|  |  |
| --- | --- |
|  | **CENTRE HOSPITALIER UNIVERSITAIRE**  **Avenue de la Côte de Nacre**  **CS 30001**  **14033 - CAEN Cedex 9** |

CCTP -

HEBERGEMENT EXTERNalise

# Table des matières

[1. Table des matières 2](#_Toc129012407)

[2. SECURITE 3](#_Toc129012408)

[3. Gestion des acces 3](#_Toc129012409)

[3.1. Interface utilisateur 3](#_Toc129012410)

[3.2. Interface habilitation 4](#_Toc129012411)

[3.3. Accès sso 4](#_Toc129012412)

[4. Environnement de production 4](#_Toc129012413)

[5. Montée de version de la solution applicative 4](#_Toc129012414)

[6. requêtage des données 5](#_Toc129012415)

[7. automatisATION de taches 5](#_Toc129012416)

[8. interfaceS 5](#_Toc129012417)

[9. SUIVI DES LOGS 6](#_Toc129012418)

[10. Communication 6](#_Toc129012419)

# SECURITE

En cas d’hébergement de données de santé, le titulaire doit apporter la preuve d’une certification permettant de garantir que l’environnement d’hébergement respecte à minima les normes de sécurité HDS en cours.

Dans le cas où les données hébergées ne sont pas de données de santé, le titulaire doit apporter la preuve d’une certification permettant de garantir que l’environnement d’hébergement respecte à minima les normes de sécurité ISO 27001 en cours.

De plus, le CHU Caen Normandie (CHU de Caen) se réserve le droit de commander un audit de sécurité indépendant (test de pénétration). Cet audit est à la charge du CHU de Caen. Le cadre de cet audit concerne la solution applicative définie dans le CCTP. Les résultats de ce test seront alors communiqués au titulaire.

Suite à cet audit, les travaux permettant de se mettre en conformité avec les recommandations de l’auditeur indépendant seront pris en charge dans le cadre de la maintenance et devront être réalisés dans les délais suivants selon la gravité de la faille détectée :

* Faille critique : doit être corrigée dans un délai d’une semaine
* Faille majeure : doit être corrigée dans un délai d’un mois
* Faille mineure : doit être corrigée dans un délai de 6 mois

En cas de détection de faille en dehors de l’audit, les conditions de résolution des failles ci-dessus s’appliquent également.

Le CHU de Caen, en qualité d’OSE, doit respecter la directive NIS et, par conséquent, le titulaire doit respecter la même directive.

# Gestion des acces

La gestion des accès est gérée par un profil ou plusieurs profils administrateurs donnés à l’établissement par le titulaire. Il est le seul est habilité à donner des droits à un utilisateur.

Le titulaire doit également proposer un système d’interface permettant de gérer les accès des utilisateurs de l’établissement à la solution applicative.

Un système d’authentification à double facteur est obligatoire.

## Interface utilisateur

Dans les cas où elle est requise, cette interface permet d’activer ou désactiver les accès utilisateurs.

Le fichier d’interface contient une liste d’adresse mailsautorisés à se connecter à la solution applicative.

Une présence dans le fichier donne accès à la solution applicative.

Une absence dans le fichier supprime l’accès à la solution applicative.

Tout ajout d’un nouvel utilisateur déclenche un mail sur son adresse professionnelle.

Ce mail permet la gestion du mot de passe.

## Interface habilitation

Cette interface permet d’associer un compte et une habilitation déjà définie dans la solution applicative.

Le fichier transmis permet d’associer une habilitation à un compte ou plusieurs spécifiques afin d’affiner les droits dans l’application.

## Accès sso

Afin de faciliter les accès à la solution applicative, le titulaire propose au choix :

* Une api jeton permettant à un utilisateur connecté sur le domaine du CHU de s’authentifier directement sur la solution applicative
* Un accès par lecture la carte professionnelle ASIP santé (carte CPE/CPA/CPS/…)
* Un accès au travers d’un compte Pro Santé connect

# Environnement de production

Le titulaire met à disposition du CHU de Caen un environnement de production dédié.

Les ressources de cet environnement de production ne sont pas mutualisées avec d’autres clients du titulaire afin de ne pas dépendre de contraintes liées à un autre client du titulaire, et qui seraient incompatibles avec les contraintes du système d’information de l’établissement.

# Montée de version de la solution applicative

Le titulaire doit proposer au CHU de Caen de tester toute nouvelle version applicative sur un environnement séparé de celui de production.

Toute montée de version en environnement de production doit être approuvée par le CHU de Caen par écrit.

Le titulaire ne peut pas imposer une montée de version en production à l’établissement si celle-ci s’avère incompatible avec son système d’information :

* Poste de travail (navigateur, suite bureautique)
* Poste de travail (nécessité de composants connexes non disponibles et nécessaires à la solution applicative)
* La GPO du CHU de Caen
* Règles de sécurité firewall en vigueur sur l’établissement
* Règles de l’antivirus en vigueur sur l’établissement
* Règles de la directive NIS

En cas d’incompatibilité de la version applicative avec le système d’information du CHU de Caen (cf. règles ci-dessus), le titulaire doit proposer une solution de contournement afin de ne pas bloquer la mise à disposition des évolutions applicatives.

En cas d’impossibilité pour le titulaire de se conformer au système d’information du CHU de Caen, le titulaire s’engage à installer, sans surcoût, sa solution applicative sur les serveurs de l’établissement. L’opérateur garantit également la récupération entière et complète des données qu’il a hébergé sur ses serveurs lors de cette opération d’installation sur les serveurs de l’établissement.

# requêtage des données

Les données étant la propriété du CHU de Caen, le titulaire doit donner accès à ce dernier à des outils de requêtage de données et d’export de données.

Si ces outils ne sont pas proposés, le service support du titulaire inclue un service permettant de répondre à des demandes de requête d’extraction. Ce service est inclus dans l’abonnement ou la maintenance.

# automatisATION de taches

La titulaire propose avec l’hébergement externalisé la même capacité d’automatisation de taches qu’en cas d’hébergement sur les serveurs du CHU de Caen.

Le titulaire ne peut imposer des actions manuelles dans la solution applicative qui pourraient être automatisables.

# interfaceS

Un système d’échange de fichiers sécurisé est proposé par le titulaire.

Ce système d’échange ne doit pas être imposé au travers d’un tunnel VPN permanent avec du CHU de Caen. Il est mis en œuvre au travers de protocole d’échanges sécurisé type https tls1.3/ftps/sftp.

Un accès est donné au CHU de Caen une supervision des interfaces permettant de s’assurer que les traitements d’import et d’export ont bien fonctionnés. Si ce système n’est pas proposé alors la supervision est faite par le titulaire afin de s’assurer d’un bon fonctionnement de traitements d’interface. Dans ce cadre, un rapport d’exécution est envoyé au CHU de Caen à fréquence régulière (minimum une fois par mois).

# SUIVI DES LOGS

Le CHU de Caen doit, au travers de la directive NIS, avoir un accès complet aux logs de la solution applicative. Les logs sont conservés à minima 6 mois.

Un système d’échange de fichiers sécurisé est proposé par le titulaire pour récupérer ces logs de façon autonome.

Ce système d’échange ne doit pas être imposé au travers d’un tunnel VPN permanent avec l’établissement. Il est mis en œuvre au travers de protocole d’échanges sécurisé type https TLS1.3/ftps/sftp.

# Communication

La communication porte sur les évolutions et les incidents déclarés ainsi que la date estimée de mise à disposition au CHU de Caen.

Les nouvelles versions applicatives et les versions réglementaires sont communiquées en amont de leur livraison.

Les évolutions règlementaires sont communiquées avec le document associé et l’écart à prendre en compte pour le CHU de Caen.

De même tout incident connu et déclaré doit être communiqué par le titulaire avec sa solution de contournement et/ou sa date de résolution estimée.