

**BUREAU ACHATS
SECTION SMSM**

MARCHÉ PUBLIC DE SERVICES

MARCHE A PRODEDURE ADAPTEE (Art. R. 2123-1-3 du code de la commande publique)

ACCORD CADRE MONO-ATTRIBUTAIRES MIXTE
Art. R.2162-6 à R.2162-9

Cahier des Clauses Techniques Particulières de l'accord-cadre à marchés subséquents

N°DAF_2024_001133/PFAF-S/ACHATS/SMSM du 03/07/2024

Relatif à

« Mise en place d'une solution informatique aboutissant sur des prestations d'interprétation à distance des examens d'imagerie médicale (Téléradiologie) réalisés dans le cadre de la permanence des soins ou en vacation en urgence et en externe, au profit des établissements du Service de Santé des Armées et d'établissements hospitaliers civils. »

SOMMAIRE

ARTICLE 1 – OBJET ET CONTEXTE DU MARCHÉ.....	4
1.1 OBJET DU MARCHÉ	4
1.2 CONTEXTE	4
PARTIE I RELATIVE AU MODULE 1 – SYSTEME D’INFORMATION	4
ARTICLE 2 – CADRE REGLEMENTAIRE	4
ARTICLE 3 – LES CONTRAINTES DU PROJET	5
3.1 ECHANGES DE DONNEES ET CONFIDENTIALITE	5
3.2 CONTRAINTES DE SECURITE INFORMATIQUE	5
3.2.1 <i>Etat de l’art</i>	5
3.2.2 <i>Labels, agréments, certifications</i>	6
3.2.3 <i>Politique, organisation et gouvernance de la sécurité</i>	6
3.2.4 <i>Existence d’un correspondant de sécurité (ou RSSI)</i>	7
3.2.5 <i>Gestion des biens</i>	7
3.2.6 <i>Sécurité physique</i>	8
3.2.7 <i>Sécurité des réseaux et de l’exploitation</i>	9
3.2.8 <i>Sécurité des postes de travail</i>	11
3.2.9 <i>Traitement des incidents</i>	12
3.2.10 <i>Continuité des services</i>	12
3.2.11 <i>Conformité, audits, inspections et contrôle</i>	13
3.2.12 <i>Obligations relatives à l’accès des personnels non permanents dans des « Zone Protégées »</i>	13
3.2.13 <i>Obligations relatives aux conditions d’intervention du titulaire dans les locaux de l’administration</i> .	14
3.2.14 <i>Habilitation des personnels mis en place par le titulaire</i>	15
3.2.15 <i>Habilitation des personnels d’administration de systèmes</i>	15
3.2.16 <i>Obligations relatives aux astreintes et à la télémaintenance</i>	16
3.2.17 <i>Obligations relatives au cours d’interconnexions entre les SI de l’acheteur et du titulaire</i>	16
3.2.18 <i>Obligations spécifiques liées aux prestations de développement</i>	17
3.2.19 <i>Obligations spécifiques liées aux achats de matériels, logiciels ou composants</i>	17
3.3 COMPATIBILITE REQUISE	18
ARTICLE 4 – LES PRESTATIONS.....	19
4.1 SOUS-MODULE 1 – FOURNITURE DU SERVICE.....	19
4.1.1 <i>Mise en place de la solution (prestation à bon de commande)</i>	19
4.1.2 <i>Formation « médico-technique » d’accompagnement au déploiement (prestation à bon de commande)</i> 19	
4.1.3 <i>Plan d’Assurance Qualité</i>	19
4.2 SOUS-MODULE 2 – PLATEFORME.....	19
4.2.1 <i>Hébergement de la plateforme</i>	19
4.2.2 <i>Intégration dans le SIH de l’établissement</i>	20
4.2.3 <i>Stockage des données</i>	20
4.3 SOUS-MODULE 3 – MAINTIEN EN CONDITION OPERATIONNELLE	20
4.3.1 <i>Maintenance corrective</i>	20
4.3.2 <i>Evolutions de la solution</i>	21
4.3.3 <i>Assistance</i>	21
4.4 SOUS-MODULE 4 – FORMATION.....	22
PARTIE II RELATIVE AU MODULE 2 – PRESTATIONS INTELLECTUELLES.....	22
ARTICLE 5 – CADRE REGLEMENTAIRE	22
ARTICLE 6 – SECRET PROFESSIONNEL.....	22
ARTICLE 7 – ORGANISATION DES PRESTATIONS.....	23
7.1 GENERALITES	23
7.2 ORGANISATION MEDICALE	23
7.2.1 <i>Workflow</i>	23
7.2.2 <i>Compte rendu</i>	24
7.2.3 <i>Points particuliers :</i>	24

7.3	DOSSIER D'INTERPRETATION RADIOLOGIQUE	25
7.3.1	<i>Informations fournies par les établissements</i>	25
7.3.2	<i>Informations fournies par le prestataire</i>	25
ARTICLE 8 – LES PRESTATIONS.....		25
8.1	SOUS-MODULE 5 : TARIFICATIONS TECHNIQUE-ADMINISTRATIVES	25
8.1.1	<i>Fonctionnement « technique et administratif » de la solution</i>	25
8.2	SOUS-MODULE 6 : TARIFICATIONS MEDICALES.....	27
8.2.1	<i>Typologie</i>	27
8.2.2	<i>Volumétrie</i>	28
8.3	SOUS-MODULE 7 : INTERFAÇAGE DU SYSTEME D'INFORMATION RADIOLOGIQUE (RIS).....	28
PARTIE III RELATIVE AUX DEMANDES GENERALES DU MARCHE		28
ARTICLE 9 – OBLIGATIONS DU TITULAIRE		28
9.1	RESSOURCES HUMAINES ET NOTAMMENT MEDICALES.....	28
9.2	PROCESSUS TECHNIQUES PERMETTANT DE SECURISER LES PRESTATIONS ET D'EN AMELIORER LA QUALITE	28
9.3	PLAN ASSURANCE QUALITE	29
9.4	CONTROLE QUALITE.....	29
ARTICLE 10 – BILANS ANNUELS		30
10.1	REUNIONS TELEPHONIQUES.....	30
10.2	VISITE ANNUELLE	30

ARTICLE 1 – OBJET ET CONTEXTE DU MARCHÉ

1.1 *Objet du marché*

Le présent marché a pour objet la mise en place d'une solution informatique aboutissant sur des prestations d'interprétation à distance des examens d'imagerie médicale (Téléradiologie) réalisés dans le cadre de la permanence des soins ou en vacation en urgence et en externe, au profit des établissements du Service de Santé des Armées et d'établissements hospitaliers civils.

1.2 *Contexte*

Les établissements hospitaliers disposent d'activités pluridisciplinaires. Ils disposent, selon les cas, de service d'urgences et de réanimation.

Un déficit chronique en médecins radiologues entraîne la nécessité d'un recours à la télé-imagerie pour l'interprétation des examens réalisés dans certaines de ces structures.

Pour ce faire, Il est tout d'abord nécessaire de disposer d'un système d'information permettant la mise en réseaux entre les bénéficiaires et les imageurs à distance (module 1 – solution informatique).

Celui-ci permet principalement de mettre à disposition les imageries médicales réalisées afin de pouvoir bénéficier de la prestation intellectuelle à distance (module 2 – interprétation).

C'est deux éléments sont totalement indissociables l'un de l'autre.

A ce titre et dans les limites du CCAP et du présent CCTP, le titulaire doit tout mettre en œuvre pour ne pas provoquer d'interruption ou de perturbation dans l'utilisation d'une solution de téléradiologie.

Il doit être force de proposition pour toute amélioration qui peut être apportée à la solution de téléradiologie.

PARTIE I RELATIVE AU MODULE 1 – SYSTEME D'INFORMATION

ARTICLE 2 – CADRE REGLEMENTAIRE

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par le décret n°2019-536 du 29 mai 2019. Site de la CNIL : <https://www.cnil.fr/professionnel>
2. Règlement de l'union européenne numéro 2016/679 du 27 avril 2016 du Parlement européen et du Conseil, 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 entré en application le 25 mai 2018. Autodiagnostic sur le site : <https://questionnairecpme.typeform.com/to/uh4NDu>
3. Code pénal : Articles 413-5 ; 413-7 ; 413-9 ; 413-12 ; R 644-1
4. Code de la commande publique
5. Articles L 1111-8, L 1111-8-1, L 1111-8-2 et L 1111-9 du code de la santé publique
6. Code de la sécurité intérieure : Articles L 114.1 ; L 234-1 ; R 114-1 ; R 114-4, concernant les conditions d'accès aux sites de la défense
7. Décret n° 2016-412 du 7 avril 2016 relatif à la prise en compte de la performance énergétique dans certains contrats et marchés publics
8. Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
9. Arrêté du 16 septembre 2009 portant approbation du CCAG-TIC
10. Arrêté du 16 septembre 2009 portant approbation du CCAG-PI
11. Arrêté du 14 décembre 2009 relatif à la dématérialisation des procédures de passation des marchés publics
12. Arrêté du 12 avril 2018 relatif à la signature électronique dans la commande publique (abroge l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics)
13. Arrêté du 29 mars 2016 fixant la liste des renseignements et des documents pouvant être demandés aux candidats aux marchés publics
14. Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale
15. Instruction ministérielle n° 900/DEF/CAB/DR du 26 janvier 2012 relative à la protection du secret de la défense nationale, (ce document « Diffusion Restreinte » est disponible sur demande auprès de l'administration et consultable par une personne habilitée)
16. Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau « Diffusion Restreinte ».
17. Avis du 31 mars 2019 relatif à la nature et au contenu des spécifications techniques dans les marchés publics

18. Avis du 27 mars 2016 relatif aux seuils de procédure et à la liste des autorités publiques centrales en droit de la commande publique
19. Avis du 27 mars 2016 relatif à la liste des dispositions internationales en matière de droit environnemental, social et du travail permettant de rejeter une offre comme anormalement basse en matière de marchés publics
20. Directive ministérielle des achats responsables n° 5864 du 05 avril 2017
21. Politique de sécurité des systèmes d'information de l'Etat (PSSI-E) portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014
22. Alertes de sécurité publiées par le centre gouvernemental d'alerte de veille et de réponse aux attaques informatiques - Site Internet <https://www.cert.ssi.gouv.fr/>
23. Référentiel général de sécurité (RGS) publié par l'ANSSI dans sa version 2.0 du 13 juin 2014
24. Instruction n°133/DEF/SEC/DIRSIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'information du ministère de la défense
25. Politique de Sécurité des Systèmes d'Information des Armées (PSSI-A)
26. Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)
27. Politique de sécurité des systèmes d'information du Service de Santé des armées (PSSI-SSA)

ARTICLE 3 – LES CONTRAINTES DU PROJET

3.1 Echanges de données et confidentialité

✎ Pour le Service de Santé des Armées, les Hôpitaux d'Instruction des Armées sont dotés d'un Système d'Information Hospitalier (SIH) comprenant un PACS (Picture Archiving and Communication System).

Le lien informatique permettant l'échange des données entre le site réalisant l'interprétation des clichés d'imagerie et les HIA, doit garantir l'intégrité, la confidentialité et la disponibilité de l'information qui y transite.

Compte tenu des obligations liées à la sécurité de la défense, le titulaire recourt uniquement à une solution de téléradiologie qu'il opère en propre. L'accès à distance au PACS des HIA ne peut être envisagé.

Les HIA disposent d'une zone démilitarisée (DMZ) dédiée pour les échanges de données entre le réseau public (extérieur) et le sien.

Cette DMZ respecte les préconisations de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).

L'architecture sécurisée mise en place au sein de l'HIA impose une rupture protocolaire donc une "proxyfication" des flux via la DMZ dédiée.

La transmission des images et plus généralement l'ensemble des flux d'échanges doivent être "proxyfiables" entre le réseau de l'HIA et les réseaux externes - soit par la fourniture d'une solution proxy propre au soumissionnaire, soit via l'utilisation de l'EAI (Enterprise Application Integration) existant dans la DMZ.

Le titulaire pourra proposer une authentification d'accès à la solution reposant sur une liaison LDAP (Lightweight Directory Access Protocol) avec l'Active Directory local de l'HIA.

Lors du dépôt de son offre, le soumissionnaire devra fournir un schéma d'architecture avec la matrice des flux entrants et sortants et les protocoles utilisés.

3.2 Contraintes de sécurité informatique

✎ Pour le Service de Santé des Armées, le candidat pourra décrire dans sa réponse son Plan Assurance Sécurité (PAS) et devra se conformer aux articles suivants.

3.2.1 Etat de l'art

Le titulaire conçoit, met en œuvre et exploite les systèmes d'informations sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière. Toutefois, il doit respecter les exigences suivantes pour les services Web et de messagerie.

Interfaces web :

- Les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc...) ou une technologie en particulier ; en cas de développement utilisant des modules spécifiques ou non standards, le titulaire s'engage à en faire état au Service de Santé des Armées avant le début des prestations ;
- Les mécanismes cryptographiques TLS ou Transport Layer Security (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications ; l'utilisation de la technologie HSTS est fortement recommandée ;
- Le protocole SSL ne devra plus être utilisé dans la sécurisation des échanges ;
- Les mécanismes de protection des cookies de session (« http Only », « Secure », « Same Site ») sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;

- Une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (XContent-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;
- Les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier « /.well-known/security.txt » pour permettre des signalements directement auprès des points de contact identifiés via un formulaire de déclaration.

Services de courriels :

- Les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc...) ;
- Dès lors que l'infrastructure le permet, la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout « DMARC » (Authentification, Rapport et Conformité des Messages basés sur le nom de Domaine)).

3.2.2 Labels, agréments, certifications

Dans le cadre des fournitures prévues par ce marché et conformément au code de la commande publique (articles R.2111-4 à R.2111-15 relatifs aux spécifications techniques), le titulaire devra utiliser uniquement des produits ou des services qualifiés figurant sur la liste des produits ou services qualifiés publiée par l'ANSSI. La liste des produits ou services qualifiés à ce jour figure en annexe 3 du CCP. Elle porte le numéro 26 et sa dernière publication date du 21/09/2020.

Cette liste est également consultable sur le site de l'ANSSI à l'adresse :

<https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf>

Si durant la durée des prestations prévues à ce marché, certains produits ou services figurants sur la liste annexée à ce CCTP ne sont plus recommandés, le Service de Santé des Armées et le titulaire pourront convenir des mesures à prendre dans le cadre éventuel d'un accord réciproque. L'adaptation de produits ou services qui ne seraient plus recommandés vers de nouveaux produits ou services recommandés par l'ANSSI ne pourra donner lieu à aucune majoration de prix.

3.2.3 Politique, organisation et gouvernance de la sécurité

Politique de sécurité du titulaire :

Le titulaire applique et fait appliquer à ses sous-contractants désignés la politique de sécurité du présent marché.

Cette politique de sécurité traite notamment des thèmes suivants :

- Organisation de la Sécurité des SI ;
- Application de la Politique de Sécurité des SI ;
- Evaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI : réseaux, systèmes ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;
- Développement et maintenance des systèmes ;
- Gestion des incidents et des alertes ;
- Gestion de la continuité d'activité des SI ;
- Conformité et démarche de contrôle interne ;
- Localisation des données.

Organisation de la sécurité adéquate :

Le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par le Service de Santé des Armées.

- Mise en œuvre d'une gestion de risques et son suivi : le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses sous-contractants éventuels.
- Gestion de crise et sécurité : sur son domaine de responsabilité SI, le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour le Service de santé des armées le respect des engagements de service et de sécurité SI contractualisés.

Ce plan précise au minimum :

- Les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- La composition de la cellule de crise : fonctions et responsabilités des membres (administration et titulaire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
- Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

3.2.4 Existence d'un correspondant de sécurité (ou RSSI)

Le titulaire désigne parmi son personnel un correspondant sécurité et un suppléant pour toute la durée de la prestation. Il sera communiqué lors de la réunion de lancement.

Ce correspondant est notamment :

- L'interlocuteur privilégié du Service de santé des armées pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par le Service de santé des armées ou le titulaire suite à des incidents de sécurité opérationnels ;
- Le signataire qui signera en son nom et pour le compte du titulaire tous les engagements relatifs à la sécurité des informations traitées et confiées au titulaire ;
- Le signataire qui signera en son nom et pour le compte du titulaire des engagements relatifs à l'application des règles de sécurité dans le traitement de ces informations.

Ce correspondant doit pouvoir rester joignable en semaine du lundi au vendredi de 8h00 à 17h30, sauf durant les jours fériés figurant à l'article L3133-1 du code du travail. Tout remplacement de ce correspondant doit être notifié au Service de santé des armées. Par défaut, et en l'absence d'un correspondant de sécurité désigné, le titulaire ou son représentant légal, signataire de l'engagement de reconnaissance de responsabilité figurant en annexe, sera le correspondant de sécurité retenu par le Service de santé des armées.

3.2.5 Gestion des biens

Séparation des données du Service de santé des armées et des données d'autres clients :

Le titulaire conserve et traite les données du Service de santé des armées de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données du Service de santé des armées suivant le principe de restriction au besoin d'en connaître ;

Protection de la documentation du Service de santé des armées sur support papier :

Le titulaire assure la protection de la documentation du Service de santé des armées sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et en garantissant sa destruction à la fin de la prestation ;

Modalités d'échanges d'informations :

Le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail au travers des différentes passerelles permettent d'en assurer la confidentialité et l'intégrité. Pour cela, il devra respecter les exigences décrites au CCAP dans la clause « Traitement des informations protégées - Sécurisation des échanges ».

Échange de supports :

Le titulaire garantit que les supports échangés ou à connecter sur un SI du Service de santé des armées n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité au moyen d'une analyse antivirus des supports fournis.

Transmission de fichiers sur un support physique :

Toute transmission de fichiers sur un support physique (HDD, DAT, CDRom, USB, etc...), par courrier externe ou par porteur, donne lieu à un accusé de réception. Il doit respecter les règles de protection des informations et documents existantes en vigueur au sein du Service de santé des armées. De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

- L'émetteur et le destinataire ;
- Le détail des opérations de transferts et notamment le nombre, la date. Sur simple demande, ce registre est mis à la disposition du Pouvoir adjudicateur par le titulaire.

Marquage des ressources techniques :

Le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées ;

Supports de stockage hébergeant des données du Service de santé des armées :

Le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données issues des SI du Service de santé des armées en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse du Service de santé des armées. Il s'agit notamment des données de santé portant la mention « Diffusion Restreinte » ou « CONFIDENTIEL MEDICAL » ou « SECRET MEDICAL », ces mentions de protection ou de manipulation pouvant être isolées ou associées entre elles ;

Traitement des informations protégées - Sécurisation des échanges

En raison de la sensibilité du contrat, le niveau de confidentialité de certaines informations pouvant relever d'un niveau engageant la sûreté de la défense nationale ou la protection des informations personnelles et/ou médicales, la communication de celles-ci doit utiliser un moyen de cryptage pour effectuer l'échange d'informations entre les deux parties au travers des réseaux externes au Ministère des Armées.

- Pour les informations DR « Diffusion Restreinte » :

Le moyen de cryptage des fichiers échangés le plus couramment utilisé par le Service de santé des armées étant à ce jour le logiciel ACID-V7 avec délivrance de certificats individuels par la direction générale de l'armement (DGA).

La procédure de demande de clefs ACID se fait auprès de la direction générale de l'armement. Le titulaire doit adresser sa demande de dotation à la boîte fonctionnelle suivante, en précisant dans quel cadre il exprime ce besoin :

dga-ssdi.acid-industriel.fct@intra.def.gouv.fr

Dans cette demande, le titulaire devra mentionner dans l'objet du message : « Demande de dotation de la solution ACID-V7 pour la protection d'information de niveau « Diffusion Restreinte ».

Le titulaire recevra en retour la procédure pour effectuer la demande de clefs de chiffrement et de fourniture du logiciel.

Le titulaire devra demander un nombre de certificats suffisants pour doter l'ensemble des personnels qui auront à traiter des informations fournies par le Service de santé des armées ou élaborées dans le cadre de ce marché et protégées au niveau « Diffusion Restreinte ». La solution permet également de protéger l'accès de fichiers ou de dossiers sur le système d'information du titulaire.

Le délai d'obtention est d'environ un mois, avec remise des clefs et du logiciel en mains propres sur le site de la DGA. En cas de difficultés pour obtenir la solution proposée par l'administration, le titulaire devra l'indiquer au Service de Santé des Armées afin qu'une intervention soulignant l'urgence puisse être effectuée.

L'administration pourra proposer une solution d'échanges sécurisés différente en fonction des outils recommandés par le ministère des armées.

- Dans le cas où le titulaire ne détiendrait pas ce logiciel durant l'exécution du marché, il devra :
 - Soit, remettre les supports d'information (papier, stockage numérisé, etc...) en mains propres au Service de santé des armées en respectant les directives en vigueur sur la protection du secret rappelées en références ;
 - Soit proposer à ses frais une infrastructure d'échanges ou un logiciel ayant reçu une certification en cours de validité auprès de l'ANSSI. Cette solution devra être compatible avec les systèmes d'exploitation utilisés par le Service de santé des armées dont la liste pourra être fournie au titulaire à sa demande. Dans ce dernier cas, le titulaire aura la charge de fournir l'ensemble des composants et des certificats nécessaires à la sécurisation des échanges.

Sont particulièrement visés par cette mesure de protection des informations, tous les échanges sur des informations réseaux (Adresses IP, protocoles et flux échangés), les informations personnelles à caractère privé ou médical ainsi que toute information exposant ou décrivant une vulnérabilité quelconque sur le système d'information exploité au titre de la prestation.

Maintien à jour et mise à disposition des données relatives à la prestation :

Le titulaire maintient à jour et est en mesure de mettre à disposition du Service de santé des armées toutes les données relatives à la prestation. Le titulaire fournit sur demande du Service de santé des armées toute la documentation générée dans le cadre de la prestation pour un archivage éventuel.

3.2.6 Sécurité physique

Changement de localisation géographique des services et des données :

En cas de changement de localisation des données ou services, le titulaire en informe préalablement l'administration.

Hébergement de données :

A la demande de l'administration, le titulaire identifie tous les supports et locaux hébergeant ou stockant les données et/ou leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès. Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources du Service de santé des armées et les équipements de sûreté.

Protection intrusion physique des locaux techniques du titulaire :

Les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc...) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements doivent être opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction. En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

Protection des plateaux mutualisés :

En cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour le Service de santé des armées (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par le Service de santé des armées, etc...).

3.2.7 Sécurité des réseaux et de l'exploitation

Cloisonnement des environnements informatiques :

Le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

Sécurisation des flux d'administration :

Le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni à aux infrastructures bureautiques du titulaire.

Règles de sécurité et d'exploitation :

L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'administration. Toute exception fera l'objet d'un accord préalable écrit des équipes du Service de santé des armées.

Anti-virus opérationnel et à jour :

Le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation. La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée au Service de santé des armées.

Gestion des mises à jour :

Le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis au Service de santé des armées.

Sauvegarde des données :

Le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur ses serveurs aux besoins de sauvegarde exprimés par le responsable de conduite de projet du Service de santé des armées dans le cadre de la prestation. Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

Stockage des sauvegardes informatiques : le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

Comptes individuels :

Le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez le Service de santé des armées) dispose d'un compte individuel qui peut être :

- Soit un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement que par cette personne tout au cours de la vie du compte ;
- Soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois. La gestion des comptes individualisés (identification du personnel à qui il a été affecté, date et heure de cette affectation) sera effectuée par le titulaire. Le Service de Santé des Armées peut à tout moment limiter le nombre de comptes attribués au titulaire dans le cadre des connexions distantes sur les systèmes d'information du Service de santé des armées.

Comptes obsolètes ou par défaut :

Le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.

Comptes techniques :

Dans le cadre de la cartographie du système d'information prévue à l'article « Cartographie et protection des systèmes d'information du titulaire » ci-dessous, le titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

Cartographie et protection des systèmes d'information du titulaire :

Le titulaire doit disposer d'un inventaire et d'une cartographie de ses systèmes d'information, notamment tous les systèmes supportant tout ou partie des informations traitées pour le compte du Service de santé des armées.

L'inventaire des composants formant les systèmes d'information ainsi que la cartographie de ces systèmes et les mesures assurant leur protection doivent pouvoir être fournis au Service de santé des armées sur demande.

Il s'agit notamment :

- Des versions des systèmes d'exploitation utilisés sur les serveurs et les postes de travail du titulaire, la politique de mise à jour de ces systèmes ainsi que les solutions techniques employées pour assurer leurs mises à jour.
- Des systèmes de filtrage employés par le titulaire pour assurer la sécurité et le cloisonnement des réseaux internes particulièrement ceux qui supportent les développements réalisés pour le compte du Service de santé des armées.
- Des mesures mises en place pour assurer la protection des données traitées pour le compte du Service de santé des armées, dans ce cas, il s'agit des mesures techniques et organisationnelles (protection des locaux, protection des supports numériques, marquages et identification, etc... - Article 19 du CCAG TIC).

Ces informations peuvent être également décrites dans le plan d'assurance sécurité (PAS) que le titulaire doit fournir, conformément à l'article 4.1.4 du présent CCTP.

Les préconisations de l'ANSSI pour la mise en place de cette cartographie sont publiées sur le site :

<https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation>

Recensement des comptes d'accès :

Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI du Service de santé des armées existants ainsi que des rôles et privilèges qui y sont associés. Il fournit cette liste à le Service de santé des armées sur demande.

Le titulaire effectue et formalise une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation :

- Une revue « d'emploi » (a minima trimestrielle) ;
- Une revue de « besoin » (a minima annuelle).

Politique du moindre privilège :

Le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont caractérisés par le principe du moindre privilège, soit un accès minimum requis.

Attaques en essai et erreurs sur secrets d'authentification :

Les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreurs sur les secrets d'authentification.

Journalisation des actions :

Le titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves.

Le titulaire collecte et stocke au minima les informations suivantes :

- Connexion et déconnexion aux équipements et applications ;
- Accès en lecture et/ou en écriture à des fichiers et dossiers « Diffusion Restreinte » marqués « CONFIDENTIEL PERSONNEL », ou tout autre mention de protection du SECRET MEDICAL ;
- Informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

Horodatage des systèmes :

Tous les systèmes et équipements utilisés dans le cadre de la prestation et comportant un système d'horodatage doivent être reliés au même serveur de temps.

Gestion des traces :

Le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque.

Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, diverses dates liées aux fichiers, clés de registres...). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.

Politique des mots de passe :

La durée de validité du mot de passe utilisateur est fixée à 90 jours, à l'issue, son changement doit être imposé par le système. Pour garantir la robustesse du mot de passe utilisateur (hors code PIN), celui-ci :

- Est composé au minimum de 9 caractères ;
- Inclut au moins trois des catégories suivantes : lettre majuscule, lettre minuscule, chiffre arabe (0 à 9), caractère spécial (sous réserve que le système d'exploitation le permette) ;
- Ne contient pas tout ou partie de l'identifiant, du nom de l'utilisateur, de son rôle ou de son grade ;
- Est différent et se distingue nettement des 6 derniers mots de passe utilisés.
- Les mots de passe d'administration respectent les règles précédentes et sont composés au minimum de 14 caractères.

Sources d'installation des logiciels :

Le titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par l'administration.

Validité des licences :

Le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou du Service de santé des armées dans le cadre de la prestation.

3.2.8 Sécurité des postes de travail

Protection contre le vol des postes de travail :

Le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivols de façon systématique sur les postes de travail portables.

Chiffrement des informations protégées :

Une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail ou les supports amovibles.

Les postes de travail utilisés dans le cas de la prestation ne doivent présenter aucun accès Internet en dehors d'une connexion sécurisée avec authentification et chiffrement dans le cadre des échanges avec l'administration. Tout poste de travail contenant des informations dont le Service de santé des armées est propriétaire dans le cadre des prestations contractualisées, ne doit pas pouvoir accéder directement au réseau Internet durant et après le traitement de ces informations. Les connexions au réseau Internet derrière un « reverse proxy » restent autorisées.

3.2.9 Traitement des incidents

Remontée d'alerte :

Le service de supervision du titulaire met en place un système de remontée d'alerte au Service de santé des armées, afin de signaler tout comportement anormal sur un périmètre SI lié à la prestation, vol ou perte d'informations sensibles appartenant au Service de santé des armées (données personnelles, données de santé, documentations techniques en particulier).

Enregistrement et traçabilité et gestion des incidents de sécurité :

Le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

Traitement des incidents de sécurité :

Le titulaire contacte les interlocuteurs sécurité du Service de santé des armées désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI du Service de santé des armées.

De plus :

- Si cet incident a lieu sur le SI du Service de santé des armées, le titulaire participera à la demande du Service de santé des armées au traitement de l'incident ;
- Si cet incident a lieu sur le SI du titulaire, le titulaire autorisera le Service de santé des armées ou un tiers désigné à participer au traitement de l'incident (si le Service de santé des armées le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec le Service de santé des armées (traitement des causes profondes).

Base de connaissance :

Le titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit au Service de santé des armées sur demande.

3.2.10 Continuité des services

- Continuité de fonctionnement et de service

Le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat selon les dispositions suivantes :

Tout logiciel figurant au marché est tenu pour indisponible lorsque l'usage en est rendu impossible, en raison d'un défaut de fonctionnement constaté par le Service de santé des armées. L'indisponibilité s'applique à la dernière version mise en œuvre pour le Service de santé des armées.

Le titulaire s'engage à rendre au Service de santé des armées l'usage du logiciel défectueux, au terme d'un délai fixé à 12 heures effectives à compter de la mise en œuvre de la dernière version ou, à défaut, à lui mettre à disposition une solution aux fonctionnalités équivalentes.

En cas de constatation de nouveaux défauts sur le logiciel en cause, le titulaire est tenu d'y apporter de nouvelles corrections aux mêmes conditions.

Pendant ce délai et jusqu'à ce que l'usage du logiciel redevienne possible, les matériels dont le Pouvoir adjudicateur ne peut faire usage, sont réputés indisponibles.

La rémunération du droit d'utilisation des logiciels indisponibles est suspendue.

L'indisponibilité s'achève par la remise à disposition du Service de santé des armées des éléments, en état de marche. Toutefois, lorsque les éléments réparés sont à nouveau indisponibles, pour les mêmes causes, dans les 8 (huit) heures d'utilisation après leur remise en état, la durée d'indisponibilité est décomptée à partir de la constatation de l'indisponibilité initiale.

Le titulaire est tenu de faire connaître au pouvoir adjudicateur la durée prévisible de l'indisponibilité lorsque celle-ci excède les seuils ci-dessus.

Sauf cas de force majeure, lorsque la durée d'indisponibilité observée dépasse les seuils ci-après, le titulaire est soumis aux pénalités prévues.

- Plan de continuité d'activité

Le titulaire fournit, à la demande de l'acheteur, la preuve de l'existence d'un plan de continuité d'activité. Ce plan est régulièrement testé pour l'ensemble des services fournis à l'acheteur. Le Service de santé des armées se réserve le droit de demander les résultats des exercices de continuité d'activité réalisés régulièrement par le titulaire.

- Remplacement du matériel endommagé ou perdu

Le titulaire prend toutes les dispositions nécessaires (matériel de remplacement à l'identique, contrats de service), en relation avec l'administration, pour remplacer rapidement et sur les différents sites du Service de santé des armées tout matériel sous sa responsabilité endommagé ou perdu (poste de travail, serveur, équipement réseau).

- Plan de continuité d'activité pour les prestations d'infogérance sur site

Dans le cadre particulier des prestations d'infogérance sur site pour le compte du Service de santé des armées, le titulaire devra fournir un plan de continuité d'activité détaillé avant le début de la prestation.

Ce plan devra prévoir notamment les conditions de disponibilité des personnels assurant l'infogérance sur site, en fonction du type de crise pouvant affecter l'indisponibilité des personnels opérant sur un site sur lequel sont déployés des systèmes d'information gérés par le Service de santé des armées et dont le titulaire assure l'infogérance.

Le titulaire devra fournir un pourcentage minimum de personnel pouvant continuer à exercer les prestations d'infogérance sur site ainsi que les horaires pouvant être garantis dans les différents cas.

Exemples :

- Intempéries majeures (neige, verglas, inondations, etc...) ;
- Pourcentage de personnel minimum garanti sur site en heures ouvrables : 80% ;
- Horaires décalés de 30 mn lors de la prise de poste et la fin de journée.

Les heures de travail non effectuées seront dues au Service de santé des armées, des conditions de réaffectation de ces heures de travail rémunérées et non effectuées seront proposées au titulaire.

En cas de force majeure, le télétravail peut être envisagé. Le plan de continuité d'activité devra également prévoir les conditions de mise en œuvre de ce télétravail.

L'administration donnera les droits nécessaires pour l'exercice du télétravail sur les systèmes d'information concernés par l'infogérance.

Le titulaire aura à sa charge la mise en place des matériels ainsi que des systèmes de communication sécurisés et agréés par le Service de santé des armées pour effectuer l'ensemble des opérations dans le cadre du télétravail. Le non-respect de la réalisation des opérations d'infogérance conformément aux dispositions prévues par le plan de continuité d'activité fourni par le titulaire du marché, entraînera des pénalités prévues.

3.2.11 Conformité, audits, inspections et contrôle

Autocontrôles de sécurité :

Le titulaire effectue des autocontrôles de conformité aux exigences du CCTP pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'administration :

En cas de non-conformité au niveau d'exigence de sécurité requis par l'administration, un plan d'actions correctives devra être formalisé par le titulaire au maximum 15 jours calendaires après la constatation des écarts.

Le titulaire doit ensuite régulariser ces écarts par l'application du plan d'actions correctives décrites dans un délai convenu en commun accord entre les deux parties.

Les représentants des deux parties ayant autorité pour valider un éventuel plan d'action sont les responsables de la sécurité des systèmes d'information, le titulaire ayant désigné le sien conformément à l'article 3.2.4 du présent CCTP. Le délai de mise en place des actions correctives sera de 15 jours calendaires minimum et de 3 mois calendaires maximum en fonction de l'incidence sur la sécurité des écarts constatés.

Le non-respect de ce délai entraînera l'application des pénalités prévues.

3.2.12 Obligations relatives à l'accès des personnels non permanents dans des « Zone Protégées »

L'accès à une zone militaire relève des dispositions du code pénal (413-5, 431-8 et R. 644-1), du code de sécurité intérieure (L. 114-1, L. 234-1, R. 114-1 et R. 114-4) et de l'instruction ministérielle IM n° 900/ARM/CAB/NP du 15 mars 2021 relative à la protection du secret et des informations diffusion restreinte et sensibles).

Délais pour première autorisation d'accès préalable :

Une enquête administrative est déclenchée par demande du titulaire et adressée à l'officier de sécurité de l'autorité contractante, au minimum 2 mois avant l'accès de tout nouveau personnel à l'intérieur de la zone protégée. Cette enquête sera établie après que le titulaire ait fourni un exemplaire renseigné de la demande de contrôle primaire figurant en annexe du règlement de consultation.

Informations des personnels concernés :

Le titulaire s'engage à informer les personnels ayant besoin d'accéder dans une zone protégée et faisant l'objet d'un affichage ad hoc au niveau de tous les accès concernés :

- Qu'ils devront se conformer strictement au règlement intérieur, aux règles de sécurité et de contrôle en vigueur dans l'établissement dans lequel sont exécutées les prestations et n'accéder qu'aux seuls locaux et installations concernés par le marché ;
- Qu'elles feront l'objet d'une enquête administrative destinée à vérifier qu'il est possible de les autoriser à accéder à ladite « Zone Protégée » conformément à l'annexe 32 de l'instruction générale interministérielle IGI n°1300 sur la protection du secret de la défense nationale approuvée par arrêté du 9 août 2021 ;
- Que cette enquête pourra donner lieu à consultation des traitements automatisés des données personnelles mentionnées à l'article 230-6 du code de procédure pénale, y compris pour les données portant sur les procédures judiciaires en cours ;
- Qu'ils ont pris connaissance des articles 413-7, 413-8 et R. 413-1 à R. 413-5 du code pénal ;
- Qu'ils devront se conformer strictement au règlement intérieur, aux règles de sécurité et de contrôle en vigueur dans l'établissement dans lequel sont exécutées les prestations et n'accéder qu'aux seuls locaux et installations concernés par le marché.

Pour les personnels non permanents ne présentant pas de badge d'identification avec photo, une procédure de filtrage avec un enregistrement des accès sera mise en place. Ces enregistrements devront comprendre :

- Prénom et Nom du visiteur (tel qu'il figure sur les documents d'identité présentés) ;
- Date et heure d'entrée ;
- Heure de sortie ;
- Personnel permanent visité (personne appartenant au Service de santé des armées accueillant le visiteur).

Une pièce d'identité officielle sera conservée durant la visite et échangée contre un badge temporaire d'accès identifiable par la mention « Visiteur ».

3.2.13 Obligations relatives aux conditions d'intervention du titulaire dans les locaux de l'administration

Respect des exigences de sécurité de l'administration :

Au même titre que les agents de l'administration, le titulaire doit prendre connaissance et appliquer les règlements internes de l'administration (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.). À ce titre, les personnels intervenants pourront être amenés à signer des engagements de responsabilité particuliers identiques à ceux signés par les personnels de l'administration, par subrogation des fonctions exercées.

Respect des standards et méthodologies de l'administration :

Le titulaire doit respecter les standards et les méthodologies préconisés par le Service de Santé des Armées. (art 4.2 et 4.3 du présent CCTP)

Respect du périmètre de la prestation :

Le titulaire ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

Connexion d'équipements au réseau de l'administration :

Le titulaire doit connecter sur le réseau interne de l'administration uniquement des équipements fournis par le Service de santé des armées. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, etc.)

Inventaire des composants mis à disposition par l'administration :

Le titulaire met en place une solution pour élaborer et maintenir un inventaire complet et à jour des composants mis à disposition par le Service de santé des armées. Cette liste pourra être vérifiée par le Service de santé des armées lors des contrôles de la sécurité des systèmes d'information.

Recensement des comptes d'accès :

Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'administration existants ainsi que des rôles et privilèges qui y sont associés. Il doit être en mesure de fournir cette liste à l'administration sur demande. Le titulaire doit également effectuer et formaliser une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre des prestations réalisées pour le compte du Service de santé des armées.

Restitution des équipements fournis par l'administration :

A la fin de la prestation, le titulaire doit restituer l'ensemble du matériel fourni par l'administration.

Restitution des informations collectées par le titulaire :

A la fin de la prestation, le titulaire doit restituer ou détruire les informations, dont l'origine provient du Service de santé des armées, en sa possession.

Un procès-verbal de destruction des données doit être signé par le titulaire.

Ce procès-verbal n'est pas nécessairement détaillé mais il doit couvrir de manière exhaustive l'ensemble des informations que possède le titulaire et qui proviennent du Service de santé des armées. Le titulaire signera un engagement de non possession de telles informations, particulièrement les données personnelles ainsi que les données de santé à la fin de la prestation.

Transfert de connaissances :

Le titulaire doit préciser la date exacte de départ des intervenants de la prestation et organiser le transfert de connaissances auprès des équipes du Service de santé des armées.

3.2.14 Habilitation des personnels mis en place par le titulaire

L'habilitation des personnels mis en place par le titulaire et exerçant dans le cadre de cette prestation doit être en conformité avec le niveau de protection affecté aux informations traitées.

Toutes les données de santé à caractère personnel doivent être traitées (quel que soit la nature du traitement concerné : recueil, stockage, tri, manipulation, échanges, etc.) dans le respect de l'article L1111-8 et suivants du code de la santé publique.

3.2.15 Habilitation des personnels d'administration de systèmes

Les personnels exerçant des fonctions d'administration de systèmes doivent détenir un niveau d'habilitation supérieure à celui du système qu'ils maintiennent.

Exemple : pour l'administration d'un système traitant d'informations niveau diffusion restreinte au sens de la Défense nationale, les administrateurs doivent détenir un niveau d'habilitation « CONFIDENTIEL DEFENSE ».

Pour les fonctions d'administration des systèmes d'information et de communication exercées par le titulaire, l'habilitation « CONFIDENTIEL DEFENSE » des personnes physiques désignées par le titulaire sera demandée, il n'y aura aucune dérogation à cette obligation.

Les fonctions concernées sont :

- Les fonctions d'administrateur des systèmes d'exploitation des serveurs dans tous les environnements concernés par l'objet du marché ;
- Les fonctions d'exploitation des systèmes sur des machines physiques ou virtuelles ainsi que l'exploitation des sauvegardes données ;
- Les fonctions d'administrateur de tous les équipements actifs de réseau (ces fonctions comprennent également le paramétrage, l'accès aux données de routage, aux adresses, ports, protocoles mis en œuvre, constitution des réseaux virtuels (VLANs), etc... ;
- Les fonctions d'administrateurs de bases de données (DBA) quel que soit la taille ou le volume de ces bases de données.

Si ces personnes ne sont pas détentrices de l'habilitation qui convient, les titulaires devront procéder à la constitution d'un dossier d'habilitation pour chacune d'elles sur : <https://www.ixarm.com/>

Conformément aux dispositions de l'arrêté du 01 juillet 2021, le titulaire devra modifier les contrats de travail des personnes de l'entreprise appelées à accéder à ces informations ou supports protégés.

En tout état de cause, toute personne non habilitée se verra refuser l'accès aux sites préposés, et ne pourra participer à l'exécution du présent accord-cadre.

En cas de refus d'habilitation, le titulaire doit remplacer ce personnel sans pouvoir prétendre à indemnités.

Les titulaires s'engagent à :

- Ne soumettre à la procédure d'habilitation que des personnes appartenant en propre à son entreprise, à l'exclusion de tout employé occasionnel, intérimaire ou embauché uniquement pour le présent accord cadre ;
- Remplacer immédiatement les personnes qui n'auront pas été habilitées par le ministère des armées ;
- Ne faire participer aux prestations du présent marché que des personnes habilitées.

3.2.16 Obligations relatives aux astreintes et à la télémaintenance

Astreinte :

Le titulaire doit prévoir un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et à la tenue des engagements. Les cas de force majeure doivent également être couverts.

Sécurisation des flux d'astreinte :

Le titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex. VPN, IPSec) pour la connexion à distance en astreinte aux réseaux utilisés dans le cadre de la prestation (que ce soient ceux du titulaire, ceux du Service de santé des armées ou les deux éventuellement).

Le Service de santé des armées fournira au titulaire les éléments nécessaires pour réaliser la sécurisation de l'accès distant.

Dans le cadre d'un accès de télémaintenance à une ressource informatique (matériel, logiciel) du Service de santé des armées, le titulaire doit présenter des mesures de sécurité renforcées validées par le Service de santé des armées.

Le personnel du titulaire devra explicitement lancer la connexion et s'authentifier pour obtenir l'accès aux SI à distance (connexion authentifiée non permanente) ou utiliser les services d'accès distants mis à disposition par le Service de santé des armées.

Chiffrement des postes d'astreinte ou de télémaintenance :

Le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte ou pour réaliser les opérations de télémaintenance.

Connexion distante :

Le titulaire restreint la connexion distante aux personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion non autorisée en horaires non ouvrés), et aux ressources nécessaires en astreinte uniquement.

Enregistrement des accès :

Les prises en main à distance (PMAD) des infrastructures du Service de santé des armées sont soumises à surveillance et enregistrement de l'activité des utilisateurs (utilisation d'un bastion).

Suivi des interventions :

Le titulaire est capable de fournir à l'acheteur, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI de l'acheteur en astreinte ou en télémaintenance.

Conformément à l'article 3.2.7 du présent CCTP un compte individualisé non nominatif (dit compte technique à attribution contrôlée) pourra être attribué à des personnes différentes au cours de la vie de ce compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

Le Service de santé des armées limite le nombre de comptes attribués au titulaire dans le cadre des connexions distantes sur ses systèmes d'information, il appartient au titulaire de rationaliser le nombre de comptes en les limitant à un seul par site géographique d'intervention au titre des astreintes ou de la télémaintenance.

La gestion des comptes techniques à attribution contrôlée (identification du personnel à qui il a été affecté, date et heure de cette affectation) sera effectuée par le titulaire qui tiendra à la disposition de l'administration la journalisation de l'attribution des comptes techniques à ses personnels nommément désignés.

3.2.17 Obligations relatives au cours d'interconnexions entre les SI de l'acheteur et du titulaire

Respect des exigences de sécurité de l'administration :

Au même titre que les agents de l'administration, le titulaire prend connaissance et applique les règlements internes du Service de santé des armées (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc...).

Respect des standards et méthodologies du Service de santé des armées :

Le titulaire respecte les standards et les méthodologies préconisés dans l'article 4.2.2 du présent CCTP.

Respect du périmètre de la prestation :

Le titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

Interconnexions des SI de l'acheteur et du titulaire :

En cas d'interconnexion des SI du Service de santé des armées et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'administration au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité propres au Ministère des armées.

Pour chaque interconnexion, les éléments suivants doivent être définis :

- Les flux et protocoles autorisés, ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ;
- Les modalités d'authentification requises : Authentification par mot de passe réutilisable, authentification forte par mot de passe unique (OTP ou one-time password) ou par certificat ;
- Les modalités de chiffrement des échanges : Le chiffrement des flux transitant sur Internet est requis ;
- Les exigences spécifiques de traçabilité des accès ;
- Les moyens de sécurité supplémentaire à mettre en œuvre : Contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif...

3.2.18 Obligations spécifiques liées aux prestations de développement

Contrôle de la qualité et de la sécurité du développement :

Le Service de santé des armées se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le titulaire, via des audits et/ou des tests d'intrusion par exemple (audit de code sur les parties les plus sensibles, etc...).

Si au cours d'un audit de sécurité réalisée à la demande du Service de santé des armées, des failles de sécurité qui auraient été déjà publiées par l'éditeur ou par un organisme reconnu comme le CERT-FR, ANSSI, etc. (Référence 22 de l'article 2 du présent CCTP) avant la livraison d'une version de développement déjà mise en pré-production ou en production sont relevées, le titulaire sera tenu d'effectuer la mise en conformité du développement ou de ces composants sans pouvoir prétendre à une révision des prix stipulés au marché.

3.2.19 Obligations spécifiques liées aux achats de matériels, logiciels ou composants

Absence de failles à la mise en production :

Le titulaire s'engage à ce que les produits fournis au titre du marché soient, au jour de leur mise en production par le Service de santé des armées, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations qu'il traite directement, ou par interconnexion à des systèmes déjà existants.

Le titulaire s'engage à vérifier que tous les paramètres par défaut mis en place par le fabricant (appelés communément « paramètres d'usine ») ont été analysés et que ces derniers ont été modifiés si nécessaire afin de les adapter aux stricts besoins du Service de santé des armées en ne configurant que les options utiles indispensables aux seules fonctionnalités du composant ou du logiciel exigées par les spécifications techniques fournies.

Toutes les modifications effectuées dans les paramétrages par défaut devront être documentées.

Dès lors que la documentation standardisée de ces matériels, logiciels, ou composants n'indique pas ces informations, le titulaire devra également indiquer les conséquences de ces modifications sur le fonctionnement global des systèmes.

Fonctionnalités liées aux télécommunications, télétransmissions et aux interfaces associées :

Le titulaire doit fournir pour chaque composant et/ou matériel qu'il livrera au Service de santé des armées les fonctionnalités de télécommunication et/ou télétransmission présentes sur ces matériels, qu'elles soient activées par défaut ou non.

Dans le cas où l'une des fonctionnalités concernées seraient présentes le titulaire doit donner l'ensemble des caractéristiques des interfaces. (Techniques mises en œuvre, force et portée des signaux émis, sensibilité de la réception, etc.).

Toute la documentation relative à ces interfaces doit impérativement être décrite en français et selon les normes européennes en vigueur dès lors qu'elles ne sont pas documentées par ailleurs.

Ces fonctionnalités doivent être désactivables si leur présence sur les composants et matériels n'a pas été expressément stipulée dans les spécifications demandées par l'administration.

Sont concernés par cette obligation de déclaration et de documentation si elles existent :

- Les interfaces de radiocommunication par ondes électromagnétiques sur tout le spectre des fréquences radio (Wifi (toutes normes existantes) ; Systèmes basse consommation (ZigBee – Rubeer- Wibreer- Z-wave, etc.) ;
- Les interfaces de communication par signaux infrarouges ;
- Les composants intégrant les communications par courants porteurs en ligne (CPL) ;
- Les interfaces de communication électromagnétiques sans contact (NFC) ;
- Et d'une manière générale tous les systèmes de communication qui ne présentent pas une interface apparente sans démontage du composant, matériel, ensemble ou sous-ensemble.

Détection d'une vulnérabilité :

En cas de mise en évidence d'une vulnérabilité affectant un produit fourni au titre du marché, le titulaire doit mettre à disposition du Service de santé des armées dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n'affectant ni les performances ni les fonctionnalités du produit concerné. Le titulaire collabore également avec le Service de santé des armées pour déterminer l'origine de la vulnérabilité et les actions à engager pour l'éradiquer.

Exigences liées à la maintenance :

On entend ici par logiciel la partie communément appelée « firmware » mise en place par le fabricant et qui peut être paramétré par le titulaire dans le cadre d'une adaptation spécifique (par exemple le BIOS d'un ordinateur, serveur, composant actif de réseau, micro logiciel sur un matériel médical ou périphérique, etc.).

Dans le cadre d'une opération de maintenance, le titulaire s'engage à chiffrer ou effacer après les avoir éventuellement sauvegardées de manière sécurisée toutes les données avant l'envoi en maintenance externe de toute ressource informatique du Service de santé des armées.

Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance externe ne peut se faire que sous couvert d'un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un personnel du Service de santé des armées chargé de la sécurité des systèmes d'information.

Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l'envoi en maintenance externe est interdit.

Tout effacement des données et/ou informations techniques appartenant au Service de santé des armées fera l'objet d'une traçabilité matérialisée par procès-verbal contradictoire par lequel cet effacement complet et sécurisé sera garanti par le titulaire.

En cas d'impossibilité de réaliser un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne, d'une impossibilité technique ou d'un dysfonctionnement), ou que le titulaire ne peut pas garantir l'effacement des données et la remise dans l'état initial du fabricant :

- Le matériel ou le composant pouvant contenir des informations appartenant au Service de santé des armées devra être démonté par le titulaire et sera conservé par l'administration en vue de sa réimplantation ou de sa destruction en fonction des possibilités techniques de réutilisation ;
- Si le matériel ou composant ne peut pas être réutilisable sur un nouvel ensemble, le titulaire ne pourra pas prétendre à une indemnisation supplémentaire pour le remplacement du matériel ou du composant concerné par cette rétention ou destruction.

Le procès-verbal d'effacement ou de destruction du matériel du composant devra comprendre :

- La nature de l'opération : (effacement sécurisé/destruction) ;
- La date de l'opération ;
- Le lieu de l'opération ;
- Le nom et la qualification des intervenants ;
- L'identification unique du matériel (ce peut être un numéro constructeur, un numéro de série, une annexe comportant une copie de l'identification apposée par le fabricant).

3.3 Compatibilité requise

La solution du titulaire installée sur les serveurs du SSA doit, **à minima**, être compatible avec les outils suivants :

- les outils bureautiques suivants :
 - MS Office 2016 ;
 - MS Project ;
 - MS Visio.
- les navigateurs suivants :
 - Mozilla Firefox – version minimale : 68.7-0 ESR;
 - Microsoft Internet Explorer et Microsoft Edge – dans les dernières versions supportées par Microsoft
- le système antivirus qui sera diffusé au titulaire lors de la réunion de lancement du projet.

Le titulaire s'engage à utiliser et à fournir aux établissements, des documents dont l'exploitation (lecture / écriture) est compatible avec les outils référencés. Les bénéficiaires se réservent néanmoins la possibilité de recourir à d'autres outils.

Il s'engage à assurer la compatibilité applicative de ses systèmes avec ces 3 navigateurs.

La langue utilisée pour l'assistance ou la formation aux utilisateurs est le français uniquement.

En cas de changement, les bénéficiaires en informent le titulaire et assure la reprise/compatibilité des données préalablement saisies.

ARTICLE 4 – LES PRESTATIONS

Les prestations se déclinent en 4 sous-modules :

- sous-module 1 : Fourniture du service ;
- sous-module 2 : Plateforme ;
- sous-module 3 : Maintien en condition opérationnelle ;
- sous-module 4 : Formation ;

4.1 Sous-module 1 – Fourniture du service

4.1.1 Mise en place de la solution

Les procédures sont définies et formalisées lors de la phase préparatoire au démarrage du service de téléradiologie. Elles comportent toutes les dispositions nécessaires à la prévention des risques induits par cette pratique.

La phase préparatoire débute par une réunion de lancement du projet où sont abordés tous les points d'ajustement du service aux besoins de l'établissement et ses modalités de mise en place.

Il est attendu une disponibilité permanente du service de télé-interprétation pendant les périodes de sollicitation définies. Le PCA standard du bénéficiaire est présenté lors de la réunion de lancement pour qu'il soit ajusté vis à vis des contraintes locales.

Lorsque la personnalisation du service est conforme aux attentes de l'établissement et qu'il en a notifié le titulaire, celui-ci devra, dans un délai d'un mois à compter de la notification d'adhésion, mettre en place dans l'établissement, les prestations de service nécessaires à la mise en œuvre de la solution technique :

- installation et paramétrage de l'ensemble de la solution sur le site ;
- mise en œuvre des connexions ;
- mise en place des outils d'échange.

4.1.2 Formation « médico-technique » d'accompagnement au déploiement

Dans le cadre de la mise en place de la prestation, le candidat doit réaliser les formations nécessaires à l'utilisation de la solution proposée, prévues pour les équipes médicales et médico-techniques intervenant dans le cadre de ce marché.

Il est attendu une offre de formation pour les phases suivantes :

- pendant la phase de mise en service du logiciel et formation à la prise en main sur site auprès des différents intervenants internes ;
- en cas d'évolution du logiciel suite à une mise à jour conséquente.

4.1.3 Plan d'Assurance Qualité

Le cadre de réponse du titulaire devra préciser les grandes lignes de son Plan d'Assurance Qualité (PAQ). Il précisera les grands principes de ses Plans de Continuité d'Activité (PCA) et Plans de Reprise d'Activité (PRA) standards. Ils seront présentés plus en détails lors de la réunion de lancement du projet et adaptés aux possibilités locales.

4.2 Sous-module 2 – Plateforme

La plateforme de téléradiologie du titulaire doit permettre l'émission de dossiers de téléradiologie et la réception de compte-rendus avec horodatage et traçabilité de l'ensemble des étapes, dans le strict respect des règles applicables en la matière.

Cette prestation consiste en la fourniture et la livraison de licences, pour la plateforme de téléradiologie dans les établissements demandeurs.

L'acquisition de cette plateforme signifie une disponibilité totale avec les mises à jour, sur une période de 10 ans.

4.2.1 Hébergement de la plateforme

Le titulaire recourt uniquement à une plateforme de téléradiologie qu'il opère en propre et qui est impérativement hébergée sur le territoire français :

- soit chez un opérateur agréé hébergeur de données de santé ;
- soit chez le titulaire qui doit être lui-même agréé hébergeur de données de santé.

4.2.2 Intégration dans le SIH de l'établissement

A la demande de l'établissement, le prestataire pourra effectuer des travaux d'intégration de la plateforme au sein de son SIH. Dans les marchés issus de l'adhésion à la convention, seront précisées les interfaces d'intérêt, par exemple :

- Identités / créations de rendez-vous (out SIH – in plateforme) ;
- Compte-rendus en entrée (in SIH – out plateforme) – exemple : téléinterprétation de l'examen ;
- Compte-rendu en sortie (out SIH – in plateforme) – exemples : scan ordos, anciens compte-rendu du patient, scan de l'ordonnance ;
- Cotations (in SIH – out plateforme).

Les normes en vigueur pour ce type de flux devront être suivies (exemples : Fire HL7, HL7 ORU, HL7 XML, Hprim XML).

Cette intégration devra impérativement respecter les contraintes d'architecture technique des établissements.

4.2.3 Stockage des données

Le stockage doit être temporaire car lié à l'externalisation de l'interprétation des images. Le stockage final des images reste le PACS et le Dossier Patient Informatisé (DPI) pour les comptes-rendus d'interprétation. La solution de téléradiologie est un outil d'échange mais pas de stockage des données patients. Ainsi le candidat décrira dans son cadre de réponse les temps de rétention des informations nécessaire au bon fonctionnement du service.

4.3 Sous-module 3 – Maintenance en condition opérationnelle

Le maintien en condition opérationnelle est compris au titre du forfait annuel et commandé par bon de commande. Les frais de déplacement et les frais de main d'œuvre, de toutes interventions (dans les périodes ouvrées de chacun des établissements) sont compris au forfait.

4.3.1 Maintenance corrective

La maintenance corrective est définie comme l'ensemble des actions nécessaires à la correction des défauts visant à rétablir la conformité et la mise à niveau des produits et données altérées.

Les activités attendues de la prestation consistent au minimum à :

- prendre en compte et tracer toute demande de maintenance corrective
- envoyer un mail de prise en compte de l'anomalie ;
- analyser les anomalies signalées et les qualifier ;
- réaliser, dans le cadre des engagements contractuels, la correction des anomalies ;
- si nécessaire, développer et documenter les outils pour corriger les bases de données en exploitation éventuellement endommagée par l'anomalie ;
- mettre à jour si nécessaire les documentations impactées par ces modifications ;

Classification des incidents :

Chaque incident est classé selon son niveau de gravité :

- Critique : le logiciel et/ou sa base de données, et/ou un de ses composants est totalement hors service.
- Majeur : le logiciel et/ou sa base de données, et/ou de ses composants est hors service, mais une solution palliative a pu être mise en application.
- Mineur : le logiciel et/ou sa base de données, et/ou de ses composants présente une dégradation, mais reste fonctionnel.
- Correction : le logiciel et/ou sa base de données, et/ou un de ses composants est fonctionnel, mais rencontre un manquement d'optimisation pour le service clinique.

Association de la gravité des problèmes des logiciels et de la base de données par rapport au niveau de l'incident :

- Niveau critique – Le système n'est pas opérationnel ; il y a un impact significatif sur la prestation de services à un nombre important d'utilisateurs; impact négatif significatif sur la fourniture des soins aux patients sur un grand nombre de patients ; perte importante des données ou corruption des données
- Niveau majeur – Système incapable, de façon intermittente, d'effectuer des fonctions essentielles, impact modéré à grave (par ex. panne périodique et corruption partielle des données)
- Niveau mineur – Petit nombre d'utilisateurs finaux incapable, de façon intermittente d'effectuer des fonctions non essentielles; l'application fonctionne et continue à être utilisée (par ex. réception de message d'erreur de façon intermittente lors de la réservation d'un patient à partir d'un poste de travail)
- Niveau correction – N'impacte pas la remise de documentation, n'impacte pas la validité des données dans l'application (par ex. erreur d'orthographe, mauvais alignement des données sur l'écran). Clarifications de l'application et demandes d'amélioration.

Délais d'intervention

Les délais d'intervention et de remise en état sont conditionnés par le niveau de gravité de l'incident. A compter de la date d'enregistrement par le support de l'incident.

Le délai d'intervention (di) court à compter de la réception de l'appel, doublé d'un courriel, de demande d'intervention du site jusqu'à l'heure de connexion à distance à la plateforme ou l'arrivée d'un technicien sur site si la connexion ne peut être établie. Il est indiqué dans la colonne (di) du tableau ci-après et s'entend pendant les heures ouvrables de l'HIA.

Le délai de remise en état (de) court à compter de la connexion à distance à la plateforme ou l'arrivée d'un technicien sur site si la connexion ne peut pas être établie, jusqu'à la remise en route du système.

Toute intervention de dépannage commencée sera poursuivie jusqu'au moment où le matériel sera remis en ordre de marche. Le délai de remise en état se terminera à la fermeture de l'incident, lorsqu'un référent de l'HIA aura confirmé par mail ou par téléphone la fin de l'incident.

Niveaux des pannes	Délai maximal	
	Intervention	Remise en état
Critique	<15 mn	<1h
Majeur	<15 mn	<4-6h
Mineur	12 heures	48 heures
Correction	3 jours	7 jours

On appellera (t) le temps pendant lequel le système a été indisponible ou défectueux. Si ce temps est supérieur au cumul des durées théoriques di + de précisées ci-dessus, il y aura application de la clause de pénalité.

Le titulaire devra préciser dans le cadre de réponse si son système de téléradiologie peut se conformer aux exigences décrites ci-dessus. Pour chaque niveau de gravité, il devra détailler les incidents associés pour que titulaire et bénéficiaire partagent le même référentiel de qualification des anomalies. Ce sera revu / réexpliqué lors la réunion de lancement du projet.

4.3.2 Evolutions de la solution

Ce module consiste à assurer la maintenance évolutive du système afin de prendre en compte les évolutions fonctionnelles et techniques du système d'information.

Les mise à jour comprennent :

- les révisions ou changements de versions de la solution, induits par les changements de versions des logiciels liés ;
- les révisions ou changements de version de la solution, induits par les évolutions légales et réglementaires et les évolutions de normes ;
- les révisions ou changements de versions de la solution du fait du titulaire (exemple : nouvelles fonctionnalités) ;
- la fourniture des supports, des procédures d'installation et de la documentation relatifs aux révisions et aux changements de versions de la solution ;
- la prise en compte et la résolution des anomalies et incidents relevés lors de la recette de toute nouvelle version et/ou révision, tout en permettant la mise en exploitation de cette version ou révision ;
- le titulaire accompagnera chaque livraison d'une nouvelle version et/ou révision de l'ensemble des documents suivants, dans les 10 jours ouvrés :
 - un document présentant les différences fonctionnelles avec la version ou la révision précédente ;
 - un document présentant les différentes techniques (architecture, installation, modèle physique de donnée à et la procédure d'installation propre à cette version ou révision par rapport la version précédente ;
 - les manuels d'utilisateurs mis à jour.

Le titulaire devra assurer la compatibilité ascendante de la solution.

En cas de mise à jour importante provoquant l'indisponibilité de la plateforme pendant plus de 72 heures, le titulaire devra en informer les établissements par mail avec accusé de réception.

4.3.3 Assistance

Le titulaire assure une assistance téléphonique et prend en compte les demandes d'assistance via la plateforme. Le service d'assistance téléphonique est actif H24 et 7j/7.

Les agents des services d'imagerie et des Services Informatique et Téléphonie (SIT) des HIA sont également habilités à ouvrir un incident via la plateforme, chez le titulaire.

Les activités attendues de la prestation de support consistent à :

- apporter conseil /aide à l'utilisation de la plateforme , analyser les demandes d'assistance transmises par le SSA,
- informer le SSA sur l'évolution et l'avancement des dossiers
- apporter rapidement une réponse aux questions posées (le titulaire a un devoir de réponse au niveau des fiches d'anomalies, des travaux de non-conformité, etc...),
- être force de proposition,
- identifier les causes de l'anomalie et lancer les actions correctives,

4.4 Sous-module 4 – Formation

Conformément à l'article 4.1.2 du présent CCTP, le titulaire s'engage à effectuer les formations initiales nécessaires à l'utilisation de la solution proposée.

L'établissement bénéficiaire se réserve tout de même le droit de procéder à des demandes supplémentaires de formations spécifique par le biais de bons de commande.

PARTIE II RELATIVE AU MODULE 2 – PRESTATIONS INTELLECTUELLES

ARTICLE 5 – CADRE REGLEMENTAIRE

Les prestations de téléradiologie s'appuieront sur des ressources externes à l'HIA dans le respect des recommandations et préconisations des organisations professionnelles (G4-Conseil Professionnel de la Téléradiologie, Conseil National de l'Ordre des Médecins) ainsi que du cadre réglementaire des pratiques de radiologie et de télémedecine, en particulier :

- le Code de la Santé Publique(CSP) encadrant les activités de télé-médecine, notamment l'art. L6316-1 et les textes réglementaires pris en application ;
- le CSP concernant l'information des usagers du système de santé et l'expression de leur volonté (Art. L1111-2 et L1111-4)
- les textes régissant les demandes d'examen d'imagerie notamment les articles R.1333-52 à R1333-56 du CSP;
- le guide pour le bon usage professionnel et déontologique de la télémedecine élaboré par le Conseil Professionnel de la Radiologie (G4) et par le Conseil National de l'Ordre des Médecins ainsi que la charte de téléradiologie du G4 et du Conseil National de l'Ordre des Médecins actualisée en décembre 2014 ;
- le décret n°2010-1229 du 19 octobre 2010 ainsi que les circulaires associées telles que celles sur la contractualisation avec l'ARS (DGOS/PF3/2012/114 du 13 mars 2012) ;
- les prérequis du socle HOP'EN (Hôpital numérique ouvert sur son Environnement) ;
- les procédures de déclaration et d'autorisation auprès de la CNIL ;
- les bonnes pratiques de la HAS ;
- le certificat de conformité du Règlement Général sur la Protection des Données (RGPD).
- RNIV (Référentiel National d'IdentitoVigilance) arrêté du 8 juin 2021 (actuellement en version 2 et de prendre en compte ses futures évolutions), en particulier concernant INS (Identité Nationale de Santé)

La société titulaire du marché devra respecter les évolutions réglementaires et procéder au fur à mesure à sa mise en conformité.

Le bénéficiaire peut prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de non-respect du cadre réglementaire et de ses évolutions.

ARTICLE 6 – SECRET PROFESSIONNEL

Le soumissionnaire s'engage à respecter les droits de la personne (art. L1110-4 et L1110-4-1 du CSP).

Les supports informatiques et documents fournis par les différents établissements au titulaire restent leur propriété.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont le titulaire prend connaissance à l'occasion de l'exécution de sa mission.

Conformément au règlement RGPD, le titulaire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le titulaire s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au marché (l'accord préalable du maître d'ouvrage est nécessaire) ;
- ne pas utiliser les documents et informations traités à des fins autres que celles relatives à l'exécution de la mission ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée de la prestation et, en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

Le bénéficiaire peut prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

ARTICLE 7 – ORGANISATION DES PRESTATIONS

7.1 Généralités

Le recours à la téléradiologie ne doit pas induire un accroissement de charges du service notamment pour les manipulateurs radio et les secrétaires.

Les procédures sont définies et formalisées avant le démarrage du service de téléradiologie lors de la phase préparatoire. Elles comportent toutes les dispositions nécessaires à la prévention des risques induits par cette pratique.

Le processus général de fonctionnement proposé est compatible avec l'organisation des services d'imagerie médicale des HIA ainsi que les services demandeurs susceptibles d'être concernés par cette activité.

7.2 Organisation médicale

7.2.1 Workflow

L'organisation médicale respecte le guide des bonnes pratiques « qualité et sécurité des actes de télé-imagerie » publié par la Haute Autorité de Santé en mai 2019 :

- justification de la nécessité de l'acte de télé imagerie dans l'intérêt du patient ;
 - information du patient et recueil de son consentement (acte et transmission de l'examen) ;
 - examen clinique préalable effectué par le médecin de l'établissement demandeur ;
 - communication du médecin demandeur avec le téléradiologue du titulaire. Des compléments d'informations peuvent éventuellement être demandés par le téléradiologue du titulaire. Lors de la demande d'un examen en urgence, un échange téléphonique entre le médecin demandeur et le téléradiologue est systématique.
 - transmission de la demande clinique par l'établissement, avec les compte rendus et les images des examens précédemment réalisés s'ils sont disponibles et pertinents ;
 - communication entre le téléradiologue du titulaire et le manipulateur radio de l'établissement selon des protocoles prédéfinis sous la responsabilité :
 - du téléradiologue du titulaire pour le suivi de la réalisation technique de l'examen ;
 - du médecin de l'établissement sur place pour la sécurité du patient pendant l'examen, en particulier en cas d'injection de produit de contraste.
 - le téléradiologue doit pouvoir suivre la réalisation des examens grâce au transfert des images en quasi temps réel, pour pouvoir faire adapter si nécessaire le protocole par le manipulateur. Cela doit en particulier permettre la prise en charge de polytraumatisés graves en urgence au scanner mais aussi de guider le manipulateur lors de la découverte de lésions inattendues, et de faire réaliser si nécessaire des séquences ou acquisitions supplémentaires.
- Les échanges entre le manipulateur réalisant l'acte et le téléradiologue doivent être simples et rapides, soit téléphoniques, soit idéalement par une messagerie instantanée (chat) sécurisée intégré à la plateforme.
- validation technique de la réception de l'ensemble des images par le système de téléradiologie du titulaire;

- analyse et interprétation, des images par le téléradiologue du titulaire en comparant si nécessaire, aux examens précédemment réalisés qui ont été transmis ;
- rédaction d'un compte-rendu écrit, transmis ou mis à disposition du médecin demandeur de l'établissement, via la plateforme :
 - pour les examens courants : au plus tard à 8h00 le lendemain ;
 - pour les examens urgents et en hospitalisation : dans un délai d'une heure maximum.
- le compte-rendu pourra être complété par un échange téléphonique avec le médecin clinicien demandeur (notamment pour les patients hospitalisés). En particulier, le téléradiologue doit alerter le médecin prescripteur de l'établissement dans les meilleurs délais en cas d'éléments nécessitant une décision thérapeutique rapide ou entraînant un risque pour le patient.
- la procédure d'annonce de diagnostic grave doit être conforme aux recommandations de l'HAS ;
- validation de la cotation CCAM par le téléradiologue qui est légalement responsable de la cotation, en cas de modification de la cotation par le téléradiologue, celle-ci doit être tracée et l'HIA informé.

7.2.2 Compte rendu

7.2.2.1 *Forme et contenu*

Le compte rendu doit respecter les obligations du CSP en particulier l'art R1333-66, les recommandations de la Société Française de Radiologie, et de la HAS. Il doit être structuré en plusieurs parties : indication, technique et résultats et conclusion.

La partie technique comporte selon les cas les incidences, acquisitions ou séquences réalisées, ainsi que les données dosimétriques et les informations sur le produit de contraste éventuellement injecté.

Le compte rendu doit être rédigé en langue française, en respectant, les règles d'orthographe, de grammaire et de ponctuation.

L'utilisation de compte rendu type structuré ou d'un système d'aide à la rédaction informatisé permettant des comptes rendus exhaustifs et homogènes dans leur forme entre les différents téléradiologues est très souhaitable.

7.2.2.2 *Délai de réalisation*

Le délai d'exécution court à compter de la transmission des images au téléradiologue.

- pour les examens courants : au plus tard à 8h00 le lendemain ;
- pour les examens urgents et en hospitalisation : dans un délai d'une heure maximum.

Le non-respect du délai d'interprétation cité ci-dessus, entraînera l'application d'une pénalité.

7.2.2.3 *Suivi automatisé des comptes rendus en retard*

Le système de téléradiologie doit gérer automatiquement un certain nombre de non-conformités, en particulier, les dossiers n'ayant pas de compte-rendu dans les délais impartis doivent être signalés et faire l'objet de rappels automatiques aux téléradiologues responsables.

7.2.2.4 *Demande de relecture*

Le praticien demandeur doit pouvoir demander la relecture d'un examen, en particulier en cas de désaccord avec la 1^{ère} interprétation, d'évolution clinique défavorable ou de modification de la symptomatologie. Cette relecture peut être demandée, même si l'examen a été réalisé lors d'une vacation antérieure par un autre téléradiologue qui n'est plus disponible.

Cette demande se fera via la plateforme, par la réouverture du dossier et n'entraînera pas de nouvelle facturation, elle sera tracée et entraînera si nécessaire la rédaction d'un nouveau compte rendu.

7.2.2.5 *Comptes rendus modificatifs*

La validation d'un compte-rendu modificatif doit être signalée sans délai au médecin demandeur et à l'encadrement du service d'imagerie pour modifier si nécessaire la prise en charge du patient.

7.2.3 Points particuliers :

7.2.3.1 *Planning des médecins en vacation*

Le médecin demandeur ou le manipulateur de l'établissement doit pouvoir joindre, avec un N° de téléphone unique, le téléradiologue du titulaire et, par défaut, le coordonnateur radiologue du titulaire.

Pour cela le titulaire s'engage à fournir, au plus tard 7 jours avant à la fin du mois précédent, un planning mensuel précisant :

- nommément les radiologues intervenant dans le cadre des prestations de télé-interprétation (il est demandé à ce que les téléradiologues intervenants soient attirés et que les équipes soit les plus réduites possibles pour chaque établissement) ;
- leurs coordonnées téléphoniques et de messagerie électronique.

Ce planning sera mis à disposition des équipes médicales et paramédicales de l'établissement.

En cas de changement de téléradiologue, la société devra le communiquer, via l'application et par email, au plus tard 7 jours, avant la prestation.

Le candidat apportera les précisions, au sein du cadre réponse, sur ses moyens de communication concernant l'évolution de son équipe de téléradiologues.

Le non-respect de la communication du changement de téléradiologues entraînera l'application des pénalités prévues

7.2.3.2 Messagerie Sécurisée de Santé (MSSanté)

Tous les échanges d'emails comportant des données médicales doivent utiliser une messagerie sécurisée de santé de l'espace de confiance partagé MSSanté.

7.3 Dossier d'interprétation radiologique

Le dossier d'interprétation radiologique regroupe l'ensemble des documents électroniques générés par l'établissement bénéficiaire et le prestataire.

7.3.1 Informations fournies par les établissements

- les informations administratives du patient et notamment son IPP générée par le logiciel de gestion administrative ou le dossier patient et son INS quand elle est disponible ;
- la demande du prescripteur comportant l'identité du prescripteur avec les informations cliniques nécessaires à l'interprétation ;
- le consentement préalable du patient ou de son entourage pour une télé interprétation radiologique (hors urgence) ;
- les fichiers images avec les informations liées à l'acte radiologique ;
- la dosimétrie ;
- les informations relatives à l'injection de produit de contraste ou de médicament en lien avec l'examen.

7.3.2 Informations fournies par le prestataire

- les demandes d'informations ou d'actes d'imagerie complémentaires ;
- les comptes rendus d'interprétation au format PDF signés numériquement, qui contiennent a minima :
 - les données relatives au patient : Noms, Prénoms, date de naissance, sexe, INS avec datamatrix, (si l'INS a été fournie lors de la demande) ;
 - les données relatives au médecin radiologue : Nom, Prénom, RPPS, interprétation des images, signature électronique ;
 - validation de la cotation de l'examen ;
 - potentiellement être couplé avec l'imagerie associée.

ARTICLE 8 – LES PRESTATIONS

Les prestations se déclinent en 3 sous-modules :

- sous-module 5 : Tarifications technico-administratives ;
- sous-module 6 : Tarifications médicales ;
- sous-module 7 : Interfaçage du Système d'Information Radiologique (RIS).

8.1 Sous-module 5 : Tarifications technico-administratives

8.1.1 Fonctionnement « technique et administratif » de la solution

Chaque établissement, suivant ses besoins, bénéficie de la possibilité d'activer ou de désactiver l'utilisation de la solution de téléradiologie.

Pour ce faire, l'établissement demandeur fait sa demande d'activation 2 semaines avant son besoin réel.

En conséquence, le forfait de fonctionnement mensuel est à prendre en compte sur les prestations à bon de commande.

Cette prestation correspond au mode de fonctionnement « technique et administratif » de la solution.

8.1.1.1 *Fonctionnement « technique » du système de téléradiologie :*

- Assurer la traçabilité de tous les accès au dossier patient ainsi que des actions réalisées.
- Pour chaque télé interprétation, assurer la traçabilité et l'horodatage de tous les flux, notamment :
 - horodatage de la demande d'interprétation ;
 - horodatage de la transmission de la demande ;
 - horodatage de la réception de la demande ;
 - horodatage de la demande de protocolisation de l'examen ;
 - horodatage du protocole d'examen par le téléradiologue ;
 - horodatage de la réception des images ;
 - horodatage de la transmission de l'interprétation ;
 - horodatage de la réception de l'interprétation ;
 - recensement de l'ensemble des actes de télé interprétation avec leur code CCAM et leur valorisation assurance maladie.
- Génération automatique des alertes de non-conformités, en particulier pour les dossiers n'ayant pas de compte-rendu dans les délais impartis qui doivent faire l'objet de rappels automatiques aux télé radiologues responsables.
- Archivage du dossier d'interprétation radiologique (sans les images) qui doit rester accessible sur le serveur le temps d'utilisation du service du titulaire par le bénéficiaire ;
- Générer un fichier PDF de synthèse reprenant toutes les étapes de la procédure avec les données saisies dans l'interface et les données d'horodatage et le transmettre au SIH (Système Informatique Hospitalier) pour archivage.

8.1.1.2 *Fonctionnement « administratif » de l'établissement :*

- Les informations administratives du patient et notamment son IPP sont générées par le logiciel de gestion administrative ou le dossier patient.
- La demande du prescripteur comporte l'identité du prescripteur avec les informations cliniques nécessaires à l'interprétation.
- Le consentement préalable du patient ou de son entourage pour une télé interprétation radiologique (hors urgence) est scanné et archivé dans le Système Informatique Hospitalier de l'établissement.
- Les fichiers images avec les informations liées à l'acte radiologique sont transmis en même temps que la demande, à minima au format DICOM.
- Si nécessaire, les imageries antérieures sont transmises en même temps que la demande.
- La dosimétrie et les informations liées à l'éventuelle injection de produit de contraste, sont transmises en même temps que les images à interpréter.
- L'acte CCAM est transmis en même temps que la demande d'interprétation – elle pourra être modifiée et sera validé par le téléradiologue.

8.1.1.3 *Fonctionnement « administratif » du prestataire :*

- Le planning mensuel des téléradiologues, de leurs coordonnées téléphoniques et de messagerie électronique sont transmis mensuellement.
- Les téléradiologues peuvent émettre des demandes d'informations ou d'actes d'imagerie complémentaires.
- Les comptes rendus d'interprétation sont transmis au format PDF. Ils contiennent à minima :
 - les données relatives au patient : les éléments de l'Identité Nationale de Santé (nom de naissance, 1^{er} prénom de l'état civil, nom et prénom utilisés, date de naissance, sexe, code INSEE du lieu de naissance et matricule INS) ;
 - les données relatives au médecin radiologue : RPPS, Nom, Prénom, interprétation des images, signature électronique..
- La mise à disposition d'un compte-rendu modificatif sur la plateforme d'échange est signalée sans délai au médecin demandeur et à l'encadrement du service d'imagerie pour intégration au dossier du patient.
- Le titulaire établit mensuellement, avant le 10 du mois suivant, un rapport d'activité dans lequel figurent en particulier :
 - la durée d'indisponibilité de la plateforme ;
 - des indicateurs de disponibilité téléphonique du service technique ;
 - en fonction des horaires, le nombre de télé dossiers traités (par modalités, par cotation CCAM) ;
 - la durée moyenne de traitement des télé dossiers par modalité d'imagerie ;
 - la durée moyenne de transfert des télé dossiers et de l'acquisition des images à la réception du dossier par le téléradiologue ;
 - le taux de télé dossiers ayant dû faire l'objet de relance de l'intervenant, de renvoi des images ou de tout autre incident ;
 - les éléments décrits dans le compte-rendu mensuel du contrôle qualité (cf infra).

La non communication mensuelle de ces documents entrainera l'administration de pénalités au titulaire.

- Une réunion annuelle est organisée au cours du 1er mois de l'année sur chaque site, durant laquelle le titulaire remet un rapport récapitulatif des actions de l'année précédente. Un bilan des différents contrôles est réalisé et évalué lors de cette réunion. Lors de cette réunion annuelle, le titulaire s'engage à fournir un catalogue complet des extensions possibles disponibles pour la plateforme. Il précise également si ces extensions sont indispensables pour le bon fonctionnement de la plateforme. Le catalogue est, quant à lui, inséré au marché par voie de certificat administratif, il sera disponible pour tous les membres de l'accord cadre. Le bénéficiaire du marché suite à la convention d'adhésion pourra, par voie des bons de commande, commander sur la base de ce catalogue.

Le rapport de cette réunion est adressé au bureau politique de la Direction des hôpitaux (DHOP), au centre de compétence Hôpital de la Direction des systèmes d'information et du numérique (DSIN) ainsi qu'à la Direction des approvisionnements en produits de santé des armées (DAPSA).

8.2 Sous-module 6 : Tarifications médicales

Cette prestation est réalisée en complément des interprétations réalisées par les médecins radiologues exerçant en présentiel dans les Hôpitaux d'Instruction des Armées et réalisant des interprétations à distance entre les HIA. Cette prestation participe au soutien médico-technique de l'ensemble des services des établissements, en particulier des services des urgences de l'établissement.

Cette prestation comprend l'interprétation des examens :

- réalisés en semaine de 8h00 à 18h00 au profit du service des urgences, des services d'hospitalisation et des patients consultants à titre externe ;
- réalisés en semaine de 18h00 à 8h00 et les WE et jours fériés (permanence des soins).

Les horaires de prise en charge de la permanence des soins sont susceptibles d'évoluer en fonction de l'évolution des modalités de permanence de soins en imagerie médicale.

Les examens urgents et des patients hospitalisés doivent être interprétés dans un délai d'une heure et les examens non urgents avant le lendemain matin 8h.

8.2.1 Typologie

Les examens réalisés en semaine de 18h00 à 8h00 et les WE et jours fériés (permanence des soins) et ceux réalisés en semaine de 8h00 à 18h00 inclus lors des vacations programmées externalisées au profit du service des urgences et des services d'hospitalisations sont principalement constitués par :

- les radiographies des membres, du rachis, du thorax, des panoramiques dentaires, de cone-beams dentaires petit champs et dento-sinusal grand champ ;
- les examens scanographiques comprenant notamment :
 - les scanners encéphaliques et thoraco abdomino-pelviens avec comparaison pour le suivi des pathologies cancéreuses, les scanners thoraco abdomino-pelviens à la recherche d'une pathologie tumorale ou de lésions infectieuses ;
 - les scanners pour l'exploration vasculaire encéphalique, des troncs supra-aortiques, de l'aorte thoracique et abdominale et des membres inférieurs ;
 - les scanners du rocher, les scanners des sinus ;
 - les scanners de l'encéphale ;
 - les scanners du rachis quel qu'il soit ;
 - les coroscanners ;
 - les scanners des membres ;
 - les scanners corps entier dans un contexte de polytraumatisme grave (ces examens devront systématiquement bénéficier d'une seconde lecture dans un délai maximum de 12 heures) ;
 - de scanners de perfusions en particulier encéphalique dans le cadre d'AVC (le téléradiologue doit impérativement pouvoir interpréter des scanners de perfusion en urgence 24h/24)
- des examens d'IRM comprenant notamment :
 - des IRM de l'encéphale, parfois avec des séquences de perfusion en particulier lors de la prise en charge d'AVC en phase aiguë (stroke center) ainsi que pour le diagnostic et le suivi de tumeurs (le téléradiologue doit impérativement pouvoir interpréter des IRM de perfusion en urgence 24h/24). Quelques IRM encéphaliques peuvent comporter des séquences de spectroscopie qui doivent pouvoir être interprétées (Cette interprétation spécialisée peut faire l'objet d'un complément de compte-rendu dans les 24h suivant la réalisation de l'examen).
 - des IRM médullaire, du rachis ;
 - des IRM ostéo-articulaires
 - des angio-IRM des troncs supra-aortiques.
 - des IRM hépatiques, rénales, pancréatiques, pelviennes (prostatique et pelvienne féminine) ;
 - des IRM ORL ;

- des IRM cardiaques ;
- des angio-IRM des troncs supra-aortiques, de l'aorte et des artères des membres inférieurs.

Cette liste est non exhaustive et peut être complétée.

8.2.2 Volumétrie

A titre indicatif, l'activité prévisionnelle en nombre de forfaits techniques ainsi qu'en nombre d'examens réalisés figure au sein des annexes au présent CCTP.

8.3 Sous-module 7 : Interfaçage du Système d'Information Radiologique (RIS)

Le Service de Santé des Armées envisage l'acquisition d'un RIS (Système d'Information Radiologique) en 2025, le titulaire devra proposer un interfaçage de sa solution de téléradiologie au RIS retenu permettant un pilotage automatique de la solution de téléradiologie à partir du RIS en particulier :

- de la création des demandes d'examen avec transfert de l'identité INS (Identité Nationale de Santé) et de la demande médicale
- de la transmission automatique de la cotation CCAM du RIS vers la solution de téléradiologie
- de la récupération automatique des données dosimétriques et d'injection de produit de contraste à partir du RIS pour l'intégration dans le compte rendu
- et du retour automatisé du compte rendu en PDF signé numériquement, comportant l'INS (Identité nationale de Santé) avec datamatrix, conformément au RNIV (Référentiel National d'IdentitoVigilance).
- Cet interfaçage automatique doit gérer les options de diffusion du compte rendu vers « Mon Espace Santé » (diffuser ou pas diffuser, invisible patient, invisible responsable légal, si possible envoi automatique après un délai défini...) et vers les messageries MS-Santé, conformément aux recommandations techniques nationales.

PARTIE III RELATIVE AUX DEMANDES GENERALES DU MARCHE

ARTICLE 9 – OBLIGATIONS DU TITULAIRE

Le prestataire s'engage à utiliser la plateforme mise à sa disposition via le module n°1 (fourniture d'un système d'information).

9.1 Ressources humaines et notamment médicales

Le titulaire devra mettre à disposition les ressources humaines nécessaires pour répondre aux besoins du présent marché, notamment des ressources médicales ayant les qualifications et compétences requises à l'interprétation des examens transmis dans le cadre de la téléradiologie, inscrits à l'ordre professionnel et disposant d'une assurance. Les attestations de formation des radiologues (notamment à la radioprotection des patients) et les diplômes doivent être disponibles en direct, via l'application.

La responsabilité du contrôle du respect de ces obligations réglementaires, incombe au prestataire avant d'inscrire un radiologue sur le planning des vacations.

Le non-respect de la disponibilité de ces documents entraînera l'application des pénalités.

Les établissements disposent de la liste à jour des médecins radiologues qui interviennent dans le cadre du marché. Il est demandé à ce que les téléradiologues intervenants soient attitrés et que les équipes soit les plus réduites possibles pour chaque établissement.

Le titulaire nomme auprès de chaque établissement un coordonnateur radiologue et assure sa suppléance par un autre radiologue coordonnateur lors de ses absences.

9.2 Processus techniques permettant de sécuriser les prestations et d'en améliorer la qualité

Le titulaire doit décrire le processus de réalisation des prestations de téléimagerie et l'ensemble des mécanismes organisationnels, techniques, logiciels, d'intelligence artificielle utilisés pour assurer la sécurité de la prestation et d'en améliorer la qualité.

Par exemple, sans être exhaustifs :

- sécurisation de l'identitovigilance pour éviter des erreurs d'interprétation entre plusieurs dossiers ;

- s'assurer que le téléradiologue dispose de l'ensemble des images de l'examen réalisé lors de son interprétation ;
- s'assurer de l'absence de confusion entre l'examen du jour et les examens précédemment réalisés ;
- éventuelle utilisation de l'IA permettant la mise à disposition d'une « worklist » de téléradiologie, permettant ainsi d'améliorer l'expérience de l'utilisateur (téléradiologue) et d'optimiser les délais d'interprétation en fonction de l'urgence des examens. Le titulaire devra décrire les mécanismes de sécurité mis en place pour ne pas retarder l'interprétation d'un examen urgent non priorisé par l'IA... ;
- en cas d'utilisation de logiciel d'IA d'aide à l'interprétation en particulier en radiographie standard (radiographie traumatique...), mécanismes mis en place pour s'assurer de la visualisation par le radiologue de l'ensemble des clichés et interdire la validation automatique de compte rendu générés automatiquement. En aucun cas un compte rendu ne peut être généré uniquement par IA, la validation humaine avec analyse des images par le téléradiologue signataire est indispensable et engage sa responsabilité ;
- utilisation de logiciels d'analyse IA des AVC, de post traitement automatisé des AVC, de détection automatique de lésion hémorragique intracrânienne, détection et analyse de lésion pulmonaire, osseuse... Le titulaire décrira les logiciels utilisés et devra s'assurer de la maîtrise des éventuels risques pouvant être générés par leur utilisation ;
- éventuelle utilisation de solution d'aide à la rédaction des compte-rendus standardisés et complets ;
- éventuelle (ou projet) d'utilisation de l'IA pour détecter les erreurs les plus fréquentes dans les compte rendus (erreur de latéralité, incohérence entre la demande, les clichés réalisés et le compte rendu, incohérence au sein du compte rendu...).

Les matériels et logiciels utilisés par les téléradiologues doivent être conformes à la réglementation, en particulier avoir les marquages CE obligatoires.

9.3 Plan assurance qualité

Le titulaire devra être à même de rendre compte de ses différentes interventions selon un processus à proposer qui devra être décrit dans son Plan d'Assurance Qualité et dans son Plan de Gestion des Risques.

Le soumissionnaire devra préciser (en nombre et diplôme) quel type de ressource interne il met en œuvre pour assurer le suivi Qualité et la Gestion des Risques.

Le titulaire assure la gestion documentaire des événements indésirables qui sera accessible aux deux parties et qui devra fournir un rapport annuel détaillé, lors de la visite annuelle, pour informer le service qualité et gestion des risques des établissements concernés.

9.4 Contrôle Qualité

Le titulaire organisera un contrôle qualité de l'ensemble du processus y compris de la qualité médicale des compte-rendus d'examens et de la prise en compte de la radioprotection des patients.

Ce contrôle qualité doit être réalisé dans des délais adaptés à la prise en charge médicale des patients en cas de détection d'erreur. Les erreurs significatives seront signalées au médecin demandeur et au service d'imagerie réalisateur, dans des délais adaptés à la prise en charge médicale des patients et un compte-rendu modificatif sera systématiquement réalisé par le téléradiologue (sans nécessité de demande ou d'intervention du service d'imagerie).

La relecture de chaque examen fera l'objet d'un signalement par email automatisé à l'établissement concerné comportant des éléments permettant d'identifier le dossier concerné, le nom du téléradiologue, du relecteur, le niveau de conformité ou non-conformité du compte rendu et les remarques associées.

Le titulaire émettra une synthèse mensuelle des contrôles et des erreurs détectés pour chaque établissement, avec les mesures prises pour y remédier et la liste de tous les dossiers relus. Elle devra notamment prendre en compte :

- la présence de l'ensemble des éléments obligatoires dans un compte-rendu d'examen (identification patient, le téléradiologue réalisateur, le relecteur si dossier relu par un autre radiologue,.....) ;
- la prise en compte de la radioprotection des patients ;
- les délais d'interprétation ;
- la qualité de la présentation (lisibilité, respect des normes typographiques, orthographiques et grammaticales...) ;
- la qualité médicale des compte-rendus.

Si ces contrôles révèlent des erreurs, des anomalies ou des non-conformités, le titulaire informera immédiatement l'établissement, analysera les causes et y remédiera. Au-delà d'un taux d'erreur grave de 1%, le titulaire devra justifier celui-ci.

En cas de problème grave ou répété, ou de perte de confiance envers un téléradiologue, les établissements peuvent demander à ne plus travailler avec celui-ci sans délai.

Le candidat déposera au sein de son offre et dans le cadre réponse, un descriptif complet de son propre contrôle qualité, le taux d'examens relus, la méthode de sélection des examens relus (qui devront porter sur tous les types d'examens et tous les téléradiologues), les éléments de preuves de la réalisation du contrôle qualité et les rapports qu'il s'engagera à fournir.

En l'absence de justification acceptable et le non-respect de cette description entraînera l'application des pénalités.

ARTICLE 10 – BILANS ANNUELS

10.1 Réunions téléphoniques

Trimestriellement, une réunion téléphonique se déroulera entre le médecin référent du titulaire et le représentant du service d'imagerie de chaque site.

10.2 Visite annuelle

Une visite annuelle sera organisée sur chaque site, avec le médecin référent, durant laquelle le titulaire remettra un rapport récapitulant les actions de l'année précédente.

Un bilan des différents contrôles sera réalisé et évalué lors de cette visite.

L'ensemble des contrôles qualités de l'année écoulée sera passé en revue et les solutions d'améliorations seront validées.

Le compte-rendu de cette visite réalisé par le médecin référent du titulaire, sera adressé à l'établissement concerné, au bureau politique de la direction des hôpitaux des armées (DHA) ainsi qu'à la direction des approvisionnements en produits de santé des armées.