



Centre Hospitalier Régional et Universitaire de Tours

**DIRECTION DES ACHATS, DE LA LOGISTIQUE, DES
APPROVISIONNEMENTS ET DE LA TRANSITION ECOLOGIQUE**

37044 Tours Cedex 9

<http://www.CHRU-tours.fr>

ANNEXE 4

SYSTEME D'INFORMATION

SYNTHESE DES PRECONISATIONS D'INFRASTRUCTURE

Procédure N°2025-DALATE-INHOT-168

**Acquisition d'une solution de stockage et de distribution
automatique et unitaire de vêtements pliés et prestations de
maintenance associées pour le CHRU de Tours.**

Le présent document comprend 10 pages

Ce document vise à présenter les préconisations d'infrastructure du CHRU de TOURS, à la date de rédaction du document.

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 7 ou 6 64 bits
 - WINDOWS 2019, 2016 ou 2012
- Base de données :
 - ORACLE19C patch 10 minimum, 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 serveurs TrendMicro

Front-end

- La compatibilité de l'application avec Windows 10
- Compatibilité de l'application si nécessaire avec Internet Explorer 11 ou Edge Chromium
- Compatibilité de l'application si nécessaire avec Citrix XenApp 7.15
- Antivirus OfficeScan de Trend sur les postes de travail
- Annuaire : Conformité avec serveur Active directory 2019 et niveau fonctionnel 2008 R2

Réseau

- Wifi : Dans le cas d'utilisation d'équipements mobiles, l'intégration à l'architecture Wifi implantée sur le CHU est obligatoire
- Si la solution nécessite un déploiement de client sur les postes de travail, celui-ci devra impérativement intégrer la plateforme SCCM
- 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 CHU
- L'équipement devra être identifiable via le NAC (Network Access Control) du CHU via le protocole 802.1x notamment

Télémaintenance

- La plateforme sécurisée d'accès à distance pour la télémaintenance est la solution IPDIVA
- Les comptes sont valables pour une durée d'un an renouvelable

1. 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.

1.1 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.

1.2 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, ...

1.3 Réseau

Le CHRU de Tours adhère au segment NTIC réseau UNIHA et ne peut acquérir des équipements que dans ce cadre. Le constructeur retenu, que ce soit dans le cadre de la rénovation ou de la mise en œuvre de nouvelles structures / bâtiments est CISCO.

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.

1.4 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 et si besoin de périphériques type lecteurs de badges, douchette codes à barres 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.

1.5 Virtualisation

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

1.6 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.

Pour les bases hors Oracle, le candidat devra intégrer obligatoirement dans sa proposition toutes les prestations liées à la supervision, l'administration, la maintenance corrective et évolutive (changement de version)

1.7 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.

1.8 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 DSI du CHRU de Tours.

5.8.2 Réseau				
Connectivité réseau cuivre sur équipements CHRU	Nécessité (O/N)	Nombre de ports physiques	Agrégation	PoE
Equipements réseau fourni par le candidat	Switch(1)	Firewall(1)	Adressage privé(1)	Equipement double carte réseau(1)
Télémaintenance	Nécessité (O/N)	Portail SSL du CHRU de Tours	Tunnel site à site	Autre (1)
Connectivité WiFi sur le réseau existant au CHU	Nécessité (O/N)	Bande passante demandée mini/moy/max	QoS demandée	Nécessite un réseau Wifi dédié (1)

(1) Doit être étudié et soumis à l'approbation de la DSI du CHRU de Tours

5.8.7 Sécurité des dispositifs connectés				
	Antivirus	Compatible antivirus CHRU	Si non compatible : éditeur (1)	Autre solution (1)
Poste de travail				
Dispositif connecté				Lu et approuvé (2) l'annexe 1 (O/N)

(1) Doit être soumis à l'approbation de la DSI du CHRU de Tours

(2) Le candidat devra expliciter les points sur lesquels il ne peut s'engager

ANNEXE 1

Politique Générale de Sécurité des Systèmes d'Informations de 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 e-santé.

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](#)

[Corpus documentaire PGSSI-S](#)

ANNEXE 2

Référentiels opposables par arrêté du ministre chargé de la santé

[Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social \[personnes morales\]](#)

[Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social \[personnes physiques\]](#)

[Référentiel d'identification électronique des usagers](#)

[Référentiel d'imputabilité](#)

[Référentiel Force Probante des documents de santé](#)

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

N°	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 (serveurs, 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

N°	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

N°	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, micrologiciel, ...) 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, micrologiciel, ...).	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

N°	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

N°	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	Palier 1
	mettre en œuvre par le client afin de réduire les risques résiduels identifiés dans le cadre des précautions d'usage du dispositif.	