



Caisse Primaire d'Assurance Maladie

**Cahier des Clauses Techniques Particulières
Enlèvement, destruction et/ou revalorisation
du matériel informatique
Marché 2026-002**

Organisme coordonnateur du groupement :

Caisse Primaire d'Assurance Maladie des Hautes-Pyrénées
8 Place au Bois
65000 TARBES
N° SIRET : 777 169 020 00016

Appel d'offres passé en application des Articles L.2124-1, L.2124-2, R.2124-1 et
R.2124-2 du Code de la Commande Publique

SOMMAIRE

ARTICLE 1. OBJET DU MARCHÉ PUBLIC	3
ARTICLE 2. PARTIES CONTRACTANTES	3
ARTICLE 3. LIEU D'EXECUTION	3
ARTICLE 4. DISPOSITIONS GENERALES	4
ARTICLE 5. MODALITES D'EXECUTION	4
5.1 Prestations attendues.....	4
5.2 Collecte, retrait et transport des équipements	4
5.3 Effacement / destruction des données sensibles sur les supports informatiques.....	4
5.4 Modalités de mise en œuvre des prestations	6
5.5 Contrôle des destructions sur le site du titulaire	6
ARTICLE 6. DONS	6
ARTICLE 7. DISPOSITIONS SPECIFIQUES AU LOT 1 - ENLEVEMENT ET DESTRUCTION DU MATERIEL INFORMATIQUE – CTI TOULOUSE	7
ARTICLE 8. DOCUMENTS A FOURNIR.....	7
8.1 Bordereau d'enlèvement	7
8.2 Bordereau de suivi des déchets	7
8.3 Procès-verbal d'effacement des données ou de destruction physique	8
ARTICLE 9. RESPONSABILITE DU TITULAIRE	9

ARTICLE 1. OBJET DU MARCHE PUBLIC

La présente consultation a pour objet l'enlèvement, destruction et/ou revalorisation du matériel informatique des CPAM, CCSS et CTI de la Région Occitanie.

La description des prestations et leurs spécifications techniques sont indiquées dans le présent cahier des clauses techniques particulières (CCTP).

Le titulaire du présent marché public s'engage à une obligation de résultat pour exécuter les prestations objet du présent marché dans les conditions définies ci-après.

Le marché public porte sur des prestations de services.

Les lots 2 à 5 du présent marché sont réservés aux entreprises adaptées (EA), aux établissements et service d'aide par le travail (ESAT) ou toutes structures équivalentes employant des personnes handicapées (relevant des articles L5213-13 du Code du Travail et L344-2 de Code de l'action sociale et des familles), mais également à des structures d'insertion par l'activité économique (SIAE) ou toute structure équivalente (relevant de l'article L.5132-4 du Code du travail), en application des articles L2113-12, L2113-13 et R2113-7 du Code de la commande publique.

ARTICLE 2. PARTIES CONTRACTANTES

En vertu des dispositions de l'article L. 2113-6 du code de la commande publique, les organismes de la région Occitanie :

La Caisse Commune de Sécurité Sociale de la Lozère,
La Caisse Primaire d'Assurance Maladie de l'Ariège,
La Caisse Primaire d'Assurance Maladie de l'Aude,
La Caisse Primaire d'Assurance Maladie de l'Aveyron,
La Caisse Primaire d'Assurance Maladie du Gers,
La Caisse Primaire d'Assurance Maladie de la Haute-Garonne,
La Caisse Primaire d'Assurance Maladie des Hautes-Pyrénées, le coordonnateur,
La Caisse Primaire d'Assurance Maladie de l'Hérault,
La Caisse Primaire d'Assurance Maladie du Lot,
La Caisse Primaire d'Assurance Maladie des Pyrénées-Orientales,
La Caisse Primaire d'Assurance Maladie du Tarn,
La Caisse Primaire d'Assurance Maladie du Tarn et Garonne,
Le Centre de Traitement Informatique de Toulouse,

Ont constitué un groupement de commandes dont le Coordonnateur est la CPAM des Hautes-Pyrénées représentée par sa Directrice, Madame Frédérique BOITARD.

Au terme de la procédure, le marché public est conclu et notifié par le représentant du Coordonnateur.

Dans le cadre de l'exécution des prestations, les parties contractantes sont :

- D'une part : les Organismes de Sécurité Sociale constituant le groupement de commande, compétents pour conclure les bons de commandes ;
- D'autre part : le prestataire de service désigné dans le présent document par l'expression « le titulaire ».

Dans le cadre de l'exécution de l'accord-cadre, le comptable assignataire est le Directeur Comptable et Financier de chaque Organisme commanditaire.

ARTICLE 3. LIEU D'EXECUTION

Les prestations, objet du présent marché, seront exécutées dans les différents sites des organismes dont le siège se situe dans 12 départements :

- Midi-Pyrénées : **Haute-Garonne (31), Ariège (09), Aveyron (12), Lot (46), Hautes-Pyrénées (65), Tarn-et-Garonne (82), Gers (32), Tarn (81) ;**
- Languedoc-Roussillon : **Pyrénées-Orientales (66), Lozère (48), Aude (11), Hérault (34) ;**

ARTICLE 4. DISPOSITIONS GENERALES

Par équipements informatiques, il y a lieu d'entendre : les supports et les matériels informatiques divers. Les supports informatiques contiennent des informations sensibles (dont des données médicales) qui doivent être détruites. Les matériels informatiques (souris, claviers, écrans) ne contenant pas de données sensibles pourront faire l'objet d'enlèvement pour revalorisation (dons, recyclage, ...).

ARTICLE 5. MODALITES D'EXECUTION

5.1 Prestations attendues

- ✓ Enlèvement des matériels informatiques aux différentes adresses des CPAM de la région Occitanie, identifiée en annexe ;
- D'autres adresses dans la région Occitanie qui ne seraient pas mentionnées dans le tableau en annexe ;
- ✓ Destruction des données sensibles sur tous supports en détenant. Les opérations de destruction des données sensibles sur tous supports seront réalisées au choix du commanditaire sur le site du prestataire ou sur le site du client.
- ✓ Revalorisation des équipements informatiques.

5.2 Collecte, retrait et transport des équipements

L'organisme établit une liste des équipements à enlever et/ ou à détruire. Cette liste, jointe au bon de commande, précisera les sites de collecte et la nature des prestations attendues.

Dans les 48h ouvrées suivant la réception de la commande, le titulaire confirmera par retour de mail, la prise en compte du bon de commande.

Les opérations de destruction par broyage (ou équivalent) devront être réalisées au choix du commanditaire, sur le site du prestataire ou sur le site du client, par camion broyeur (ou équivalent).

Pour les opérations d'enlèvement pour revalorisation des équipements informatiques divers, sans données, le titulaire se chargera de récupérer le matériel sur le lieu où il est entreposé ainsi que de l'acheminement nécessaire des supports et matériels informatiques vers le centre de traitement.

En s'adaptant au volume du matériel concerné, il fournira à cet effet les fournitures requises pour le conditionnement :

- Palettes, cartons, film étirable etc. pour les petits matériels ;
- Contenants/Caisse-palette pour le matériel davantage volumineux ;

Le transport devra être réalisé par le biais d'un camion sécurité (camion scellé ou scellé des conteneurs transportant le matériel), prévu à cet effet.

Un agent de l'organisme supervisera l'enlèvement de ces équipements.

Attention : Pendant le trajet, la responsabilité est portée par le propriétaire des données (le responsable des traitements, càd. le Directeur de l'organisme concerné) jusqu'à la destruction.

5.3 Effacement / destruction des données sensibles sur les supports informatiques

En application de l'instruction fonctionnelle de sécurité interne, lorsqu'un support informatique est amené à quitter définitivement un organisme, les données stockées :

- doivent être effacées de manière sécurisée
- ou
- le support d'information doit être détruit

Le tableau ci-dessous illustre les actions à réaliser pour la mise au rebut par catégorie de matériel :

MISE AU REBUT			
SUPPORTS	Endommagé empêchant l'effacement	Données chiffrées : Bitlockées ou autre	Données non chiffrées
SSD y compris supports externes (hors serveurs)	DESTRUCTION SUPPORT	REINITIALISATION PUCE TPM BIOS + SECURE ERASE	SECURE ERASE via BIOS ou via OUTIL CONSTRUCTEUR ou destruction
Disques mécaniques y compris supports externes (hors serveurs)	DESTRUCTION SUPPORT	REINITIALISATION PUCE TPM BIOS + effacement sécurisé une passe	EFFACEMENT MULTIPASSE ou DESTRUCTION SUPPORT
Serveur SSD	DESTRUCTION SUPPORT	REINITIALISATION PUCE TPM BIOS + SECURE ERASE	SECURE ERASE via BIOS ou via OUTIL CONSTRUCTEUR ou destruction
Serveur HDD	DESTRUCTION SUPPORT	REINITIALISATION PUCE TPM BIOS + effacement sécurisé une passe	EFFACEMENT MULTIPASSE ou DESTRUCTION SUPPORT
Imprimante	DESTRUCTION SUPPORT	Soit procédure marché soit destruction hors marché national	Soit procédure marché soit destruction hors marché national
Téléphone mobile	ANALYSE DE RISQUES POUVANT MENER A LA DESTRUCTION si REINITIALISATION USINE IMPOSSIBLE et DONNEES CONFIDENTIELLES ou	REINITIALISATION USINE	REINITIALISATION USINE
Tablette	ANALYSE DE RISQUES POUVANT MENER A LA DESTRUCTION si REINITIALISATION USINE IMPOSSIBLE et DONNEES	REINITIALISATION USINE	REINITIALISATION USINE
supports externes (Clé USB, carte mémoire...)	DESTRUCTION SUPPORT	DESTRUCTION SUPPORT	DESTRUCTION SUPPORT
Switch	DESTRUCTION SUPPORT	REINITIALISATION USINE cf. référentiel switch DR	REINITIALISATION USINE cf. référentiel switch DR

L'effacement des données sensibles ou la destruction des supports doit s'appuyer sur les méthodes décrites dans les articles 5.4.1 à 5.4.3 du CCTP.

5.3.1 Effacement logique des données

Les procédés d'effacements logiques, appelés « wiping » ou « shredding » en anglais, consistent à écrire sur le support une ou plusieurs séries d'octets, déterminés ou aléatoires, en vue de rendre extrêmement difficile la récupération des données initiales. Le support reste parfaitement utilisable par la suite.

Les préconisations techniques :

- pour réinitialiser la puce TPM : opération à effectuer depuis le bios
- pour effacer de manière sécurisée les données qui se trouvent sur un SSD, il faut utiliser un procédé intégré à leur micrologiciel appelé Secure Erase / Sanitize.

Il peut être lancé :

- directement depuis une fonctionnalité présente dans le BIOS du PC (ex : SSD **M2** des portables HP)
- à l'aide d'un outil fournit par le fabricant du SSD (Micron, Sandisk)
- à l'aide d'un outil dédié comme PartedMagic (ex : SSD **SATA** des ACER 2019).
- Pour effacer de manière sécurisée les données qui se trouvent sur les disques mécaniques : faire un effacement logique en utilisant un utilitaire d'effacement de type ShredOS (méthode nwipe multipasse type US DoD 5220.22-M Sort Wipe)

Pour les imprimantes : utiliser la fonction intégrée aux imprimantes du marché, à défaut détruire les supports.

Préférez, s'ils existent, des outils utilisant une méthodologie recommandée par l'ANSSI : <https://cyber.gouv.fr/produits-certifies>

5.3.2 Démagnétisation des supports

Cette opération consiste à « dégausser » (ou démagnétiser) le support avec une suite d'impulsions électromagnétiques.

Elle ne s'applique donc qu'aux disquettes, disques durs et bandes de sauvegarde, mais ne s'applique pas aux supports à mémoire flash (clef USB et disque SSD).

Elle nécessite un matériel spécialisé et blindé pour ne pas endommager les cartes crédits, téléphones portables et autres équipements des personnes qui manipulent l'outil de démagnétisation.

La démagnétisation a l'avantage de pouvoir être appliquée même si le support est endommagé ou ne fonctionne plus. En effet, il est possible de démonter un disque dur qui ne fonctionne plus, généralement à cause de la machinerie qui permet de faire tourner les plateaux, pour récupérer les plateaux et les placer dans un autre disque pour relire les données.

Il est important de noter que certains supports, comme les disques durs modernes, deviennent inutilisables après une démagnétisation, sauf en effectuant un formatage de bas niveau uniquement réalisable par le constructeur du support. Il n'est donc pas envisageable d'utiliser ce procédé si le support doit être réutilisé (cession au « Domaine » ou aux employés de vieux serveurs ou PMFs par exemple).

5.3.3 Destruction physique

Avertissement : aucune solution technique ne garantit l'effacement total des données sur un support (magnétique ou non magnétique) hormis la destruction physique.

Après un effacement logique ou une démagnétisation, il est impossible de garantir qu'il ne reste aucune trace exploitable par des laboratoires équipés de moyens importants ou dotés d'une connaissance fine du mode de fonctionnement des supports. Outre les risques de rémanence d'informations résiduelles, les disques modernes, de plus en plus variés et complexes, présentent en effet un nombre croissant de fonctionnalités (rattrapage de secteurs défectueux, masquage de partitions, etc.) qui contribuent à rendre des portions entières du support inaccessibles via des commandes standards, alors qu'un attaquant ayant la connaissance d'éventuelles commandes spécifiques aux constructeurs ou équipé de matériels adéquats, pourrait retrouver les données qui y sont stockées.

La destruction physique s'applique à tous les supports informatiques.

Les méthodes utilisées par le titulaire peuvent être les suivantes :

- Lumière ultraviolette : pour les EPROM
- Incinération : Bande magnétiques, supports optiques (CD, DVD, BD) , USB, SSD
- Broyage : Disque durs mécaniques, supports optiques (CD, DVD, BD), USB, SSD, (SmartPhone, Tablettes)

S'agissant des serveurs uniquement, la destruction devra obligatoirement être effectuée par BROUAGE.

5.4 Modalités de mise en œuvre des prestations

L'effacement sécurisé ou la destruction sont délégués au titulaire uniquement après signature d'une convention avec remise d'un certificat de destruction et/ou d'effacement.

Un modèle de convention est présenté en annexe.

Cette convention permettra à l'organisme de s'assurer que le prestataire garantit la sécurité des données qui lui sont confiées.

Le prestataire devra compléter, signer et transmettre le procès-verbal d'effacement des données et/ou de destruction physique présenté en annexe.

5.5 Contrôle des destructions sur le site du titulaire

Le pouvoir adjudicateur pourra demander qu'un agent de l'organisme soit présent lors des opérations.

Un procès-verbal signé contradictoirement par les deux parties rend compte obligatoirement de la procédure réalisée pour la destruction de données sensibles.

ARTICLE 6. DON

Le titulaire pourra, dans le cadre de l'exécution du marché, décider de faire don du matériel aux associations/établissements possédant un tel besoin. Dans ce cas, il identifiera l'entité bénéficiaire auprès du pouvoir adjudicateur.

ARTICLE 7. DISPOSITIONS SPECIFIQUES AU LOT 1 - ENLEVEMENT ET DESTRUCTION DU MATERIEL INFORMATIQUE – CTI TOULOUSE

Le Centre de Traitement Informatique (CTI) de Toulouse est une entité qui héberge des données de santé et est, à ce titre, certifié HDS (Hébergeur de Données de Santé). Cette certification impose des missions spécifiques à prendre en compte lors de la réalisation des prestations.

Le CTI Toulouse dispose de salles informatiques sur 2 bâtiments, distants de 300 mètres l'un de l'autre.

Préalablement à toutes prestations, le Titulaire devra avoir signé un Engagement de Confidentialité et respecter le Règlement Général de Protection des Données (RGPD), présent en annexe.

Prestations à réaliser par le titulaire :

- Déplacement des matériels à détruire du bâtiment 2 vers le bâtiment 1 ;
- ⇒ **Ce déplacement est centralisé dans la zone spécialement affectée à ces actions (bât 1).**

Cette centralisation des opérations de destruction informatique permet aux services du CTI Toulouse, en charge de la supervision des opérations et de l'application des consignes, de s'assurer du bon effacement des données et de la bonne destruction des matériels.

Il est important de souligner le poids conséquent de certains matériels informatiques qui peut dépasser la tonne à l'unité, nécessitant des moyens de manutention adaptés ainsi que des plaques de roulement pour les sols.

Les supports de stockage devront être détruits par **BROYAGE NORME H4 minimum** afin de respecter les normes en rigueur (certification HDS).

Lorsque les opérations de destruction se dérouleront sur plusieurs journées, un point d'avancement devra être réalisé en fin de journée avec le Titulaire.

L'ensemble des règles générales évoquées dans les articles précédents sont également applicables au présent lot.

ARTICLE 8. DOCUMENTS A FOURNIR

8.1 Bordereau d'enlèvement

Au moment de l'enlèvement des équipements informatiques, sans données sensibles, pour revalorisation, un bordereau d'enlèvement (présent en annexe) sera fourni et sur lequel devra figurer :

- La date de collecte
- Le type d'équipement informatique
- Les quantités
- Le numéro de série
- Le numéro d'inventaire des matériels collectés

Il sera co-signé par l'agent habilité de l'organisme, supervisant cette opération, et la personne collectant les équipements informatiques habilité par le Titulaire.

8.2 Bordereau de suivi des déchets

Le bordereau de suivi des déchets est un modèle CERFA 12571*01 présent en annexe, conformément au décret n°2005-635 du 30 mai 2005 relatif à la récupération des matériels et à l'élimination des déchets.

Exemple ci-dessous :

Bordereau de suivi des déchets

Page n° /

- À REMPLIR PAR L'ÉMETTEUR DU BORDEREAU -

Bordereau n° : _____	
1. Emetteur du bordereau <input type="checkbox"/> Producteur du déchet <input type="checkbox"/> Collecteur de petites quantités de déchets relevant d'une même rubrique (joindre annexe 1) <input type="checkbox"/> Personne ayant transformé ou réalisé un traitement dont la provenance des déchets reste identifiable (joindre annexe 2) <input type="checkbox"/> Autre détenteur N° SIRET : [] [] [] [] [] [] [] [] NOM : _____ Adresse : _____ Tél : _____ Fax : _____ Mél : _____ Personne à contacter : _____	2. Installation de destination ou d'entreposage ou de reconditionnement prévue Entreposage provisoire ou reconditionnement <input type="checkbox"/> oui (cadres 13 à 19 à remplir) <input type="checkbox"/> non N° SIRET : [] [] [] [] [] [] [] [] NOM : _____ Adresse : _____ Tél : _____ Fax : _____ Mél : _____ Personne à contacter : _____ N° de CAP (le cas échéant) : _____ Opération d'élimination / valorisation prévue (code D/R) : _____
3. Dénomination du déchet Rubrique déchet : [] [] [] [] [] [] [] [] Dénomination usuelle : _____	
4. Mentions au titre des règlements ADR, RID, ADN, IMDG (le cas échéant) _____	
5. Conditionnement : <input type="checkbox"/> benne <input type="checkbox"/> citerne <input type="checkbox"/> GRV <input type="checkbox"/> fût <input type="checkbox"/> autre (précisez) : _____ Nombre : _____	
6. Quantité : <input type="checkbox"/> réelle <input type="checkbox"/> estimée tonne(s) : _____	
7. Négociant (le cas échéant) N° SIREN : [] [] [] [] [] [] [] [] NOM : _____ Adresse : _____ Récépissé n° : _____ Département : _____ Limite de validité : _____ Personne à contacter : _____ Tél : _____ Fax : _____ Mél : _____	
- À REMPLIR PAR LE COLLECTEUR-TRANSPORTEUR -	
8. Collecteur-transporteur N° SIREN : [] [] [] [] [] [] [] [] NOM : _____ Adresse : _____ Tél : _____ Fax : _____ Mél : _____ Personne à contacter : _____ Récépissé n° : _____ Département : _____ Limite de validité : _____ Mode de transport : _____ Date de prise en charge : / / Signature : _____ <input type="checkbox"/> Transport multimodal (Cadres 20 et 21 à remplir)	
- DÉCLARATION GÉNÉRALE DE L'ÉMETTEUR DU BORDEREAU -	
9. Déclaration générale de l'émetteur du bordereau Je soussigné certifie que les renseignements portés dans les cadres ci-dessus sont exacts et établis de bonne foi. NOM : _____ Date : / / Signature et cachet : _____	
- À REMPLIR PAR L'INSTALLATION DE DESTINATION -	
10. Expédition reçue à l'installation de destination N° SIRET : [] [] [] [] [] [] [] [] NOM : _____ Adresse : _____ Personne à contacter : _____ Quantité réelle présentée : _____ tonne(s) Date de présentation : / / Lot accepté : <input type="checkbox"/> oui <input type="checkbox"/> non Motif de refus : _____ Signature : _____ Date : / / Signature et cachet : _____	11. Réalisation de l'opération Code D/R : _____ Description : _____ Je soussigné certifie que l'opération ci-dessus a été effectuée NOM : _____ Date : / / Signature et cachet : _____
12. Destination ultérieure prévue (dans le cas d'une transformation ou d'un traitement aboutissant à des déchets dont la provenance reste identifiable le nouveau bordereau sera accompagné de l'annexe 2 du formulaire CERFA n°12571*01) Traitements prévus (code D/R) : _____ N° SIRET : [] [] [] [] [] [] [] [] NOM : _____ Adresse : _____ Personne à contacter : _____ Tél : _____ Fax : _____ Mél : _____	

8.3 Procès-verbal d'effacement des données ou de destruction physique

Le PV d'effacement des données ou de destruction physique, présent en annexe, devra être complété par le Titulaire et récapitulera l'ensemble des matériels et supports informatiques pris en charge.

En cas de destruction physique, le titulaire devra indiquer des informations relatives au tonnage du matériel détruit.

Enfin, en cas de support de stockage, le titulaire devra indiquer dans l'attestation de destruction le numéro de série des supports détruits.

ARTICLE 9. RESPONSABILITE DU TITULAIRE

Le retrait des équipements entraine le transfert de la garde de la chose. Le Titulaire est responsable de tout dysfonctionnement et anomalie dès le retrait desdits équipements.

Il est également responsable du fait de son transporteur.