Centre Hospitalier Régional et Universitaire de Tours

Direction des Achats, de la Logistique, des Approvisionnements, et de la Transition Écologique

37044 Tours Cedex 9

http://www.chu-tours.fr

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Marché des Techniques de l'Information et de la Communication (TIC)

Procédure N° 2026-DALATE-DSI-145

FOURNITURE, MISE EN ŒUVRE, MAINTENANCE ET PRESTATIONS ASSOCIEES D'UNE SOLUTION DE GESTION LOGISTIQUE DU BLOC OPERATOIRE AU CHRU DE TOURS

Période :

24 mois à compter de la date de notification

Reconductible 2 fois 12 mois

SOMMAIRE

1. GLOSSAIRE 3

2. GENERALITES 4

2.1 Obligations du Titulaire 4
2.2 Réversibilité 4
2.3 Exécution 4
2.4 RGPD et Hébergement de données de santé 5
2.5 Confidentialité des informations 5
2.6 Autres contraintes réglementaires 6

3. OBJET DU MARCHE 6

3.1 Contexte 6

4. PRESENTATION DE LA STRUCTURE 7

4.1 Présentation du CHRU de TOURS 7
4.2 Présentation de la pharmacie 7
4.3 Présentation de la DSISN 7

5. PRESENTATION DU PROJET NHT 8

6. DESCRIPTION FONCTIONNELLE DE LA SOLUTION ATTENDUE 9

6.1 Contraintes générales 9
6.2 Description de l'organisation existante 9
6.3 Spécifications fonctionnelles « Processus Arsenal Central » 9

7. EXPRESSION DES BESOINS TECHNIQUES 26

7.1 Architecture technique du CHRU Tours 26
7.2 Exploitation et maintenance technique 31
7.3 Sécurité 32
7.4 Préconisation d'infrastructure et éléments à fournir 33
7.5 Sécurité et fonctionnement applicatif 35
7.6 Ergonomie 41
7.7 Conduite de Projet 42
7.8 Maintenance et support applicatif 45

8. L'EXPRESSION DES BESOINS FONCTIONNELS ET TECHNIQUES – CADRE DE REPONSE 48

ANNEXE 1 - REFERENTIELS OPPOSABLES PAR ARRETE DU MINISTRE CHARGE DE LA SANTE PGSSI-S PUBLIE PAR L'ANS (AGENCE DU NUMERIQUE EN SANTE) 49

ANNEXE 2 - REFERENTIELS OPPOSABLES PAR ARRETE DU MINISTRE CHARGE DE LA SANTE 50

ANNEXE 3 - REGLES POUR LES DISPOSITIFS CONNECTES D'UN SYSTEME D'INFORMATION DE SANTE – ASIP SANTE PGSSI-S 51

ANNEXE 4 - CONDITIONS DE MAINTENANCE – A COMPLETER PAR LE TITULAIRE 56

ANNEXE 5 - ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES (AIPD) 58

1. GLOSSAIRE

Notion	Description
CCAP	Cahier des Clauses Administratives Particulières
CCTP	Cahier des Clauses Techniques Particulières
DM	Dispositif Médical
DMI	Dispositif Médical Implantable
DMR	Dispositif Médical Réutilisable
DMS	Dispositifs Médicaux Stériles
DPI	Dossier patient informatisé
DPP	Dossier Patient Partagé (DPI du CHRU de Tours)
DSISN	Direction du Système d'Information et de la Stratégie Numérique
LH	Logistique Hôtelière (ou magasin général)
NHT	Nouvel hôpital Trousseau
POP	Pack Opératoire Programmé (1 POP est lié à une opération / un patient)
POU	Pack Opératoire d'Urgence
PPH	Préparateur en Pharmacie Hospitalière
SIH	Système d'Information Hospitalier
Thésaurus	Répertoire des interventions, ou actes chirurgicaux réalisés au CHRU de Tours
WMS	Warehouse Management System

2. Généralités

2.1Obligations du Titulaire

Ressources

Le Titulaire met en œuvre, sous sa seule responsabilité, l'ensemble des ressources humaines nécessaires, en nombre, expérience et compétence à la réalisation des services objets du marché.

2.2Réversibilité

A l'expiration de la durée contractuelle ou en cas de résiliation du Marché, pour quelque motif que ce soit, le Titulaire garantit et s'engage à assurer la réversibilité des données :

- (1) Permettre au CHRU de Tours de prendre en charge ou de faire prendre en charge tout ou partie des [Données] par un repreneur tiers (ci-après « Repreneur ») choisi par le CHRU de Tours ;
- (2) Minimiser tout risque lié au transfert des données du Titulaire au CHRU de Tours ou au Repreneur.

Le Titulaire s'engage à mettre en œuvre, pendant toute la durée du Marché, tous les moyens matériels, humains, logistiques et autres, nécessaires afin de permettre cette reprise en tout ou partie des données, dans leur état d'avancement et dans les meilleures conditions.

Le Titulaire élaborera donc un plan de réversibilité (« le Plan de réversibilité ») avant la signature de la VA pour définir les conditions de transfert des données du Titulaire au CHRU de Tours ou à un Titulaire tiers. Les conditions de transfert opérationnel des données et les différentes tâches incombant aux parties sont décrites dans ce Plan. Il doit aussi répertorier l'ensemble des données de reprise, ainsi que d'autres informations (instructions, spécifications). Il appartient au Titulaire d'assurer la mise à jour du Plan de réversibilité.

A la décision de mise en œuvre de la réversibilité une vérification contradictoire sera engagée entre le CHRU et le Titulaire. Le Titulaire s'engage à apporter toutes modifications résultant de cette vérification.

Le Titulaire s'engage notamment à détailler :

- l'ensemble de ses responsabilités et de ses obligations au titre du Marché ;
- tout facteur de risque significatif lié à la réversibilité des données qu'il pourrait identifier.

Le Titulaire est tenu de restituer les Données qui lui ont été confiées soit sous forme de Dump ou de sauvegarde soit sous un format requêtable par des outils disponibles sur le Marché soit sous la forme d'un « fichier plat », étant précisé que ce choix appartient au CHRU de Tours. Le Titulaire s'interdit de conserver une copie des Données restituées y compris des données sauvegardées.

2.3Exécution

Le Titulaire organise et propose une offre conforme au descriptif de la documentation fournie dans son offre (en On premise ou en mode SaaS s'il ne permet pas le mode On Premise). En mode SaaS, la solution devra être hébergée en HDS en France (ISO 27001).

Le Titulaire détaillera notamment dans son offre les services suivants : Maintenance, Niveaux de services, conformité RGPD, sécurité et réversibilité.

2.4RGPD et Hébergement de données de santé

Le Titulaire fournira les éléments nécessaires à la constitution de la déclaration dans le registre des traitements.

Les référentiels sur l'hébergement des données de santé, leur sécurité et leur confidentialité. En particulier dans le cas où la prestation nécessiterait le transfert de données de santé sur un système du prestataire, celui-ci devra impérativement détenir l'agrément des hébergeurs de données de sante à caractère personnel.

Le RGPD impose que les organismes accédant à des données à caractère personnel en garantissent la sécurité, la confidentialité et l'intégrité. Lors des maintenances réalisées sur l'application, qu'elles soient réalisées sur le site client, par télémaintenance ou chez le fournisseur, l'organisme s'engage à mettre toutes les précautions utiles, au regard de la nature des données pour empêcher que les données soient déformées, endommagées, et que les tiers non autorisés y aient accès.

L'organisme s'engage à ce que ses prestataires intervenants sur les dispositifs du client se conforment au RGPD. L'organisme met en œuvre des mesures techniques et d'organisation appropriée afin de protéger les données à caractères personnels.

Enfin, le fournisseur s'engage à faire signer un « engagement de confidentialité » à ses salariés en contact avec les données à caractère personnel du responsable de traitement (client) ou prévoit dans les contrats de travail une clause de confidentialité spécifique concernant les données.

A ce titre, le candidat complètera l'annexe 1 RGPD du CCAP.

2.5Confidentialité des informations

Ce document, ceux qui y sont attachés et ceux qui seront constitués au cours du projet contiennent des informations précises sur les aspects organisationnels, fonctionnels et techniques du système d'information hospitalier du CHRU de Tours. L'offreur doit respecter la confidentialité de l'ensemble de ces documents.

Le prestataire s'engage, sous peine de poursuite, à :

- Ne pas diffuser ce document, ses annexes ainsi que les documents qui seront constitués au cours du projet.
- Ne communiquer les informations relatives aux systèmes d'informations du CHRU de Tours qu'aux intervenants nommément présentés au CHRU de Tours.
- Ne divulguer en aucun cas toutes les informations recueillies au CHRU de Tours concernant les systèmes d'information, les conclusions de la mission, ainsi que toutes les informations nominatives, confidentielles ou médicales qu'il aura pu récupérer par quelque moyen que ce soit à l'extérieur de sa société.
- Mettre en œuvre toutes les mesures techniques et organisationnelles afin d'assurer la sécurité et la confidentialité de tous les éléments, documents, informations et données que le CHRU de Tours lui aura communiqués ou auxquels le prestataire aura accédé dans le cadre de ce projet. En particulier, les transmissions de documents et d'informations confidentielles en rapport avec le CHRU de Tours devront être chiffrées afin d'empêcher à un tiers de les obtenir.
- Utiliser les matériels et les logiciels mis à sa disposition uniquement pour la réalisation de la prestation.
- Assurer la protection physique du matériel mis à sa disposition et en particulier, ne pas permettre l'accès aux personnes non autorisées par le CHRU de Tours dans les locaux du CHRU de Tours comme dans ses propres locaux.

- Communiquer au CHRU de Tours, dès l'ouverture des autorisations d'accès au système et en cas de changement, le nom des intervenants et l'identification utilisateur associé.
- Faire respecter la protection, la non-divulgation et le non partage du mot de passe des intervenants qui doivent en assurer une utilisation strictement personnelle.
- Respecter la Charte des Systèmes d'Information du CHRU de Tours.
- Signer la « Charte d'accès au SI du CHRU de Tours pour les fournisseurs » pour les soumissionnaires si le CHRU de Tours l'exige.

Le CHRU de Tours indiquera à l'issue de la prestation au titulaire retenu sa décision quant à la possibilité d'être cité comme référence externe pour ce type de projet.

De même, le CHRU de Tours s'engage à respecter la confidentialité des informations qui lui seront envoyées. Elles ne pourront être divulguées que dans la situation exceptionnelle d'un audit ou d'une expertise relatifs à la sécurité informatique (dont les prestataires seront également soumis à confidentialité).

2.6Autres contraintes réglementaires

Si le présent projet présente également d'autres obligations règlementaires, le titulaire en informera le CHRU de Tours et lui transmettra l'ensemble des informations à sa disposition afin d'en assurer la conformité.

3. OBJET DU MARCHE

3.1 Contexte

Le Centre Hospitalier Universitaire de Tours mène actuellement un projet de reconstruction du site de Trousseau avec un regroupement d'activités médicales et chirurgicales sur ce site.

Ce nouveau bâtiment comprendra, dans sa partie plateau médico-technique, 35 salles de blocs opératoires dont 25 salles de bloc conventionnel, les autres étant dédiées à l'interventionnel. Il sera également équipé d'un arsenal de bloc centralisé (sur 2 étages) et d'une stérilisation située à l'étage supérieur.

L'objectif de ce marché est de mettre en place un logiciel capable de :

- Gérer les stocks de l'arsenal de bloc (environ 1500 références de DM, plus les DMR)
- Gérer la constitution des chariots opératoires cible : 140 POP environ / Jour ; 5000 lignes de produits environ à préparer
- Être paramétré et adapté au contexte du CHRU de Tours
- S'interfacer avec les applications du SIH du CHRU

Le logiciel attendu est décrit sous le nom de LOGICIEL DE GESTION LOGISTIQUE DU BLOC ou LOGICIEL ARSENAL dans la suite du document.

Le système proposé devra être diffusé et maintenu par une société disposant de références dans le domaine. Ces références seront précisées dans la réponse. Le système devra répondre aux contraintes réglementaires, notamment sur les règlementations liées aux produits pharmaceutiques et à l'identification des patients.

4. PRESENTATION DE LA STRUCTURE

4.1 Présentation du CHRU de TOURS

Le CHRU de TOURS est composé de trois établissements (Trousseau, Bretonneau et Clocheville), d'un établissement SSR EHPAD (Ermitage) et d'un hôpital psychiatrique (NHP). Il compte au total 1568 lits.

La Pharmacie à Usage Intérieur du CHRU et ses activités couvrent également le CH de Luynes.

4.2 Présentation de la pharmacie

La Pharmacie à Usage Intérieur du CHRU de Tours est répartie sur les 3 sites principaux. Elle couvre l'ensemble des missions pouvant être autorisées pour une PUI.

A Trousseau : Pharmacie centrale et Pharmacie de site, activité de stérilisation et de radiopharmacie

A Bretonneau : Pharmacie de site, activité de reconstitution des anticancéreux, stérilisation et radiopharmacie

A Clocheville : Pharmacie de site, activité de préparations stériles, dont la préparation des poches de nutrition parentérales.

Dans le cadre du projet logistique du nouveau plateau technique, seule la pharmacie centrale est un maillon de la chaine logistique.

Par ailleurs, il est à noter que la stérilisation de Bretonneau et de Trousseau seront fusionnées à l'ouverture du NHT (Nouvel Hôpital Trousseau), et la stérilisation centrale sera située à l'étage supérieur des blocs opératoires.

Pour ce dossier, la pharmacie est en charge de l'approvisionnement, de la gestion et de la délivrance des DMS, des DMI et des DMR.

4.3 Présentation de la DSISN

La Direction du Système d'Information et de la Stratégie Numérique (DSISN) du CHRU regroupe 80 personnes réparties sur 3 secteurs : Infrastructures numériques (conception, production et centre de service) - Solutions Métiers (domaines médicaux, médico-techniques, SIRH, administratifs et logistiques) – AMOA Accompagnement des professionnels de santé.

Le service est basé sur le site de l'hôpital Bretonneau dans le centre-ville de Tours.

Chargée de fournir et maintenir des services numériques sécurisés aux différentes corps de métiers de l'institution, la DSISN supervise plus d'une centaine de logiciels métiers dont le Dossier Patient Informatisé, le Système de Gestion de Laboratoire, les logiciels d'Imagerie, et la suite administrative, logistique et financière. Le portefeuille de projets tant techniques que fonctionnels s'enrichit de nouveaux challenges avec le programme Horizon 2030 associé à l'ouverture du Nouvel Hôpital Trousseau, l'urbanisation de l'offre logicielle avec les programmes nationaux (feuille de route nationale du numérique de santé), les projets innovants s'appuyant sur l'IA, dans le respect des bonnes pratiques de Qualité et de Sécurité informatique.

La DSISN du CHRU de Tours pilote également la convergence du Système d'Information Hospitalier au sein du Groupement Hospitalier de Territoire Touraine Val de Loire.

5. PRESENTATION DU PROJET NHT

Le CHRU de Tours verra au 2ème semestre 2028 l'ouverture d'un bâtiment de plus de 52 000m², nommé NHT (Nouvel Hôpital Trousseau), comprenant un Plateau Médico-Technique et un Bâtiment d'Hébergement.

Le Plateau Médico-Technique regroupera tous les blocs opératoires du CHRU (à l'exception de la Gynécologie (7 salles dont 2 obstétriques), de l'Urologie (4 = salles 3 + 1 ROBOT) et des 6 salles de blocs opératoires pédiatriques du site de Clocheville), ainsi que les réanimations, la stérilisation, un plateau d'imagerie, les urgences …

L'Arsenal Central sera composé de 2 arsenaux distincts : le premier, situé au 1er étage , même étage que les blocs, accueillera tous les stocks de Dispositifs Médicaux stériles à usage unique (DMS) ainsi que des DM non stériles actuellement gérés par la PUI, et le deuxième, situé en proximité immédiate de la stérilisation, au 2eme étage, accueillera tous les DMR gérés par la Stérilisation.

Les produits nécessaires à une intervention chirurgicale seront présentés sous la forme de « packs opératoires programmés » (POP) (avec un ou plusieurs chariots physiques) préparés au sein de l'Arsenal, en amont de l'intervention, et en lien avec la programmation opératoire.

Vous trouverez ci-dessous le nombre de salles de blocs estimés avec le nombre d'interventions concernés par la préparation de POP (chiffres de 2024) :

- Nb Salles de Bloc Vasculaire : 2 ; nb inter. = 1013
- Nb Salles de Bloc Cardiaque : 2 ; nb inter. = 699
- Nb Salles de Bloc Thoracique : 2 ; nb inter. = 481
- Nb Salles de Bloc Ortho : 3 (+1 avec salle des urgences) ; nb inter. = 3744
- Nb Salles de Bloc Maxillo : 2 ; nb inter. = 1281
- Nb salles de Bloc Chirurgie Plastique et Reconstructive : 1 ; nb inter. = 333
- Nb salles de Bloc Viscéral Digestif : 2 ; nb inter. = 2436
- Nb salles de Bloc UDTA : 3 ; nb inter. = 3661 (Dermato, Dig, Maxillo, Ortho, Plastique, Vasculaire)
- Nb salles de Bloc Neurochirurgical : 2 ; nb inter. = 1650
- Nb salles Bloc Ophtalmologique : 3 ; nb inter. = 3831
- Nb salles Bloc ORL : 2 ; nb inter. = 1781

L'Arsenal sera règlementairement sous responsabilité pharmaceutique et l'activité quotidienne sera co-pilotée par la PUI et les Blocs. Des préparateurs en pharmacie (PPH) seront par ailleurs positionnés aux côtés des équipes IBODE du bloc, afin de faciliter le lien entre les deux entités et apporter leurs compétences en matière de gestion des stocks de proximité.

En France à ce jour, seuls quelques centres hospitaliers ont déployé un arsenal mutualisé sous gestion pharmaceutique. En parallèle, la densification des stocks et la rationalisation des surfaces de stockage représentent un défi supplémentaire.

Les objectifs du projet sont multiples :

- Sécuriser et optimiser le circuit des DM (flux et stockage)

- Décharger les personnels soignants (IBODE et IDE notamment) de leurs activités logistiques, afin de leur permettre de se recentrer sur leur cœur de métier : le soin auprès du patient

- Pérenniser et fiabiliser cette organisation en renforçant l'attractivité et l'implication des professionnels, à la fois pharmaceutiques et soignants.

6. DESCRIPTION FONCTIONNELLE DE LA SOLUTION ATTENDUE

6.1 Contraintes générales

Les solutions proposées devront impérativement respecter les contraintes suivantes :

- La solution doit être calibrée et dimensionnée pour supporter les volumes et les activités tels que décrits dans le présent document.
- Le logiciel doit être proposé dans une configuration On Premise ou en mode SaaS s'il ne permet pas le mode On Premise. En mode SaaS, la solution devra être hébergée en HDS en France (ISO 27001).

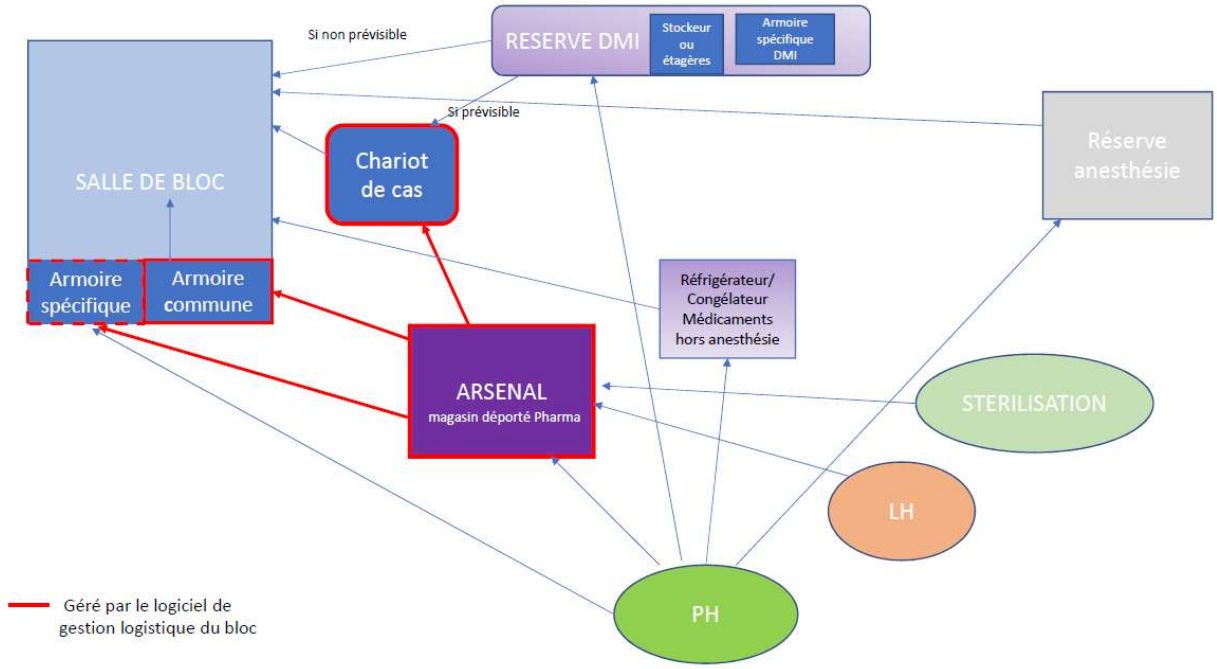
6.2 Description de l'organisation existante

6.2.1 Architecture logicielle actuelle sur le périmètre de la solution attendue

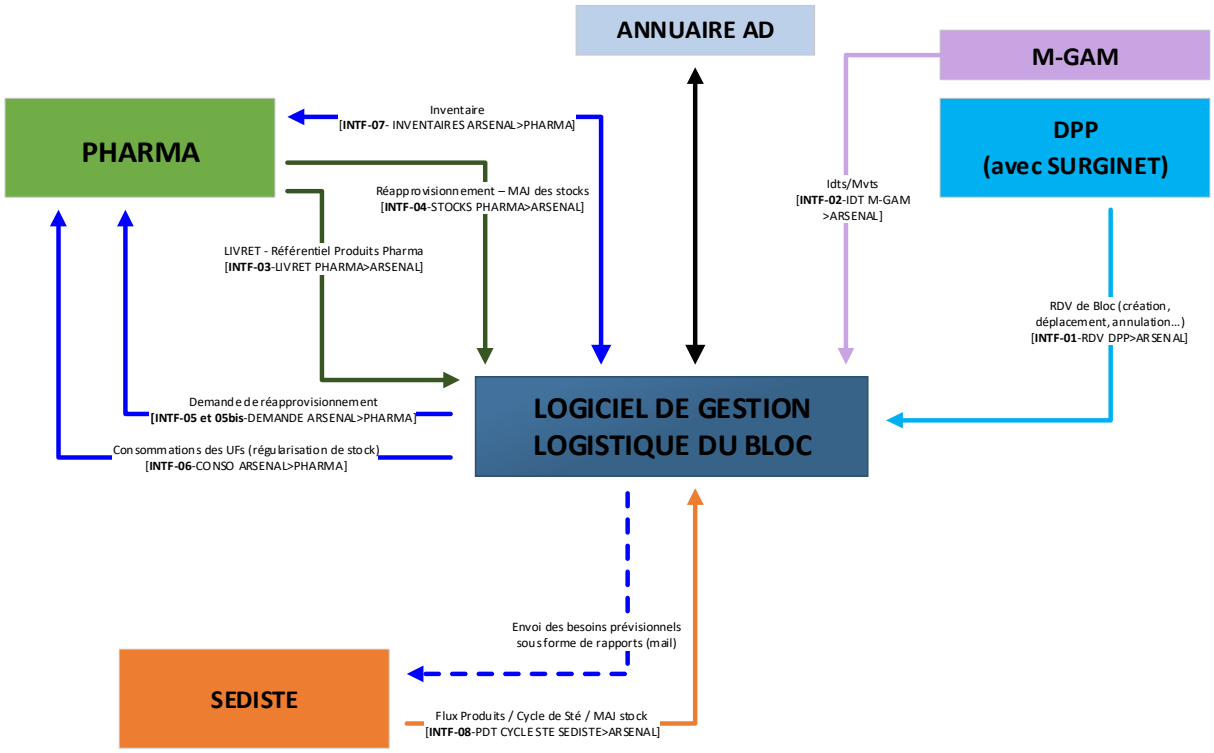
- Serveur d'Identités/Mouvements : M-GAM de MainCare Solutions en synchronisation bidirectionnelle avec le DPP
- Dossier Patient et planification opératoire : MILLENIUM de CERNER, appelé DPP (Dossier Patient Partagé)
- Visualisation du Planning Opératoire : SURGINET de CERNER, module du DPP
- Logiciel de la gestion de la Pharmacie (Marché, Produits) : PHARMA de Computer Engineering
- Logiciel de traçabilité de la Stérilisation : SEDISTE de SEDIA interfacé avec les équipements matériels (laveurs désinfecteurs, stérilisateurs à la vapeur d'eau)
- Annuaire LDAP Active Directory (en version Windows 2016) pour la gestion des utilisateurs

6.3 Spécifications fonctionnelles « Processus Arsenal Central »

6.3.1 Cartographie globale



6.3.2 *Interopérabilité*



6.3.3 *Description des processus*

Nous définissons le terme de « **Matériel** » comme étant un composant d'un POP, sauf équipement biomédical. Le terme de « **Stocks de proximité** » concernera les armoires communes, armoires de spécialité ou étagères dans certains lieux des blocs chirurgicaux.

A-Programmation opératoire de l'intervention et demande de matériel

Qui : Le chirurgien et/ou la secrétaire

Quoi : inscription au programme opératoire de l'intervention devant être réalisée pour le patient : date, acte selon thésaurus, matériel à prévoir ou à commander

Quand : de immédiatement à plusieurs mois à l'avance

<u>Programmation dans DPP en 3 étapes :</u>

1. Demande d'intervention par le chirurgien
2. Programmation de l'intervention par le chirurgien ou la secrétaire par la pose d'un RDV de bloc dans le DPP : l'intervention est mise en programme. Cette étape intervient après la consultation chirurgicale
3. Validation finale de la programmation lors des staffs chirurgicaux et de la cellule de régulation avec une validation sur le matériel (DMS, DMR, DMI) et des ressources.

En cas de non validation, le RDV est soit reprogrammé dans le DPP, soit mis en attente avec une désactivation de la prévision de POP dans le logiciel arsenal.

Comment :

Récupération par l'outil Arsenal :

- des Identités/Mouvements issus de M-GAM [**INTF-02**-IDT M-GAM>ARSENAL]
- des Rendez-vous du planning opératoire avec les données nécessaires pour la création du listing de POP depuis le logiciel DPP (création, déplacement, mise en attente, annulation…) [**INTF-01**-RDV DPP>ARSENAL] :
    - Acte (exemple : CA_PAC, CA_Rempla valvulaire aortique) : 1 ou plusieurs déclarés amenant à plusieurs POP pour un seul RDV de DPP
    - Motif (exemple : RBE : GENOU GAUCHE / MPFL)
    - Opérateur (chirurgien avec RPPS, matricule, nom, prénom)
    - Identité patient (traits stricts et complémentaires)
    - UF, Libellé, Code Bloc, libellé Bloc
    - Date et heure d'intervention
    - Numéro de la salle / nom de salle (critères non bloquants pour les restes de garde)
    - Matériel à prévoir ou à commander (DMIs, prêts de matériel – dépôt temporaire, hors matériel biomédical) : (exemple : SUTURE TAK+ARTHRO GENOU+MECHES CANULEES (TUNNEL LARGE AU FEMUR) + VIS INTERERANCE)
    - Commentaire du RDV

B- Référentiel des POP, documents opératoires et création de la demande de préparation

Le logiciel Arsenal connaîtra les produits DMS de la pharmacie grâce à un flux LIVRET de PHARMA (Catalogue) vers le logiciel Arsenal [**INTF-03**-LIVRET PHARMA>ARSENAL].

B-1- Référentiel de la composition des POP

Toutes les interventions réalisées au CHRU de Tours sont listées dans le Thésaurus, spécialité par spécialité. A chaque intervention correspond une fiche de préparation.

Le logiciel doit permettre de paramétrer et maintenir le Référentiel des Fiches de Préparation des POP.

Le référentiel est constitué de fiches. Chaque fiche est :

- nommée par un titre (différent du nommage des actes du Thésaurus du CHRU. Une fiche du référentiel peut être commune à plusieurs actes du Thésaurus)
- constituée par une liste des matériels nécessaires à un (ou aux) actes correspondant(s) ; chaque matériel doit pouvoir être typé « dispensable = non obligatoire » ou non (au sens de l'arsenal). La notion de « dispensable » est attachée au matériel et à la fiche. Un matériel peut donc être dispensable sur une fiche et indispensable sur une autre fiche. Chaque matériel doit pouvoir être paramétré avec une référence/coordonnée d'emplacement ou un emplacement générique.
  Cette liste énumèrera les matériels à prélever dans l'arsenal, mais aussi les matériels connus de l'arsenal à prélever dans les « stocks de proximité » : il est demandé à ce que l'on puisse indiquer le lieu de prélèvement sur les matériels paramétrés dans la liste (n° de localisation dans l'arsenal, armoire commune, armoires de spécialité, étagère…) par les IDE de bloc. Par défaut, les matériels des stocks de proximité seront typés « dispensable ».

- implémentée par des options de matériels supplémentaires (ou compléments) en fonction d'autres critères que l'acte (ou les actes), par exemple un chirurgien qui demande du matériel propre à sa pratique…

Le candidat doit proposer un paramétrage ergonomique :

- permettant de dupliquer des fiches déjà existantes pour créer de nouvelles fiches
- permettant de répercuter le remplacement d'un matériel sur un certain nombre de fiches sélectionnées préalablement par l'utilisateur. Il doit être possible de faire une mise à jour sur toutes les fiches contenant le matériel concerné (par exemple dans le cas des changements de marché ou d'une rupture de stock).

B-2- Import et mise à disposition de document relatif au référentiel

L'outil doit proposer une possibilité d'importer un ou plusieurs documents opératoires (PDF, docx…), précisant notamment l'installation, associés à chaque acte du thésaurus et à chaque fiche de préparation. Ces documents doivent pouvoir être appelés à tout moment sur terminal mobile ou ordinateur lorsque l'utilisateur (IBODE d'ordonnancement, IDE de bloc) accède à un POP prévisionnel ou préparé dans le logiciel.

B-3- Création de la demande de préparation

Avec les informations du RDV DPP et du référentiel de fiches, le (ou les) POP prévisionnels (avec leurs matériels) est (sont) implémenté(s) dans la liste des POP en attente de validation pour préparation. Le logiciel Arsenal doit permettre d'indiquer, à la lecture de la liste, les POP concernés par une même opération.

Avec les informations d'Idts/Mvts et RDV, le logiciel Arsenal doit être en mesure de faire le listing des POP ainsi créés comportant :

- L'identité du patient, le chirurgien, le bloc et la salle concernée, l'acte
- Date et heure de l'intervention
- Les matériels nécessaires (référence, quantité) à la réalisation de l'acte ou des actes sur les chariots, compléments liés à l'opérateur ou au patient…
- Les matériels à prévoir ou à commander
- Commentaire

Le logiciel doit donner la possibilité de créer manuellement une demande de POP dans la liste :

- ⇨ La préparation d'un POP supplémentaire avec un nouvel acte chirurgical pour 1 RDV patient ayant au moins déjà 1 POP (de prévu, en préparation, ou libéré)
- ⇨ La préparation d'un POP pour un patient non inscrit au programme (court-circuit de DPP) avec :
  - un acte
  - une identité connue du SIH ou momentanément inconnue
  - une régularisation de l'identité et le RDV pendant ou après l'opération
- ⇨ La préparation et le maintien d'un POU (Pack Opératoire d'Urgence) non associé à un patient avec :
  - Un acte
  - des produits à l'état « Réservé » et une possibilité d'ajout, de remplacement, et d'enlèvement des produits

- une possibilité de lancer ce chariot dans une opération avec une identité connue ou inconnue du SIH
- une régularisation possible de raccrocher un patient par rapport à un RDV DPP qui arriverait plus tard

C- Ordonnancement et vérification des stocks

Quoi : Les demandes de préparation de POP rejoint une file de POP qui doit ensuite être ordonnancée avant le lancement en préparation :

- Dès l'arrivée d'une nouvelle demande de préparation, celle-ci se range dans la liste selon la date prévue de réalisation de l'opération chirurgicale (ordonnancement automatique). Si un changement est réalisé sur le programme opératoire pour cette demande, l'ordonnancement de celle-ci doit se mettre à jour.
- Un ordonnancement manuel doit être proposé afin d'organiser l'ordre de préparation, notamment pour prendre en compte les urgences (sur demande téléphonique du bloc).

Lors d'un changement d'ordre ou à l'arrivée de nouveaux POP dans la file, les disponibilités des matériels (DMS, DMR) doivent être calculées en temps réel par interrogation du stock arsenal, en fonction des autres demandes de préparation. Ce calcul de stock doit être accessible à tout moment à l'arsenal et au bloc.

A ce stade, l'ensemble du matériel est à l'état « stocké ». L'outil doit permettre de simuler les préparations à venir sur une période donnée (qui, dans la pratique, n'excèderait pas 7 jours) afin d'indiquer si un produit ne serait pas disponible pour un POP, car l'ensemble du stock est déjà positionné sur les autres POP classés avant dans la file.

L'outil doit permettre de modifier le contenu des POP dans la file (en ajout ou suppression).

L'outil doit permettre une visualisation des états des préparations des POP directement en salle de bloc : Une remontée d'alerte doit être réalisé par l'outil, accessible au bloc (par exemple : matériel non livré, livré en attente de réception, non stérilisé, POP non libéré…).

Dans le cas de plusieurs POP pour un RDV patient, l'IBODE d'ordonnancement aura la charge d'enlever certaines lignes de matériels dans les POP secondaires sur le logiciel (afin d'éviter des matériels sortis en double inutilement).

D- Lancement et Préparation de POP

<u>Etape 1 : Lancement de la préparation</u>

Quand : A J-1 de l'intervention (voire 1 demi-journée avant)

Qui : IBODE d'ordonnancement, en lien avec le bloc

Comment : le déclenchement de la préparation peut être manuel (ordonnancement et lancement) ou automatisé selon le jour et l'heure des opérations chirurgicales.

Si un RDV a plusieurs POP, aucun POP ne peut être validé automatiquement. Ils doivent être validés manuellement par l'IBODE d'ordonnancement, une fois qu'elle a enlevé ce qui n'était pas nécessaire.

Ensuite, la préparation est disponible sur les terminaux mobiles. Un agent logisticien peut s' attribuer la préparation sur son terminal et initier le picking. Le logisticien doit pouvoir distinguer les produits qu'il doit prélever à l'arsenal, de ceux qui seront à prélever au niveau des blocs par le IBODE « typés stock de proximité ».

Etape 2 : Préparation

Qui : *Personnel de l'arsenal sous la responsabilité de l'IBODE d'ordonnancement*

Quoi : 1 ou plusieurs POP créé(s) à partir d'une demande d'intervention ou plusieurs POP sur 1 Chariot

Comment :

La préparation doit pouvoir se faire en deux étapes puisque les produits nécessaires à une intervention sont stockés dans un arsenal situé à deux étages différents : DMR (étage 2 : stérilisation) puis DMS (étage 1 : salles de blocs opératoires).

Dans la phase du picking, en cas d'erreur de scann, le terminal doit alerter l'opérateur que le produit ne fait pas partie de la liste du POP.

En cas de produit défectueux lors du picking, une sortie de stock manuelle (sortie au rebus) pourra être faite manuellement.

L'outil doit permettre de paramétrer les emplacements, avec édition d'étiquette pour chaque emplacement (avec QR Code / Datamatrix).

Cas n°1 : 1 POP créé à partir d'une demande d'intervention : 1 chariot

Phase 1: Chariots de POP vides stockés dans l'arsenal des DMR (2ème étage)

Phase 2: Le professionnel scanne le chariot de POP pour l'associer à l'intervention avec un terminal mobile.

Phase 3: Le professionnel débute son picking, au 2eme étage

La liste de picking est optimisée, dans l'ordre de la localisation, et le chemin de picking doit être calculé pour être le plus court possible.

Les rangements sont optimisés par type de produits (volume, poids, fragilité …) L'outil doit permettre renseigner des informations de poids et de volumes pour permettre cette optimisation.

L'agent scanne les code-barres d'emplacement (et non pas les codes produits) pour les DMS et les code-barres de chaque composition pour les DMR.

Après le scan de l'emplacement, l'outil doit afficher la référence à prélever. L'outil doit indiquer le conditionnement à prendre et doit alerter l'opérateur si un produit doit être prélevé dans un conditionnement.

L'opérateur confirme qu'il a prélevé la demande sur le terminal mobile. Le produit sur le chariot passe d'un statut « stocké » au statut « réservé » dans le logiciel de l'arsenal. La quantité prélevée n'entre ainsi plus dans le calcul de la disponibilité pour les autres POP prévus de la liste d'ordonnancement.

Point sur les statuts des matériels au niveau stock :

Le logiciel de gestion logistique du bloc doit proposer plusieurs statuts lorsqu'on interroge une référence de DMS/DMR :

- Statut « stocké » : signifie que le DMS/DMR est présent dans l'arsenal
- Statut « Réservé » : signifie que le DMS/DMR est présent sur un chariot de cas ou en cours d'utilisation au bloc. L'utilisateur doit pouvoir identifier le POP concerné, par exemple dans le cas où il doit prendre en urgence un DMS/DMR dans un chariot de cas préparé pour le lendemain alors qu'une intervention urgente est programmée le jour même avec ce DMS/DMR. Le produit n'est pas décrémenté en stock mais est mis dans un état réservé

ou « sous-stock réservé non disponible POP », qui signifie que le stock disponible Arsenal est réduit de la quantité des produits sur les POP.

Le professionnel dispose et positionne les produits dans le chariot de POP selon une organisation prédéfinie en lien avec le déroulé opératoire et la typologie de produit. L'outil doit assister le professionnel dans l'organisation du POP.

En particulier pour les DMR :

Pour les DMR, la gestion au lot est demandée. Lors de la préparation, le logiciel indiquera à l'agent logistique le numéro de lot à prélever.

Il doit aussi créer une alerte (mail, rapport) des DMR présents en stock pour lesquels les dates de péremption arrivent à échéance.

Un flux d'interface des DMR envoyé par le Service de Stérilisation à l'arsenal [**INTF-08** – PDT CYCLE STE SEDISTE > ARSENAL] enverra les informations de la boîte, avec le n° de cycle de stérilisation, la référence et l'intitulé unique du DMR, la date d'expiration, la date de stérilisation, le service destinataire et le commentaire associé. Plusieurs références/libellés peuvent correspondre à un seul Produit Arsenal : par exemple **LAPARO1TB3/LAPAROTOMIE 1** et **LAPARO12TB3/LAPAROTOMIE 12** correspond au même produit appelé **LAPAROTOMIE**.

Il est attendu que l'outil Arsenal connaisse et gère dans le détail toutes les boîtes avec les dates de péremption/commentaire. Au picking, le terminal doit proposer la boîte ayant une péremption la plus proche (FEFO - First Expired First Out).

Dans le cas d'une boite défectueuse, le logisticien aura la possibilité de faire une sortie de stock manuelle « rebus » et l'outil devra proposer une nouvelle boîte de substitution à la place de la boite défectueuse, en tenant compte des dates d'expiration.

A chaque réception d'une boîte, le stock devra s'incrémenter sur ce produit. Par paramétrage, l'outil doit permettre de ranger toutes les références par produit Arsenal. C'est la référence produit Arsenal qui doit être utilisé dans le référentiel des fiches de préparation de POP.

Le logiciel Arsenal doit pouvoir émettre un rapport (1 fois / jour à définir – Envoi par mail) permettant de lister toutes les prévisions d'utilisation de DMR (disponible à l'arsenal) avec les POP concernés (horaire/actes/salle), y compris les DMR déjà réservés.

Phase 4: Le professionnel descend avec son POP à l'aide du Monte Charges dédié et continue son picking dans l'arsenal des DMS au 1er étage.

NB :

L'outil doit nous indiquer si la préparation en cours est au 2eme ou au 1er étage.

Le fonctionnement du logiciel doit pouvoir autoriser un picking commencé par un professionnel à l'étage 2, mis en attente, puis repris par un autre professionnel à l'étage 1.

Phase 5 : Une fiche POP (liste de contrôle de préparation), doit être imprimée avec un code-barre faisant état du nom du patient, du nom de l'intervention, du nom du chirurgien, de la date et heure d'intervention, code ou/et libellé de l'acte chirurgical, nom du préparateur, liste des produits préparés présents dans le POP, la liste des produits manquants le cas échéant, la liste des produits à compléter par l'IBODE en stock de proximité, l'état du POP (libéré ou non, cf point E.). Le champs « Matériel à prévoir» transmis du DPP au logiciel Arsenal doit être mis dans une partie commentaire sur la fiche pour l'IBODE.
Le professionnel positionne cette liste sur le chariot et place le chariot à l'emplacement dédié dans l'arsenal (zone d'attente - partie complet / partie incomplet). Il y a autant de fiches que de POP concernés pour une intervention, sauf dans le cas de chariots multi-POP.

L'outil doit alerter l'IBODE de référencement du manque de matériel DMS ou DMR.

Les utilisateurs (stérilisation et bloc) sont alertés par l'IBODE d'un manque de matériel selon la criticité des produits manquants.

L'IBODE d'ordonnancement doit pouvoir écrire un commentaire lié au POP dans le logiciel de l'arsenal. Ce champ doit être reporté sur la fiche de préparation du POP lors de son édition.

L'IBODE en salle doit avoir une visu sur l'avancée des préparations de chariots sur le logiciel (sur ordinateur)

<u>Cas n°2 :</u> 1 POP créé à partir d'une demande d'intervention : plusieurs chariots (type ortho)

Reprise des étapes du cas 1, avec les particularités suivantes :

- Déclaration de plusieurs chariots (avec une notion de bis pour le 2ème par exemple)
- Les x chariots sont associés à 1 POP sans détail des chariots pour chaque matériel.
- Le système enregistre un lien qui lui permet de savoir que les chariots sont liés les uns aux autres
- La fiche imprimée doit mentionner les noms et le nombre de chariots utilisés pour un POP

<u>Cas n°3 :</u> Plusieurs POP sur 1 Chariot : Ce cas particulier concerne notamment les interventions très rapides (type cataracte).

Reprise des étapes du cas 1, avec les particularités suivantes :

- Un chariot peut être constitué pour plusieurs interventions dédiées à une seule salle non dépendant du chirurgien, avec des patients différents, correspondant à plusieurs POP pour une période ou un cochage des POP concernés par le préparateur. Chaque sous-partie du chariot appelé « bac » est identifié par une étiquette à scanner, éditée et gérée par le logiciel.
- L'agent logistique scanne le chariot et ensuite tous les bacs des POP à préparer. Le logiciel doit pouvoir associer l'ensemble des bacs à un chariot, afin de pouvoir utiliser le scann chariot pour les étapes suivantes (Point E, F, G…) sans avoir à rescanner les bacs par la suite. Le terminal mobile permet un picking optimisé pour la série de POP sélectionnée en demandant de prendre en un seul circuit tous les matériels nécessaires à la liste des POP définis.
- Génération d'une feuille unique rassemblant tous les POP avec les commentaires et matériels à préparer. La fiche imprimée doit aussi mentionner le nombre de POP sur un chariot.

<u>Cas n°4 :</u> Plusieurs POP sur plusieurs chariot (type plusieurs équipes chir pour 1 patient ex polytrauma):

Reprise des étapes du cas 1, avec les particularités suivantes :

- Chaque POP est géré de manière indépendante à la préparation, avec leurs chariots indépendants, mais le système enregistre un lien qui lui permet de savoir que les POP sont liés

les uns aux autres. Cette information sera utile dans le cadre des retours afin de ne pas bloquer l'opérateur en lui permettant de doucher un seul chariot, n'importe lequel). L'outil génère une feuille unique pour chaque POP, en indiquant le n° de POP et le nombre de POP concerné par l'intervention (ex : n°1/3).

Cas (exemple)	Nombre de patient	Nombre de POP	Nombre de chariot
1	1	1	1
2 (orthopédie)	1	1	x
3 (cataracte)	x	x	1
4 (plusieurs spécialités chir)	1	x	x

E-Libération du POP :

L'outil doit permettre de libérer automatiquement ou manuellement les POP selon les cas suivants :

Cas (exemple)	Automatique	Manuellement = intervention IBODE
1 (1 POP/1 patient/1 chariot)	Tous les produits sont présents ou si les produits absents sont dans la catégorie « Dispensable » ou « Stocks de proximité »	Il manque un produit dans la liste des matériels à charger **hors** catégorie « Dispensable » ou « Stocks de proximité »
2 (1 POP/1 patient/ x chariots)	Tous les produits sont présents ou si les produits absents sont dans la catégorie « Dispensable » ou « Stocks de proximité » Il est unique pour 1 RDV patient	Il manque un produit dans la liste des matériels à charger **hors** catégorie « Dispensable » ou « Stocks de proximité »
3 (x POP= multi-POP/X patients/1 chariot) Système association chariot/bac)	Tous les produits sont présents ou si les produits absents sont dans la catégorie « Dispensable » ou « Stocks de proximité »	Il manque un produit dans la liste des matériels à charger **hors** catégorie « Dispensable » ou « Stocks de proximité » Les bacs incomplets sont sortis du chariot initial et mis dans un nouveau chariot en attente d'être complété. L'outil doit permettre de désassocier les bacs avec des produits manquants du chariot, et associer un nouveau chariot IBODE d'ordonnancement ne libère pas un POP mais un chariot (coche tous les POP concernés)
4 (X pop/1 patient/X chariots)		L'IBODE libère manuellement chacun des POP. Puis libère les POP « allégés » au fur et à mesure.

L'outil informe l'IBODE d'ordonnancement quand un produit/matériel manquant est de nouveau disponible (Matériel revenu en stock récemment).

L'IBODE d'ordonnancement analyse et valide la préparation du POP et indique via l'outil si (le ou) les chariots sont prêts à être envoyés.

Comme pour la préparation, l'IBODE d'ordonnancement doit pouvoir analyser et lister les produits quel que soit les cas.

A cette étape, l'ensemble des produits contenus dans les chariots sont à l'état « réservé »

La libération du POP se fera manuellement par validation de l'IBODE :

- Validation auprès de l'équipe du bloc que le POP peut partir avec un produit manquant
- Validation auprès de l'équipe du bloc qu'un produit peut être substituée par un autre ; l'outil doit permettre de réaliser la substitution informatiquement sur le POP concerné
- Validation après arrivée en stock des produits manquants
  Un produit manquant considéré indispensable va pouvoir être disponible à temps pour l'intervention (dans ce cas, le chariot est mis en attente dans une zone spécifique de l'arsenal).

F-Expédition POP

La fiche imprimée doit pouvoir identifier les POP libérés et placés en zone d'expédition.

Le chariot est scanné par un professionnel de l'arsenal au moment du départ de l'arsenal, afin de valider informatiquement l'expédition. En chariot multi-POP, l'expédition est validée pour l'ensemble des POP. Pour plusieurs chariots d'un POP, le système indique au professionnel que d'autres chariots sont associés et demande à doucher les autres chariots concernés. Enfin, pour plusieurs POP associés à une intervention, le terminal mobile propose le scan des autres POP associés.

L'outil doit identifier l'adresse de destination (zone de dépose par spécialité).

G-Réception du POP au bloc

Le professionnel récupère le chariot dans la zone de dépose des POP par spécialité.

Après déplacement du chariot, celui-ci est scanné au moment de l'arrivée au bloc, afin de valider informatiquement la réception. Le professionnel scanne également l'emplacement de dépose afin d'opérer un contrôle du bon adressage du chariot. De la même manière que l'expédition, la tablette doit proposer de doucher les autres chariots concernés par le POP ou par plusieurs POP associés à une intervention.

H-Complétion et vérification finale du POP au bloc

L'IBODE de salle :

- Peut ajouter au POP :
  - les produits à compléter mentionnés sur la liste des produits DMS à prélever en stock de proximité sur la feuille précédemment générée par l'outil,
  - et les autres produits DMS,DMI ajoutés par le chirurgien à la planification à prélever des armoires spécifiques DMI et aussi en stock de proximité.
- vérifie la conformité du contenu du POP.

Les armoires communes ou spécifiques (hors DMI) seront alimentées en partie ou totalement par des produits de l'arsenal gérés dans l'outil, sans gestion de stock à leur niveau. Les produits dans ces armoires ne sont plus en stock et sont considérés comme consommés. Un circuit de demande de chargement de ces armoires avec une liste de produits à fournir doit être proposé (picking, livraison…)

I-Mise en attente des POP suite décalage d'intervention

Pour une intervention prévue le jour J et finalement décalée à J+1, le POP devra être retourné à l'arsenal , dans une zone dédiée.

Après la reprogrammation de l'intervention, la fiche d'intervention pourra être réimprimée avec les nouvelles données (numéro de salle, heure d'intervention, etc).

Le souhait est qu'un POP ne soit pas conservé plus de 24h dans cette zone d'attente de l'arsenal mais remis en stock au-delà de 24h.

J-Circuits des Retours du POP

Pour information, deux types de contenants de retour :

- les chariots de POP ayant servi à la préparation et étant restés (dans ou) aux abords des blocs, qui servent de contenant pour les retours DMS/DMR non utilisés vers l'arsenal
- les contenants pour les retours DMR utilisés vers la zone de la pré-désinfection (aux abords des salles). Ceux-ci sont envoyés à la stérilisation après lavage.

J-1- Vers Arsenal Central :

Avant que les sessions de retours soient réalisées, le produit (DMS/DMR) est à l'état « réservé ». Le produit n'est pas décrémenté en stock mais est mis dans un « sous-stock réservé non disponible POP », ce qui signifie que le stock disponible Arsenal est réduit de la quantité des produits sur les POP. Le logiciel Arsenal doit pouvoir gérer les retours à l'arsenal central ; et lors de la validation d'une session de retour, il doit d'effectuer **une régularisation des stocks** :

- les matériels scannés passent du sous-stock « réservé » au stock disponible arsenal (remise en stock)
- les matériels non scannés sont décrémentés du sous-stock avec flux de régularisation dans PHARMA [**INTF-06**-CONSO ARSENAL>PHARMA]

Une session de retour est initiée par le scann la fiche d'un POP (ou multi-POP) sur le terminal mobile, ou en absence de celle-ci, le chariot, ou saisie manuelle d'information du patient, ou de l'intervention ou autre.

La liste des produits des POP doit s'afficher sur le terminal. L'opérateur doit pouvoir sélectionner les produits en retour, valider se liste de retour et débuter sa session de retour. Le terminal doit proposer un circuit de retour optimisé en affichant les produits dans un ordre de rangement.

Le terminal affichera les produits sur la tablette avec l'indication de l'emplacement :

- Pour les DMS, l'opérateur se déplacera à l'emplacement indiqué par la tablette, scannera l'emplacement en indiquant le nombre de produit remis en stock et le produit (sélectionné automatiquement par l'information d'emplacement) est indiqué comme retourné sur la tablette.
- Pour les DMR, l'opérateur peut doucher le code barre du DMR et l'emplacement pour faire le retour.

Les chariots POP de retour arrivent à l'arsenal du 1er étage pour le déchargement DMS, et sont ensuite remontés à l'arsenal du 2ème étage pour le déchargement des DMR. Le logiciel sur le terminal mobile doit permettre de valider la fin du retour pour le POP concerné et permettre de désassocier le chariot du POP.

Si le chariot revient vide, il est scanné (fiche POP ou chariot) pour signifier la fin du cycle d'utilisation des produits préparés pour l'intervention.

Pour un chariot multi-POP, au scan du chariot, tous les POP concernés entrent dans la cession de retour.

Pour un POP avec plusieurs chariots, la fiche POP (ou 1 des chariots, ou autre) est scanné par le logisticien, qui peut ne pas être le primaire. Le système détecte le POP ainsi que les autres chariots concernés sans avoir à rescanner les autres. Lors de la validation de retour, le système doit désassocier tous les chariots du POP concerné.

Lors d'un POP associé à d'autres POP pour une même intervention, une des fiches POP (ou un des chariots ou autre) est scanné par le logisticien. Le système détecte les autres POP concernés avec leurs chariots et propose une seule session de retour pour les x chariots en même temps (cas où tous les DMS/DMR retournés ne sont pas mis sur le bon chariot pour le bon POP).

L'opérateur peut décider de faire un retour de plusieurs POP en même temps (non reliés sur un chariot ou pour l'intervention). Il doit pouvoir charger le périmètre qu'il prend en charge sur la tablette par scann des POP souhaités. Ensuite, le terminal mobile lui propose une liste de rangement à réaliser dans un ordre permettant le chemin de rangement le plus optimisé possible. A chaque matériel, le terminal mobile indique au préparateur l'emplacement de rangement.

Il doit être possible de mentionner un commentaire lié au retour d'un matériel (ex : produit abimé). L'objectif est de pouvoir extraire ces données dans le cadre de l'analyse du référentiel des fiches de préparation pour aider à leur mise à jour.

J-2- Vers stock de proximité ou armoire de spécialité

Les produits non utilisés issus des armoires communes, du stock de proximité ou de l'armoire de spécialité y sont remis par les IBODE sans aucune saisie sur le terminal. Ces produits ne sont plus gérés en stock car déjà consommés. C'est l'IDE de bloc qui récupère ces produits, sans aller à l'arsenal.

6.3.4 Réassort des stocks de proximité (armoires, étagères aux blocs) et POU

<u>Demande de service - Stocks de proximité (DMS) :</u>

Fonctionnement de la demande de service pour les stocks de proximité :

Les armoires/étagères et les emplacements dans les armoires/étagère sont identifiées par des étiquettes avec une référence de localisation et un code-barre. Un stock mini et un stock maxi sont déterminés dans le logiciel pour chaque emplacement et chaque produit. L'IDE de bloc constate visuellement que le stock mini est atteint. Avec un fonctionnement sur seuil, avec le terminal mobile, elle scanne le QR code de l'armoire (exemple : N°3 de la salle 3), puis l'étiquette d'emplacement produit. L'IDE indique le nombre de produit en présence et l'outil qui connaît la dotation détermine le nombre de produit à réapprovisionner (par soustraction).

L'outil devra laisser la possibilité pour l'IDE de changer la quantité proposée par le système, si besoin.

La liste de course s'établit au fur et à mesure des scanns et saisies de l'IDE. A la validation, la demande de réapprovisionnement est envoyée à l'arsenal sous forme d'une demande de service.

Picking à l'arsenal :

Le logisticien reçoit la demande sur le terminal, et réalise le picking avec scann des codes barre d'emplacement (et non pas les codes produits).

Après le scann de l'emplacement, l'outil doit afficher la référence à prélever. L'outil doit indiquer le conditionnement à prendre et doit alerter l'opérateur si un produit doit être prélevé dans un conditionnement.

L'opérateur confirme qu'il a prélevé la quantité sur le terminal mobile. A la validation, la quantité prélevée n'est plus en stock à l'arsenal, et donc n'entre plus non plus dans le calcul de la disponibilité pour les POP prévus de la liste d'ordonnancement.

Une liste de livraison est éditée et posée sur le chariot de livraison.

Rangement des livraisons de l'arsenal dans les armoires de proximité:

Le rangement doit se faire avec la liste de livraison contenant le détail des produits à ranger.

- Armoire commune de salle (Produit Arsenal et Logistique Hôtelière)

  Recomposition journalière à chaque fin de journée par le personnel de l'arsenal avec l'outil de gestion logistique du bloc (et l'outil WMS pour la logistique hôtelière, hors périmètre)

- Armoire spécifique de salle (par spécialité) : produits connus que de la pharmacie et ceux de l'arsenal

  Réapprovisionnement (par l'IBODE référente de spécialité) par demande de service à la PUI via le logiciel Pharma, et pour certains produits également à l'arsenal central (via l'outil de gestion logistique, même process que pour l'armoire commune de salle).

- POU : DMS/DMR

Le POU, disponible en proximité des salles de bloc, est préparé comme un POP sans être relié à un patient et à une intervention. Sa préparation et son réapprovisionnement se font sur le même processus des POP.

En cas d'utilisation du POU pour un patient, le POU doit être rattaché au patient. Le POU est transformé en POP

S'il s'agit d'un réapprovisionnement de maintien, le POP ayant été libéré sans patient, ni intervention, les produits sont toujours à l'état « réservé », car non retournés. L'outil doit permettre de rebasculer le POU en mode préparation afin de substituer des DMS/DMR et compléter les éléments manquants.

6.3.5 Réassort de l'Arsenal central

6.3.5.1 DMR - A partir de la stérilisation

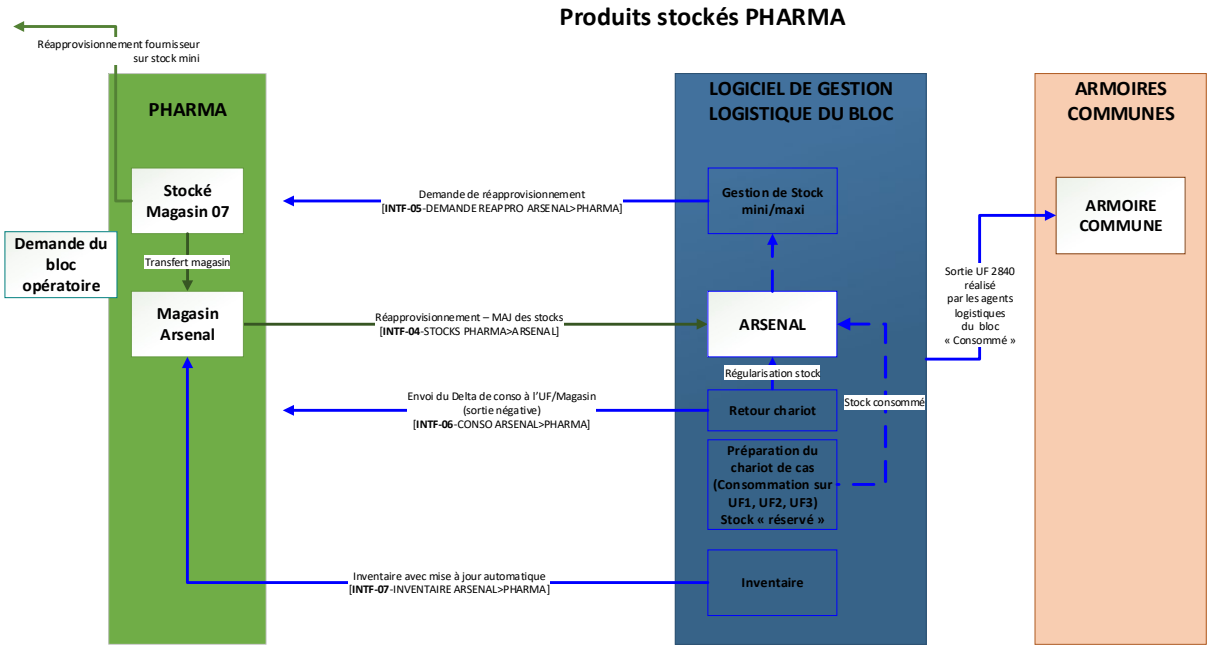
A l'issue du retraitement en stérilisation, les DMR entrant dans la composition de POP peuvent prendre 2 orientations. L'orientation doit être automatiquement proposé par le terminal mobile de l'opérateur :

- 1- DMR non attendu dans un POP : Réception par l'Arsenal pour intégration en stock avec rangement : Le Logiciel SEDISTE envoie un message au logiciel Arsenal avec les DMR sortant de la stérilisation via le flux [**INTF-08**-PDT CYCLE STE SEDISTE>ARSENAL]**.** Les DMR arrivent en « attente de réception » dans l'outil. Le préparateur réalise la réception sur le terminal mobile et range les DMR en scannant l'emplacement, ce qui incrémente le stock pour le produit (exemple : LAPAROTOMIE) et ajoute les DMR dans la liste des références unique de DMR (exemple : LAPARO1TB3/LAPAROTOMIE 1)
- 2- DMR attendu dans un POP : Réception sans rangement à l'arsenal et envoie directement sur le POP (en zone de préparation ou au bloc) : A l'arsenal, si le DMR est attendu sur un POP, le terminal indique immédiatement vers quel POP (ou/et salle) il doit être envoyé sans tarder. L'opérateur réalise la réception et valide sur le terminal qu'il est positionné sur le POP directement (statut « Réservé »).

6.3.5.2 DMS - A partir de la PUI

Produits en stock Arsenal (en stock Pharmacie) :

Le logiciel de gestion de l'arsenal est le maître dans la définition des règles de stock mini/maxi. En conséquence, il envoie la demande de réappro à PHARMA.



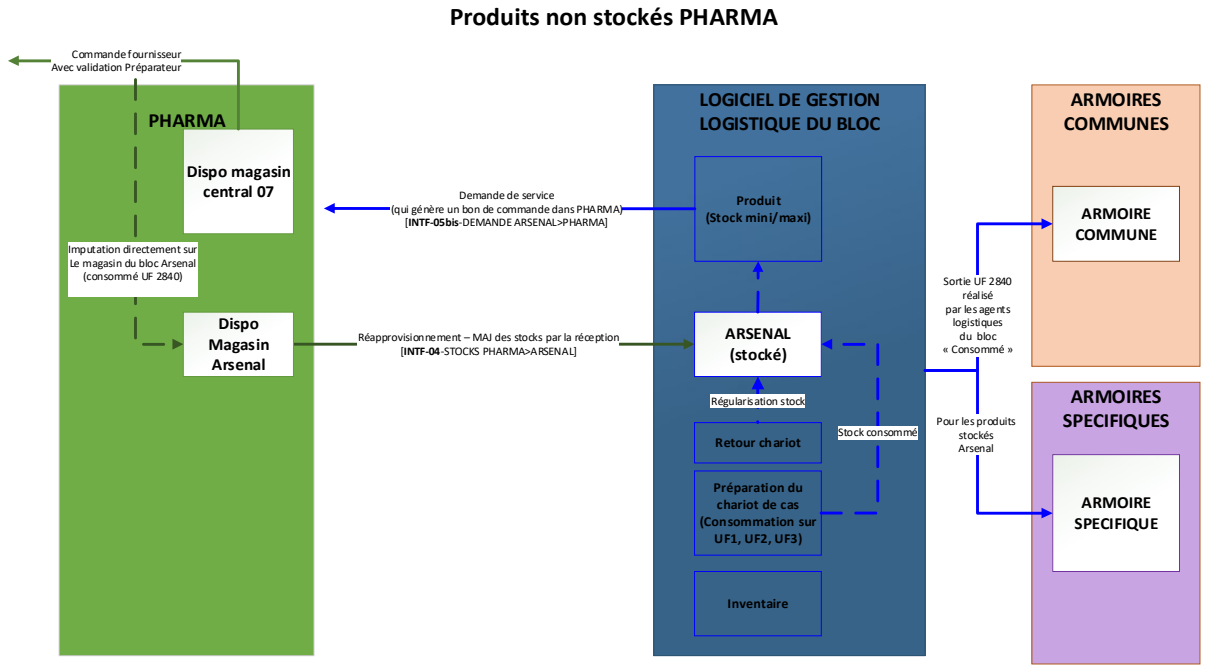
Le scan des produits au retour du bloc permet de faire une régularisation du stock disponible du logiciel Arsenal. Le stock des produits en retour passe de l'état réservé à l'état disponible et le stock de ceux non retournés est décrémenté. L'information est remontée à PHARMA par le flux [**INTF-06**-CONSO ARSENAL>PHARMA].

Le logiciel arsenal vérifie régulièrement ou en temps réel l'état des stocks disponibles et émet un ordre de réapprovisionnement au logiciel de la PUI [**INTF-05**-DEMANDE REAPPRO ARSENAL>PHARMA]. PHARMA réalise le réapprovisionnement par transfert de magasin ou passe commande auprès du fournisseur. Lorsque les produits sont préparés par la Pharmacie et envoyés à l'arsenal, PHARMA envoie les informations [**INTF-04**-STOCKS PHARMA>ARSENAL] de livraison de produits au logiciel Arsenal.

L'opérateur acquitte la livraison sur le terminal. Ensuite, l'opérateur procède au rangement avec la liste des produits implémentés sur l'écran. Il sélectionne le 1er produit sur la liste, l'outil donne l'indication de l'emplacement de rangement. Ensuite l'opérateur range le produit par scann de l'emplacement et valide sur la tablette chaque produit et sa quantité. Avec ces actions, le stock de l'arsenal est incrémenté en conséquence à l'issue du rangement ou au fur et à mesure. Si un produit est en sur stock du fait d'un nombre de retours importants, le système peut proposer un emplacement 'débord' pour stocker temporairement le produit.

Au niveau du réapprovisionnement, la pharmacie peut avoir substitué un produit par un autre ou changé les quantités (à la hausse ou à la baisse). Le terminal doit pouvoir afficher le nouveau produit, les produits demandés mais avec des nouvelles quantités, avec leur commentaire. Lorsqu'un produit connu de l'arsenal (par le catalogue PHARMA), mais n'ayant pas d'emplacement prévu, l'opérateur doit pouvoir sélectionner l'emplacement du produit substitué ou bien choisir un emplacement manuellement.

Produits en stock Arsenal (en hors-stock Pharmacie) :



Le scan des produits au retour du bloc permet de faire une régularisation du stock disponible du logiciel Arsenal.

Le stock des produits en retour passe de l'état « réservé » à l'état «Stocké » et le stock de ceux non retournés est décrémenté.

Le logiciel arsenal vérifie régulièrement ou en temps réel l'état des stocks disponibles et émet un ordre de réapprovisionnement au logiciel de la PUI [**INTF-05bis**-DEMANDE REAPPRO ARSENAL>PHARMA]. PHARMA réalise le réapprovisionnement par commande auprès du fournisseur.

Lorsque les produits sont préparés par la Pharmacie et envoyés à l'arsenal, PHARMA envoie les informations **[INTF-04**-STOCKS PHARMA>ARSENAL] de livraison de produits au logiciel Arsenal. L'opérateur acquitte la livraison sur le terminal. Ensuite, l'opérateur procède au rangement avec la liste des produits implémentés sur l'écran. Il sélectionne le 1er produit sur la liste, l'outil donne l'indication de l'emplacement de rangement. Ensuite l'opérateur range le produit par scann de l'emplacement et valide sur la tablette chaque produit et sa quantité. Avec ces actions, le stock de l'arsenal est incrémenté en conséquence à l'issue du rangement ou au fur et à mesure. Si un produit est en sur stock du fait d'un nombre de retours importants, le système peut proposer un emplacement 'débord' pour stocker temporairement le produit.

6.3.6 Gestion des dépôts temporaires (prêts)

L'information de demander un prêt de matériel est indiquée sur la demande d'intervention DPP et transmise à l'outil Arsenal [**INTF-01**-DPP>ARSENAL]. Un commentaire saisi dans DPP décrit le besoin exprimé par le chirurgien.

La demande auprès du fournisseur et son suivi est gérée via la plateforme Ascaly selon la procédure en vigueur.

Les DMR en prêts auront un emplacement générique unique au sein de l'arsenal sans informatisation de Référence, ni de stock.

6.3.7 Optimisation du système

Par l'analyse des consommations, l'outil Arsenal doit proposer des préconisations et ainsi permettre d'optimiser :

-le rangement des produits dans l'arsenal afin de favoriser le chemin de préparation le plus court

-le niveau de stock pour chaque produit (stock mini, stock opti)

-le contenu des POP (après analyse des retours) (produits manquants trop fréquent / Produits retournés trop souvent)

- Retours sur les produits en visant les POP concernés

- Retour sur les POP pour cibler les produits problématiques

NB : Les données des DMS retournés alimentent les préconisations faites par le système pour optimiser les POP. Le candidat précisera les modalités (ex :analyse des retours des produits qui reviennent trop fréquemment…).

6.3.8 Inventaires

Il sera procédé à des inventaires complets ou partiels, périodiques ou à la demande, par produit, par emplacement, par ensemble d'emplacements (zone, allée, niveau…), par produit dont la quantité en stock est inférieure à une donnée d'entrée (exemple : inventorier tous les articles avec un stock =1), par produit en fonction de son taux de rotation…

La fonction inventaire devra être accessible depuis un terminal mobile.

Après saisie des quantités inventoriées par emplacement, le stock physique sera comparé au stock informatique du logiciel de gestion logistique du bloc. Les emplacements pour lesquels le logiciel signalera un écart entre le physique et l'informatique devront être ré inventoriés. Si l'écart persiste, le responsable de l'inventaire devra effectuer un 3ème comptage et statuer sur la quantité à retenir. Une fois les écarts corrigés, le logiciel transmettra à PHARMA un état du stock des produits inventoriés ce qui permettra de mettre à niveau les deux progiciels [**INTF-07**- INVENTAIRES ARSENAL<>PHARMA].

Le système devra être en mesure de fournir un état des emplacements inventoriés depuis une date choisie ainsi qu'un état des emplacements restants à inventorier.

Il devra également permettre de réaliser des statistiques par zone inventoriée et par produit inventorié.

6.3.9 Indicateurs de pilotage

- Gestion quotidienne, taux de réalisation de l'activité de préparation programmée
- Taux de couverture du stock, avec la prise en compte de l'activité à J+1, J+3..
- Paramétrage d'indicateurs personnalisables
- Reporting

7. Expression des besoins Techniques

7.1Architecture technique du CHRU Tours

Préambule pour le Candidat : en cas d'incompatibilité de la solution proposée avec les attentes du CHRU de Tours, les écarts seront clairement indiqués et une solution alternative sera soumise à l'approbation du CHRU de Tours. Dans tous les cas, le candidat devra décrire la solution technique permettant de valider ou non l'adéquation aux prérequis décrits ci-dessous.

7.1.1 Topologie

Aujourd'hui le CHRU met en place une politique de consolidation de son architecture afin d'éviter toute disparité dans les types de matériels, systèmes d'exploitation et système de gestion des bases de données.
Le CHRU dispose historiquement de deux salles serveur sur le site de Bretonneau. Depuis 2021, un datacenter a été créé sur le site de Trousseau distant de 10 Km. Les nouveaux équipements en haute disponibilités sont ainsi répartis entre ces deux sites.

7.1.2 Systèmes

Pour la production, l'architecture système est composée de 2 châssis C7000 dotés de la Technologie Virtual Connect, eux-mêmes constitués de serveurs type lame BL460c Gen9 Bi-pro. Ces châssis sont répartis entre les 2 salles machines (B01 et B54) du campus de Bretonneau distantes de 700m longueur fibre.
Pour la préproduction l'architecture est également composée de 2 autres châssis C7000 répartis entre les 2 mêmes salles de production, et équipés de lames BL460c.

La nouvelle architecture est composée de :

- Dell PowerEdge R6515 pour les bases Oracle consolidées
- Dell PowerEdge R7515 pour les machines virtuelles

Cette nouvelle infrastructure sera répartie entre les salles de Bretonneau (B01) et Trousseau (T24)

7.1.3 Stockage

Pour la production ainsi que la préproduction, le stockage est composé de deux baies EMC Unity XT680 dans chacune des salles de production de Bretonneau, en backup l'une de l'autre. La virtualisation du stockage est assurée par des clusters VPLEX, assurant la haute disponibilité. Des clusters de VM délivrent les services NFS et CIFS et assurent la HA au niveau files. Un 3ème site équipé d'une VNX 5100 permet d'héberger les VM d'arbitrage de l'ensemble des dispositifs en haute disponibilité.

7.1.4 Systèmes d'exploitation

Le CHRU gère trois types de système d'exploitation :

- Windows : la logique est d'implémenter sur la version de Windows Server la plus à jour, en version 64bit. L'implémentation des versions de Windows non supportées par Microsoft à la date de parution de l'offre, c.-à-d. en dessous de Windows Server 2022 est strictement interdite.

- Linux : Le CHRU installe actuellement la distribution RedHat Enterprise 64 bits 8.x ou 9.x. Le CHRU n'implémente pas les distributions tierces comme Suse, Debian, Centos, Fedora et autres.
- Oracle Linux : Cette distribution est installée en 64 bits pour la gestion de bases Oracle

7.1.5 Virtualisation

Hormis pour les produits Oracle, la politique du CHRU de Tours est d'installer les systèmes sur des Machines Virtuelles VMware.
Les systèmes installés sur ces serveurs sont des hyperviseurs Vsphere ESXi Enterprise version 6.5.
Pour la production, la répartition actuelle de l'architecture est constituée de serveurs HP BL460c Gen9 sous Vshpere ESXi Enterprise dans chacune des 2 salles machines (B01 et B54). La haute disponibilité est donc assurée simultanément en local et à distance en cas de désastre d'une salle. Les datastores de production sont des luns en réplication synchrone entre les 2 salles. Tous les datastores sont des distributed devices VPLEX en Cross Connect.
2 Clusters de 2 nœuds sont également mis en place sur des sites distants :

- 2 DL360p Gen8 à la Blanchisserie
- 2 DL380p Gen8 sur Trousseau

Pour la préproduction, la répartition actuelle de l'architecture est également constituée de lames HP BL460c sous Vshpere ESXi Enterprise.

7.1.6 Architecture Citrix

Le CHRU est pourvu d'une ferme Citrix installée sur l'architecture de virtualisation Vmware décrite ci-dessus. Cette ferme est en version 7.15 et publie principalement les applications Evoluance (éditeur MainCare) pour la gestion administrative du patient, la gestion économique et financière de l'établissement, la gestion des ressources humaines et d'autres applications.

7.1.7 Bases de données

7.1.7.1 Architecture des applications

Le CHRU a pour politique la mise en œuvre d'architecture 3 tiers (séparation des données de base par rapport aux progiciels applicatifs). La partie applicative est de préférence hébergée par des machines virtuelles. La partie donnée, dans le cas de bases de données ORACLE est hébergée sur des clusters dédiés ne contenant aucun programme éditeurs.

7.1.7.2 Architecture bases de données ORACLE

Le CHRU privilégie les bases de données ORACLE. A ce jour, dans le cadre de sa politique de sécurité, l'architecture mise en place par le CHRU est la suivante :

- 19C patch 28 (à la date de rédaction du présent CCTP).
- Mise en œuvre architecture RAC
- Stockage de type ASM (réplication assurée par VPLEX)
- Insertion et monitoring des bases dans l'outil Cloud Control 13c du CHRU
- La production est assurée par quatre clusters ORACLE RAC en stockage ASM
- Supervision avec l'outil Cloud Control V13

Le Titulaire devra spécifier le type et la version de sa base de données. Il devra aussi préciser les volumétries initiales des bases, ainsi que les taux prévisionnels d'accroissement ou les formules permettant de le calculer. Les stratégies rman et datapump des bases sont à préciser avec les rétentions sur disque (ainsi que la volumétrie générée). Les mécanismes de sécurisations supportés et privilégiés devront être explicitement décrits (Dataguard, RAC, …).

7.1.7.3 Architecture bases de données SQL Server

Le CHRU exploite également une architecture consolidée pour les bases de données SQL Server permettant une haute disponibilité pour les bases hébergées sur ces instances.

Cette architecture consolidée est composée d'un cluster composé de 2 nœuds à la date de rédaction du présent CCTP). Il héberge le moteur SQL Serveur 2017 permettant d'assurer la compatibilité des instances de 2008 à 2017.

L'ensemble des procédures d'exploitation sont prises en charge par les procédures standards mises en place au CHRU (sauvegardes, rebuild des index, …).

Toute base SQL Server devra s'intégrer à cette architecture. Le Titulaire devra spécifier le type et la version de sa base de données. Il devra aussi préciser les volumétries initiales des bases, ainsi que les taux prévisionnels d'accroissement ou les formules permettant de le calculer. L'ensemble de ces informations sera recueilli par un formulaire fourni par le CHRU de Tours et rempli par le Titulaire.

Dans l'hypothèse où un éditeur ne souhaiterait pas intégrer sa ou ses bases SQL Server sur l'une des architectures consolidées, le CHRU de Tours ne traitera pas celles-ci comme bases de données SQL Server mais comme une application. En conséquence, les tâches de sauvegarde et d'exploitation des bases seront à la charge et sous la responsabilité de l'éditeur. Il devra, de plus, faire la preuve de leurs mises en œuvre avant passage en production.
Les fichiers résultant des dumps réalisés par les procédures de l'éditeur seront récupérés lors de la sauvegarde quotidienne du serveur via l'outil AVAMAR

7.1.7.4 Autres SGBD

Dans le cas où le type de base de données n'est pas Oracle ou SQL Server ou que la base de données n'intègre pas nos pré requis technique dont la consolidation, la supervision, l'administration, la maintenance corrective et évolutive (changement de version) devront être assurés par le Titulaire par le biais de la solution de télémaintenance proposée par le CHRU.

Le CHRU de Tours ne traitera pas ces bases en tant que bases de données SQL mais comme une application. En conséquence, les tâches de sauvegarde et d'exploitation des bases seront à la charge et sous la responsabilité de l'éditeur. Il devra, de plus, faire la preuve de leurs mises en œuvre avant passage en production.

7.1.8 Réseau

7.1.8.1 Réseaux de datacenter

La connexion des serveurs se fait au travers d'une infrastructure de type fabric ACI de Cisco répartie entre les sites de Bretonneau et Trousseau (liaison niveau 2). Les flux entrants et sortants des réseaux de datacenter sont filtrés par des firewalls Palo Alto placés en coupure via deux liens 10 Gb/s.

7.1.8.2 Equipements Wifi

Le CHRU dispose d'un réseau Wifi répondant aux normes 802.11n (2,4 / 5 / 6 Ghz) composé de bornes C2702I-E, C2802I-E C9164-I-E gérées par deux contrôleurs Cisco répartis entre Trousseau et Bretonneau.

Actuellement seuls les bâtiments accueillant du soin et des services tertiaires sous couverts.
L'accroissement de la couverture est en cours pour atteindre une couverture totale en 2029 (tous bâtiments et tous étages).

Dans le cas où le projet à mettre en place nécessite des accès sans fil, le candidat devra utiliser le réseau mis en place par le CHRU.
En tout état de cause le candidat devra se conformer aux recommandations de l'ASIP décrites dans le « Guide pratique spécifique pour la mise en place d'un accès Wifi » (Annexe 1).

7.1.8.3 Authentification (NAC)

Le CHRU dispose d'un mécanisme d'authentification (NAC : Network Access Control) des équipements connectés au réseau. Il permet de n'autoriser la communication que si l'équipement est reconnu selon différents critères (appartenance au domaine, présence d'un certificat, adresse mac autorisée…).
L'équipement devra dans la mesure du possible implémenter le protocole 802.1x pour valider cette authentification.

7.1.8.4 Accès Internet

L'accès Internet principal du CHRU est constitué de deux liens opérateur redondants à 1 Gb/s, l'un arrivant sur le site de Bretonneau et l'autre sur le site de Trousseau.
En outre des accès Internet de type FTTH sont déployés pour des besoins spécifiques et lorsque l'accès Internet doit être dissocié de la sortie principale.

7.1.8.5 Sécurité des flux externes

La protection des accès vis-à-vis d'Internet est obtenue par une plateforme Checkpoint HA offrant les principales briques nécessaires à sa sécurité IPS, filtrage URL, contrôle des accès, IPSec-VPN, antivirus WEB. Les fonctions antivirales de messageries sont effectuées par la solution HA IMSVA de TREND.
Les flux SSL sont soumis à un décryptage et une analyse antivirale en dehors des exceptions légales.

7.1.8.6 Sécurité des flux internes

Les flux internes suivants sont filtrés par des firewalls Palo Alto :

- Flux entrants du datacenter
- Flux sortants du datacenter
- Flux entre la VRF biomed et la VRF bureautique
- Flux entre catégories de réseaux de serveurs

7.1.8.7 Postes de travail

7.1.8.7.1 Les micro-ordinateurs

Le parc est constitué de micro-ordinateurs âgés de 0 à 6 ans. Les configurations matérielles les plus basses sont des matériels équipés de micro-processeurs Celeron avec 1 Go de RAM et 300 Go d'espace disque. Chaque poste est issu d'un disque maitre en Windows 11 64 bits (depuis la version 2502 jusqu'à dernière version).
Tous les postes et les imprimantes sont en DHCP.
Certains logiciels sont installés de base :

Sur le système d'exploitation Windows 11 2502 :

- Pack Office 2019 ou 2024 (32Bits)
- Accrobat reader version 2025.001.21228 (et ultérieure) en 64Bits
- Edge Chromium version 143.0.3650.80 (et ultérieure) en 64Bits
- Client Citrix 2203
- FrameWork 4.8

Dans la mesure où cela est possible le candidat s'appuiera sur la configuration des postes de travail présentée ci-dessus et privilégiera la version 11 de Microsoft Windows.

7.1.8.7.2 Les postes légers mobiles

Le CHRU a équipé ses services de soins de clients légers mobiles. Ces matériels sont connectés actuellement en Wifi sur l'application dossier patient par l'intermédiaire d'un client Citrix.
Le candidat pourra éventuellement rendre son application accessible sur ces matériels au travers d'une page Web ou du client Citrix après une étude de faisabilité (compatibilité, volumétrie des échanges, authentification, etc …) Toute installation d'un réseau Wifi distinct, dédié, sera soumise à l'approbation de la DSISN du CHRU de Tours, le CHRU se réservant le droit d'imposer les bandes de fréquences autorisées.

7.1.8.7.3 Les imprimantes

Les imprimantes sont essentiellement des imprimantes laser noir et blancs installés en réseau. Des serveurs d'impressions sont en cours de déploiement mais pas de généralisation pour le moment.

7.1.8.7.4 La télédistribution

La télédistribution sur les postes Windows se fait via la plate-forme SCCM. Cette plateforme permet la distribution de « packages » réalisés par l'outil ADMINSTUDIO.

Aucune installation manuelle d'application hors package SCCM n'est prévue

En conséquence, le titulaire s'engage donc fournir :

- Les sources nécessaires à l'application (de préférence MSI)
- La documentation d'installation associée
- La liste des prérequis nécessaires à son utilisation
- Si besoin, les sources et documentation des prérequis
- Une assistance sur place ou à distance permettant la réalisation du package applicatif
- Une procédure ou une assistance permettant la validation du package réalisé

De plus, lors de l'évolution du produit (changement de version ou autres), le titulaire s'engage à en informer le Département Technique et de fournir tous les éléments décrits ci-dessus permettant la prise en charge de cette évolution

7.1.8.7.5 Client java

Le client java de l'éditeur Oracle ayant une nouvelle politique tarifaire dans l'usage de ce logiciel, il est acté qu'au sein de l'établissement de Tours, le candidat **ne devra pas installer et utiliser ce logiciel (java Oracle)**.

Le CHRU de Tours préconise l'utilisation du client java de l'éditeur Adoptium dans les versions LTS 25 ,21, 17, 11 ou 8 (Home | Adoptium : https://adoptium.net/fr).

Voici un lien qui recense les différentes versions disponibles de cet éditeur : Latest Releases | Adoptium (https://adoptium.net/fr/temurin/releases?version=8&os=any&arch=any).

7.2Exploitation et maintenance technique

7.2.1 Télémaintenance

Le titulaire s'engage à n'utiliser que les outils de télémaintenance (portail Wallix) mis à disposition par les équipes de la DSISN, respectant ainsi la politique de sécurité mise en œuvre par l'institution (sécurité antivirale, cryptage, confidentialité, traçabilité). Ces outils donnent l'accès aux ressources internes de type Microsoft ou Posix.

Les transferts de fichiers peuvent être assurés via un serveur FTP sécurisé (FTPs) en DMZ, sous réserve de limitations en volume et en durée de stockage.

La mise en œuvre de tunnel SSL crypté, entre le siège du titulaire et les équipements dont il a charge de maintenance dans l'établissement, n'est autorisée que si le CHRU de Tours peut en assurer le déchiffrement (analyse comportementale et antivirale).

En tout état de cause le candidat devra se conformer aux recommandations de l'ASIP décrites dans le guide des « Règles pour les interventions à distance sur les systèmes d'information de santé » (Annexe 1).

7.2.2 Système.

Le CHRU adhère au marché UNIHA pour la partie maintenance de serveurs, de baies de stockage et de librairies de backup. Les nouveaux éléments acquis sont sous garantie constructeur initiale. A la sortie de celle-ci, la politique du CHRU est d'intégrer les éléments aux contrats de maintenance UNIHA (marchés détenus aujourd'hui par BULL) plutôt que de renouveler la maintenance constructeur. Différents types de SLA sont envisageables selon la criticité des serveurs et le type d'architecture.

7.2.3 Réseau

Le CHRU adhère au marché UNIHA pour la partie maintenance des équipements constituant son réseau. Cette maintenance garantit, en cas de dysfonctionnement, un retour en fonctionnement normal de 12H heures ouvrées. Ce délai est acceptable dans la mesure où chaque équipement sensible, s'il n'est pas doublé, peut disposer de deux cartes réseau raccordées à deux équipements distincts. Sur qualification particulière d'application sensible, après accord de la DSISN, cette GTR peut être ramenée à 4H.

7.2.4 Supervision

La supervision des équipements réseau et de certains serveurs peut être assurée par une plateforme de supervision NAGIOS. Le CHRU est en cours de mise en place de l'outil SCOM qui permettra de superviser l'ensemble des serveurs sous système d'exploitation WINDOWS :

- Soit c'est l'établissement qui assure cette supervision par le biais d'outils existants et qui, pour certains, ouvre les appels chez les mainteneurs,
- Soit cette supervision est assurée par le Titulaire, par le biais de connexion authentifiée conforme à la politique de sécurité de l'établissement et validée par la DSISN entre l'établissement et le site du candidat.

La supervision des bases de données ORACLE est assurée via l'outil GRID CONTROL 12c implémenté au CHRU. D'autre part, le CHRU dispose d'une assistance extérieure (société DIGORA) pour la supervision de bases de données ORACLE à condition que celles-ci intègrent l'architecture cluster RAC 19C décrite ci-dessus.

7.3Sécurité

7.3.1 Sécurité des accès

La politique du CHRU est d'intégrer l'ensemble des serveurs et des postes de travail dans l'Active Directory. Tous les postes de travail se connectent au domaine Active Directory en respectant la politique de sécurité mise en place. Le mot de passe doit respecter des exigences de complexités. le mot de passe doit avoir une longueur d'au moins 8 caractères, contenir des caractères de 3 des 4 catégories suivantes (Caractères majuscules de l'alphabet (A à Z), Chiffres (0 à 9), Caractères minuscules de l'alphabet (a à z), Caractères non alphabétiques (!, $, #, %)). Lors du changement de mot de passe le nouveau doit être différent des 3 derniers déjà utilisés.

7.3.2 Sauvegardes

Le CHRU utilise la solution logicielle AVAMAR société EMC avec des Baies DATADOMAIN pour le stockage des sauvegardes.

Le candidat devra, prévoir une intégration avec la solution AVAMAR/DATADomain.

Le Titulaire devra préciser :

- L'emplacement des données à sauvegarder
- Les récurrences des sauvegardes
- Les durées de rétention
- Les commandes à insérer dans les scripts de prétraitement et de post-traitement…
- L'estimation de l'accroissement des volumétries

7.3.3 Antivirus

Le CHRU dispose de la suite de sécurité de l'éditeur Trend Micro. Notamment :

- La suite Apex One du même éditeur est implémentée sur les serveurs et les postes de travail.
- La solution Deep Security du même éditeur est installée sur tous les serveurs pour le virtual patching. Elle a en plus le rôle d'antivirus sur les serveurs 2003/2008 qui ne sont plus supportés par Apex One.
- Ces solutions sont gérées via une console centrale.
- Ces solutions s'appuient sur des serveurs de sandboxing et de partage des mises à jour / signatures.

Le paramétrage des serveurs, des exclusions de répertoires et des privilèges particuliers (désactivation Real Time Scan…) sont paramétrables via un formulaire spécifique.
Dans le cas où le candidat propose des dispositifs connectés dans son offre, il s'engagera à ce que ses équipements comportent des moyens de sécurité permettant de détecter et de répondre aux menaces liées au codes malveillants. La solution Trend devra être privilégiée.
Dans le cas où le candidat propose une solution différente de celle installée au CHRU, il devra s'assurer de la bonne mise à jour de sa solution et de la remontée en temps réel des alertes.

La solution Checkpoint sécurise la partie accès WEB vers Internet en inspectant les flux.

7.3.4 EDR

L'EDR Trend Micro Vision One est déployé sur tous les postes et serveurs connectés au réseau. Il permet de collecter de la télémétrie sur l'usage du poste/serveur dans un datalake hébergé en mode cloud.
Un moteur de corrélation permet de détecter des signaux faibles et de générer des alertes de sécurité ou de détecter des vulnérabilités de manière proactive.
L'agent permet de faire des actions de remédiations (isolation du poste, déconnexion de l'utilisateur, réinitialisation du mot de passe…) mais n'agit pas sur les fichiers et les processus.

7.4Préconisation d'infrastructure et éléments à fournir

Le logiciel doit être proposé dans une configuration On Premise ou en mode SaaS s'il ne permet pas le mode On Premise.

7.4.1 Synthèse des préconisations d'infrastructure informatique

En synthèse, les préconisations d'infrastructure du CHRU de TOURS, à la date de rédaction du document, sont :

Back-end

- Mise en œuvre des techniques de Haute Disponibilité
- Architecture 3 tiers (séparation couche applicative, couche base de données, clients)
- Pour la couche applicative, virtualisation sur une architecture VMWARE
    - OS serveurs applicatifs (virtualisé)
        - RHEL 8.x ou 9.x 64 bits
        - WINDOWS 2025 ou 2022
- Base de données :
    - ORACLE19C patch 28, gestion ASM, RAC, RMAN pour les sauvegardes, OS ORACLE LINUX 64 bits
    - SQL Server 2017 Always On
- Stockage : Intégration obligatoire au stockage unifié du CHRU de TOURS basé sur deux baies Unity XT680 avec couche VPLEX.
- Archivage : Pas de solution d'archivage
- Sauvegarde : Intégration au logiciel AVAMAR/DATADOMAIN EMC
- Antivirus Deep Security et EDR Vision One de Trend installés sur les serveurs

Front-end

- La compatibilité de l'application avec Windows 11 2502
- Compatibilité de l'application si nécessaire avec Edge Chromium
- Compatibilité de l'application si nécessaire avec Citrix XenApp 2203
- Antivirus Apex One et EDR Vision One de Trend installés sur les postes de travail
- Annuaire : Conformité avec serveur Active directory 2019 et niveau fonctionnel 2016
- Si la solution nécessite un déploiement de client sur les postes de travail, celui-ci devra impérativement intégrer la plateforme SCCM

Réseau

- Wifi : Dans le cas d'utilisation d'équipements mobiles, l'intégration à l'architecture Wifi implantée sur le CHRU est obligatoire
- Si l'équipement doit accéder à Internet, il doit être en mesure d'intégrer le certificat SSL du CHRU

- L'équipement ne pourra pas être connecté à la fois sur le réseau du CHRU et à la fois sur un lien communiquant avec l'extérieur (Modem 3G/4G, VPN, lien dédié…)
- Le plan d'adressage sera fourni par le CHRU
- L'équipement devra être identifiable via le NAC (Network Access Control) du CHRU via le protocole 802.1x notamment

Télémaintenance

- La plateforme sécurisée d'accès à distance pour la télémaintenance est la solution WALLIX
- Les comptes sont désactivés par défaut et ne permettent l'accès aux ressources uniquement dans le périmètre d'intervention
- Les accès sont ouverts à la demande par l'interlocuteur du CHRU et pour la durée de l'intervention

7.4.2 Eléments à fournir par le candidat

Il est mentionné ci-dessous les marchés d'acquisition contractés par le CHRU. Il est attendu du candidat d'une part qu'il complète si besoin les fournitures nécessaires à son offre et non couvertes par les marchés cités et d'autre part qu'il indique les configurations que le CHRU devra acquérir au travers de ses marchés.

7.4.2.1 Serveurs

Le CHRU fait ses acquisitions de serveurs au travers du marché UGAP ou UNIHA.
Le candidat devra donner la configuration la plus exhaustive possible de ses besoins.

7.4.2.2 Stockage

Le CHRU a l'obligation d'utiliser le marché UNIHA pour l'acquisition de stockage. Le candidat devra donner la configuration la plus exhaustive possible de ses besoins : volumétries, accroissement et performances, type de stockage, ...

7.4.2.3 Réseau

Le CHRU de Tours adhère au segment réseau du marché CAIH. Le constructeur retenu, que ce soit dans le cadre de la rénovation ou de la mise en œuvre de nouvelles structures / bâtiments est Cisco pour la partie switch.

Le candidat devra exprimer ses besoins en nombre de ports, débit par port, degré de sécurisation (agrégations de ports sur deux équipements distincts, teaming actif/passif, actif/actif), besoins en PoE, …) et approuver l'utilisation du mode de télémaintenance en vigueur au CHRU de Tours.

Une matrice des flux (IP source / IP Destination / Protocole / Port) devra être fournie aussi bien pour la communication en interne (AD, DNS…) qu'en externe.

7.4.2.4 Poste de travail

Le CHRU de Tours adhère au segment NTIC UNIHA pour l'acquisition d'ordinateurs, d'écrans, et d'imprimantes.
Le candidat fournira ses prérequis en matière de postes de travail, terminaux mobiles, douchettes ou tout autre type de périphériques etc…
Dans la mesure où les prérequis du candidat en termes de postes de travail et de périphériques correspondent à ceux proposés dans le cadre du marché, le matériel sera acquis par cet intermédiaire.

En ce qui concerne les licences Microsoft, le CHRU de Tours adhère au segment NTIC Accord Cadre Microsoft ce qui permet pour un coût annuel par poste, de bénéficier de la quasi-totalité du catalogue de produits Microsoft.

7.4.2.5 Virtualisation

Le CHRU adhère au marché UNIHA pour la partie acquisition de licences Vmware (via APX).

7.4.2.6 Oracle /SQL Server

Le CHRU adhère au marché UNIHA ORACLE et via le CAIH au marché Microsoft.
Il fournira donc les licences Oracle Entreprise et Microsoft SQL Server.
Pour les bases hors Oracle et SQL Server, le candidat devra l'intégrer obligatoirement dans sa proposition les licences.

7.4.2.7 Sécurité des dispositifs connectés

Dans le cas où l'offre comporte des dispositifs connectés, le candidat devra s'engager à respecter les règles de l'ASIP énoncées dans l'annexe 1, en particulier, il indiquera clairement les moyens mis en œuvre pour la protection de ses équipements contre les codes malveillants.

7.4.2.8 Cadre de réponse obligatoire

Dans le cas où le candidat met en œuvre et/ou utilise des ressources informatiques dans les domaines suscités il devra impérativement, fournir des réponses explicites sur les éléments exigés par la DSISN du CHRU de Tours dans le tableau de l'expression des besoins techniques paragraphe 7.3.

7.5 Sécurité et fonctionnement applicatif

7.5.1 Gestion de la connexion à l'application

La politique au sein du CHRU de Tours est d'intégrer l'ensemble des applications (On-premise et SaaS), des serveurs et des postes de travail dans l'AD (Active Directory). Ils doivent se connecter au domaine AD en respectant la politique de sécurité mise en place. Le mot de passe doit respecter des exigences de complexités.
Le mot de passe doit avoir une longueur d'au moins 8 caractères, contenir des caractères de 3 des 4 catégories suivantes (Caractères majuscules de l'alphabet (A à Z), Chiffres (0 à 9), Caractères minuscules de l'alphabet (a à z), Caractères non alphabétiques (!, $, #, %)). Lors du changement de mot de passe le nouveau doit être différent des 3 derniers déjà utilisés.

L'application doit gérer le renouvellement du mot de passe demandé par l'AD.

Le candidat précisera sous quelles conditions le système proposé pourra s'intégrer à une solution d'authentification unique (SSO).

Le système est conforme aux exigences spécifiées dans les documents suivants :

- Politique Générale de Sécurité des Systèmes d'Informations de Santé –PGSSI-S publié par l'ANS (Agence du Numérique en Santé) (Annexe 1)
- Référentiels opposables par arrêté du ministre chargé de la santé (Annexe 2)
- PGSSI-S : Politique générale de sécurité des systèmes d'information de santé : Règles pour les dispositifs connectés d'un Système d'Information de Santé (SIS) « ASIP Santé / Pôle Technique et Sécurité » (voir extrait en annexe 3).

Le candidat précisera les capacités de connexion sur les terminaux mobiles avec les badges des agents du CHRU de Tours, basés sur la bi-technologie Mifire/Desfire (ev3). Le candidat précisera tout élément utile sur ce sujet.

7.5.2 Gestion de la déconnexion

Afin de garantir l'imputabilité des actions aux utilisateurs, il est important de définir un délai de verrouillage ou déconnexion sur une temporisation d'inactivité avec masquage des données affichées. Afin de protéger les données, de garantir la sécurité du système et de s'assurer de la traçabilité des actions, le système permet :

- de définir un temps d'inactivité pour verrouillage du poste de manière centralisée pour tous les utilisateurs authentifiés,
- à un utilisateur de retrouver sa session de travail après s'être ré-authentifié en cas de changement d'utilisateur pour les postes partagés.

7.5.3 Paramétrage des utilisateurs, droits d'accès

Le système permet de paramétrer les personnels et leur profil métier.
Le système permet de paramétrer des groupes de personnels.
Le système permet d'attribuer des droits d'accès en lien avec les profils métiers pour créer le plan d'habilitation (attribution des droits d'accès et habilitations).
Le système permet d'attribuer plusieurs profils à un même utilisateur ou même groupe de personnes.
Le système permet le paramétrage de droits d'accès différenciés par écran, en lecture / insertion / mise à jour / suppression.
Le système permet l'attribution de comptes Administrateur spécifiques nominatifs.

7.5.4 Intégrité et traçabilité

Le système doit disposer d'outils permettant la non altération des données saisies.

La traçabilité des connexions et des modifications de données doit être assurée, aussi bien sur les actions métiers que sur le paramétrage :
- Qui a créé, modifié ou supprimé des informations, par quel moyen (manuel, batch..) et quand ?
- Qui a créé, modifié ou supprimé des droits, par quel moyen (manuel, batch..) et quand ?
- Quelles étaient les autorisations d'un utilisateur à un moment donné ou pendant une période donnée ?

Dans le cadre de la revue des comptes utilisateurs, le système doit permettre sur une période donnée d'extraire l'ensemble des mises à jour liées à la gestion des droits.

Les traces enregistrées dans les journaux d'audit de sécurité du système doivent comprendre au minimum :

- L'identifiant des utilisateurs,
- Les dates et heures d'ouvertures de sessions,
- La date et l'heure de l'événement,
- L'identification du terminal utilisé,
- Les références aux traitements réalisés,
- La description de l'opération ou de l'événement journalisé,
- La valeur de la donnée avant et après modification.

L'exploitation des traces de connexions doit être possible sans recours au fournisseur de la solution.
Ces traces devront être accessibles sur une année glissante à minima.
Le candidat exposera dans son mémoire technique les moyens utilisés, le contenu et les modalités d'exploitation de ces traces.
Le candidat décrira aussi les besoins en matériel complémentaire et l'espace disque nécessaire.

7.5.5 Immunité

Le candidat précisera les actions prises par le système pour se protéger lui-même des infections des programmes non autorisés ou indésirables comme par exemple les virus, les vers, les chevaux de Troie.

7.5.6 Indisponibilité

L'application doit pouvoir fonctionner 24 heures sur 24 et 7 jours sur 7 avec un taux d'indisponibilité maximal de 0.1% (= 99.9% de taux de disponibilité)

En conséquence :

- Le candidat proposera une configuration serveurs qui permettra de garantir cette exigence,
- Il décrira dans sa réponse, à titre d'information les règles à respecter en matière de réseau,
- Il s'engagera à pouvoir assurer les mises à jour de version logicielles dans les conditions précisées ci-dessus.

La durée maximale d'indisponibilité du produit lors d'une mise à jour sous réserve du respect, par l'établissement, des prérequis techniques fournis par le titulaire, sera de 2 heures maximum entre le début de l'intervention et la remise en production. Cette intervention devra être planifiée entre 3 heures et 5 heures du matin.

En cas de panne bloquante, le délai maximal d'intervention est fixé à 1 heure.

7.5.7 Mise à jour des versions

Le candidat indiquera la procédure de mise à jour du produit en mode On Premise ou en mode SaaS (Qui, comment , quand, Patch , Version Majeure).
Le candidat indiquera sa capacité à mettre en œuvre un système de mise à jour à chaud.
Le candidat indiquera s'il lui est possible, et dans quelles conditions, de réaliser la mise à jour en dehors des heures ouvrées, à la demande du client.
En mode Saas, le candidat expliquera pour des terminaux mobiles présents sur site au CHRU de Tours :

- Comment et qui assure la mise à jour du logiciel mobile sur les terminaux ?

7.5.8 Interfaces

Le candidat doit interfacer sa solution Logistique Arsenal avec la solution DPP/SEDISTE/PHARMA et l'annuaire AD.

7.5.9 Supervision

7.5.9.1 Supervision en mode On Premise

Le candidat expliquera les composants pouvant être supervisé par le CHRU pour le bon fonctionnement du logiciel.

7.5.9.2 Supervision en mode SaaS

Le candidat assumera :

- Une supervision du bon fonctionnement du logiciel, notamment par l'administration des serveurs hébergés
- Un monitoring des interfaces à son niveau
- Une surveillance de l'interconnexion entre le CHRU de Tours et la solution (VPN)

Le candidat expliquera notamment, pour ce mode, le fonctionnement des terminaux mobiles présents sur site au CHRU de Tours communiquant avec des serveurs hébergés à distance :

- Quelle est la couverture de la supervision sur ces terminaux par le candidat ?

7.5.9.3 Outil de pilotage et de supervision/correction des interfaces

Quelque soit le mode d'installation, un outil de pilotage et de supervision/correction des interfaces doit être proposé aux administrateurs du Service Informatique, afin de fiabiliser et maintenir la qualité de fonctionnement des interfaces mises en place

7.5.10 Robustesse, tolérance aux pannes et mode dégradé

Le candidat indiquera comment la solution permet de gérer correctement un arrêt programmé (ou non) jusqu'au redémarrage du système.
En cas de panne, le système doit disposer d'une procédure dégradée.

Il est attendu que l'outil extrait plusieurs fois par jour en automatique le détail des POP en cours (horaire, patient, Acte chirurgical, salle, chirurgien, liste des matériels, commentaires…), ou en prévisionnel sous forme de fichiers informatiques qui puissent être déposés sur d'autres supports (PC portables, clés USB…). De la même manière, l'outil doit pouvoir extraire automatiquement tout le référentiel des fiches avec l'ensemble des critères.

Le candidat décrira en détail les procédures de secours et de gestion en mode dégradé, à savoir :

- Les procédures de restauration des données,
- Les modalités de retour à l'état antérieur pour certains types de transactions,
- La méthodologie d'arrêt d'urgence,
- La méthodologie de reprise après incident et du retour au mode nominal,
- La méthodologie de vérification de l'intégrité de l'application,
- La méthodologie de vérification de l'intégrité des données,
- Le périmètre fonctionnel du mode dégradé,
- Les éventuelles restrictions de performance.

Le candidat précisera le mode de reprise d'une transaction interrompue suite à un incident (le système doit pouvoir repartir là où il s'est arrêté sans perte de données)

Le candidat précisera si la solution permet de fonctionner en mode hors réseau et si elle permet aux utilisateurs de continuer à travailler. Dans ce mode de fonctionnement, il précisera notamment les

fonctionnalités accessibles ou non, ainsi que les modalités de retour à la normal, avec remise à niveau des données de la base de production.

Le candidat précisera le fonctionnement de l'application mobile si perte du WIFI :

- Mode déconnecté avec déversement des mises à jour de données lors du rétablissement du WIFI,
- Ou bascule sur Poste Fixe pour réaliser les mêmes actions.

Le candidat proposera une procédure permettant de changer rapidement le routage imprimante en cas de panne imprimante ou réseau.

La base de données devra être en outre facilement accessible en lecture par un moyen de requête externe en cas de défaillance du produit.

Le candidat proposera des extractions régulières (historiques, table article, UF, fournisseur, état du stock détaillé par emplacement, …) mises à disposition sous forme de fichiers. Ces fichiers pourront être utiles en cas d'indisponibilité du logiciel de gestion logistique du bloc.

En cas de cyberattaque, le candidat précisera les modalités pouvant être mise en œuvre pour un usage de la solution avec les données du CHRU de Tours pendant la durée de la crise (Hors CHRU ou pas).

Le candidat prévoit dans son offre d'assister l'établissement pour un test de restauration des sauvegardes complètes sur le domaine de TEST. Ce test fera l'objet d'un PV signé par les 4 parties : le candidat, la DSISN et les directions fonctionnelles. Le candidat prévoit un mode opératoire et un transfert de compétences vers les établissements, pour que les équipes soient autonomes sur ce test qui doit être réalisé une fois par an (dans le cadre du Plan de Reprise d'Activités).

7.5.11 Cycle de vie des données métiers

Le candidat précisera le cycle de vie des données métiers (Archivage ? purge ? par type de donnée, selon la durée de vie de la donnée, ou gestion d'un changement d'état de la donnée …)

7.5.12 Mise en place environnement de TEST

Le candidat propose un environnement de TEST complet (imprimantes, terminaux mobile, interfaces de TEST)

Le candidat propose dans son offre une procédure de rafraichissement des données du domaine de TEST à partir des données du domaine de PRODUCTION pour permettre aux établissements de tester les nouvelles versions.

Le candidat propose un transfert de compétences vers les établissements, afin que les équipes soient autonomes.

7.5.13 Paramétrage de l'application

Le candidat proposera une formation au paramétrage de l'application permettant à l'établissement d'être autonome (métier et informatique) pour assurer les évolutions de paramétrage une fois le projet lancé.

Le candidat mettra à disposition de l'établissement une documentation spécifique reprenant les paramétrages effectués lors du projet.

Le candidat précisera les modalités pour réaliser le transfert d'un paramétrage d'un environnement A vers un environnement B.

7.5.14 Rendement - Rapidité d'exécution et de temps de latence

Les temps de réponse attendus doivent être précisés par le candidat sur postes fixes et terminaux mobiles. On spécifiera en particulier les temps de réponse suivants :

- À la connexion,
- En utilisation à vide (un seul utilisateur connecté),
- En utilisation en charge,
- En usage des liens contextuels et interfaces.
- Les temps de réponse des procédures types.

En routine (sur base de données et en fonctionnement réel), les temps de réponse resteront dans les limites suivantes :

- Le passage d'une zone à la suivante sera inférieur à 0,2 seconde dans 98% des cas,
- Le passage d'un écran au suivant ou le changement de fonction sera inférieur à 0,5 seconde dans 98% des cas, exclusion faite des interrogations portant sur l'ensemble ou un sous-ensemble de la base de données.

Les temps de réponse du système devront être identiques sur l'ensemble des postes et terminaux installés.
Les temps de réponse devront rester stables quel que soit le moment de la journée où les utilisateurs y accéderont notamment lors des pics de consultation prévisibles.

7.5.15 Dimensionnement et performances

Le candidat indiquera le dimensionnement préconisé et la méthode de calcul pour chaque établissement.
Le candidat peut s'appuyer sur l'estimation de la volumétrie précisée auparavant par les deux secteurs ou interroger l'établissement si besoin de précisions..
Le candidat indiquera les capacités maximales de son système en nombre de postes à la base de données et le nombre d'utilisateurs simultanés.
Au regard de cette volumétrie maximale, les performances de l'application doivent être conformes à la description du point sur la rapidité d'exécution et le temps de latence.

7.5.16 Adaptabilité

La solution devra suivre les évolutions technologiques, en terme notamment :

- De systèmes d'exploitation « serveurs »,
- De versions de base de données,
- De navigateurs,
- De norme d'interopérabilité,
- D'outils bureautiques.

7.6Ergonomie

7.6.1 Homogénéité

Afin d'assurer une cohérence globale de l'interface homme/machine : la logique des commandes doit être la même :

- Les fenêtres doivent suivre le même schéma d'agencement,
- La sémantique des boutons de la souris doit être constante,
- Le même vocabulaire doit être utilisé pour désigner les commandes du logiciel.

7.6.2 Souplesse

À moins que cela ne soit imposé par la réglementation ou les bonnes pratiques en vigueur dans la profession, le système n'impose pas à l'utilisateur d'accomplir les tâches de son activité dans une séquence particulière.
À tout moment, l'utilisateur doit pouvoir suspendre sa saisie pour obtenir les informations dont il a besoin dans un autre endroit sur le logiciel.

7.6.3 Gestion des erreurs

La gestion des erreurs concerne tous les moyens permettant d'une part d'éviter ou de réduire les erreurs et, d'autre part, de les corriger lorsqu'elles surviennent.
L'utilisateur doit pouvoir annuler un traitement informatique qu'il aurait demandé ou revenir à une étape antérieure du processus.
Le système doit protéger l'utilisateur contre les erreurs en lui demandant de confirmer les actions dont les effets sont irréversibles.
Le système doit permettre à l'utilisateur de corriger ses erreurs, en lui fournissant des messages d'erreurs clairs.

7.7Conduite de Projet

7.7.1 Planning du projet

Le CHRU de Tours prévoit :

- le début de projet sur le 1er trimestre 2027
- le déploiement sur le bloc d'une 1ère spécialité pour la préparation des chariots de POP en septembre 2028, suivi du déploiement progressif de la totalité des blocs concernés par le NHT sur 2028.

Le Candidat devra proposer un planning détaillé respectant les jalons mentionnés dans le présent cahier des charges.

Jalons
Mise en place plateforme technique de la solution et transfert de compétences équipe informatique prod/test
Installations des progiciels prod/test
Présentation de la solution à l'équipe projet
Analyse fonctionnelle
Interfaces
Initialisation et Reprise de données
Mise en Ordre de Marche
Test et validation de l'ensemble
Proposition d'une bascule à blanc
Vérification d'Aptitude
Formation des utilisateurs finaux
Démarrage
Assistance au démarrage et période d'observation de 6 mois
Vérification de Service Régulier

7.7.2 Mise en place des applicatifs et des interfaces

Le Candidat prend en charge l'installation applicative (en Test et en Production) sur leur environnement (mode SaaS) ou sur le (ou les) serveur(s) des progiciels, ainsi que sur les terminaux mobiles fournis et les imprimantes. Il prend en charge, le cas échéant, l'installation sur 1 à 2 postes clients avec fourniture d'une procédure d'installation. Les installations « On-Premise » s'effectueront dans un contexte de transfert de compétences vers l'équipe informatique du CHRU Tours.

7.7.3 Initialisation des données

Certains référentiels doivent pouvoir être importés dans le logiciel du candidat par fichier informatique (*.xlsx, *.csv) :

- Le thésaurus du CHRU de Tours rassemblant tous les libellés des opérations chirurgicales (plus de 3.000 références)
- Les fiches de préparations de chariots de cas avec les informations sur les produits et les matériels utilisés
- Les praticiens chirurgiens
- Le livret pharmaceutique complet issu du logiciel PHARMA de Computer Engineering
- La liste des références de matériels (boîtes) de la stérilisation et la table de correspondance (exemple de la LAPARO p.15)
- La déclaration des emplacements de rangement
- Les utilisateurs IBODE, logisticiens…

De manière générale, le candidat s'engage à proposer une méthodologie de reprise de données pour tous les éléments à importer dans le logiciel Arsenal (fichiers d'import standardisés ou autre).

7.7.4 Méthodologie de conduite de projet

Le Candidat explique sa méthodologie de conduite de projet en tant que maîtrise d'œuvre. Il gère son équipe et ses ressources et s'engage à mettre en adéquation les ressources avec la charge de travail identifiée. Il s'engage sur les dates des étapes, gère le planning et les ressources en conséquence.

Le Candidat mettra à disposition une équipe projet composée d'un Chef de Projet, d'un ou plusieurs référents techniques et formateurs.

Le chef de projet est l'interlocuteur principal pour le CHRU de Tours. Il aura pour objectif de planifier le déploiement de la solution avec les différents interlocuteurs et de suivre le bon déroulement. Il organisera les comités de suivi et/ou pilotage.

Il jouera également un rôle auprès des éditeurs des logiciels périphériques (PHARMA, SEDISTE,…) dans le cadre des interfaces.

Le candidat décrira brièvement le profil du chef de projet pressenti pour le projet de l'établissement et de son expérience dans des projets similaires. Pour le CHRU de Tours, une expérience de projets sur des établissements de taille similaire serait appréciée.

Le Candidat indique les moyens qu'il compte mettre en œuvre afin de maintenir une équipe projet stable en effectif et en compétence. Il désignera un interlocuteur privilégié pour le client. Il indiquera les modalités de modification de l'équipe projet et le transfert systématique de compétences avec un objectif de qualité visant à minimiser l'impact sur le projet pour le client. Le Candidat informera le CHRU préalablement à toute modification de l'équipe projet.

Pour le CHRU de Tours, une équipe sera constituée avec un Chef de projet Métier, un Chef de projet DSISN et des référents si besoin.

Le candidat s'engage à fournir un plan de charge pour chaque étape du projet en spécifiant :

- Ses ressources (profils des intervenants).
- Les ressources CHRU à mettre en corrélation (profils des intervenants),
- Le temps alloué.

7.7.5 Coordination de la recette applicative

Le titulaire assure la coordination des tests de la solution intégrée (interfaces comprises) : production du cahier de recette, assistance des professionnels du CHRU de Tours pour la conduite des tests, analyse et bilan des résultats, préparation de la mise en production, suivi de la résolution des anomalies.

Dans sa réponse, le candidat devra évaluer la charge de travail des chantiers de tests pour ses propres ressources et pour les ressources du CHRU de Tours.

7.7.6 Rédaction de l'analyse d'impact relative à la protection des données (AIPD)

La rédaction d'une analyse d'impact relative à la protection des données (AIPD) par le CHRU est dorénavant un prérequis pour toute nouvelle mise en place d'une solution IT métier au CHRU de Tours.

Le candidat s'engage donc à fournir les éléments nécessaires à cette rédaction lors de la réalisation du projet et 3 mois avant la mise en production des 1ères fonctionnalités (Annexe 5). Ils peuvent être fournis dans le cadre d'un document d'architecture technique qui présente les aspects sécurités, RGPD et architecture de la solution (Dossier d'Architecture Technique).

7.7.7 Documentation

Le Candidat fournira toutes les documentations technique et fonctionnelles, en français :

- Description de l'organisation pour le support de la solution – Éditeur
- Contrat de maintenance et de support
- Dossier d'Architecture Technique (DAT) (Serveurs, matrices des flux, matrice réseau, certificats…)
- Manuel(s) d'utilisation
- Guides utilisateurs adaptés au site
- Manuels d'installation, d'administration et de paramétrage
- Un document décrivant les prérequis techniques et fonctionnels à respecter par l'établissement,
- Manuel d'exploitation spécifique pour l'établissement pour le démarrage et l'administration (ce manuel sera utilisé dans le cadre du transfert de compétences)
- Manuel de description et exploitation des interfaces (description des flux, du fonctionnement et du traitement des anomalies)
- Procédure de Gestion des Accès
- Procédures de sauvegarde et de restauration
- Plan des tests (unitaires / interopérabilité / TGN / procédures dégradées) et points d'attention
- Support de formations
- Procédures dégradées en cas de panne de la solution principale
- Eléments nécessaires à la constitution de la déclaration dans le registre des traitements (CNIL/RGPD)
- Analyse de risques RGPD (AIPD)
- Cartographie applicative (serveurs, interfaces, interconnexions…)
- Certification de l'application

La documentation sera fournie sous forme numérique, non en lecture seule (document Word).
Le CHRU de Tours se réserve le droit d'extraire certaines parties des documentations standards, uniquement afin de constituer ses propres documentations internes, en tant que manuels de procédures.
A chaque mise à jour d'une nouvelle version du système, le Candidat remet à l'établissement les documentations mises à jour si nécessaire (Prérequis, guide d'exploitation, guide utilisateur, guide de paramétrage, documentation technique, …)
La version de l'application proposée doit être intégralement en langue française même si le système est d'une origine étrangère. Aucun mot ou texte de la langue d'origine (si ce n'est pas le français) ne doit être visible par un utilisateur de la solution.

7.7.8 Formation / Transfert de compétence

La formation est dispensée dans les locaux du CHRU. Elle pourra être dispensée à distance avec l'accord de l'établissement. Lors de chaque formation, le formateur fait remplir par les participants une fiche de présence. A l'issue de la formation, chaque participant remplit une fiche d'évaluation.
Le transfert de connaissances/compétences vise l'objectif principal d'acquérir la maîtrise des différents modules du progiciel pour l'administrer au quotidien et pour gérer efficacement son utilisation. Il

s'adresse à la fois aux utilisateurs de la solution, aux administrateurs métier et informatique de la solution.

Le Candidat proposera un plan de formation ainsi qu'un support adapté au projet du CHRU.
Le candidat précisera dans sa réponse s'il bénéficie du statut d'organisme de formation agréé.

7.8Maintenance et support applicatif

7.8.1 Contrat de maintenance et de support

Le CHRU de Tours attend du Titulaire un contrat de maintenance et support, l'engagement étant de 1 an (renouvelable 3 fois). Le Titulaire remplira l'annexe 4 afin d'établir une fiche signalétique de maintenance.
Le contrat prend effet à l'issue de la période de garantie, concernant les vices de fabrication et de fonctionnement à compter de la vérification d'aptitude. D'une durée de 1 an minimum, le suivi progiciel sous garantie est effectué à titre gratuit (non facturable) par le Titulaire.

Il recouvre :

- La maintenance corrective (anomalies) a pour but de rétablir les fonctions d'un bien après la défaillance de celui-ci ou la dégradation de ses fonctions,
- La maintenance adaptative (évolution imposée par une nouvelle version de logiciels système : un changement d'environnement. Exemple, changement de système d'exploitation ou de Base de données sur l'établissement ou sur l'HDS de l'éditeur),
- La maintenance évolutive (évolution de la réglementation sur les DM et évolutions fonctionnelles décidées par un club utilisateur s'il en existe un ou par le Titulaire). L'éditeur précisera le périmètre de la maintenance évolutive (mode de fonctionnement, la périodicité des réunions). Il fournira un compte rendu de la dernière réunion…
- L'assistance, dont le périmètre de base concerne les jours ouvrables. Il appartient au Titulaire de préciser le périmètre : l'assistance technique, l'assistance utilisateurs ou d'autres formes d'assistance,
- Les webinaires de formation et aux documentations liées aux évolutions/corrections réalisées sur le logiciel.

Ce contrat doit préciser :

- Le mode d'intervention proposé (prise de contrôle à distance par exemple). Le Titulaire doit se conformer aux exigences du paragraphe 7.2.1).
- Les modalités de gestion du support : incidents et demande de support
- Les délais d'intervention selon une gravité :
    - Anomalie Critique : signifie risque potentiel ou avéré dans la prise en charge médicale ou soignante du malade, en l'absence de procédure de contournement acceptable et sécurisée.
    - Anomalie Majeure : signifie l'interruption d'une fonction de l'application ou la production de résultats anormaux sur un traitement qui entraîne des conséquences importantes soit en termes de qualité de prise en charge des patients, soit en termes de sécurité juridique ou financière pour l'établissement.

    - Anomalie Gênante : signifie l'indisponibilité d'une fonction non critique de l'application ou à une altération significative de la qualité / de la continuité de service. Elle induit un dysfonctionnement des services utilisateurs par une solution de contournement lourde.
    - Anomalie Mineure : signifie une anomalie non perturbante qui n'entraîne qu'une gêne mineure pour les utilisateurs ou qui a une solution de contournement acceptable.
- Le Titulaire décrira la procédure standard pour lui signaler les anomalies détectées.
- Les clauses de confidentialité entre le Titulaire et l'établissement.

Le Titulaire tient à jour un registre des interventions sur son système relatif pour le compte du CHRU de Tours mentionnant clairement et en français pour chaque intervention l'identification nominative de l'intervenant, le début, la fin et l'objet de l'intervention. Ce registre des interventions est soit partagé en continu avec l'établissement à travers un site internet par exemple, soit communiqué à l'établissement selon une périodicité mensuelle à minima.

Dans le cadre du fonctionnement en mode SaaS, le Titulaire doit informer au préalable le client avec un délai de prévenance compatible au fonctionnement du CHRU de 4 mois minimum pour la mise en place des mises à jour de version…

Pour le support utilisateur, un centre d'appel assurera l'enregistrement d'ouverture du dossier. Ce centre notera entre autres, la nature de l'appel (matériel, progiciel, modules ou fonctions, la date et l'heure, et la criticité de l'appel). Il fournira à l'établissement un numéro de dossier. Le Titulaire précisera si un site Internet permet l'enregistrement des appels.

Il est attendu du candidat :

- Une couverture de maintenance 7 jours sur 7 et 24H/24.
- La présence d'un support de Niveau 1 et Niveau 2 sur la solution,
- Selon le niveau de gravité préconisé, les délais de prise en compte des anomalies sont les suivants :
    - Anomalie Critique: 1 Heure ouvrée,
    - Anomalie Majeure: 1h30 Heures ouvrées,
    - Anomalie Gênante: 1 Jours ouvrés,
    - Anomalie Mineure: 10 Jours.

Dans le cas d'une panne non bloquante, le candidat s'engage à intervenir dans la journée.

En cas d'anomalie critique ou d'arrêt total du système à partir de l'enregistrement de l'appel, le Titulaire doit :

- intervenir dans un délai maximum fixé à 2 heures jusqu'à remise en service normal de l'équipement,
- détailler les prérequis CHRU nécessaires pour une remise en route complète la plus rapide possible.

Dès qu'il a connaissance d'une nouvelle anomalie, le Titulaire en informe l'établissement en lui transmettant la liste actualisée de toutes les anomalies en cours. Dans l'éventualité où le Titulaire détecte un événement indésirable critique, il en informe l'établissement sans délai selon les modalités à proposer.

7.8.2 Veille réglementaire et mise à jour

Le candidat doit s'engager à adapter son système en cas d'évolution réglementaire et à réaliser les mises à jour nécessaires avant ou à la date de mise en application des réglementaires.

7.8.3 Gestion des versions du progiciel

7.8.3.1 Dépôt des codes sources

Le fournisseur indiquera si ses programmes sources sont déposés à l'APP ou auprès d'un organisme équivalent accrédité pour la protection des programmes, à chaque version majeure ou au moins une fois par an.
Il précisera par quels moyens et avec quelle périodicité ces dépôts sont actualisés auprès de cet organisme.

7.8.3.2 Mise à disposition du plan produit (ROADMAP)

Le Titulaire met à la disposition de l'établissement un plan de développement produit qui liste les différentes versions distribuées du produit, et donne le prévisionnel des versions futures (court terme 1 an et moyen terme 2 à 3 ans) :

- Nouvelle application
- Réécriture d'applications existantes
- Nouveaux outils de développement
- Nouveaux SGBDR

Pour chacune des versions (distribuées ou futures) le plan produit précise :

- La nature de la version selon les catégories définies par l'industriel dans son processus de modification de la conception et du développement (par exemple « version majeure », « version mineure/intermédiaire »),
- la liste des fonctionnalités ajoutées ou modifiées par la version,
- pour une version distribuée, la référence de la documentation de la version qui détaille le contenu de la version,
- la date (connue ou projetée) de libération de la version,
- la liste des versions compatibles des logiciels tiers nécessaires à l'utilisation du produit.

Le plan produit précise pour chacun des logiciels tiers les dates prévisionnelles de mise en service, de fin de distribution ou de commercialisation, de fin de maintenance et de fin de support.

Le Titulaire met à disposition de l'établissement la documentation d'une version distribuée d'un produit. Cette documentation comprend au minimum :

- la liste des fonctionnalités nouvelles ou ayant évolué, avec la documentation afférente,
- la liste des anomalies corrigées,
- la date de libération de la version,
- la liste des versions compatibles des logiciels tiers nécessaires à l'utilisation de cette version du produit.

Le Titulaire met régulièrement à jour la liste des anomalies connues sur une version des produits livrés et la met à disposition du CHRU.

Le Titulaire ne pourra pas imposer une nouvelle version dont l'installation impliquerait une rupture avec le matériel ou les progiciels généraux existants.

8. L'expression des besoins fonctionnels et techniques – Cadre de réponse

L'expression des besoins fonctionnels et techniques est recensé dans le fichier « Cahier des charges - Outil Logistique Blocs - Cadre de réponse ». Le candidat doit compléter ses réponses dans les 3 onglets proposés dans le fichier :

- Spéc. FONCTIONNELLES
- Spéc. TECHNIQUES
- Documentations attendues au cours du projet

Pour les réponses, le candidat remplira un cartouche de ce type sauf pour les lignes grises :

Référence	Réponse du candidat	
col.1	col.2	col.3

– rempli par le CHRU

- **colonne 1** : le n° de paragraphe sert de référence à rappeler . En face du chiffre indiqué, sur la même ligne, vous devez obligatoirement compléter la colonne 2, voire la colonne 3

– rempli par le candidat

- **colonne 2 :**

O =	**Oui**, tel que formulé dans le CCTP, opérationnelle sur site
F =	oui dans le **Futur** en standard - en cours de réalisation ou planifié
D =	**Différent** de la formulation du cahier des charges, ou partiellement offert, opérationnelle sur site
S =	réalisable en **Spécifique**
N =	Mise à disposition **Non** prévue

- **colonne 3 :**
  - la présence et ses références pour un renvoi aux détails de sa réponse, à un commentaire, à une documentation standard fournie (exemple : suite à une réponse D pour expliquer l'écart entre ce qui est demandé et ce qu'il propose).
  - dans le cas d'une réponse F, le délai de disponibilité de la fonctionnalité par rapport à la date présumée de démarrage (0 pour réaliser au moment du démarrage, délai 3 mois, 6 mois, 1 an) + commentaires
  - dans le cas d'une réponse S, le délai de disponibilité de la fonctionnalité considérée, la charge en nombre de jours et l'évaluation du montant.

ANNEXE 1 -
Référentiels opposables par arrêté du ministre chargé de la santé PGSSI-S publié par l'ANS (Agence du Numérique en Santé)

Le corpus documentaire de la PGSSI-S, Politique Générale de Sécurité des Systèmes d'Information de Santé, offre le cadre de référence nécessaire à la mise en œuvre des règles de sécurité en matière de esanté.
L'usage du numérique en santé contribue à l'amélioration de la prise en charge du patient. Cependant, face
aux menaces engendrées par ces usages, l'Etat a mis en œuvre une politique de gestion des risques.
L'Agence du numérique en Santé (ANS) met en place les cadres de référence pour sécuriser les pratiques
en matière de e-santé pour les usagers et les professionnels des secteurs sanitaires.
La Politique Générale de Sécurité des Systèmes d'Information en Santé (PGSSI-S) est un maillon important
de cet ensemble normatif.

Ses objectifs :

- Aider les porteurs de projet dans la définition des niveaux de sécurité attendus
- Permettre aux industriels de préciser les niveaux de sécurité de leurs offres
- Soutenir les établissements de santé dans le choix et l'application de leur politique de sécurité

La PGSSI-S s'applique aussi bien au secteur public qu'au secteur privé, aux professionnels de santé, du
médico-social et social, aux établissements de soin et aux offreurs de service.

Fiche thématique de la PGSSI-S :
https://esante.gouv.fr/sites/default/files/media_entity/documents/180528_PGSSI-S_0.pdf

Corpus documentaire PGSSI-S :
https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

ANNEXE 2 -
Référentiels opposables par arrêté du ministre chargé de la santé

Référentiels opposables par arrêté du ministre chargé de la santé :
https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel-didentification-electronique---acteurs-des-secteurs-sanitaire%2C-medico-social-et-social-%5Bpersonnes-morales%5D_0_0.zip

Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes morales] :
https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel-didentification-electronique---acteurs-des-secteurs-sanitaire%2C-medico-social-et-social-%5Bpersonnes-physiques%5D_1.zip

Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes
physiques] :
https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel-didentification-electronique---usagers_0.zip

Référentiel d'identification électronique des usagers :
https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi_referentiel_imputabilite_v1.0_0.pdf

Référentiel d'imputabilité :
https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi_referentiel_imputabilite_v1.0_0.pdf

Référentiel Force Probante des documents de santé :
https://esante.gouv.fr/sites/default/files/media_entity/documents/force-probante.zip

ANNEXE 3 -
Règles pour les dispositifs connectés d'un Système d'Information de Santé – ASIP Santé PGSSI-S

Deux paliers sont définis pour la mise en œuvre des exigences de sécurité applicables aux dispositifs connectés : un palier intermédiaire (Palier 1), porteur des exigences prioritaires, et un palier supérieur (Palier 2) reprenant les exigences prioritaires et les complétant afin d'offrir un meilleur niveau de sécurité.

Gestion des configurations

Nº	Exigence	Niveau d'exigibilité
	Gestion des configurations [G]	
[G1]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation (accessible par exemple au travers d'un espace client sur Internet) l'ensemble des composants matériels (serveur s, périphériques, …) et logiciels (versions des logiciels, systèmes d'exploitation, bases de données, …) informatiques standards constituant le dispositif connecté ainsi que leurs principales caractéristiques.	Palier 1
[G2]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation l'ensemble des spécifications portant sur le poste d'administration/ utilisation du dispositif connecté (caractéristiques matérielles du poste, version du système d'exploitation, middleware et pilotes, services activés, périphériques, …).	Palier 1
[G3]	Le système dispositif connecté doit fournir une interface permettant à un système de management des configurations (CMDB) d'un SIS ou à un service de télémaintenance (par exemple pour un Professionnel de Santé en exercice libéral) d'obtenir automatiquement la configuration du système dispositif connecté	Palier 2

Sécurité physique

Nº	Exigence	Niveau d'exigibilité
	Sécurité physique [S]	
[S1]	Le fournisseur et/ou le fabricant doit identifier dans sa documentation l'ensemble des mesures de sécurité physique (sécurité des locaux, clés du coffret protégeant le dispositif connecté, contraintes d'environnement notamment compatibilité électromagnétique (réseau WiFi, téléphone mobile), sécurité des câblages…) préconisées pour la mise en œuvre du système dispositif connecté au sein du SIS.	Palier 1
[S2]	Le dispositif connecté doit mettre en œuvre des moyens de sécurité physique permettant de détecter toute tentative d'accès physique aux composants internes sensibles (disque dur, interfaces internes, paramétrages matériels par cavaliers par exemple, …).	Palier 2

Exploitation et communications

Nº	Exigence	Niveau d'exigibilité
	Exploitation et communications [E]	
	Vérification du bon fonctionnement	
[E1]	Les dispositifs connectés doivent disposer d'une fonction permettant de garantir l'intégrité des logiciels et des données sensibles du dispositif au démarrage du dispositif et lors de son fonctionnement. La date de dernière modification des logiciels et des données sensibles dont celles inhérentes à l'appareil est présentée lors de la connexion des utilisateurs.	Palier 1
	Mise à jour des dispositifs	
[E2]	Les dispositifs connectés et les logiciels des postes utilisateurs doivent disposer d'une fonction de mise à jour sécurisée des logiciels (logiciels, microgiciel, …) permettant de garantir l'origine et l'intégrité des mises à jour.	Palier 1
[E3]	Les dispositifs connectés doivent vérifier la bonne installation d'une mise à jour logicielle avec une possibilité de retour arrière en cas de dysfonctionnement détecté.	Palier 1
[E4]	Les dispositifs connectés et les logiciels des postes utilisateur doivent disposer d'une fonction de mise à jour sécurisée avec notification automatique de l'existence d'une mise à jour des logiciels (logiciels, microgiciel, …).	Palier 2
	Protection contre les codes malveillants	
[E5]	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants notamment dans le cas d'utilisation de supports amovibles. Si le dispositif ne comporte pas de solution de type antivirale l'utilisation de support externe est interdite.	Palier 1
[E6]	Les postes utilisateurs des dispositifs connectés doivent s'adapter ou comporter des moyens de sécurité permettant de détecter et de répondre aux menaces liées aux codes malveillants. Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés installés sur les postes utilisateurs sont compatibles avec des solutions de sécurité contre les codes malveillants. Le fabricant doit fournir la liste des outils avec lesquels ses logiciels et matériels sont compatibles.	Palier 1
	Sécurité des réseaux	
[E7]	La documentation du dispositif connecté (accessible par exemple au travers d'un espace client sur Internet) doit comporter une matrice des flux réseau (types de protocoles, origine/destination des flux, plan d'adressage…) exhaustive.	Palier 1
[E8]	Les dispositifs connectés doivent comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, …).	Palier 2
[E9]	Les postes utilisateurs des dispositifs connectés doivent comporter des moyens de sécurité permettant de filtrer les données échangées sur les réseaux (types de protocoles, origine/destination des flux, …). Dans ce sens, les logiciels spécifiques à la gestion des dispositifs connectés, installés sur les postes de travail, sont compatibles avec les solutions de sécurité de filtrage réseaux de type firewall personnel.	Palier 1
[E10]	En cas de mise en œuvre de communications sans fil, le dispositif connecté doit être conforme aux exigences en vigueur dans les bonnes pratiques. Concernant le mode WiFi, se référer aux documents de référence dans le domaine.	Palier 1
	Sécurité des données	
[E11]	Afin de garantir la confidentialité des données médicales personnelles stockées localement, le dispositif connecté doit embarquer un dispositif de chiffrement des données. Le fournisseur et/ou le fabricant pourra se référer au Référentiel Général de Sécurité (RGS) qui comporte une annexe décrivant les exigences relatives à la fonction de sécurité « confidentialité ».	Palier 2
[E12]	Afin de garantir l'intégrité des données, le dispositif connecté doit mettre en œuvre des protocoles de transmission adaptés permettant de vérifier l'équivalence des données reçues à celles émises.	Palier 1
[E13]	Lors de la numérisation et de la compression des images (imagerie médicale), des procédures normalisées doivent être mises en œuvre afin de garantir l'intégrité de ces données.	Palier 1

[E14]	Les échanges de données du dispositif connecté doivent être conformes aux exigences de sécurité (notamment authentification et chiffrement) identifiées dans le Cadre d'Interopérabilité des SIS publié par l'ASIP Santé.	Palier 1
[E15]	Les échanges de données entre le dispositif connecté et les postes utilisateurs doivent être protégés en confidentialité et intégrité.	Palier 2
[E16]	L'accès aux fonctions d'export de données du dispositif connecté doit être limité à des personnes dûment habilitées.	Palier 1
	Gestion des supports amovibles	
[E17]	La fonction de démarrage du dispositif connecté à partir d'un support amovible doit être désactivée en fonctionnement nominal.	Palier 1
	Surveillance	
[E18]	Le dispositif connecté doit comporter une fonction d'alerte locale permettant de surveiller le bon fonctionnement, et tout événement pouvant avoir un impact critique sur son fonctionnement.	Palier 1
[E19]	Le dispositif connecté doit comporter une fonction d'alerte s'appuyant sur des mécanismes standards permettant au SIS de surveiller le bon fonctionnement, le contrôle des connexions au dispositif, et tout événement pouvant avoir un impact critique sur son fonctionnement (mise à jour du logiciel, modification de paramètre critiques, …).	Palier 2
	Journalisation	
[E20]	Le dispositif connecté doit comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif connecté et de tout événement pouvant avoir un impact critique sur son fonctionnement en particulier les événements identifiés par la règle E18. Le fabricant doit indiquer dans sa documentation les modalités de mise en œuvre de la journalisation en particulier les capacités de stockage de journaux du dispositif connecté et les recommandations en matière de sauvegarde des journaux.	Palier 1
[E21]	Le dispositif connecté doit comporter une fonction de gestion des traces s'appuyant sur des mécanismes standards permettant au SIS de conserver des enregistrements de tout événement pouvant avoir un impact critique sur le fonctionnement du dispositif connecté avec une garantie d'imputabilité pour l'ensemble des opérations effectuées sur ce dispositif. Ces journaux doivent permettre l'analyse ultérieure des causes des dysfonctionnements.	Palier 2
	Sauvegardes	
[E22]	Le dispositif connecté doit comporter une fonction de sauvegarde conforme aux exigences en vigueur dans les bonnes pratiques.	Palier 1
	Règles de destruction de données lors du transfert de matériels informatiques	
[E23]	Le fournisseur doit mettre en œuvre des fonctions de sécurité d'effacement des données conformes aux exigences en vigueur dans les bonnes pratiques.	Palier 1
	Maîtrise des accès [A]	
	Contrôle d'accès au réseau	
[A1]	Le dispositif connecté doit comporter une fonction standard d'identification et d'authentification réseau du matériel, par exemple par l'utilisation du protocole 802.1X.	Palier 2
	Authentification des utilisateurs	
[A2]	Le dispositif connecté doit comporter une fonction d'authentification des utilisateurs sur la base de comptes nominatifs et au minimum de mots de passe modifiables par les utilisateurs. Les mots de passe par défaut doivent être changés lors de l'installation ou de la première connexion d'un utilisateur et être spécifiques à chaque client.	Palier 1
[A3]	Le dispositif connecté doit comporter une fonction d'authentification forte des utilisateurs pour certains profils (administration, maintenance,…).	Palier 2
[A4]	Le dispositif connecté doit permettre d'imposer une politique de mots de passe (période de renouvellement, règles de constitution des mots de passe, réutilisation d'anciens mots de passe, …)	Palier 2
[A5]	Tout accès au système dispositif connecté nécessite une authentification préalable.	Palier 1
[A6]	La date de dernière connexion au système dispositif connecté doit être présentée lors de la connexion d'un utilisateur	Palier 1
[A7]	Les logiciels du système dispositif connecté doivent offrir des fonctionnalités de verrouillage automatique en cas d'inactivité prolongée et de blocage de comptes en cas de tentative d'accès non autorisé répétée.	Palier 1
	Droits d'accès	
[A8]	Les droits d'accès des utilisateurs doivent être organisés selon des rôles.	Palier 1

[A9]	L'accès aux fonctions de mise à jour des logiciels ou de modification des paramètres sensibles nécessite une authentification forte des utilisateurs. Toute action de validation dans ces contextes nécessite une double confirmation (ex.la validation d'une demande de modification de paramètres sensibles ouvre une fenêtre de dialogue rappelant l'impact d'une telle modification et demandant la confirmation de la demande).	Palier 2

Développement et maintenance des logiciels

Nº	Exigence	Niveau d'exigibilité
Développement et maintenance des logiciels [D]		
[D1]	Le fournisseur et/ou le fabricant s'engage à n'installer que les seuls logiciels nécessaires au fonctionnement du dispositif connecté. Le fournisseur et/ou le fabricant s'engage à n'activer que les seuls services nécessaires au fonctionnement du dispositif connecté.	Palier 1
[D2]	L'architecture générale du système dispositif connecté et des logiciels développés doit être sans adhérence avec les briques système standards utilisées, en vue de faciliter les migrations de versions de logiciels. A défaut, le fournisseur doit assurer la compatibilité ascendante avec les évolutions des briques adhérentes.	Palier 1
[D3]	Le processus de développement doit prévoir la gestion des exceptions (débordement de plages de valeurs, erreurs internes des composants, …).	Palier 1
[D4]	Le fournisseur et/ou le fabricant doit implémenter une fonction permettant de vérifier l'intégrité des logiciels lors de leur démarrage ou lors de leur mise à jour	Palier 1
[D5]	Le fournisseur du dispositif connecté doit assurer un suivi permanent des incidents liés aux dispositifs connectés et met à disposition de ses clients, les correctifs nécessaires. Ce suivi s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.	Palier 1
[D6]	Le fournisseur du dispositif connecté doit assurer un suivi permanent des vulnérabilités liées aux technologies mises en œuvre dans ses produits et met à disposition de ses clients les correctifs nécessaires. Ce suivi s'inscrit dans le cadre du guide d'organisation de la sécurité de la PGSSI-S.	Palier 1
[D7]	Les fonctionnalités de télémaintenance du dispositif connecté doivent être conformes au guide PGSSI-S – Règles pour les interventions à distance sur les SIS.	Palier 1
[D8]	Les modes de tests et de maintenance du dispositif connecté doivent être exclusifs du mode opérationnel.	Palier 1
[D9]	Le dispositif connecté doit disposer d'un mode dégradé (sécurisé) permettant son fonctionnement déconnecté du SIS avec une fonction de reprise des données lors du retour en mode nominal.	Palier 1
[D10]	Le fabricant doit mener des tests de la robustesse des dispositifs connectés (tests aux limites, injection de données malformées, …)	Palier 1
[D11]	Le fournisseur et/ou le fabricant doit proposer des solutions de restitution des données permettant une reprise de celles-ci par le client notamment en cas de changement d'équipement, dans un format réutilisable par le client.	Palier 1
[D12]	Le fournisseur et/ou le fabricant doit réaliser des tests de non régression à chaque évolution du logiciel ou matériel du dispositif connecté.	Palier 1

Conformité

Nº	Exigence	Niveau d'exigibilité
	Conformité [C]	
[C1]	Il est du ressort du fournisseur d'acquérir et de concéder au client l'ensemble des licences d'utilisation nécessaires au fonctionnement du dispositif connecté sauf condition spécifique du client. Ceci concerne les droits d'usage des progiciels, des matériels et de l'ensemble des couches logiques utilisées (Système d'exploitation, algorithme, progiciels sécuritaires, progiciels réseaux, progiciels de base de données, progiciels systèmes, progiciels de transfert et de prise de main à distance, progiciels applicatifs, etc.).	Palier 1
[C2]	Le fournisseur et/ou le fabricant doit réaliser une analyse de risques du système dispositif connecté et doit adapter les mesures de sécurité à mettre en œuvre dans ses produits au regard des risques résiduels. Il doit informer le client de la méthode d'analyse de risques retenue, des risques couverts et des risques résiduels qui seront portés par le client. Il peut en outre préconiser des mesures de sécurité à mettre en œuvre par le client afin de réduire les risques résiduels identifiés dans le cadre des précautions d'usage du dispositif.	Palier 1

ANNEXE 4 -

Conditions de maintenance – A compléter par le Titulaire

Dans tous les cas, le Titulaire sera joint :

	oui	non
Par téléphone		
Par fax		
Par courriel		
Par courrier		
Autres propositions :		

Nature de la maintenance

	oui	non
Sur Site		
Télémaintenance		

Équipe de maintenance

Effectifs de l'équipe de maintenance :
Localisation de l'équipe de maintenance :

Couverture de la maintenance

La maintenance sera assurée au minimum du lundi au vendredi de 8H à 18H.

Extensions d'horaires proposés Jours – Heures	de	à

	En Heures
- Délai maximal de prise en compte d'un dysfonctionnement **bloquant l'utilisation**	
- Délai maximal de prise en compte d'un dysfonctionnement **ne bloquant pas l'utilisation**	
Délai maximal de réparation d'un dysfonctionnement **bloquant l'utilisation**	
Délai maximal de réparation d'un dysfonctionnement **ne bloquant pas l'utilisation**	

Certification

	oui	non
La maintenance est-elle organisée suivant les normes ISO		
Le Titulaire a-t-il obtenu une certification (si oui la fournir)		

Exercice de la maintenance

La maintenance est exercée par :	oui	non
le Titulaire		
l'éditeur, propriétaire : (identification)		
un tiers : (Identification)		

ANNEXE 5 -
Analyse d'impact relative à la protection des données (AIPD)

Voici les informations relatives demandées par le CHRU relatives avant toute mise en production :

RGPD et Données personnelles :

- Accord RGPD
- Certification et coordonnée de votre Hébergeur de données de santés (sous -traitant)
    - Les conditions de restitution et/ou de destruction des données en fin du contrat
- Politique de sécurité du système d'information du candidat

Au niveau RGPD, nous avons besoin d'un complément d'informations sur les points suivants :

- Quelles sont les données mémorisées sur les agents (autres que celles du paramétrage du compte) ? Date/heure et machine de la dernière connexion, Actions horodatées… ?
- Les données agents sont-elles conservées pendant la durée de fonctionnement de l'applicatif du candidat sur l'établissement ? Pouvez-vous nous lister les informations concernées ?
- Quelles sont les données conservées pendant un certain temps avant archivage (si existant) ?

- Extrait de la déclaration de vos traitements de votre registre CIL/RGPD pour les données personnelles des agents du CHRU de Tours
    - CIL/DPD du candidat ?
    - Identifier clairement les données et les traitements qui passeront dans la solution du candidat ?
    - Avec notamment les conditions de restitution et/ou de destruction des données en fin du contrat

- Comment les personnes concernées peuvent-elles exercer
    - leur droit d'accès et droit à la portabilité ? (art. 15 et 20 du RGPD) ?
    - leur droit de rectification et droit à l'effacement (Droit à l'oubli) ? (art. 17 fu RGPD) ?
    - leur droit de limitation et droit d'opposition ? (art. 18 et 21 du RGPD) ?

- Les obligations du candidat sont-elles clairement définies et contractualisées ? Est-ce qu'il y a un document de l'éditeur ?

Sécurité :

- Quels sont les supports des données ? (Collecte / traitement / transit / stockage…) : nous aurions besoin d'un document général sur l'infrastructure de la solution du candidat
- Pourriez-vous nous envoyer des documents sur les moyens (audit de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le candidat en matière de protection des données ?
- Chiffrement : Moyens mis en œuvre pour assurer la confidentialité des données conservées (en base de données, dans des fichiers plats, dans les sauvegardes, etc.) ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.)

- Anonymisation / Pseudonymisation : Description des mécanismes d'anonymisation, des garanties qu'ils apportent contre une réidentification éventuelle et à quelle fin ils sont mis en œuvre.
- Cloisonnement : Méthodes utilisées pour cloisonner le traitement. Les bases de données sont distinctes et dédiés à un seul projet. Les environnements (production, test…) sont clairement identifiés et séparés.
- Contrôle des accès logiques :
    - Description de la manière dont les profils utilisateurs, patients sont définis et attribués. Il conviendra de détailler les moyens d'authentification mis en œuvre en précisant, le cas échéant précisez les règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).
    - Pour l'usage des terminaux mobile : Moyen d'authentification
- Journalisation : Politiques de journalisation des événements et de conservation des traces qui en résultent.
- Archivage : Politique de conservation et gestion d'archives électroniques contenant des données à caractère personnel destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire
- Sauvegarde des données : Existence d'une politique de sauvegarde permettant d'assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité (régularité des sauvegardes, chiffrement du canal de transmission des données, test d'intégrité, etc.)
- Protection des sites WEB : Méthodes et moyens mis en place pour diminuer la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel (référentiel général de sécurité, chiffrement TLS des flux, politique de dépôt de cookies, audits de sécurité, etc.).
- Les règles de gestion et de notification des incidents. Celles-ci devraient comprendre une information du responsable de traitement en cas de découverte de faille de sécurité ou d'incident de sécurité et cela dans les plus brefs délais lorsqu'il s'agit d'une violation de données à caractère personnel.
- Traçabilité : Existence de mesures mises en place pour être capable de détecter les incidents concernant des données à caractère personnel de façon précoce et de disposer d'éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes (architecture et politique de journalisation, respect des obligations en matière de protection des données à caractère personnel, etc.)
- Sécurisation des terminaux mobiles : Existence de mesures prises pour diminuer la possibilité que les terminaux soient exploités pour porter atteinte aux données à caractère personnel (inventaire, cloisonnement, redondance matérielle, limiter l'accès, etc.)