour les interventions réalisées hors Union Européenne ; ► Le prestataire est tenu de déclarer tout changement relatif à sa situation administrative ; ► Le prestataire doit soumettre toute sous-traitance de prestation à l'autorisation du responsable du SIS.	Palier 2
[G2]	Si le prestataire recourt à la sous-traitance, il doit pour chaque sous-traitant ultérieur : ► Répercuter les exigences qui lui sont applicables vers le sous-traitant. Chaque sous-traitance ultérieure doit être encadrée par un contrat qui comporte notamment les mentions suivantes : les activités sous-traitées, l'identité et les coordonnées du sous-traitant, les dates du contrat	Palier 2

N°	Règle	Paliers d'applicabilité
	de sous-traitance, la répartition des rôles et responsabilités entre le prestataire et son sous-traitant ; ► S'assurer que le sous-traitant respecte les mêmes obligations de sécurité que celles du contrat conclu avec son client ; ► S'assurer que le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques, juridiques et organisationnelles adaptées à la prestation de service.	
[G3]	Les clauses de sécurité suivantes doivent figurer aux contrats : ► Le prestataire doit s'engager à protéger la confidentialité des informations présentes sur les supports de données qui lui sont confiés pour destruction, et plus généralement à ne pas tenter d'accéder à ces informations ; ► Le prestataire doit avoir établi une charte de sécurité ou un document équivalent, opposable à son personnel participant aux prestations de service fournies, fixant les bonnes pratiques, interdictions et obligations auxquels ce personnel est soumis, et rappelant notamment les dispositions du RGPG, celles relatives au secret professionnel et les sanctions applicables en cas de manquement ; ► Chaque personne susceptible de manipuler ces supports doit avoir signé un engagement individuel de confidentialité et de respect de la charte mentionnée ci-dessus ; ► Le prestataire doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour assurer la traçabilité des supports de données qui leur sont confiés et lutter contre les incidents pouvant affecter la confidentialité des données qu'ils contiennent ; ► Le prestataire doit, sur demande du responsable du SIS, communiquer à ce dernier le rapport de synthèse d'un audit menée par un tiers et confirmant la bonne mise en œuvre de moyens et procédures prévues pour la traçabilité de supports de donnée et la protection de la confidentialité des données qu'ils contiennent ; ► Le responsable du SIS doit avoir la possibilité de faire réaliser des audits de sécurité portant sur les dispositions mises en œuvre par le fournisseur pour la réalisation de sa prestation.	Palier 2

4.4.2. Contrats d'externalisation de la destruction des supports de données

Afin d'assurer la destruction des supports de données qui le requiert tout en respectant les obligations relatives au traitement des déchets d'équipements électriques et électroniques, il est généralement nécessaire de recourir à un prestataire spécialisé.

Dans ce cas, les règles suivantes doivent être prises en compte dans le contrat de prestation en complément de celles indiquées au chapitre 4.4.1.

N°	Règle	Paliers d'applicabilité
[D1]	Le processus de destruction de matériel stockant des données doit être précisé dans le contrat ou dans une annexe au contrat. Ce processus doit comprendre : ► Au moment du transfert effectif du matériel à détruire au prestataire : • La remise par le prestataire d'une attestation de prise en charge de matériel pour destruction précisant notamment les supports de stockage de données à traiter spécifiquement,	Palier 2

N°	Règle	Paliers d'applicabilité
	• La remise au prestataire d'un récépissé pour l'attestation de prise en charge reçue ; ► Après la destruction effective de l'ensemble des supports de stockage de données portés sur la même attestation de prise en charge : • La remise par le prestataire d'un procès-verbal de destruction répondant aux exigences de la règle [P6] fixée au chapitre 4.3 ; ► 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.	
[D2]	Le contrat doit préciser : ► L'engagement du prestataire quant au délai maximal entre la prise en charge par le prestataire les supports de stockage de données à détruire et la destruction effective de ces supports ; ► L'engagement du prestataire quant au délai maximal entre la destruction effective des supports de stockage de données et la remise du procès-verbal de destruction ; ► L'engagement du prestataire à mettre en œuvre des mesures répondant aux règles [P1] et [P5] fixées au chapitre 4.3.	Palier 2

4.4.3. Contrats de location et/ou de maintenance de matériel informatique ou informatisé

Lorsque le responsable du SIS s'appuie sur des contrats de location et/ou de maintenance de matériel informatique ou informatisé, des règles spécifiques concernant la gestion du matériel et la destruction des données doivent être intégrées à ces contrats de prestation en complément de celles indiquées au chapitre 4.4.1.

N°	Règle	Paliers d'applicabilité
[M1]	Toute intervention du prestataire sur un support de données ou sur un matériel comportant des supports de données ne doit être mené qu'avec l'autorisation explicite du responsable du SIS ou de son représentant, et le cas échéant sous sa supervision s'il le juge nécessaire.	Paliers 1 et 2
[M2]	Tout retrait de support de données ou de matériel comportant des supports de données, à fin de maintenance, dans le cadre d'un retour en fin de contrat de location ou pour toute autre raison, ne peut avoir lieu qu'avec l'autorisation explicite du responsable du SIS ou de son représentant, et en respectant les processus établis afin d'assurer la traçabilité de l'opération et la protection de la confidentialité des données.	Paliers 1 et 2
[M3]	Sauf si une défaillance du matériel l'interdit, l'ensemble du processus d'effacement préalable à tout transfert de support de données à un tiers doit être appliqué par les personnes autorisées par le responsable du SIS avec la remise effective du matériel au prestataire.	Paliers 1 et 2
[M4]	Un support de données ne peut être transféré au prestataire que selon l'une des modalités suivantes, si elle est prévue au contrat, et applicable selon la nature du matériel et son état de fonctionnement :	Palier 2

N°	Règle	Paliers d'applicabilité
	► Si une méthode garantissant l'inaccessibilité définitive des données et non destructive pour le support de données, conforme aux exigences du palier 2, a pu être appliquée avec succès au support de données, ce support peut être transféré au prestataire ; ► Si seule une méthode n'assurant que l'écrasement logique des données, conforme au palier 1, a pu être appliquée avec succès au support de données, ce support peut être transféré au prestataire s'il s'engage à en interdire toute réutilisation et en assurer ou en faire assurer la destruction. Les modalités énoncées au chapitre 4.4.2 doivent alors être intégrées. ► A défaut, le responsable de traitement ou son représentant doivent fournir au prestataire un engagement de destruction du support concerné, et transmettre au prestataire -s'il le souhaite- une copie du procès-verbal de destruction une fois celle-ci effectuée. La dernière modalité, étant une solution de dernier recours qui intègre notamment l'absence de retour du matériel en cas de panne sous garantie, doit impérativement être prévue au contrat, avec le cas échéant les modalités spécifiques associées (*par exemple production d'un diagnostic de défaillance par un outil fourni par le constructeur, compensation financière*…).	

5. RECOMMANDATIONS

Les recommandations qui suivent visent à faciliter les opérations de destruction des données et/ou à en réduire les coûts financiers ou environnementaux (réutilisation du matériel plutôt que destruction).

Protection de la confidentialité des données :

- Appliquer systématiquement le palier 1 en cas de transfert interne à la structure de support de données, même si ce support n'a a priori jamais stocké de données sensibles.

Simplification des procédures de gestion des supports de données :

- Appliquer systématiquement le palier 2 dès lors que l'équipement est transféré à un tier[7]. Ce principe évite notamment de devoir conserver l'historique des affectations de l'équipement et de la potentielle présence de données sensible sur ses supports de stockage à un moment ou un autre de son utilisation ;
- Utiliser un logiciel spécialisé dans l'effacement des données, qui sélectionne généralement la méthode optimale en fonction des capacités fonctionnelles du disque, et intègre la vérification du bon effacement des données (quand c'est pertinent) ;
- Mettre en œuvre, au niveau applicatif ou au niveau du systèmes d'exploitation ou système de fichiers, un chiffrement des données stockées conforme à la règlementation et état de l'art en la matière (voir chapitre 3.3) en assurant le stockage des clés cryptographiques utilisées sur un support duquel elles pourront être effacée de façon sûre et simple (*par exemple un « Self-Encrypting Drive » - voir ci-dessous*)

Sélection des supports de stockage ou des matériels intégrant un stockage de données :

- Pour les « disques durs », favoriser les disques intégrant le chiffrement des données (« Self-Encrypting Drive » ou SED) et proposant une fonction d'« effacement » de type « Cryptographic Erase » par lequel les clés de chiffrement/déchiffrement utilisées pour le chiffrement intégré peuvent être réinitialisées. Cette fonction rend ainsi inaccessibles « en clair » les données (puisque chiffrées avec une clé désormais inutilisable) sans nécessiter un effacement effectif de l'ensemble du disque, cette opération ne nécessitant généralement que quelques minutes ;
- Parmi les « Self-Encrypting Drive », favoriser les disques indiquant être conforme aux spécifications « TCG Storage Security Subsystem Class: Opal Specification » [Opal] ;
- S'assurer que le constructeur du matériel met à disposition une fonctionnalité ou un utilitaire permettant d'exploiter la fonctionnalité d'effacement des données ou de « réinitialisation usine ».

[7] A l'exception des mesures de destruction confiées au prestataire en charge de la destruction des supports quand c'est à lui et dans ce cadre que les supports sont transférés.

Annexe 1 : Fondements du guide

Le présent guide propose des dispositions de sécurisation permettant d'encadrer la destruction des données lors 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.

Elles sont issues des bonnes pratiques en matière de SSI notamment celles identifiées dans les documents de référence suivants :

- CNIL : Effacer ses données d'un ordinateur, d'un téléphone ou d'une tablette avant de s'en séparer (16/12/2020)
  https://www.cnil.fr/fr/effacer-ses-donnees-dun-ordinateur-dun-telephone-ou-dune-tablette-avant-de-sen-separer
- ISO/IEC 27040:2015 - Technologie de l'information - Techniques de sécurité - Sécurité de stockage
- NIST Special Publication 800-88 Revision 1 – December 2014 (05/02/2015) - Guidelines for Media Sanitization
  https://doi.org/10.6028/NIST.SP.800-88r1
  NIST (National Institute of Standards and Technology - USA)
- NSA/CSS Storage Device Sanitization And Destruction Manual 04/12/2020
  https://www.nsa.gov/Resources/Media-Destruction-Guidance/
  NSA/CSS (National Security Agency/Central Security Service - USA)
- TCG Storage Security Subsystem Class: Opal Specification
  https://trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/
  TCG (Trusted Computing Group)
- ANSSI : Produits certifiés CSPN, section Effacement de données
  https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/

Annexe 2 : Documents cités en référence

Réglementation

Renvoi	Document
[DEEE]	En France, l'organisation de la filière des DEEE est réglementée par l'article L.541-10-2 et les articles R.543-172 à R.543-206 du Code de l'environnement pris notamment par le décret n° 2014-928 du 19 août 2014 relatif aux DEEE et aux équipements électriques et électroniques usagés et modifiés par le décret n° 2020-1725 du 29 décembre 2020 portant diverses dispositions d'adaptation relatives à la responsabilité élargie des producteurs.
[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 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
[L78-17]	Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et libertés »
[CSP-L1470]	Articles L. 1470-1 à 1470-5 du code de la santé publique (issus de l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464
[RGS]	Référentiel Général de Sécurité - Version 2.0 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[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

Documents techniques

Renvoi	Document
[Produits]	ANSSI : Produits certifiés CSPN, section Effacement de données https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/
[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/
[ISO27040]	ISO/IEC 27040:2015 - Technologie de l'information - Techniques de sécurité - Sécurité de stockage
[Opal]	TCG (Trusted Computing Group) TCG Storage Security Subsystem Class: Opal Specification https://trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/
[Wei]	Reliably Erasing Data From Flash-Based Solid State Drives - Michael Wei, Laura M. Grupp, Frederick E. Spada†, Steven Swanson, University of California, San Diego https://cseweb.ucsd.edu/~m3wei/assets/pdf/FMS-2010-Secure-Erase.pdf https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf

Annexe 3 : Glossaire

Sigle / Acronyme	Signification
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANS	Agence du Numérique en Santé
ATA	Advanced Technology Attachment
CD	Compact Disc
CST	Centre de la sécurité des télécommunications Canada
DDS	Digital Data Storage
DEEE ou D3E	Déchets d'Équipements Électriques et Électroniques
DLT	Digital Linear Tape
ES	Etablissement de Santé
GT	Groupe de Travail
HDS	Hébergeur de Données de Santé
LTO	Linear Tape - Open
MBR	Master Boot Record
NISP	National Industrial Security Program, Etats Unis
NIST	National Institute of Standard and Technology, Etats Unis
NSA	National Security Agency, Etats 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
SED	Self-Encrypting Drive
SIS	Systèmes d'Information de Santé
USB	Universal Serial Bus