Connexion d’un équipement sur le réseau HCL (s’il y a lieu).

Les équipements informatiques (serveurs, postes de travail, composants et logiciels) connectables au réseau informatique HCL sont conformes à l’annexe technique standard de la Direction des services Numériques (DSN) et ses annexes (jointe au présent document**).**

Cette conformité, pour les composants concernés, a été évaluée à l’aide du questionnaire relatif à la conformité aux standards techniques informatiques annexé à l’acte d’engagement. Tout point de non-conformité a fait l’objet d’une acceptation par la Direction des services Numériques.

Attention : les exigences 0.x de l’annexe informatique (la partie sécurité informatique « de base ») sont éliminatoires en cas de non-respect.

Echange de données avec Internet (s’il y a lieu).

Le principe de fonctionnement général est de refuser toute communication directe avec Internet (quel que soit le sens des flux : Internet 🡺 Réseau interne HCL ou Réseau Interne HCL 🡺 Internet) à partir du moment où elle n'est pas spécifiquement et explicitement autorisée.

Toute autre communication avec Internet, en dehors de cas cités dans les exigences de l’annexe précitée est contrôlée par l’intermédiaire d’un dispositif de sécurité HCL adapté.

En cas de besoin, le fournisseur communique aux HCL ses besoins de filtrage spécifiques qui pourront être mis en place par les HCL sous réserve d’être compatibles avec la Politique Globale de Sécurité des HCL.

Zoom sur la sécurité informatique

Dans un cadre de niveau de menace cyber élevé, les HCL prennent des mesures de protection de leur infrastructure informatique. Ces mesures s’appliquent aux équipements HCL mais, pour des raisons évidentes, doivent également s’appliquer aux équipements des fournisseurs qui seront installés sur le réseau des HCL. Elles consistent en une série d’exigences de base de sécurité informatique et constituent un prérequis à l’acceptation de la solution fournisseur.

* Les standards de sécurité HCL imposent au fournisseur l’application, idéalement sur une base mensuelle, des mises à jour de sécurité du système d’exploitation et des logiciels supports et applicatifs. Cela inclut les montées de version du système d’exploitation ou des logiciels avant que ceux-ci arrivent en fin de support.  
  Dans le cas où l’équipement est un PC Windows, le déploiement des mises à jour doit être fait automatiquement via le logiciel de gestion (MECM) des HCL ou manuellement (en présentiel ou télémaintenance) par le fournisseur. Les HCL n’appliqueront pas eux-mêmes de mises à jour manuelles sur les équipements fournisseurs.
* Les standards de sécurité HCL imposent au fournisseur l’installation de l’antivirus Windows Defender pour les équipements Windows. Le choix de l’antivirus est laissé libre pour les équipements Linux. La mise à jour des définitions AV doit se faire de manière journalière et automatiquement.
* Les standards de sécurité HCL imposent au fournisseur l’installation de l’EDR Microsoft Defender For Endpoint sur les équipements Linux, Windows et MacOS, si possible en mode protection mais à minima en mode détection. Si cela n’est pas possible, en raison du caractère dit « embarqué », le fournisseur doit fournir une description des techniques de durcissement mises en place. Ce durcissement doit être basé sur des guides de durcissements reconnus (CIS, ANSSI…) et inclure la mise en place d’un logiciel d’autorisation permettant d’empêcher l’exécution de code non validé par le fournisseur (logiciel dit de « liste blanche » ou allow-listing).
* Les standards de sécurité HCL imposent au fournisseur l’utilisation du portail de télémaintenance des HCL (portail web de type « Bastion ») via une connexion HTTPS puis RDP ou SSH vers ses équipements à l’intérieur du LAN HCL. La connexion se fera en MFA.

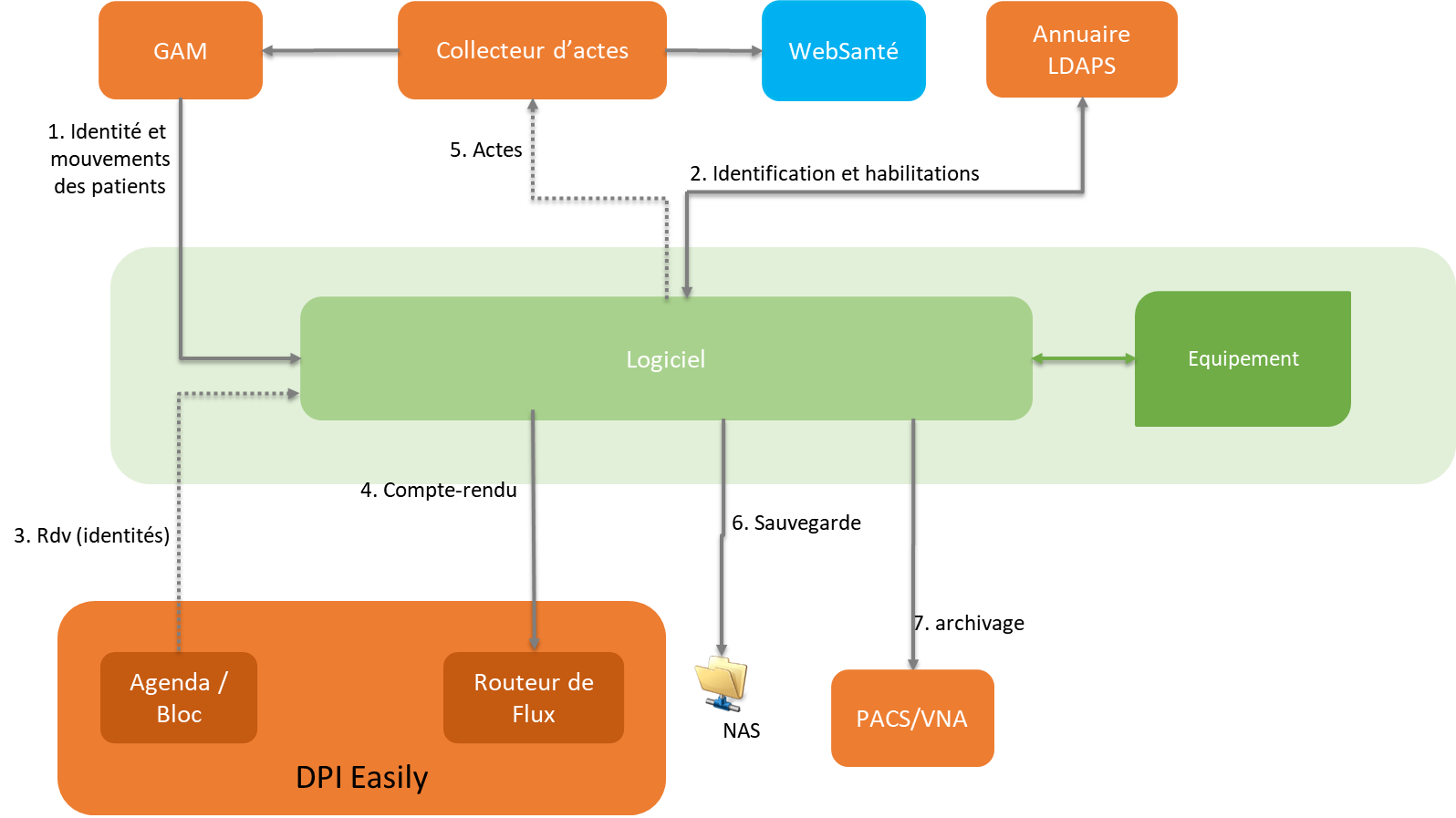
***Contraintes d’intégration et de sécurisation des données au SIH des HCL (s’il y a lieu).***

L’intégration de la solution au SIH des HCL peut conduire à la mise en œuvre d’un certain nombre d’interfaces présentées sur le schéma ci-dessous.

Sont obligatoires dans le cadre de cette consultation les interfaces suivantes :

* Interface identité patients
* Identification et habilitations
* Sauvegarde et archivage des données

La capacité de mise en œuvre des interfaces optionnelles doit aussi être précisée dans la réponse au présent CCTP.



* Identité Patient

L'archivage à des fins réglementaires des contenus multimédias produits par le système nécessite une identification sécurisée du patient en amont de sa prise en charge.

Le système doit être en capacité de récupérer l’identité des patients attendus pour proposer une liste de travail à l’utilisateur connecté en mettant en œuvre une des deux interfaces décrites ci-dessous.

Tout système de saisie manuelle de l’identité est proscrit.

* Option 1 : Interface identité GAM

*cf E210120- Annexe Technique IDTMVT-IHEPAM\_20211020.pdf*

Le système de Gestion Administrative des Malades (GAM) utilisé aux HCL est le logiciel PASTEL.

Les informations véhiculées dans l’interface en provenance de PASTEL sont l’identité du patient, sa venue au sein de l’hôpital et les mouvements dans les différentes unités de l’hôpital durant sa venue. Le flux transmis contient tous les patients de l’établissement.

La solution doit proposer des filtres natifs pour permettre une identification/sélection facile des patients attendus dans le contexte de travail de l’utilisateur.

* Option 2 : Interface Rdv EASILY

*cf GD\_Agenda\_HL7\_IN\_Format\_Messages\_SIU.pdf*

*cf GD\_Agenda\_HL7\_OUT\_Parametrage\_Template\_SIU.pdf*

Selon le contexte de prise en charge du patient, une programmation préalable de l’acte médical est réalisée dans les modules du DPI EASILY BLOC ou AGENDA.

Ces modules peuvent transmettre au système vidéo un flux basé sur la norme HL7 SIU version 2.5 qui contient les rendez-vous de la journée pour permettre de constituer la Worklist des examens de la journée.

L’échange des messages est réalisé selon le protocole MLLP (Minimum Lower Layer Protocol) avec accusé de réception réalisé par l’application qui traite les messages.

* Identification et habilitations ***(s’il y a lieu).***

*cf E170015 - Annexes CCTP Gestion des identités et habilitations.pdf*

La solution doit s’interfacer à l’active Directory des HCL en respectant le protocole LDAPS, pour à l’authentification des utilisateurs.

Idéalement, les habilitations doivent pouvoir s’appuyer sur des groupes utilisateurs définit dans l’AD pour faciliter la gestion des accès au quotidien au travers des groupes AD.

* Exports vers le DPIHCL ***(s’il y a lieu).***

Le DPI EASILY dispose d’un module ROUTEUR DE FLUX permettant de recevoir des compte-rendu d’examen et de les intégrer dans le dossier du patient.

Le format d’échange se base sur la norme HL7 ORU version 2.5.

Les informations obligatoires à véhiculer dans ce flux sont :

\* L’Identifiant Permanent du Patient (IPP)

\* Le compte-rendu (en PJ encapsulé ou le chemin d’accès au fichier s’il est déposé)

\* Le type de document ; cette information permet de classer le compte-rendu dans le dossier du patient.

D’autres informations pourront être renseignées en fonction du contexte du service (IEP, spécialités, numéro RPPS du médecin, …)

* Saisie des actes ***(s’il y a lieu).***

Le Collecteur d’actes est un serveur d’activité, permettant de recueillir les données d’activité saisies en temps réel dans différents logiciels Métier, de les contrôler, de les stocker et de les rediriger vers d'autres applicatifs tels que des logiciels centralisés de facturation et/ou de PMSI.

Le format d’échange se base sur la norme Hprim XML en version 2.00.

Le transfert des fichiers se fait par FTP. Après le traitement du fichier ou en cas d’erreur, un fichier d’acquittement peut être envoyé à l’application émettrice.

Sauvegarde et archivage des données (s’il y a lieu).

Afin de sécuriser les données, le titulaire indique le processus de sauvegarde des données et le processus d’archivage de ces données qu’il a prévus dans sa solution pour répondre aux questions suivantes :

* Archivage des données nécessaire au sens médico-légal, de façon pérenne et sécurisée.
* Utilisation de ces données à l’extérieur des HCL de façon anonymisées si nécessaire

Cette sauvegarde doit systématiquement être proposée et adaptée en fonction des contraintes et horaire de fonctionnement des équipements. Elle doit permettre de redémarrer la solution à l’identique après réinstallation des composants logiciels à la date de la dernière sauvegarde.

**L’utilisation de dispositifs mobiles tels que disques dur externes, clés USB, … doit être proscrit.**

Dans cet objectif, les HCL préconisent d’utiliser un support de sauvegarde ou d’archivage délocalisé au travers du réseau et peuvent fournir un serveur centralisé (NAS) et/ou une solution d’archivage des données sur un serveur situé dans le Datacenter des HCL.

Les volumétries estimées des données sauvegardées et archivées, la durée de conservation ainsi que les comptes nécessitant un droit d’accès à ces données (archives/sauvegarde) doivent être précisés.

Modalités de télémaintenance pour les équipements connectés au réseau informatique des H.C.L. S’il y a lieu

Des services VPN-SSL ont été mis en place afin de permettre à des intervenants extérieurs aux HCL de se connecter de façon privilégiée pour des opérations contractuelles de maintenance.

Aucune autre solution de télémaintenance n’est acceptée.

La demande d’accès en télémaintenance suit un processus spécifique qui pourra être déclenché après la notification de marché. Elle suppose de déclarer nominativement les intervenants qui se connecteront (compte personnel). Bien entendu, elle présuppose que les équipements ciblés remplissent préalablement les exigences de sécurité pour être connectés au réseau de l’établissement.

Le portail de télémaintenance est géré et maintenu par la DSN, les comptes nominatifs sont revus chaque année avec le référent HCL de la société.