C.A.I.H.

Partenariat d'Innovation « Alternative Open Source »

Programme Fonctionnel et Annexes – Version DCE v20251211

Les marques sont citées à titre indicatif pour description fonctionnelle ; des solutions équivalentes peuvent être proposées conformément à l'article R2111-12 du Code de la commande publique.

Table des matières

Préambule – Sensibilité des données traitées et justification des exigences en matière d'hébergement et de souveraineté

Nature des données traitées dans le cadre du présent marché

Le présent marché porte sur des prestations impliquant le traitement, l'hébergement et l'exploitation de **données à caractère personnel de santé**, au sens de la réglementation européenne et nationale en vigueur.

Conformément à l'article 4, §15 du Règlement (UE) 2016/679 (RGPD), constituent des données concernant la santé l'ensemble des informations relatives à l'état de santé physique ou mentale d'une personne physique, y compris celles liées à la prévention, au diagnostic, aux soins ou au suivi médico-administratif.

Ces données relèvent des **catégories particulières de données à caractère personnel** visées à l'article 9 du RGPD, dont le traitement est, par principe, interdit sauf exceptions strictement encadrées, et qui appellent un **niveau de protection renforcé**.

Niveau de risque et obligations renforcées de sécurité

En application de l'article 32 du RGPD, les responsables de traitement et leurs sous-traitants sont tenus de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Les données de santé présentent, par nature :

- un **risque élevé pour les droits et libertés fondamentales** des personnes concernées ;
- un **impact potentiellement grave** en cas de violation de données (atteinte à la vie privée, discrimination, préjudice moral, atteinte à la dignité, voire risques pour la prise en charge médicale) ;
- une **criticité accrue** du point de vue de la continuité de service, de l'intégrité et de la disponibilité des systèmes.

À ce titre, le pouvoir adjudicateur considère que la mise en œuvre de garanties de sécurité standards ne saurait être suffisante et qu'il est nécessaire d'exiger des **dispositifs de sécurité formalisés, audités et reconnus**, adaptés au secteur de la santé.

Justification de l'exigence de certification HDS

Conformément à l'article L.1111-8 du Code de la santé publique, toute activité d'hébergement de données de santé à caractère personnel pour le compte de tiers doit être réalisée par un prestataire disposant d'une **certification d'Hébergeur de Données de Santé (HDS)** en cours de validité.

Cette obligation :

- est **d'ordre public** ;
- s'impose indépendamment du rôle exact du prestataire (hébergeur, opérateur de plateforme, infogérant, etc.) dès lors qu'il participe à l'hébergement ou à l'administration de données de santé ;
- vise à garantir un niveau homogène et vérifiable de sécurité, de traçabilité, de gouvernance et de continuité d'activité.

L'exigence de certification HDS dans le cadre du présent marché ne constitue donc ni une exigence supplémentaire, ni une contrainte facultative, mais la **stricte application du cadre légal et réglementaire applicable aux données de santé**.

Enjeux de souveraineté et maîtrise juridique des traitements

Au-delà des exigences de sécurité opérationnelle, le pouvoir adjudicateur a conduit une analyse spécifique des **risques juridiques et stratégiques** pesant sur les traitements de données de santé, notamment au regard :

- des risques d'accès non autorisé par des autorités étrangères ;
- des législations extraterritoriales susceptibles de s'imposer à certains opérateurs, indépendamment de la localisation physique des données ;
- de la dépendance économique ou capitalistique à des entités non européennes.

Il est rappelé que la localisation des données sur le territoire de l'Union européenne ne suffit pas, à elle seule, à garantir une protection effective contre les risques d'ingérence juridique ou d'accès contraint.

Pour des données de santé, dont la sensibilité est particulièrement élevée, le pouvoir adjudicateur considère que ces risques ne peuvent être traités uniquement par des clauses contractuelles ou des engagements déclaratifs, mais nécessitent des **garanties structurelles** portant sur la gouvernance, la chaîne de sous-traitance et le contrôle capitalistique des opérateurs.

Justification des exigences alignées sur le référentiel SecNumCloud 3.2

Dans ce contexte, le pouvoir adjudicateur retient des exigences s'alignant sur les principes du référentiel SecNumCloud 3.2, notamment en matière :

- de maîtrise capitalistique et de gouvernance de l'opérateur ;
- d'immunité juridique vis-à-vis de législations extraterritoriales incompatibles avec le droit européen ;
- de contrôle effectif de la chaîne de sous-traitance ;
- de sécurité opérationnelle et organisationnelle renforcée.

Ces exigences sont considérées comme **nécessaires et proportionnées** au regard :

- de la nature des données traitées ;
- de la durée et de l'ampleur des traitements envisagés ;
- de la criticité des usages pour les établissements de santé ;
- des responsabilités légales incombant au pouvoir adjudicateur en tant que responsable de traitement ou responsable conjoint.

Principe de proportionnalité et lien avec l'objet du marché

Les exigences en matière de certification HDS et de garanties capitalistiques renforcées sont **directement liées à l'objet du marché** et à ses conditions d'exécution.

Elles visent exclusivement à :

- assurer la conformité réglementaire des traitements ;
- protéger efficacement les droits des personnes concernées ;
- garantir la continuité, la sécurité et la souveraineté des systèmes d'information de santé.

À ce titre, elles respectent pleinement les principes de **nécessité, de proportionnalité et de non-discrimination**, tels qu'issus tant du RGPD que du droit de la commande publique.

Préambule – Continuité d'activité, résilience systémique et nécessité d'une approche Open Source souveraine

Contexte de dépendance technologique et enjeux pour le secteur sanitaire

Les systèmes d'information des établissements sanitaires français reposent aujourd'hui de manière majoritaire sur des **écosystèmes technologiques propriétaires fortement intégrés**, en particulier autour des offres Microsoft, Oracle et Broadcom/VMWare, tant pour les infrastructures que pour les couches applicatives, d'annuaire, d'authentification, de virtualisation et de bases de données.

Cette concentration technologique, si elle a permis des gains d'industrialisation, engendre néanmoins une **dépendance systémique** caractérisée par :

- l'usage de **technologies homogènes** sur un très grand nombre d'établissements ;
- la centralisation des mécanismes d'administration et d'authentification ;
- le recours massif à des **datacenters et plateformes cloud reposant sur les mêmes socles techniques**.

Dans un contexte hospitalier, cette homogénéité constitue un **facteur de vulnérabilité collective**, incompatible avec les exigences de continuité d'activité et de résilience à long terme.

Limites des PCA fondés sur des écosystèmes technologiques dominants

Un Plan de Continuité d'Activité reposant sur les **mêmes technologies, les mêmes éditeurs et les mêmes plateformes cloud** que celles utilisées quotidiennement par les établissements ne permet pas de couvrir les scénarios de défaillance systémique, notamment :

- défaillance logicielle globale liée à une mise à jour centralisée ;
- indisponibilité étendue d'un service transverse critique (authentification, DNS, supervision) ;
- incident majeur affectant une plateforme cloud largement mutualisée ;
- vulnérabilité de sécurité exploitée à grande échelle sur un socle homogène.

Dans ces scénarios, la redondance géographique ou logique ne suffit plus : la dépendance à un **même écosystème technologique** peut entraîner une **indisponibilité simultanée** des environnements de production et de secours.

Principe de diversification systémique par l'Open Source souverain

Afin de répondre à ces risques, le pouvoir adjudicateur considère que la continuité d'activité dans le secteur sanitaire nécessite une **rupture technologique volontaire**, fondée sur des **socles Open Source souverains**, distincts des environnements majoritairement déployés dans les établissements.

Cette approche repose sur les principes suivants :

- utilisation de **technologies Open Source maîtrisées**, auditables et interopérables ;
- indépendance vis-à-vis des chaînes de dépendance propriétaires dominantes ;
- capacité à opérer des environnements critiques sans dépendance à des mécanismes d'activation, de licence ou de contrôle centralisé ;
- diversification effective des stacks logicielles, des outils d'administration et des modes d'exploitation.

L'objectif n'est pas l'exclusion de technologies existantes, mais la constitution d'un **socle alternatif résilient**, capable de prendre le relais en cas de défaillance majeure des environnements dominants.

Hébergement sur des datacenters distincts et non corrélés

Dans cette logique, le PCA attendu doit s'appuyer sur des **datacenters distincts**, répondant aux critères suivants :

- séparation physique et logique vis-à-vis des plateformes massivement utilisées par les établissements sanitaires ;
- indépendance des chaînes d'administration, de supervision et de support ;
- conformité aux exigences HDS et aux référentiels de sécurité applicables ;
- gouvernance et exploitation sous contrôle européen.

Cette séparation vise à éviter toute **corrélation de risques** entre les environnements opérationnels quotidiens des établissements et les environnements de continuité.

Proximité territoriale et maîtrise des flux réseau

Le pouvoir adjudicateur attache une importance particulière à la proximité territoriale des infrastructures de continuité avec les établissements sanitaires français.

Les candidats devront démontrer :

- une faible latence réseau, compatible avec les usages cliniques et médico-administratifs ;
- des liaisons fibre et des équipements réseau diversifiés ;
- l'absence de dépendance critique à des points de transit internationaux pour les services essentiels.

Cette proximité contribue à la robustesse opérationnelle, à la prévisibilité des performances et à la capacité de fonctionnement en situation de crise nationale.

Continuité d'activité, souveraineté et maîtrise opérationnelle

Le recours à un socle Open Source souverain permet :

- une maîtrise complète des mécanismes de continuité ;
- une capacité d'adaptation rapide en cas de crise ;
- une transparence accrue sur les mécanismes de sécurité et de bascule ;
- une limitation des risques juridiques et contractuels.

Dans le contexte hospitalier, la continuité d'activité ne peut reposer exclusivement sur des plateformes industrielles globales, mais doit intégrer des capacités autonomes, maîtrisées et pérennes, compatibles avec les exigences de souveraineté numérique.

Proportionnalité et finalité des exigences

Les exigences formulées au présent article sont directement liées :

- à la criticité des missions hospitalières ;
- à la sensibilité des données traitées ;
- aux obligations réglementaires en matière de sécurité et de continuité.

Elles visent à garantir que le PCA ne constitue pas une simple redondance technique, mais une **véritable stratégie de résilience**, reposant sur la diversification technologique et l'Open Source souverain comme leviers de sécurité collective.

Article préliminaire - Exigences minimales de la solution ALTERNATIVE

Généralités

Le Partenariat d'Innovation « Alternative Open Source » impose la création d'une suite complète de briques open source couvrant le Modern Workspace, l'identité numérique (ID CAIH), l'infrastructure/virtualisation, les postes de travail et l'IA. Toutes les briques doivent être interopérables, sécurisées, souveraines, réversibles et adaptées aux besoins de la CAIH dans l'Union européenne.

Exigences minimales en termes conformité numérique

Les solutions doivent être conformes au **RGPD**, à **NIS2**, aux référentiels **HDS**, **PGSSI-S** et aux doctrines ANS/DINUM. L'hébergement doit être opéré exclusivement en Europe sur des briques elles même Open Source, obligatoirement **HDS**, avec possibilité **SecNumCloud**. Aucun transfert ou administration hors UE n'est autorisé. La maîtrise des données, leur portabilité et l'usage de **formats ouverts** sont des exigences minimales.

- Le Modern Workspace doit intégrer une messagerie, un calendrier, une suite bureautique open source, la coédition, la GED, la visio, et des connecteurs compatibles avec Microsoft (WOPI, formats Office).
- La brique ID CAIH doit offrir un IAM complet (SSO, MFA, annuaire, rôles) et être obligatoirement interopérable avec Pro Santé Connect, CPS et e-CPS.
- L'infrastructure doit s'appuyer sur des hyperviseurs open source (Proxmox, oVirt, OpenStack), une orchestration souveraine, des bases PostgreSQL/MariaDB, un stockage chiffré, un PRA/PCA, une supervision complète et une migration progressive depuis les environnements propriétaires.
- La brique Postes & Parc doit fournir une distribution Linux hospitalière sécurisée avec télédistribution, MDM, supervision et ergonomie adaptée.
- La brique IA doit fournir un LLM Open Source souverain, un assistant conversationnel interne et une reconnaissance vocale, si possible adaptée au médical.

Toutes les briques doivent respecter les principes de **Security & Privacy by Design** : MFA, chiffrement, segmentation, journalisation certifiée, supervision temps réel, gestion de vulnérabilités, audits et tests d'intrusion. Le PAS doit intégrer une anticipation **post-quantique** (PQC) et un plan de migration cryptographique.

Le Titulaire doit produire des prototypes, POC, pilotes, kits de migration et de formation, ainsi qu'un catalogue de services industrialisés incluant hébergement souverain, MCO, RUN, support N2/N3, automatisation, supervision centralisée et documentation complète.

Il doit accompagner les éditeurs métiers (API, SDK, guides, ateliers), participer à la commercialisation sous pilotage CAIH, maintenir la neutralité commerciale et contribuer à la recherche de subventions nationales et européennes.

Enfin, un pilotage agile trimestriel est imposé, avec des indicateurs techniques, sécurité, usage, TCO, conformité et contributions open source, alimentant les comités CAIH et la feuille de route nationale.

Exigences minimales en termes de souveraineté

Le présent partenariat d'innovation est soumis à des exigences de souveraineté qui ne peuvent faire l'objet de négociations. Ces exigences se justifient en regard de la sensibilité particulière des données qui seront traitées dans la suite logicielle visée.

Les données particulièrement sensibles traitées dans le cadre du projet

Désignent les données traitées par le Titulaire, ses sous-traitants, et tous autres intermédiaires, dans le cadre de l'exécution du marché, surtout dans sa phase « Acquisition et maintien en condition opérationnelle », en routine.

La protection de ces informations s'impose pour la sécurité publique, la santé et la vie des personnes, conformément aux dispositions légales .

Définition du qualificatif souverain au sens du présent marché

Désigne, compte tenu de la sensibilité particulière des données qui seront traitées dans le cadre des prestations prévues au présent marché et de la nécessité de protéger ces informations pour la sécurité publique, la santé et la vie des personnes, tous services, actions et activités exigées du Titulaire au titre du présent marché devant s'exécuter dans les conditions assurant leur protection contre toute ingérence par des Etats tiers et contre tout accès par des autorités publiques d'Etats tiers non autorisé par le droit de l'Union européenne ou d'un Etat membre.

Définition de l'hébergement souverain

Désigne, compte tenu de la sensibilité particulière des données qui seront traitées dans le cadre des prestations prévues au présent marché et de la nécessité de protéger ces informations pour la sécurité publique, la santé et la vie des personnes, un hébergement mettant en œuvre des critères de sécurité et de protection des données garantissant la protection des données traitées ou stockées contre tout accès par des autorités publiques d'Etats tiers non autorisé par le droit de l'Union européenne ou d'un Etat membre.

L'hébergement des données sensibles dans des datacenters situés sur le territoire de l'UE est requis mais n'est pas suffisant pour répondre à l'exigence de souveraineté

Bien que nécessaire, la localisation sur le territoire de l'UE ne suffit pas à garantir la protection des données sensibles contre tout accès par des autorités publiques d'Etats tiers et contre toute ingérence par des Etats tiers.

C'est pourquoi la CAIH utilisera des critères de détention capitalistique pour qualifier le soumissionnaire et son offre initiale, ainsi que le Titulaire.

Les critères de détention capitalistique applicables au marché

Les critères pour garantir dans le cadre de l'exécution du présent marché, la protection des données contre tout accès par des autorités publiques d'Etats tiers et toute ingérence par des Etats tiers sont inspirés par le référentiel SecNumCloud 3.2.

Pour autant, si elle est fortement recommandée, la certification SecNumCloud 3.2 n'est pas exigée en tant que telle pour la passation et l'exécution du présent partenariat d'innovation, ni au stade de la candidature, ni au stade de l'offre.

Sans certification SecNumCloud 3.2, la CAIH utilisera les critères de conformité suivants pour garantir l'exigence d'immunité de la solution du Titulaire à l'égard des lois étrangères d'application extraterritoriale :

- Le siège statutaire, administration centrale et principal établissement du prestataire d'hébergement doivent être établis au sein d'un Etat membre de l'UE ;
- **Le capital social et les droits de vote dans la société du prestataire d'hébergement ne doivent pas être, directement ou indirectement : individuellement détenus à plus de 24%, et collectivement détenus à plus de 39% par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non-membre de l'UE.**
- **Si le capital détenu par ces entités tierces se présente sous la forme d'actions admises aux négociations sur un marché réglementé, ces entités tierces sont celles déclarées conformément au I de l'article L.233-7 du code de commerce. Ces entités tierces susmentionnées ne peuvent pas individuellement ou collectivement en vertu d'un contrat ou de clauses statutaires, disposer d'un droit de véto ou en vertu d'un contrat ou de clauses statutaires, désigner la majorité des membres des organes d'administration, de direction ou de surveillance du prestataire.**

En cas de recours par le prestataire d'hébergement, dans le cadre des services fournis à la CAIH, aux services d'une société tierce - y compris un sous-traitant - possédant son siège statutaire, administration centrale ou principal établissement au sein d'un État non-membre de l'UE ou appartenant ou étant contrôlée par une société tierce domiciliée en dehors l'UE, cette société tierce ne doit pas avoir la possibilité technique d'obtenir les données opérées au travers du service. Ces données visées sont celles qui sont confiées au prestataire d'hébergement par la CAIH ainsi que toutes données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, données manipulées par le *Software Defined Network*, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) comprenant des informations sur les commanditaires.

Le cas échéant, si la société tierce, sous-traitante, doit pouvoir accéder aux données d'une sensibilité particulière du projet pour assurer sa pleine exécution, les critères de détention capitalistique susvisés s'appliqueront au sous-traitant concerné.

Pour les besoins de la présence clause, la notion de contrôle est entendue comme étant celle mentionnée au II de l'article L233-3 du code de commerce.

Par ailleurs, toute société tierce à laquelle le prestataire d'hébergement recourt pour fournir tout ou partie du service rendu à la CAIH, doit garantir au prestataire d'hébergement une autonomie d'exploitation continue dans la fourniture des services d'informatique en nuage qu'il opère ou doit être qualifié SecNumCloud 3.2. Pour les besoins de la présente clause, la notion d'autonomie d'exploitation est entendue comme étant la capacité de maintenir la fourniture du service d'informatique en nuage en faisant appel aux compétences propres du prestataire d'hébergement ou en recourant à des prestations disponibles auprès d'au moins deux sociétés tierces.

Le respect de ces critères sera contrôlé tout au long de l'exécution du partenariat d'innovation.

Le Titulaire est tenu d'informer de tous changements susceptibles d'affecter sa qualification au regard des critères susvisés.

En cas de non-respect de cette obligation d'information ou de changement de situation impactant le respect des critères susmentionnés, la CAIH pourra décider de résilier le marché public dans les conditions prévues au CCAP.

Article 1 – Contexte général et finalité du partenariat d'innovation

Les établissements sanitaires et médico-sociaux adhérents à la CAIH utilisent aujourd'hui majoritairement des environnements logiciels et services propriétaires intégrés, dépendant d'éditeurs internationaux dominants.

Cette situation génère :

- Un coût global annuel d'exploitation (« run ») devenu difficilement soutenable ;
- Une dépendance structurelle à des technologies étrangères non maîtrisées ;
- Un risque de verrouillage technologique et de perte de souveraineté sur les données ;
- Une faible interopérabilité avec les initiatives open source nationales et européennes.

Le présent partenariat d'innovation a pour objet de concevoir, expérimenter, qualifier et industrialiser une suite logicielle open source couvrant les principaux besoins de l'environnement de travail, de l'identité numérique, de la virtualisation et de l'infrastructure hospitalière, y compris les bases de données et socles applicatifs.

L'objet du marché est le développement, la fourniture et l'accompagnement d'une solution collaborative, interopérable et conforme aux exigences de sécurité, de maîtrise et de réversibilité des données, garantissant l'autonomie opérationnelle et stratégique des acteurs publics.

Les solutions proposées devront obligatoirement :

- Assurer la maîtrise complète des données et des flux (hébergement, chiffrement, réversibilité, portabilité).
- Garantir la conformité au cadre réglementaire européen (RGPD, directives NIS2, schéma de certification européen).
- Favoriser l'indépendance technologique et l'interopérabilité, notamment par le recours à des standards ouverts et des composants logiciels libres.
- Être hébergées dans un environnement offrant des garanties équivalentes à celles requises pour les données de santé à caractère personnel (HDS, HDS + SecNumCloud).
- Permettre une gouvernance des données contrôlée par des acteurs soumis au droit européen.

Le niveau d'autonomie, de contrôle et de réversibilité offert à l'acheteur public dans l'exploitation de la solution constituera un élément d'appréciation.

Le titulaire favorise la mise à disposition en open source des développements spécifiques financés sur fonds publics (licence compatible EUPL v1.2, GPL ou équivalent).

L'objectif est d'obtenir, à périmètre fonctionnel équivalent :

- Une réduction significative des coûts de licences d'usage (infrastructure, postes de travail, messagerie, collaboration, virtualisation);
- Une baisse significative des coûts de services associés (support, maintenance, renouvellements) ;
- Une réduction durable du coût récurrent par utilisateur grâce à l'usage d'outils open source, d'une gestion unifiée des identités et d'une infrastructure serveur rationalisée (CAL et serveurs résiduels conservés uniquement pour les besoins techniques non substituables intégrés dans le calcul du gain).

Cette trajectoire vise à :

- Réinternaliser la maîtrise technique et budgétaire des composants essentiels du système d'information.
- Limiter la dépendance contractuelle vis-à-vis d'un fournisseur unique.
- Réallouer les économies générées à la cybersécurité, à la formation et à la modernisation du poste de travail hospitalier.
- Renforcer la sécurité, la résilience et la souveraineté des données.

L'objectif du présent Partenariat d'Innovation est la construction d'une offre Open Source stable, sécurisée et industrialisable globale et sa maintenance technique, fonctionnelle et sécuritaire et des livrables permettant leur essaimage accéléré.

En cas d'acquisition finale, le déploiement sera porté par le titulaire du partenariat d'innovation pour les établissements membres du groupement de commandes. Le déploiement généralisé auprès des autres adhérents de la CAIH sera assuré par les titulaires des marchés d'AMOE, d'AMOA de la CAIH.

L'ensemble des briques fonctionnelles doit être interopérable et validé dans sa globalité par le comité d'experts techniques et fonctionnels. Elles doivent obligatoirement être proposées On Premise comme en mode "IaaS/PaaS/SaaS". Elles devront co-exister avec l'environnement Microsoft omniprésent dans les SI de santé.

Les éditeurs de progiciels métiers hospitaliers (DPI, pharmacie, RH, finances, imagerie, etc.) sont associés au projet afin d'assurer la continuité applicative et la réversibilité de leurs solutions vers les briques open source déployées dans le cadre du partenariat.

Article 2 – Objectifs stratégiques

1. Optimisation durable des coûts d'exploitation ;
2. Réduction de la dépendance aux technologies propriétaires et non souveraines ;
3. Renforcement de la souveraineté numérique et de la maîtrise des infrastructures critiques ;
4. Conformité aux cadres réglementaires et de sécurité (RGPD, ANS, PGSSI-S, NIS 2, IA Act, Data Act);
5. Structuration d'une offre open source pérenne et industrialisée, validée par les autorités publiques ;
6. Développement d'un écosystème industriel open source santé, garantissant mutualisation et interopérabilité ;
7. Migration progressive des socles de virtualisation et de bases de données vers des alternatives ouvertes, performantes et maintenables à long terme ;
8. Mise en place d'un programme d'accompagnement des éditeurs métiers pour la migration technique et fonctionnelle de leurs solutions propriétaires vers des socles open

source interopérables, sécurisés et durables. Le titulaire participera, à ce titre, à un groupe open source éditeurs UNIHA CAIH.

L'objectif est de migrer vers la solution coconstruite plus de 10% du parc des adhérents de la CAIH (soit 100 000 postes et 250 000 d'utilisateurs) depuis les logiciels propriétaires vers la solution globale Open Source d'ici 2030 au plus tard.

Article 3 – Description fonctionnelle des besoins

Les besoins sont structurés autour de cinq briques principales à co-construire en sécurity by design :

- Modern Workspace,
- Gestion des identités,
- Infrastructure,
- Parc & postes de travail,
- et Intelligence Artificielle.

Les éditeurs métiers participeront aux travaux d'interopérabilité (API, formats d'échange, macros, scripts) afin de garantir la compatibilité de leurs outils avec les briques open source développées.

Leur participation aux ateliers de conception et aux hackathons permettra d'adapter leurs produits et d'en faciliter la migration progressive.

Les solutions proposées devront démontrer leur capacité à :

- Maîtrise et réversibilité des données
- Fournir un plan de réversibilité complet (format, durée, coûts, procédures).
- Garantir la portabilité des données dans des formats ouverts (ODF, JSON, CSV, etc.).
    - Indicateur : taux de composants utilisant des standards ouverts ≥ 90 %[1].
- Localisation et contrôle juridique
    - Hébergement certifié HDS dans l'Union européenne par un prestataire soumis exclusivement au droit européen.
    - Administration exclusivement depuis un pays de l'Union Européenne
    - Interdiction de transfert ou de transit de données vers des pays tiers non couverts par une décision d'adéquation de la Commission européenne.
    - La proposition d'un hébergement optionnel qualifié SecNumCloud est un élément d'appréciation de l'offre.
- Transparence et auditabilité

[1] 100% Open Source avec tolérance de briques propriétaires pour assurer l'interopérabilité avec l'environnement Microsoft. La minimisation de l'utilisation de briques propriétaires est une priorité et un élément d'appréciation de l'offre.

    - Fournir la documentation technique, les journaux d'accès et les codes sources critiques sur demande de l'autorité contractante.
    - Indicateur : taux de composants open source; auditabilité du code garantie par un tiers agréé.
- Interopérabilité et indépendance technologique
    - Utilisation d'API ouvertes documentées (REST, GraphQL, etc.).
- Compatibilité avec les principaux formats bureautiques et protocoles de messagerie.
    - Indicateur : conformité à au moins 3 standards internationaux reconnus (ISO/IEC, ETSI, W3C, OASIS...).
- Respect du RGPD, de la directive NIS2 et du cadre européen de cybersécurité
    - Indicateur : présence d'un DPO identifié et d'un plan de conformité RGPD validé.
- Formation des équipe IT des établissements du groupement de commande (et uniquement eux) : Pour chacune des briques logiciel le candidat devra démontrer sa capacité à former et accompagner au changement les équipes IT et, pour les briques directement utilisées par les professionnels de santé, proposer des modules d'apprentissages adaptés.

3.1. Brique « Espace de travail collaboratif » (Modern Workspace)

Le titulaire proposera une suite collaborative intégrée comprenant :

- Une suite bureautique (traitement de texte, tableur, présentation) ;
- Des outils de messagerie, calendrier et gestion des contacts ;
- Des fonctionnalités de coédition et partage documentaire sécurisé ;
- Une gestion électronique des documents (GED) ;
- Une intégration privilégiée d'une des solutions institutionnelles françaises ou européennes : LibreOffice, OnlyOffice, BlueMind, Nextcloud, Jitsi, Mattermost, WOPI.

La suite bureautique devra être hébergée chez l'établissement de santé, et de façon optionnelle, proposée en mode SaaS.

Il conviendra de proposer une solution permettant de contourner l'utilisation locale de Microsoft Word par les progiciels métiers. Par exemple, lorsqu'une application métier comme le DPI nécessite d'ouvrir winword.exe afin d'éditer le compte-rendu de sortie du patient.

La CAIH privilégie la collaboration avec la DINUM concernant cette brique.

3.2. Brique « Gestion des identités – ID CAIH »

Le titulaire concevra un système de gestion des identités et des accès (IAM) open source comprenant :

- Un annuaire centralisé des identités ;
- Une gestion des rôles et des habilitations ;
- Une authentification forte et fédérée (MFA/IAM/SSO);
- Une interopérabilité obligatoire avec Pro Santé Connect, CPS et e-CPS / Hospiconnect;
- Une conformité stricte aux cadres d'interopérabilité de l'ANS et de la DNS.

Cette brique devra être pleinement fonctionnelle « On premise », et avoir des extensions hybrides et cloud permettant une gestion unique de l'identité quel que soit le service numérique requis par l'utilisateur final

3.3. Brique « Infrastructure hybride, virtualisation, serveurs et bases de données »

Le titulaire proposera une infrastructure souveraine, modulaire et ouverte, couvrant :

- Les services d'infrastructure (fichiers, impression, stockage, supervision) ;

- Une couche de virtualisation et d'orchestration basée sur une ou plusieurs des technologies ouvertes (Proxmox VE, oVirt, KVM, Xen Project, OpenStack, ou équivalents) ;
- Une gestion de clusters et d'allocation dynamique des ressources pour environnements hospitaliers à haute disponibilité ;
- Une migration progressive des socles virtualisés propriétaires vers des environnements ouverts interopérables ;
- Des bases de données open source relationnelles et objets (PostgreSQL, MariaDB, MySQL, CouchDB) assurant la compatibilité fonctionnelle avec les environnements propriétaires actuels ;
- Une interopérabilité complète avec les outils d'administration et d'automatisation (Ansible, Terraform, GLPI) ;
- La gestion unifiée de la performance, de la sécurité et de la supervision sur l'ensemble des couches virtualisées et des moteurs de données.

3.4. Brique « Gestion du parc et postes de travail »

Le titulaire proposera :

- Une distribution open source qualifiée et sécurisée adaptée au contexte hospitalier ;
- Des outils de gestion de parc, télédistribution, supervision et métrologie ;
- Le maintien d'une ergonomie proche des environnements actuels ;
- Une intégration simplifiée dans les systèmes de supervision et d'assistance mutualisés.

3.5. Brique « Intelligence artificielle »

Le titulaire proposera un service d'intelligence artificielle conversationnelle open source (LLM) opérant dans un environnement souverain et maîtrisé, garantissant la confidentialité des données et la maîtrise des modèles utilisés.

Elle est complétée par une fonctionnalité de reconnaissance vocale avec, si possible, une extension dans le domaine médicale

L'objectif est de retenir la distribution Open Source et les composants techniques. Leurs personnalisations seront initialement limitées à l'intégration dans les autres briques.

Article 4 – Sécurité, conformité et hébergement

Le titulaire doit fournir un plan garantissant la continuité de service sans dépendance exclusive à un fournisseur tiers.

Le titulaire devra élaborer, mettre en œuvre et maintenir un Plan d'Assurance Sécurité (PAS) couvrant l'ensemble du périmètre du partenariat d'innovation.

Ce plan visera à garantir un niveau de sécurité conforme aux exigences hospitalières, réglementaires et stratégiques de la CAIH, et à anticiper les évolutions liées aux nouvelles menaces technologiques, notamment l'informatique quantique.

Les éditeurs de progiciels métiers sont consultés pour garantir la sécurité applicative et la compatibilité de leurs interfaces avec les mécanismes de chiffrement, de supervision et de migration post-quantique définis dans le PAS.

Ils appuient les industriels pour la validation sécurité applicative et la conformité RGPD/HDS.

4.1. Cadre normatif et réglementaire

Le PAS devra assurer :

- La conformité aux référentiels de l'ANS (PGSSI-S, doctrine technique, référentiels d'interopérabilité et d'identité numérique) ;
- Le respect du Règlement Général sur la Protection des Données (RGPD) et des obligations applicables aux hébergeurs de données de santé (HDS) ;
- La conformité à la directive NIS 2 en matière de gouvernance, d'analyse de risque, de journalisation, et de notification des incidents de sécurité ;
- La prise en compte des bonnes pratiques de l'ANSSI et du guide d'hygiène informatique.

L'hébergement des solutions devra s'effectuer sur des infrastructures souveraines certifiées HDS et, - de façon optionnelle- SecNumCloud, opérées en France ou dans l'Union européenne.

4.2. Principes de sécurité by design

Le titulaire appliquera les principes de Security & Privacy by Design et by Default à chaque étape du projet, incluant :

- Une approche de sécurisation par défaut de tous les composants logiciels et matériels ;
- La segmentation des environnements (développement, intégration, production) ;
- la traçabilité et l'auditabilité de toutes les actions et des flux de données ;
- La limitation stricte des privilèges et l'application du principe du moindre droit ;
- La mise en œuvre d'un dispositif de supervision continue des journaux et événements de sécurité ;
- L'intégration d'un plan de gestion des vulnérabilités et d'un processus documenté de patch management.

4.3. Anticipation des risques liés à l'informatique quantique

Le titulaire intégrera dans son PAS une analyse prospective des risques cyber induits par l'émergence de l'informatique quantique, notamment sur la cryptographie asymétrique et la pérennité des données chiffrées.

Cette anticipation inclura :

- La réalisation d'une cartographie des algorithmes sensibles (RSA, ECC, TLS, S/MIME, etc.) exposés à une obsolescence post-quantique ;
- L'évaluation des impacts de la cryptanalyse quantique sur les mécanismes de chiffrement, d'authentification et de signature électronique utilisés dans les solutions proposées ;
- La définition d'un plan de migration vers des algorithmes post-quantiques (PQ) validés par l'ANSSI et alignés sur les standards du NIST PQC ;
- La mise en place d'une veille technologique active sur les évolutions normatives (ETSI, ISO, NIST) et les stratégies nationales et européennes de cybersécurité quantique ;
- L'implémentation, dans les prototypes et versions stabilisées, de mécanismes de chiffrement hybrides combinant les approches classiques et post-quantiques afin d'assurer une transition sécurisée.

Le PAS devra préciser la stratégie de bascule vers des modules cryptographiques post-quantiques, incluant les conditions de compatibilité ascendante, de test et de qualification dans les environnements hospitaliers.

4.5. Gouvernance et reporting sécurité

Le titulaire mettra en place une gouvernance sécurité dédiée comprenant :

- Un RSSI projet identifié ;
- Des revues de sécurité trimestrielles en comité technique ;
- Un rapport de conformité semestriel transmis à la CAIH et aux autorités compétentes ;
- Des tests de pénétration et audits indépendants à chaque phase clé (prototype et industrialisation) ;
- La traçabilité de l'ensemble des incidents, alertes et vulnérabilités corrigées.
- Un registre sécurité devra être maintenu tout au long du projet, incluant la cartographie des risques, les mesures de protection mises en œuvre, les résultats d'audit et les actions correctives.

4.6. Livrables attendus

Plan d'Assurance Sécurité (PAS) initial et ses mises à jour semestrielles ;

- Registre de gestion des vulnérabilités et incidents ;
- Plan de migration cryptographique post-quantique ;
- Rapports d'audit et de test de pénétration ;
- Rapport de conformité RGPD / HDS / NIS2.

Article 5 – Service Support et accompagnement

L'offre du le candidat devra démontrer la capacité à accompagner les équipes IT vers une formation et une expertise des solutions Open Source proposées.

A partir des mises en production réelle chez nos adhérents, le titulaire mettra en œuvre un centre de services unique pour la gestion des incidents, un support technique de niveau 2 et 3, des référentiels de configuration validés, et un accompagnement des DSI.

Selon la sensibilité des actifs en production, le support initialement demandé en 5j/7 8h/24 devra pouvoir évoluer vers un support 7/24 avec prise en charge sous 4 heures.

Le démarrage du support, son extension en 7/24 seront décidées par le comité de pilotage

Article 6 – Phasage du partenariat et livrables attendus (S2 2026 /2027)

Le partenariat d'innovation est organisé en 2 phases :

La Phase R&D, elle-même composée de 3 séquences :

Séquence 1 : Conception & développement

Séquence 2: Prototypage et expérimentation

Séquence 3 : Pré-industrialisation

La Phase Acquisition

Chacune des phases et des séquences fera l'objet d'une décision d'admission dans les conditions prévues à l'article 7.1 du CCAP. Le passage d'une séquence à une autre, ainsi que d'une phase à une autre, fera l'objet d'une demande par le Titulaire et sera validé par décision notifiée par la CAIH.. Le démarrage d'une phase ne vaut pas admission tacite de la phase précédente.

6.1. Phase R&D

Séquence 1 : Conception et développement

Objectifs généraux

La Séquence 1 constitue la première étape de la Phase R&D. Elle vise à définir l'architecture cible, les choix technologiques, les trajectoires de migration et à produire les premiers livrables techniques majeurs permettant d'amorcer le prototypage.

La Séquence 1 doit produire :

- l'architecture cible complète ;
- les distributions open source personnalisées ;
- l'initialisation des services en ligne selon le calendrier de l'offre ;
- les prototypes initiaux des cinq briques fonctionnelles ;
- les kits de migration (technique + organisationnelle) ;
- le PAS initial et les dossiers sécurité ;
- les premières documentations, chabots et kits de formation.

À l'issue de la séquence 1, le titulaire devra remettre les livrables suivants :

L1. Livrables de conception et de cadrage stratégique & fonctionnel

L1.1. Architecture cible et socles techniques

- Architecture cible globale validée par le groupement de commande couvrant les 5 briques :
  Modern Workspace, ID CAIH, Infrastructure & Virtualisation, Parc & Postes, IA.
- Cartographie détaillée des modules, composants, dépendances et interfaces inter-briques.

L1.2. Personnalisation et qualification des distributions open source

- Sélection d'une ou plusieurs distributions adaptées au contexte hospitalier.
- Personnalisation initiale (ergonomie, sécurité, compatibilité applicative).
- Catalogue des modules intégrés (bureautique, gestion de parc, outils de supervision…).
- Premiers ISO ou images « preview » destinées aux tests futurs.

L1.3. Spécifications fonctionnelles détaillées

- Parcours utilisateurs cibles (métiers, DSI, RSSI).
- Exigences fonctionnelles et de sécurité transversalement aux briques (RGPD, NIS2, HDS, PGSSI-S).
- Définition des cas d'usage prioritaires du partenariat (coédition, authentification PSC, migration VM, etc.).

L1.4. Trajectoires de migration initiales

- Roadmap de migration vers les socles souverains : virtualisation, bases de données, annuaires, Workspace.
- Analyse des coexistences nécessaires avec Microsoft (interopérabilité, formats, protocoles).
- Définition des scénarios de réversibilité et de portabilité.

L2. Livrables techniques de première mise à disposition

L2.1. Premiers modules techniques « pré-prototypes » dans un bac à sable numérique

Pour chaque brique, le titulaire devra produire un premier ensemble de composants opérationnels :

- **Modern Workspace** :
  - Configuration de base d'un service de messagerie / calendrier / GED open source.
  - Intégration initiale d'une suite bureautique.
  - Connecteurs de coédition (WOPI ou équivalents).
- **ID CAIH** (IAM open source) :
  - Annuaire central initial.

    - Maquette du SSO / MFA.
    - Début d'intégration PSC, CPS, e-CPS.
- **Infrastructure & Virtualisation** :
    - Premier cluster virtualisation / stockage / réseau en environnement de test.
    - Connexion initiale avec les moteurs de bases de données open source.
- **Parc & Postes** :
    - Prototype de distribution hospitalière.
    - Démonstrateur de télédistribution / supervision de base.
- **Intelligence artificielle** :
    - Prototype de LLM open source dans un environnement souverain.
    - Démonstrateur de reconnaissance vocale.

L2.2. Initialisation des services en ligne selon le calendrier de l'offre

- Mise en ligne des premiers services (workspace, ID, virtualisation, IA) dans un environnement démo.
- Configuration des accès équipes CAIH / établissements experts.
- Jeux de données simulés pour tests.

L2.3. Premiers mécanismes de sécurité by design

- Application initiale des principes PAS : MFA, journaux, chiffrement, segmentation.
- Début de cartographie des vulnérabilités.

L3. Livrables « kits » structurants

L3.1. Kit de migration technique

- Outillage de migration des environnements virtualisés (VM → Proxmox/KVM/…).
- Premiers scripts d'extraction / migration bases de données (Oracle/SQL → PostgreSQL/MariaDB).
- Outillage de coexistence : Hyperviseur, stockage, annuaires, connecteurs API, formats bureautiques.

L3.2. Kit de migration organisationnelle & conduite du changement

- Guide de transition pour les DSI / RSI / RSSI.
- Identification des impacts métiers (ergonomie, formats bureautiques, workflows).
- Premières recommandations pour la migration du poste de travail hospitalier.

L4. Livrables sécurité, conformité & hébergement

L4.1. Plan d'Assurance Sécurité (PAS) – Version initiale

- Alignement RGPD, HDS, PGSSI-S, NIS2.

- Analyse des risques quantiques et premières recommandations PQC.

L4.2. Plan d'hébergement souverain initial

- Architecture HDS / SecNumCloud
- Modalités d'administration 100 % européenne.

L5. Livrables formation et documentation

L5.1. Kits de formation IT

- Installation, configuration, supervision.
- Premiers supports standardisés pour les DSI.

L5.2. Kits de formation utilisateurs

- Guides de prise en main workspace.
- Tutoriels ergonomie / nouveaux usages.

L5.3. Documentation de cadrage

- Document d'architecture générale.
- Dossier d'interopérabilité.
- Guides API / flux principaux.
- Protocole de tests techniques pour la future Séquence 2.

Validation intermédiaire avant passage en séquence 2

Admission validant décision de poursuivre

Séquence 2 : Prototypage et expérimentation

Objectif général

La Séquence 2 vise à transformer les livrables de la Séquence 1 en solutions opérationnelles, testées et validées dans des environnements hospitaliers réels.
Elle doit démontrer :

- la **faisabilité opérationnelle** des briques open source,
- leur **interopérabilité** avec les environnements SI hospitaliers (incluant Microsoft),
- leur **performance**, **ergonomie** et **robustesse**,
- leur **conformité réglementaire** (RGPD, HDS, NIS 2, PGSSI-S),
- leur **généralisation** à l'échelle de plusieurs centaines d'établissements.

Cette séquence prépare directement la pré-industrialisation (Séquence 3).

Démarche générale

La démarche s'appuie sur un enchaînement progressif :

1. **POC techniques et fonctionnels** dans des environnements contrôlés, à partir des pré-prototypes de la Séquence 1 ;
2. **Analyse détaillée des retours**, correctifs techniques, ergonomiques et sécurité ;
3. **Consolidation des briques** pour atteindre une version pilote ;
4. **Déploiement de sites pilotes par thématique** au sein d'établissements experts ;
5. **Évaluation croisée** (technique, fonctionnelle, réglementaire, économique) ;
6. **Préparation du passage en pré-industrialisation**.

Les POC et pilotes sont potentiellement réalisés **avec les éditeurs métiers**, afin de garantir l'interopérabilité applicative et la continuité des usages professionnels.

Objectifs spécifiques

La Séquence 2 a pour objectifs de :

- Transformer les prototypes d'architecture en **solutions fonctionnelles opérationnelles** ;
- Expérimenter les briques dans des environnements hospitaliers réels : messagerie, collaboratif, ID CAIH, virtualisation, infrastructure, supervision, IA ;
- Corriger les anomalies issues des POC et ajuster les composants open source ;
- Valider l'**interopérabilité technique et applicative**, incluant les dépendances Microsoft (formats, protocoles, connecteurs) ;
- Vérifier la **conformité réglementaire** et mettre à jour le PAS (évaluations RGPD/HDS/NIS 2, sécurité post-quantique) ;
- Évaluer l'**ergonomie**, l'adoption utilisateur et la réversibilité ;
- Consolider le **modèle économique** (TCO, ROI, coûts réels POC/pilotes) ;
- Produire la documentation technique, sécurité, fonctionnelle et utilisateur et un chat bot dédié par cible utilisateur;
- Préparer le passage en Séquence 3 (pré-industrialisation).

Structuration de la phase

La Séquence 2 est structurée autour de **trois ateliers / hackathons**, suivis d'une campagne de **sites pilotes thématiques**.

Hackathon « Usages » et POC fonctionnels

Objectifs :

- Déployer les premiers prototypes de : workspace, ID CAIH, postes & parc, IA, virtualisation ;
- Tester les fonctionnalités clés ;
- Recueillir les retours utilisateurs (ergonomie, compréhension, parcours, contraintes métiers) ;
- Identifier les **écarts d'usage** avec les environnements actuels (Microsoft et progiciels métiers) ;
- Produire un **rapport d'usages** consolidé, incluant priorisation des améliorations.

Livrables intermédiaires :

- Scénarios d'usage ;
- Scores d'ergonomie ;
- Tests d'intégration avec éditeurs métiers ;
- Préconisations d'amélioration à intégrer dans la version pilote.

Hackathon « Technologies » et POC techniques

Objectifs :

- Tester l'interopérabilité entre briques principales :
  - workspace ↔ ID CAIH (IAM, SSO, MFA) ;
  - virtualisation ↔ bases de données ↔ supervision ;
  - IA ↔ sécurité / conformité RGPD ;
- Tester les connecteurs avec les éditeurs métiers (API, macros, formats, WOPI) ;
- Vérifier les performances : latence, montée en charge, scalabilité ;
- Réaliser des **tests de résilience**, reprise après incident, portabilité ;
- Mettre à jour le **Plan d'Assurance Sécurité (PAS)** : journalisation, chiffrement, MFA, segmentation, sécurité post-quantique ;
- Exécuter des **audits de sécurité** (interne + tiers indépendant si requis) ;
- Intégrer les correctifs avant déploiement pilote.

Livrables intermédiaires :

- Rapports de tests techniques ;
- Rapport de performance ;
- Mise à jour du PAS ;

- Correctifs applicatifs et sécurité.

Hackathon « Modélisation financière et plan de généralisation pilote »

Objectifs :

- Analyser les **coûts réels** des POC ;
- Mettre à jour la **modélisation économique** :
  - coûts de déploiement pilote,
  - coûts d'exploitation (RUN),
  - gains attendus et ROI,
  - comparaison au scénario propriétaire ;
- Construire le **modèle économique cible** et la trajectoire de migration ;
- Définir le **plan de lancement des sites pilotes** : calendrier, ressources, prérequis, risques.

Livrables intermédiaires :

- Modélisation financière actualisée ;
- Analyse des coûts & gains ;
- Plan détaillé de généralisation pilote.

Validation intermédiaire avant expérimentation des sites pilotes **Admission validant décision de poursuivre**

Expérimentation sur les sites pilotes thématiques

Après consolidation finale des POC :

- Chaque brique est déployée au sein d'un ou plusieurs **établissements experts volontaires**.
- Les sites pilotes sont organisés par thématique :
  - **Modern Workspace** (suite collaborative, messagerie, coédition, GED) ;
  - **ID CAIH** (identité fédérée, PSC/CPS/e-CPS, SSO, MFA) ;
  - **Infrastructure & Virtualisation** (hyperviseurs souverains, stockage, bases open source, supervision) ;
  - **Postes & Parc** (distribution hospitalière Linux, télédistribution, MDM, ergonomie) ;
  - **Intelligence Artificielle** (assistant conversationnel, reconnaissance vocale, sécurité IA).

- Les éditeurs métiers volontaires participent éventuellement aux tests d'intégration et valident la compatibilité applicative.
- Un **comité inter-pilotes CAIH** coordonne l'ensemble des pilotes et consolide les résultats.

Les pilotes permettent de valider :

- la performance,
- la sécurité,
- la conformité réglementaire,
- la facilité de déploiement et de maintenance,
- la satisfaction et l'adhésion des utilisateurs,
- la capacité de réversibilité.

Livrables attendus

À l'issue de la Séquence 2, le titulaire fournit un **dossier complet**, comprenant au minimum :

S2L1. Livrables techniques

- Prototypes consolidés et validés (version pilote).
- Dossiers techniques détaillés pour chaque site pilote : configurations, dépendances, prérequis, scénarios de déploiement.
- Rapports de performance : latence, disponibilité, scalabilité, résilience.
- Rapports de sécurité et conformité : RGPD, HDS, NIS 2, PAS mis à jour.
- Dossiers d'interopérabilité : Microsoft, ANS, DINUM, éditeurs métiers.
- Registre de sécurité (incidents, vulnérabilités, correctifs).

S2L2. Livrables fonctionnels et d'usage

- Rapport consolidé des retours POC + pilotes (usages, ergonomie, adoption).
- Grilles d'évaluation fonctionnelle par thématique.
- Tableau de suivi des incidents et correctifs.
- Plan d'amélioration continue avant industrialisation.

S2L3. Livrables économiques

- Modélisation financière actualisée (POC + pilotes).
- Analyse TCO et ROI consolidée.
- Bilan R&D complémentaire : investissements à prévoir pour la Séquence 3.

S2L4. Livrables organisationnels et de gouvernance

- Comptes rendus des trois hackathons et des comités inter-pilotes.
- Planning consolidé de la Séquence 3 avec points de bascule.
- Tableau de bord global des expérimentations (maturité, performance, sécurité, adoption).

S2L5. Livrables de validation

- **Dossier de Synthèse Phase 2** :
  - résultats des POC,
  - résultats des sites pilotes,
  - conformité, performance, sécurité, usages,
  - ajustements avant pré-industrialisation.
- **Restitution officielle en Comité Technique CAIH**, incluant :
  - présentation PowerPoint,
  - note de synthèse ≤ 20 pages.

Validation intermédiaire avant passage en séquence 3 **(Admission valant décision de poursuivre)**

Séquence 3 : Pré-industrialisation

Objectif général

La Séquence 3 constitue la phase de **pré-industrialisation** du Partenariat d'Innovation « Alternative Open Source ».
Elle vise à stabiliser, sécuriser et packager les briques open source validées lors des pilotes, à préparer leur **déploiement national**, et à construire un **modèle d'hébergement souverain, sécurisé et industrialisé**, conforme aux exigences de la CAIH.

Elle doit permettre :

- la **stabilisation technique** des briques validées (workspace, identité, infra, postes, IA),
- la constitution des **kits de déploiement et d'exploitation**,
- la définition d'un **service d'hébergement souverain mutualisé**,
- la formalisation du **service MCO / Évolution continue / Support N2–N3**,
- et la préparation de la **généralisation progressive** dans les établissements CAIH.

Les déploiements, hors établissements du groupement de commande, seront ensuite assurés par des prestataires AMOA/AMOE spécialisés santé, sur la base des kits produits dans cette séquence.

Objectifs spécifiques

La Séquence 3 doit :

- Finaliser les versions **stabilisées, sécurisées et industrialisées** des briques open source ;
- Industrialiser les livrables (documentation, packaging, automatisation, supervision, PRA/PCA) ;
- Construire l'ensemble des **services d'hébergement souverain**, incluant :
  - Hébergement Cloud souverain (SecNumCloud, HDS),
  - modes mutualisé / dédié ou hybride,
  - services de sécurité managés,
  - journalisation et preuve numérique,
  - PRA/PCA industrialisé ;
- Publier un **catalogue de services d'hébergement et d'exploitation**, incluant les niveaux de service, SLA, capacités et métriques ;
- Produire les **kits AMOA/AMOE** pour les intégrateurs santé ;
- Formaliser le service **MCO / Support N2/N3 / Évolutions réglementaires** ;
- Préparer la **montée en compétence**, la réversibilité et l'autonomie des prestataires CAIH ;
- Assurer la conformité complète RGPD / HDS / NIS2 / ANSSI.

Structuration de la Séquence 3

La séquence s'articule autour de trois axes, complétés par la construction du service d'hébergement mutualisé.

Le titulaire proposera une méthodologie visant à répondre aux objectifs et livrables attendus suivants :

3.1. « Intégration & industrialisation technique »

Objectifs

- Finalisation et stabilisation des architectures logicielles ;
- Normalisation des référentiels de configuration ;
- **Industrialisation complète des procédures de déploiement automatisé** : Ansible, Terraform, Helm, GitOps, images ISO/OVA/containers ;
- Packaging des briques validées sous forme de **kits installables reproductibles** :
  - Workspace (suite collaborative, coédition, GED, visio, messagerie),
  - ID CAIH (fédération d'identité, PSC/CPS/e-CPS, MFA),

  - Infrastructure & Virtualisation (hyperviseurs open source, stockage, bases),
  - Supervision (OpenObserve/ELK/Prometheus/Grafana),
  - Parc & Postes (distribution hospitalière Linux, MDM),
  - IA (LLM souverain, outils métiers, copilote hospitalier),
- **Tests d'intégration croisée** (brique↔brique + éditeurs métiers) ;
- **Validation de la conformité RGPD, HDS, NIS2** via un audit indépendant.

Livrables intermédiaires

- Kits techniques versionnés ;
- Images reproductibles ;
- Rapports techniques & sécurité ;
- PAS finalisé.

3.2. « Transfert opérationnel & kits AMOA / AMOE »

Objectifs

- Production des **kits de transfert** pour les sociétés AMOA/AMOE :

Kits AMOE (techniques)

- installation, configuration, automatisation, durcissement ;
- exploitation, supervision, sécurité, PRA/PCA ;
- qualification, tests, checklists, monitoring ;
- processus MCO ;

Kits AMOA (fonctionnels)

- guides utilisateurs ;
- supports de formation ;
- parcours métiers et repères "avant/après" ;
- procédures de migration ;
- modèles de communication interne ;
- Formation et certification des AMOA/AMOE ;
- Co-validation avec les intégrateurs et éditeurs métiers ;
- Structuration du **référentiel de supervision et d'alerting partagé**.

Livrables intermédiaires

- Documentation AMOA/AMOE ;
- Plan de formation ;
- Référentiel supervision-alerting ;
- Plans de migration et méthodes.

3.3. « Service MCO & Support mutualisé »

Objectifs

- Conception complète du **service MCO mutualisé national**, incluant :
  - correctifs, patchs de sécurité, mises à jour majeures,
  - évolutions réglementaires (HDS, NIS2),
  - évolutions fonctionnelles (workspace, identité, IA…),
  - support N2 pour établissements + support N3 pour les intégrateurs ;
- Définition des **indicateurs et SLA** du service CAIH :
  - disponibilité cible ≥ 99,8 % ;
  - délais de prise en charge : N2 ≤ 4h ouvrées / N3 ≤ 8h ouvrées ;
  - publication mensuelle des correctifs sécurité ;
  - publication trimestrielle des versions majeures ;
- Construction du **référentiel national RUN** : journalisation, gestion incidents, sécurité, vulnérabilités ;
- Préparation de la contractualisation des prestataires MCO.

Livrables intermédiaires

- Catalogue MCO ;
- SLA et métriques ;
- Référentiel RUN ;
- Dossiers d'exploitation durcis.

Services d'hébergement attendus

« Hébergement souverain » désigne, compte tenu de la sensibilité particulière des données qui seront traitées dans le cadre des prestations prévues au présent marché, un hébergement mettant en œuvre des critères de sécurité et de protection des données garantissant la protection des données traitées ou stockées contre tout accès par des autorités publiques d'Etats tiers non autorisé par le droit de l'Union européenne ou d'un Etat membre.

Le titulaire doit fournir un **hébergement souverain**, certifié et conforme, comprenant les services suivants :

Hébergement souverain

- Offre SecNumCloud ou équivalent européen non soumis à extraterritorialité ;
- Certification HDS (ou équivalent reconnu) pour les données de santé ;
- Hébergement dans datacenters situés en France ou Union Européenne, opérés par un acteur européen ou contrôlé par un capital européen.

Services d'infrastructure

- Machines virtuelles, clusters virtualisés, stockage chiffré, réseau isolé ;
- Services de bases de données open source managées ;
- Object storage S3-compatible souverain ;
- Services réseau : VPN site-à-site, VLAN, firewall, reverse proxy, WAF.

Services de sécurité managés

- MFA, SSO, durcissement système ;
- Journalisation certifiée (tamponnée, horodatée) ;
- SIEM fédéré ;
- SOC 24/7 optionnel ;
- Détection d'intrusions (IDS/IPS) ;
- Gestion des vulnérabilités continue ;
- Réponse à incident.

Disponibilité, continuité et réversibilité

- PCA (haute disponibilité multi-zone) ;
- PRA (reprise d'activité < 4h) ;
- Réversibilité complète ;
  export VM, conteneurs, bases, fichiers, journaux, configurations ;
- Portabilité vers un autre opérateur souverain.

Supervision & monitoring

- Plateforme centralisée :
  - métriques, logs, traces, audit ;
  - tableaux de bord CAIH ;
  - alerting N2/N3 ;

Catalogue de services associés

S3A. Services d'hébergement & infrastructure

- Environnements mutualisés sécurisés ;
- Hébergement dédié haute performance ;
- Hébergement hybride (on-prem + cloud souverain) ;
- Sauvegarde managée (3-2-1) ;
- PRA/PCA ;

- Stockage objet, blocs, bases.

S3B. Services de sécurité

- Audit sécurité annuel + audit continu ;
- Durcissement OS et middleware ;
- MFA, SSO, FedID PSC/CPS/e-CPS ;
- Journalisation certifiée & forensic ;
- Anti-DDoS, WAF, IDS/IPS ;
- Tests d'intrusion.

S3C. Services d'exploitation (RUN)

- Supervision 24/7 ;
- Mises à jour de sécurité ;
- Mises à jour fonctionnelles ;
- Gestion des incidents ;
- Availability Management ;
- Capacity Planning.

S3D. Services MCO

- Correctifs applicatifs et sécurité ;
- Mises à jour trimestrielles ;
- Suivi des vulnérabilités ;
- Reporting mensuel CAIH.

S3E. Services Support

- Support N2 (établissements) ;
- Support N3 (intégrateurs) ;
- Portail de tickets & base de connaissances ;
- Observabilité partagée CAIH.

S3F. Services d'accompagnement

- Formation AMOA/AMOE ;
- Accompagnement migration ;
- Conduite du changement ;
- Coaching DSI/RSSI.

6. Livrables attendus

1. Techniques

- Kits de déploiement reproductibles
- Scripts d'automatisation
- Documentation exploitation + supervision + PRA/PCA
- Catalogue technique & compatibilité
- Rapport d'audit RGPD/HDS/NIS2
- Documentation infrastructure & hébergement (HLD/LLD)

2. Fonctionnels & organisationnels

- Kits AMOA & AMOE complets
- Modèle de service MCO
- Référentiel support N2/N3
- Plan de continuité & réversibilité

3. Économiques & contractuels

- Grille tarifaire hébergement & exploitation
- TCO RUN vs solutions propriétaires
- Modèle contractuel CAIH pour :AMOA, AMOE, MCO, Hébergement
- Rapport de soutenabilité économique 3–5 ans
- Bordereau de prix unitaire final et complet avec modalités de catalogue promotionnel et de révision de prix

4. Gouvernance & suivi

- Registre incidents & évolutions
- Plan de pilotage post-projet
- Rapport de clôture PI
- Feuille de route nationale 2027–2030

Validation de la séquence et de la phase R&D **Admission validant décision de poursuivre**

6.2. PHASE ACQUISITION

Objectif général

Cette phase doit permettre :

- au **groupement de commandes** d'acquérir en premier lieu la solution complète,
- puis aux **adhérents de la CAIH** d'en bénéficier à travers un catalogue de services industrialisés, souverains et ouverts.

Cette phase vise à mettre à disposition une **offre complète, stable, documentée et industrialisée**, intégrant les briques open source développées lors du Partenariat d'Innovation, ainsi que les services nécessaires à leur déploiement, hébergement, exploitation, maintenance et évolution.

Elle constitue le **point d'entrée dans le cycle de vie opérationnel** des solutions, incluant leur maintien en conditions opérationnelles (MCO), leur sécurité, leur conformité réglementaire et leur amélioration continue.

Objectifs spécifiques

La phase d'acquisition vise à :

- Mettre à disposition des établissements une **offre prête à l'emploi**, packagée et industrialisée.
- Permettre aux adhérents CAIH d'acquérir la solution selon un **modèle de services souverains et mutualisés**, modulables selon les besoins.
- Garantir la **continuité de service**, la conformité réglementaire (RGPD, HDS, NIS2), la sécurité et la performance.
- Proposer un **service complet de maintenance, d'évolution, de support et d'adaptation** aux environnements SI des établissements de santé.
- Assurer un **hébergement souverain**, opéré exclusivement dans l'Union européenne, conforme aux référentiels HDS et, éventuellement, SecNumCloud.
- Permettre la **montée en charge**, la généralisation progressive et l'intégration aux systèmes existants.

Périmètre fonctionnel et technique couvert

La phase d'acquisition couvre l'ensemble des composants validés en fin de phase R&D.

1. Solutions open source packagées

Modern Workspace

- Suite collaborative
- Messagerie
- GED / coédition
- Visio / communication unifiée
- Suite bureautique open source

ID CAIH

- Gestion fédérée des identités
- SSO, MFA
- Interopérabilité PSC / CPS / e-CPS
- Référentiels ANS

Infrastructure hybride & virtualisation

- Hyperviseurs souverains
- Stockage chiffré
- Bases de données open source
- Orchestration / supervision
- Intégration on-premise ↔ cloud souverain

Parc & postes de travail

- Distribution hospitalière Linux
- Télédistribution / MDM
- Supervision et inventaire
- Sécurisation du poste de travail

IA & automatisation

- LLM Open Source souverain
- Assistant conversationnel métier
- Automatisation des processus (support, logs, documentation)

2. Services associés

Hébergement souverain

- Hébergement **dans l'Union européenne**, hors extraterritorialité.
- Certification **HDS** pour les données de santé.
- Qualification **SecNumCloud** ou équivalent européen.
- Administration **exclusivement européenne et auditée**.
- Modes disponibles : mutualisé, dédié, hybride, on-premise étendu.

Maintenance réglementaire, technique et sécuritaire

- Application des patchs, mises à jour de sécurité, correctifs.
- Surveillance continue RGPD / HDS / NIS2 / PGSSI-S.
- Gestion automatisée des vulnérabilités.
- Supervision proactive (infrastructure, services, sécurité).
- Rapports mensuels : incidents, disponibilité, SLA, sécurité.

Maintenance évolutive & fonctionnelle

- Prise en charge des nouvelles fonctionnalités open source.

- Évolutions réglementaires (PGSSI-S, NIS2, référentiels ANS/DINUM).
- Mise à jour du code, de la documentation et des configurations.
- Roadmap annuelle validée par la CAIH.

Services d'adaptation des SI adhérents (sur devis / TJM)

- Intégration dans les environnements hospitaliers existants.
- Interopérabilité applicative (connecteurs métiers, API, formats).
- Sécurité des flux inter-applicatifs.
- Assistance à la migration (technique + conduite du changement).
- Accompagnement DSI/RSSI dans les projets de certification.

Prestations attendues du titulaire

Le titulaire devra fournir :

1. Hébergement souverain (On-Premise, IaaS, PaaS, SaaS)

- Options mutualisées ou dédiées.
- Garantie de disponibilité ≥ **99,8 %** chaque mois.
- PRA/PCA documentés.

2. Maintenance complète (corrective, évolutive, sécuritaire)

- Engagements SLA contractuels.
- Mise à jour continue (patchs, versions).
- Surveillance et intervention N2 / N3.

3. Évolution fonctionnelle & technique

- Roadmap annuelle d'évolutions validée par la CAIH.
- Processus d'intégration des besoins utilisateurs.

4. Prestations sur mesure (TJM)

- Audits SI, interopérabilité et sécurité.
- Intégration dans les SI.
- Services de migration.
- Formation / transfert de compétences.
- Aide à la conformité HDS / NIS2.

Livrables attendus

1. Livrables contractuels

- Mise à jour du **contrat d'acquisition et d'exploitation** :
  - droits d'usage,
  - clauses de réversibilité,
  - conditions de maintenance,
  - gestion des briques Microsoft nécessaires à l'interopérabilité,
  - absence de redevances ou royalties pour les briques open source développées.
- Catalogue de services mis à jour :

- hébergement,
- maintenance,
- évolution,
- prestations à la journée (TJM).

2. Livrables techniques & opérationnels

- Environnements hébergés, supervisés, prêts à l'emploi.
- Registre de maintenance et rapports de supervision.
- Plan de gestion des vulnérabilités et mises à jour.
- Architecture opérationnelle (HLD/LLD).
- Plan d'amélioration continue.

3. Livrables de support & d'accompagnement

- Guides d'intégration dans les SI.
- Guides de migration et de conduite du changement.
- Documentation utilisateur et administrateur.
- Modèles de convention d'adhésion au service CAIH.
- Rapports mensuels de suivi : incidents, disponibilité, performance, conformité.

Modalités de pilotage

- Mise en place d'un **Comité de suivi de l'acquisition**, piloté par la CAIH, réunissant :
  - les établissements pilotes,
  - les AMOA/AMOE,
  - le titulaire.
- **Revue trimestrielle de performance**, portant sur :
  - disponibilité,
  - incidents,
  - sécurité,
  - conformité réglementaire,
  - satisfaction utilisateurs.
- Production d'un **rapport annuel de soutenabilité**, incluant :
  - coûts réels,
  - économies générées,
  - vision à 3 ans et 5 ans,
  - recommandations d'évolution du service.

Article 7 – Prestations intellectuelles associées à l'ensemble des phases et des séquences

7.1. Les catégories de prestation à couvrir

Les catégories doivent être structurées en **5 grandes familles**, correspondant aux 5 briques du programme fonctionnel :

A – Infrastructure & Hébergement Souverain

(OpenStack, Proxmox, stockage, supervision, sécurité, HDS/SecNumCloud)

B – ID CAIH / IAM

(Identité, SSO, MFA, provisioning SCIM, interop PSC/CPS)

C – Modern Workspace

(Collaboration, messagerie, GED, visioconf, bureautique)

D – Virtualisation & Cloud

(Hyperviseurs, orchestration, provisioning, CI-CD, containers)

E – Interopérabilité / Migration / Déploiement

(API, FHIR, connecteurs, migration données, conduite du changement)

Et 1 famille transversale :

F – Cybersécurité & SOC

(RSSI technique, audit, durcissement, SOC, SIEM, IAM-security)

7.2. Les types de prestations à couvrir

Pour chaque brique, les prestations doivent couvrir :

1. Développement OSS

- customisation distributions Linux
- développement modules (MW, IAM, supervision)
- packaging, scripts Ansible/Terraform
- automatisation intégration continue

2. Intégration & Migration

- interopérabilité ANS/Microsoft
- connecteurs LDAP/SCIM
- migration boîtes mails, GED, identités
- configuration hébergement HDS/SNC

3. Versionning / CI-CD

- gestion pipelines
- publication version annuelle consolidée
- gestion branches / releases / rollback
- conformité code RGPD / sécurité

4. Hébergement souverain

- exploitation clusters OpenStack
- supervision 24/7
- PRA/PCA
- pilotage HDS / SecNumCloud

5. MCO / Support N2 / N3

7.3. Liste des profils

A. INFRASTRUCTURE & HÉBERGEMENT

A1.1 – DevOps / Build Infrastructure

- Réf : **TJM-Infra-Dev-[Jun/Con/Sen/Exp]**
- Compétences : CI-CD, pipelines, packaging, scripts Ansible/Terraform, images ISO, hardening Linux.

A1.2 – Administrateur système souverain

- Réf : **TJM-Infra-Admin-[Jun/Con/Sen/Exp]**
- Compétences : OS, réseau, sécurité, configuration serveurs, clusters.

A1.3 – Ingénieur Hébergement HDS / SecNumCloud

- Réf : **TJM-Infra-HDS-[Con/Sen/Exp]**
- Compétences : sécurité, conformité HDS/SNC, PRA, PCA, audit, journaux.

A1.4 – Architecte Infrastructure

- Réf : **TJM-Infra-Arch-[Sen/Exp]**
- Compétences : architecture cible, haute dispo, multi-zone, stockage Ceph.

B. IDENTITÉ – ID CAIH (IAM / SSO / MFA)

B1 – Développeur IAM

- Réf : **TJM-IAM-Dev-[Jun/Con/Sen/Exp]**
- Compétences : OIDC, OAuth2, SAML, SCIM, API IAM.

B2 – Intégrateur IAM

- Réf : **TJM-IAM-Int-[Con/Sen]**
- Compétences : provisioning identités, MFA, connecteurs AD / eCPS / PSC.

B3 – Architecte IAM

- Réf : **TJM-IAM-Arch-[Sen/Exp]**

C. MODERN WORKSPACE (MW)

C1 – Développeur MW

- Réf : **TJM-MW-Dev-[Jun/Con/Sen]**
- Compétences : modules GED, messagerie, suites office OSS.

C2 – Intégrateur MW

- Réf : **TJM-MW-Int-[Jun/Con/Sen]**

C3 – Expert MW

- Réf : **TJM-MW-Exp**
- Compétences : tuning, interop, migration mails / GED.

D. VIRTUALISATION / CLOUD

D1 – Spécialiste Virtualisation

- Réf : **TJM-Virtu-Int-[Jun/Con/Sen]**
- Compétences : Proxmox, OpenStack, oVirt, migration VM.

D2 – Développeur Cloud Automatisation

- Réf : **TJM-Virtu-Dev-[Jun/Con/Sen/Exp]**
- Compétences : Terraform, API OpenStack, CI-CD.

D3 – Architecte Cloud

- Réf : **TJM-Virtu-Arch-[Sen/Exp]**

E. INTEROPÉRABILITÉ / MIGRATION / DÉPLOIEMENT

E1 – Ingénieur Interopérabilité (API / FHIR / SCIM)

- Réf : **TJM-Inter-API-[Jun/Con/Sen]**

E2 – Ingénieur Migration & Déploiement

- Réf : **TJM-Depl-Int-[Jun/Con/Sen]**

E3 – Expert AMOA / conduite du changement

- Réf : **TJM-AMOA-[Sen/Exp]**

F. CYBERSÉCURITÉ / SOC

F1 – Analyste SOC / sécurité opérationnelle

- Réf : **TJM-Cyber-SOC-[Jun/Con/Sen]**

F2 – Ingénieur Cybersécurité

- Réf : **TJM-Cyber-Int-[Con/Sen]**

F3 – Architecte Sécurité

- Réf : **TJM-Cyber-Arch-[Sen/Exp]**

Article 8 – Politique de mise à jour, versions majeures et support long terme (LTS)

Les solutions, briques logicielles et services fournis dans le cadre du présent partenariat d'innovation font l'objet d'une politique de mise à jour structurée et maîtrisée, visant à garantir leur sécurité, leur conformité réglementaire, leur stabilité opérationnelle et leur soutenabilité économique sur toute la durée du marché.
Une mise à jour annuelle est organisée sous la responsabilité du Titulaire. Elle couvre, a minima, les correctifs de sécurité, les mises en conformité réglementaires (RGPD, HDS, NIS2, PGSSI-S,

référentiels ANSSI), la correction des anomalies, ainsi que les évolutions techniques et fonctionnelles maîtrisées issues des versions stables des composants open source retenus. Les correctifs de sécurité critiques peuvent être déployés en dehors de ce cycle annuel selon une procédure d'urgence validée par la CAIH.
Les évolutions sont structurées selon une politique de versionnement distinguant explicitement les mises à jour majeures et les versions à support long terme (LTS). Les versions LTS constituent les versions de référence pour l'exploitation en production. Pour chaque brique fonctionnelle, le Titulaire s'engage à maintenir au minimum une version LTS active, bénéficiant d'un support d'une durée minimale de trente-six (36) mois, incluant les correctifs de sécurité, les mises en conformité réglementaires et la correction des anomalies bloquantes.
Toute mise à jour majeure, entendue comme une évolution susceptible d'entraîner un changement significatif de version, d'architecture, de dépendances, d'interfaces ou d'usages, fait l'objet d'une proposition formalisée du Titulaire et est soumise à validation préalable expresse de la CAIH. Son déploiement n'est jamais automatique. La CAIH se réserve la faculté de différer la mise à jour majeure, d'en limiter le périmètre ou de maintenir tout ou partie des établissements sur une version LTS existante.
La migration d'une version LTS vers une version issue d'une mise à jour majeure est conditionnée à la validation par la CAIH d'un plan de migration dédié, précisant notamment les impacts techniques, fonctionnels et organisationnels, la compatibilité applicative (y compris avec les éditeurs métiers et les environnements Microsoft), les modalités de tests, d'accompagnement et de formation, ainsi que les conditions de réversibilité. Une coexistence temporaire de plusieurs versions peut être organisée afin de garantir la continuité de service.
Les mises à jour correctives, réglementaires et de sécurité des versions LTS sont réputées incluses dans les prestations de maintien en conditions opérationnelles (MCO). Les mises à jour majeures ne peuvent entraîner ni augmentation automatique des coûts, ni remise en cause des engagements contractuels existants. Lorsqu'elles introduisent des évolutions fonctionnelles substantielles ou des impacts significatifs sur les environnements, elles peuvent faire l'objet d'une instruction contractuelle spécifique, après validation expresse de la CAIH.
Le Titulaire assure la traçabilité complète de cette politique de mise à jour au travers d'une roadmap pluriannuelle, d'un journal de versions détaillé et d'un tableau de suivi des versions déployées, présentés au minimum annuellement dans le cadre de la gouvernance du marché et intégrés au rapport annuel de soutenabilité technique et économique.

Principes généraux

Le Titulaire s'engage à structurer les évolutions des solutions et services fournis selon une politique de gestion de versions maîtrisée, distinguant explicitement :

- les mises à jour correctives et réglementaires ;
- les mises à jour majeures ;
- les versions à support long terme (LTS).

Cette politique vise à garantir la stabilité opérationnelle, la sécurité, la conformité réglementaire et la prévisibilité budgétaire des solutions déployées auprès des établissements adhérents de la CAIH.

Versions LTS – Définition et engagements

Les versions LTS constituent les versions de référence pour l'exploitation en production.

À ce titre, le Titulaire s'engage à :

- maintenir au minimum une version LTS active pour chaque brique fonctionnelle ;
- assurer pour chaque version LTS :
    - les correctifs de sécurité, y compris critiques ;
    - les mises en conformité réglementaires (RGPD, HDS, NIS2, PGSSI-S, ANSSI) ;
    - la correction des anomalies bloquantes ;
- garantir une durée minimale de support LTS de trente-six (36) mois, sauf évolution réglementaire ou de sécurité imposant une migration anticipée.

Les versions LTS sont privilégiées pour les déploiements mutualisés et généralisés au sein des établissements de santé.

Mises à jour majeures – Encadrement et validation

Une mise à jour majeure s'entend de toute évolution impliquant :

- un changement significatif de version logicielle ;
- une modification de l'architecture, des dépendances ou des interfaces ;
- une évolution notable des fonctionnalités ou des usages ;
- un impact potentiel sur l'exploitation, la sécurité ou la formation des utilisateurs.

Toute mise à jour majeure :

- fait l'objet d'une proposition formalisée du Titulaire ;
- est soumise à validation préalable expresse de la CAIH ;
- ne peut être déployée sans accord écrit de l'acheteur.

La CAIH peut décider :

- de différer la mise à jour majeure ;
- de la réserver à certains périmètres pilotes ;
- ou de maintenir les établissements sur une version LTS existante.

Articulation entre versions LTS et mises à jour majeures

La migration d'une version LTS vers une version issue d'une mise à jour majeure :

- n'est jamais automatique ;
- fait l'objet d'un plan de migration dédié, incluant :
    - analyse d'impact,
    - compatibilité applicative (éditeurs métiers, interopérabilité Microsoft),
    - modalités de tests,
    - accompagnement et formation,
    - conditions de réversibilité.

La CAIH conserve la faculté de :

- maintenir une version LTS existante jusqu'à la fin de sa période de support ;
- organiser une coexistence temporaire de versions, si nécessaire à la continuité de service.

Cadre contractuel et financier

Les mises à jour correctives, réglementaires et de sécurité des versions LTS sont incluses dans les prestations de MCO.

Les mises à jour majeures peuvent :

- soit être intégrées sans surcoût lorsqu'elles sont imposées par des exigences réglementaires ou de sécurité ;
- soit faire l'objet d'une instruction contractuelle spécifique, si elles introduisent des évolutions fonctionnelles substantielles ou des impacts significatifs sur les environnements existants.

Aucune mise à jour majeure ne peut entraîner :

- une augmentation automatique des coûts ;
- une remise en cause des engagements contractuels existants ;
- une perte de compatibilité ou de réversibilité.

Traçabilité, transparence et gouvernance

Le Titulaire tient à jour :

- une roadmap de versions pluriannuelle, distinguant versions intermédiaires et LTS ;
- un journal de versions (changelog) détaillé et accessible ;
- un tableau de suivi des versions déployées par établissement.

Ces éléments sont présentés au minimum annuellement en comité de gouvernance CAIH et intégrés au rapport annuel de soutenabilité technique et économique.

ANNEXE 1 Lexique complet – Acronymes, termes techniques, marques et mentions légales

Acronymes et termes techniques

Acronyme / Terme	Signification	Domaine	Définition détaillée
CAIH	Centrale d'Achat de l'Informatique Hospitalière	Gouvernance	Centrale d'achat mutualisée dédiée au secteur sanitaire et médico-social, permettant la passation de marchés nationaux.

Acronyme / Terme	Signification	Domaine	Définition détaillée
DPO	Délégué à la Protection des Données	RGPD	Responsable interne garant de la conformité GDPR / protection des données.
DSI	Direction des Systèmes d'Information	Gouvernance	Direction en charge de la stratégie numérique d'un établissement.
RSSI	Responsable Sécurité des SI	Cybersécurité	Pilote la sécurité, les risques, les audits et les actions SSI.
AMOA	Assistance à Maîtrise d'Ouvrage	Projet	Accompagnement fonctionnel (usages, besoins, conduite du changement).
AMOE	Assistance à Maîtrise d'Œuvre	Technique	Assistance technique pour le déploiement, l'intégration, l'interopérabilité.
PI	Partenariat d'Innovation	Marchés publics	Procédure permettant d'acheter R&D + acquisition d'une solution innovante non disponible sur le marché.
DCE	Dossier de Consultation des Entreprises	Contrats	Ensemble des documents contractuels d'un marché.
BPU	Bordereau des Prix Unitaires	Achat	Tableau listant l'ensemble des unités d'œuvre tarifaires.
MW	Modern Workspace	Bureautique	Suite collaborative open source : messagerie, GED, coédition, visio.
ID CAIH	Identité fédérée alternative	IAM	Alternative open source à Azure AD / Entra ID, interconnectée PSC/CPS/e-CPS.
IAM	Identity & Access Management	Identité	Gestion des identités, habilitations, authentification et SSO.

Acronyme / Terme	Signification	Domaine	Définition détaillée
SSO	Single Sign-On	Identité	Authentification unique pour accéder à plusieurs applications.
MFA	Multi-Factor Authentication	Sécurité	Authentification forte reposant sur plusieurs facteurs.
PSC	Pro Santé Connect	Identité santé	Service d'identification des professionnels de santé édité par l'ANS.
CPS / e-CPS	Carte Professionnel de Santé	Identité	Identité numérique certifiée ANS.
ANS	Agence du Numérique en Santé	Institutions	Porte les référentiels numériques de santé.
DINUM	Direction Interministérielle du Numérique	Souveraineté	Dresse les standards de l'État (cloud, sécurité, outils).
RGPD / GDPR	Règlement Général sur la Protection des Données	Conformité	Cadre juridique européen pour la protection des données personnelles.
HDS	Hébergeur de Données de Santé	Sécurité	Certification obligatoire pour héberger des données de santé.
SecNumCloud	Référentiel d'hébergement souverain ANSSI	Sécurité	Norme garantissant un cloud souverain (administration EU-only).
NIS2	Directive européenne de sécurité	Sécurité	Renforce les obligations de cybersécurité pour les secteurs critiques.
PGSSI-S	Politique Générale SSI Santé	Cybersécurité santé	Référentiel national de sécurité pour les SI de santé.

Acronyme / Terme	Signification	Domaine	Définition détaillée
PRA / PCA	Reprise / Continuité d'Activité	Résilience	Plans garantissant la survie ou récupération des services en cas de panne majeure.
POC	Proof of Concept	R&D	Prototype permettant de valider la faisabilité d'une technologie.
Pilotage	Gestion projet	Gestion	Suivi administratif et stratégique d'un projet.
MCO	Maintien en Conditions Opérationnelles	Exploitation	Gestion des incidents, correctifs, mises à jour, supervision.
Build / Run	Construction / Exploitation	DevOps	Build = développement ; Run = exploitation quotidienne.
DevOps	Développement + Opérations	Méthodologie	Automatisation CI/CD, conteneurs, pipelines, supervision.
CI/CD	Intégration & Déploiement continus	DevOps	Automatisation des builds, tests, déploiements.
API	Interface de Programmation	Interop	Mécanisme structuré d'échanges entre logiciels.
FHIR	Fast Healthcare Interoperability Resources	Santé	Standard international structurant les données médicales.
SaaS / PaaS / IaaS	Modèles Cloud	Cloud	Modes de services hébergés : logiciel, plateforme, infrastructure.
On-Premise	Sur site	Hébergement	Infrastructure localisée physiquement dans l'établissement.
OpenStack	Infrastructure Cloud Open Source	Virtualisation	Plateforme de cloud souverain open source.

Acronyme / Terme	Signification	Domaine	Définition détaillée
Proxmox / oVirt	Hyperviseurs open source	Virtualisation	Solutions de virtualisation souveraines pour serveurs.
LLM	Large Language Model	IA	Modèles IA avancés (ex: GPT, Mistral) pour assistants intelligents.
SOC	Security Operations Center	Cybersécurité	Centre de supervision en continu des menaces et incidents.
UE / UO	Unité d'Œuvre	Achat	Valeur mesurable tarifée dans le BPU (jour, serveur/mois…).
TJM	Taux Journalier Moyen	Achat prestations	Coût journalier d'un type d'expertises (junior → expert).
SLA	Service Level Agreement	Contrat	Engagements contractuels de performance du service.
ISO (image)	Image système ISO	Poste	Image déployable d'un système d'exploitation.
Ansible / Terraform	Automatisation IaC	DevOps	Automatisation configuration et infrastructure-as-code.
Alerting / Monitoring	Supervision	Exploitation	Détection et alertes sur incidents ou dégradation service.
Gestion du versioning	Versionning Git	Dev	Suivi officiel des versions de code, modules, documents.
Réversibilité	Processus de sortie de contrat	Juridique	Engagement contractuel permettant de récupérer toutes les données, configurations et VM.
PUPA	*Plan d'Urbanisation et de Pilotage Applicatif* (définition adaptée CAIH)	Urbanisation SI	Document définissant la structure cible du SI, les domaines fonctionnels, les flux d'interopérabilité, la cartographie

Acronyme / Terme	Signification	Domaine	Définition détaillée
			des applications et leur gouvernance.

Marques citées et mentions légales

Marque / Produit	Titulaire	Mentions légales
Microsoft 365, Azure AD, Entra ID, Teams	Microsoft Corporation	Marques déposées Microsoft. *« Microsoft®, Azure®, Microsoft 365® sont des marques déposées de Microsoft Corporation »*.
Proxmox VE	Proxmox Server Solutions GmbH	Solution open source ; noms et logos protégés par trademark Proxmox.
OpenStack®	Open Infrastructure Foundation	Marque déposée de la OpenInfra Foundation.
oVirt	Red Hat (communauté)	Open source ; nom protégé, sous licence Apache 2.0.
Nextcloud®	Nextcloud GmbH	Marque déposée ; utilisée dans MW éventuel.
OnlyOffice®	Ascensio System SIA	Marque déposée ; bureautique collaborative.
Collabora Office	Collabora Productivity Ltd.	Version open source de LibreOffice ; marque Collabora.
LibreOffice	The Document Foundation	Open source LGPL ; nom LibreOffice protégé par trademark.
Mattermost®	Mattermost Inc.	Solution collaborative open source ; marque déposée.
Keycloak®	Red Hat	IAM open source ; licence Apache 2.0 ; trademark Red Hat.

Marque / Produit	Titulaire	Mentions légales
Mistral AI	Mistral AI SAS	LLM open source ou propriétaire ; nom protégé.
GLPI	Teclib Group	ITSM open source ; marque Teclib.
Jitsi®	8x8, Inc.	Plateforme de visioconférence open source ; marque déposée.
Firefox®, Thunderbird®	Mozilla Foundation	Marques déposées.