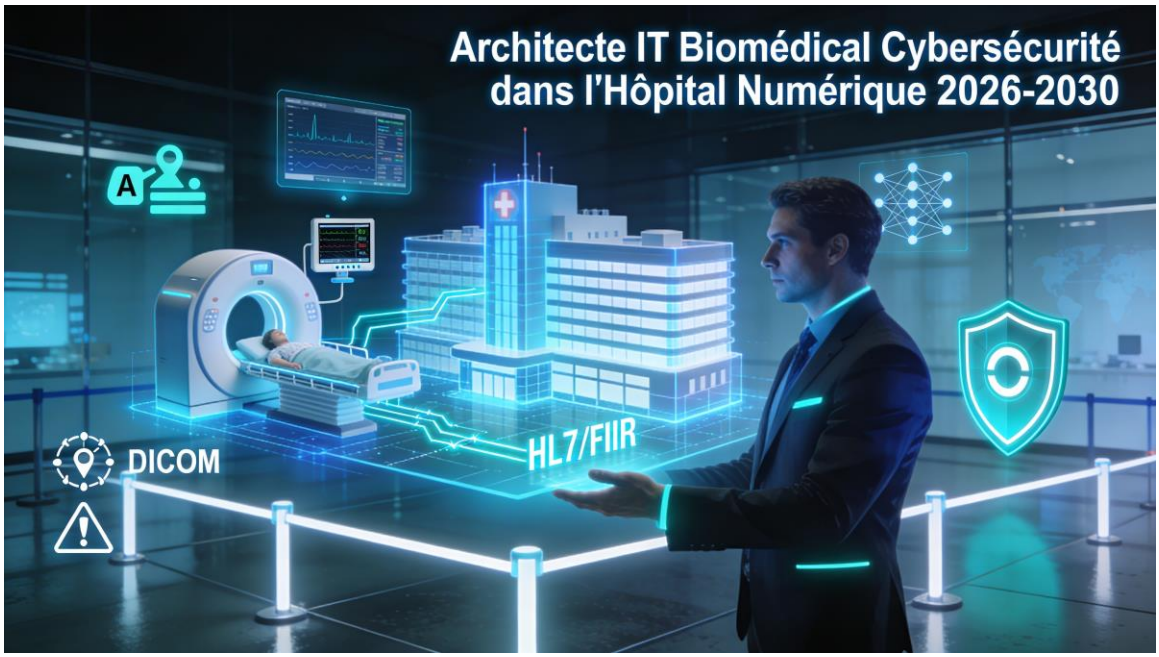
Livre Blanc

Le rôle d'Architecte IT Biomédical & Cybersécurité dans l'hôpital numérique

Enjeux, missions, compétences et feuille de route

2026 - 2030



Convergence Santé
www.inkkreation.com

Résumé Exécutif : Piloter la Convergence entre Soin et Technologie (2026-2030)

L'Enjeu : Une Mutation Critique de l'Hôpital

L’hôpital moderne traverse une phase d’hybridation profonde où la frontière entre le système d’information (SIH) et les dispositifs médicaux (DM) s’efface.

Aujourd'hui, un scanner, un moniteur de réanimation ou un automate de biologie ne sont plus de simples outils isolés, mais des **nœuds réseau critiques** injectant des données vitales dans le parcours de soin.

Cette transformation, bien qu'essentielle pour l'efficacité clinique, expose l'établissement à de nouveaux risques majeurs : cyberattaques ciblant directement les DM, ruptures de flux de données et complexité réglementaire accrue (NIS2, MDR).

La Solution : Le Rôle Pivot d’Architecte IT Biomédical & Cybersécurité

Pour répondre à cette complexité, ce livre blanc définit une fonction nouvelle et indispensable : **l’Architecte IT Biomédical & Cybersécurité**. Ce rôle ne se limite pas à la technique ; il est le garant de la **résilience hospitalière** en assurant trois missions stratégiques:

1. **Sécurisation du "Cœur de Métier"** : Protéger les dispositifs médicaux contre les menaces cyber pour garantir la continuité des soins et la sécurité des patients.
2. **Accélération de l'Interopérabilité** : Fluidifier les échanges de données (DICOM, HL7, FHIR) entre les équipements et le dossier patient pour une prise en charge plus rapide et sans erreur d'identitovigilance.
3. **Gouvernance de l’Innovation** : Encadrer l’arrivée massive de l’Intelligence Artificielle clinique en évitant le "Shadow AI" (solutions installées hors cadre sécurisé).

Valeur Ajoutée pour le Décideur

L'institutionnalisation de cette fonction permet de transformer une contrainte technique en levier de performance :

- **Maîtrise du Risque Financier** : Réduction du coût d'indisponibilité lié aux arrêts de plateaux techniques (blocs, imagerie) suite à un incident cyber.

- **Optimisation des Investissements** : Mutualisation des infrastructures et réduction des coûts d'intégration spécifiques à chaque fournisseur grâce à une architecture de référence.
- **Conformité Juridique** : Alignement rigoureux avec les exigences européennes (MDR, NIS2) et les normes de gestion des risques (ISO 14971).

Feuille de Route Stratégique

Le déploiement de cette expertise s'articule sur un plan de 4 ans:

- **Horizon 1 an** : Cartographie exhaustive des flux et premiers gains de sécurisation par segmentation réseau.
- **Horizon 2 ans** : Standardisation des méthodes d'intégration et outillage de surveillance.
- **Horizon 3-4 ans** : Industrialisation de la gouvernance IA et optimisation continue de la résilience.

Conclusion : L'Architecte IT Biomédical & Cybersécurité est le maillon manquant pour sécuriser la transformation numérique de votre établissement. Investir dans cette compétence, c'est protéger durablement la qualité des soins et la souveraineté des données de vos patients.

Introduction

Ce livre blanc définit le métier d'Architecte IT Biomédical & Cybersécurité, un rôle pivot pour orchestrer la convergence entre dispositifs médicaux (DM), systèmes d'information hospitaliers (SIH), exigences réglementaires et cybersécurité.

Il présente les enjeux qui rendent ce rôle incontournable, détaille les missions et compétences associées, propose une méthodologie opérationnelle et illustre des cas d'usage concrets.

Enfin, il offre une feuille de route 2026–2030 pour installer durablement cette fonction dans la gouvernance des établissements de santé et :

- Répondre à la complexité croissante des flux cliniques et des DM connectés
- Réduire les risques cyber tout en garantissant la continuité des soins
- Accélérer l'interopérabilité (DICOM, HL7 v2, IHE, FHIR) et la qualité des données
- Outiller l'intégration sécurisée des DM et l'adoption responsable de l'IA clinique
- Structurer une collaboration efficace DSI – Biomédical – RSSI – Clinique

Les hôpitaux entrent dans une phase d'hybridation profonde : les DM deviennent des nœuds réseau, les applications cliniques s'ouvrent par API, l'IA arrive au plus près du soin, tandis que les menaces cyber ciblent les chaînes de prise en charge. Dans ce contexte, l'Architecte IT Biomédical & Cybersécurité émerge comme l'interlocuteur capable de concevoir des architectures sûres, interopérables et résilientes, en alignant technique, clinique et réglementation.

Ce document vise à :

- Cadrer les enjeux
- Formaliser les responsabilités et livrables
- Décrire les compétences essentielles
- Proposer une méthodologie et des outils
- Fournir des cas d'usage
- Donner une feuille de route organisationnelle et de compétences à horizon 2030

Attention, il n'est en aucun cas exhaustif mais sera plus un guide pour tout ceci.

PARTIE I – Les nouveaux enjeux de l'hôpital numérique

1.1 Mutation rapide des systèmes cliniques

Le portefeuille applicatif clinique (PACS, RIS, LIS, DPI, ISCV, PDMS, plateforme d'IA) s'étend et se spécialise.

Les volumes d'images et de données patient augmentent, les attentes de disponibilité s'intensifient et les workflows se multiplient (urgences, bloc, réanimation, imagerie, cardio, télémédecine). L'interopérabilité devient un impératif, non un luxe.

1.2 Explosion des dispositifs médicaux connectés

Moniteurs multiparamétriques, ventilateurs, injecteurs, IRM, échographes, ECG : une part croissante du parc DM expose des interfaces réseau.

Les contraintes propres aux DM (systèmes d'exploitation legacy, fenêtres de maintenance limitées, validation fabricant) complexifient la gestion de la sécurité et des mises à jour.

1.3 Menace cyber et impact patient

Les attaques par rançongiciel et par la chaîne d'approvisionnement visent désormais les DM et les plateformes cliniques.

Au-delà de l'impact financier et réputationnel, le risque principal est clinique : retard de prise en charge, indisponibilité d'équipements, altération de la qualité des données.

1.4 Cadre normatif et réglementaire

L'architecte doit opérer dans un environnement normatif exigeant (gestion des risques, sécurité des DM, interopérabilité, protection des données).

L'intégration d'IA clinique impose une gouvernance rigoureuse du cycle de vie, de la validation à la surveillance post-déploiement.

- **Règlementation Européenne : MDR** (Medical Device Regulation) pour la partie logicielle et la directive **NIS2** pour la cybersécurité hospitalière.
- **Normes de gestion des risques : ISO 14971** (gestion des risques pour les DM) et l'**IEC 80001-1** (application de la gestion des risques aux réseaux informatiques supportant des DM).

PARTIE II – Un rôle devenu indispensable

2.1 Une vision transverse unique

L'Architecte IT Biomédical & Cybersécurité comprend les contraintes cliniques, biomédicales et IT, et parle les langages des différentes parties prenantes.

Il cartographie, arbitre et sécurise les flux critiques qui relient le soin au système d'information.

2.2 Résilience et continuité des soins

Concevoir des architectures tolérantes aux pannes, segmentées et surveillées permet de préserver la qualité et la disponibilité des services cliniques, même en cas d'incident cyber ou technique.

2.3 Gouvernance et aide à la décision

Le rôle apporte des livrables décisionnels (dossiers d'architecture, analyses de risques, plans de sécurisation) et pilote des arbitrages entre coût, performance, sécurité et exigences réglementaires.

PARTIE III – Missions et responsabilités

3.1 Architecture technique et fonctionnelle du SI biomédical

- Modéliser les flux entre DM, middleware, archives, DPI et analytics
- Définir les exigences de sécurité, disponibilité, journalisation et traçabilité
- Concevoir l'adressage, la segmentation VLAN et les contrôles d'accès
- Documenter la topologie et les dépendances critiques

3.2 Intégration des dispositifs médicaux

- Paramétrer les worklists et la conformité DICOM/HL7
- Gérer les protocoles propriétaires et les passerelles
- Organiser les tests d'interopérabilité et de bout-en-bout
- Fournir les fiches d'installation et d'exploitation sécurisée

3.3 Cybersécurité biomédicale

- Appliquer une démarche de gestion des risques dédiée aux DM
- Piloter l'inventaire, le durcissement et la gestion des vulnérabilités
- Mettre en place une surveillance réseau et des journaux exploitables
- Coordonner les plans de réponse et de continuité spécifiques aux DM

3.4 Gouvernance de l'IA clinique

- Évaluer la qualité des données et la robustesse des modèles
- Concevoir les points d'intégration (PACS/DPI/API)
- Mettre en place des garde-fous éthiques et opérationnels
- Organiser la surveillance post-déploiement et la traçabilité

3.5 Gestion de projet et conduite du changement

- Cadrage, planning, lotissements et jalons
- Implication des utilisateurs finaux et formation
- Accompagnement des équipes biomédicales et IT
- Mesure de la valeur clinique et opérationnelle

PARTIE IV – Compétences essentielles

4.1 Techniques IT et interopérabilité

- Réseaux, DNS/DHCP/NTP, PKI, supervision, sauvegarde
- Interopérabilité DICOM, HL7 v2, IHE profils, FHIR et APIs REST
- Modélisation des flux, architecture applicative, intégration continue
- Sécurité des environnements Windows/Linux et durcissement

4.2 Biomédical et clinique

- Typologie DM (imagerie, monitoring, thérapie)
- Contraintes fabricants, cycles de vie et validations
- Impact clinique, criticité et workflows de soins
- Qualité métrologique et traçabilité

4.3 Cyber spécifique DM

- Segmentation réseau, contrôle d'accès, inventaire
- Gestion des vulnérabilités et patching adapté
- Journaux sécurité et détection d'anomalies
- Plan de réponse et continuité orientés DM
- **"Shadow AI"** : Détecter et encadrer les solutions d'IA installées "à la volée" par des services cliniques sans passer par l'architecture sécurisée de référence.

4.4 Transverses et leadership

- Communication interdisciplinaire et pédagogie
- Gestion de conflit et arbitrage
- Rédaction documentaire et normalisation
- Pilotage budgétaire et indicateurs de valeur
    - **Réduction du coût d'indisponibilité :** Importance du coût d'une salle d'imagerie ou d'un bloc opératoire arrêté par une cyberattaque.
    - **Optimisation des investissements :** L'architecture de référence permet de mutualiser les passerelles et de réduire les coûts d'intégration spécifiques à chaque fournisseur.

4.5 Zoom Expert : L'Urgence de la Gouvernance face à la "Shadow AI"

Dans l'hôpital numérique actuel, le risque ne vient plus seulement des infrastructures non patchées, mais de l'**IA invisible**.

La "Shadow AI" désigne l'utilisation par les services cliniques de solutions d'intelligence artificielle (souvent en mode SaaS ou via des applications mobiles) sans validation préalable par la DSI, le biomédical ou le RSSI.

1. Les Risques de l'IA Hors-Cadre

L'absence de l'Architecte IT Biomédical dans le choix de ces outils expose l'établissement à trois dangers majeurs :

- **Fuite de données de santé (HDS)** : Envoi massif d'images ou de comptes-rendus vers des serveurs tiers non certifiés pour l'hébergement de données de santé.
- **Biais Clinique et Sécurité Patient** : Utilisation d'algorithmes dont la robustesse n'a pas été testée sur les données réelles de l'établissement, créant un risque de dérive du modèle.
- **Faille de Sécurité (Backdoor)** : Intégration sauvage de connecteurs API ou de logiciels sur des stations cliniques, contournant la segmentation réseau (VLAN) et le principe du Zero Trust.

2. La Stratégie de l'Architecte IT : De la Détection à l'Encadrement

Pour contrer ce phénomène, l'Architecte IT Biomédical & Cybersécurité déploie une méthodologie en trois étapes :

- **Détection Passive** : Utilisation d'outils de surveillance réseau pour identifier les flux anormaux vers des domaines liés à des services d'IA externes.
- **Validation Clinico-Technique** : Création d'une "Sandbox d'intégration" pour tester les solutions d'IA avant tout déploiement, en vérifiant la qualité des données et les connecteurs DICOM/FHIR.
- **Gouvernance Agile** : Mise en place d'un "Comité d'architecture clinique" permettant aux médecins de proposer des outils d'IA tout en garantissant un cadre sécurisé et interopérable dès la phase de conception.
- **L'enjeu 2026-2030** : Passer d'une posture d'interdiction (souvent inefficace face à l'urgence clinique) à une posture d'**adoption responsable** orchestrée par l'Architecte.

PARTIE V – Méthodologie et outils

5.1 Cartographie des flux et vues d’architecture

Produire des vues logique, applicative, réseau et sécurité. Définir des contrats d’interface et des responsabilités d’exploitation. Maintenir un référentiel vivant, versionné et partagé.

5.2 Évaluation des risques et criticité

Qualifier la probabilité et l'impact clinique, opérationnel, légal. Prioriser les mesures : segmentation, durcissement, supervision, sauvegarde, PRA. Aligner les niveaux de service et les plans de tests.

5.3 Architecture sécurisée de référence

- Zones et flux autorisés, principe du moindre privilège
- Journalisation horodatée et corrélation des événements
- Gestion des identités et authentification forte
- Surveillance réseau et détection des comportements anormaux

5.4 Livrables et checklists

- Dossier d'architecture et matrice de flux
- Modèles de fiches d'intégration DM
- Plan de tests et PV d'homologation
- Dossier d'exploitation et de sécurité

PARTIE VI – Cas d'usage

Cas 1 – Échographie cardio avec Worklist ISCV

Objectif : standardiser le workflow d'acquisition, d'interprétation et d'archivage.

Points clés : configuration des worklists, gestion des métadonnées DICOM, routage vers archive/VNA, traçabilité des versions, sécurité des interfaces. Bénéfices : réduction des erreurs d'identitovigilance, gain de temps opérateur, traçabilité complète.

Cas 2 – Segmentation d'un parc de scopes et ventilateurs

Objectif : réduire la surface d'attaque et contenir les incidents.

Actions : VLAN dédiés, filtrage Est-Ouest, inventaire exhaustif, supervision passive, procédures de mise à jour. Résultats : moindre exposition, détection rapide d'anomalies, continuité améliorée.

Cas 3 – Intégration d'une solution d'IA d'imagerie

Objectif : intégrer un moteur d'IA pour triage/quantification.

Prérequis : qualité des données, connecteurs DICOM/FHIR, validation clinique, supervision des performances. Risques : biais, dérive du modèle, sécurité des échanges.

Mesures : sandbox d'intégration, jeux de tests, KPI cliniques.

Cas 4 – Modernisation d’un parc legacy non patchable

Objectif : sécuriser sans modifier le logiciel embarqué.

Mesures : micro-segmentation, application whitelisting via proxy, bastion d’accès support, supervision réseau, sauvegardes d’images systèmes.

Impact : réduction du risque sans rupture de service.

Cas 5 – Architecture Zero Trust pour DM

Objectif : appliquer le moindre privilège et la vérification continue.

Composants : identité des appareils, validation de posture, accès conditionnel, chiffrement bout-en-bout, télémétrie continue.

Bénéfices : limitation de mouvements latéraux et amélioration de la traçabilité.

Cas 6 – Démantèlement et intégration d’une "Shadow AI" en Radiologie

Contexte et Problématique : Un service de radiologie utilise, à l'insu de la DSI et du Biomédical, une solution d'IA en mode SaaS (Cloud externe) pour l'aide au diagnostic des fractures. Les images sont envoyées via un navigateur web par les praticiens pour obtenir un second avis rapide.

Risques identifiés par l’Architecte :

- **Fuite de données de santé** : Envoi d'images DICOM non anonymisées vers un serveur hors Union Européenne (non-conformité HDS/RGPD).
- **Rupture de l'identitovigilance** : Les résultats de l'IA ne sont pas réintégrés automatiquement dans le compte-rendu du Dossier Patient Informatisé (DPI).
- **Insécurité du poste de travail** : Utilisation de plugins de navigateur non validés, créant une porte d'entrée potentielle pour des malwares.

Intervention de l’Architecte IT Biomédical & Cybersécurité :

1. **Audit de conformité** : Évaluation du marquage CE (MDR) de la solution et négociation de clauses contractuelles de cybersécurité avec l'éditeur.

2. **Architecture de flux sécurisée** : Mise en place d'une passerelle (Gateway) DICOM locale pour anonymiser les données avant envoi et chiffrer les échanges de bout-en-bout (Zero Trust).

3. **Intégration logicielle** : Configuration d'un connecteur HL7/FHIR pour que le résultat de l'IA soit automatiquement horodaté et versé dans le PACS et le DPI.

4. **Surveillance** : Ajout du flux dans l'outil de supervision réseau pour détecter toute dérive de volume ou d'utilisation anormale.

Bénéfices et Résultats :

- **Souveraineté des données** : L'établissement reprend le contrôle sur les flux sortants et assure sa conformité NIS2.
- **Sécurité Clinique** : Le diagnostic de l'IA est désormais tracé, versionné et lié de manière unique à l'identité du patient.
- **Efficience** : Suppression des doubles saisies manuelles pour les radiologues, accélérant le workflow de prise en charge.

PARTIE VII – Feuille de route 2026–2030

7.1 Organisation cible et gouvernance

- Positionnement de l'architecte entre DSI, Biomédical et RSSI
- Comité d'architecture clinique et sécurité des DM
- Catalogue de services et RACI inter-équipes : A définir selon les structures et organisations internes
- KPI : disponibilité, incidents évités, délais d'intégration, conformité

7.2 Compétences et certifications

- Interop : IHE, HL7/FHIR, DICOM (analyse et tests)
- Cyber : principes Zero Trust, gestion vulnérabilités DM
- Normatif : gestion des risques, qualité et sécurité des DM
- Leadership : conduite du changement, valeur clinique

7.3 Feuille de route par étapes

- 12 mois : inventaire, cartographie, quick wins de segmentation
- 24 mois : architecture de référence, outillage et catalogues
- 36 mois : gouvernance IA clinique et industrialisation
- 48+ mois : optimisation continue et alignement stratégique

Conclusion

L’Architecte IT Biomédical & Cybersécurité est devenu un maillon indispensable de la résilience hospitalière.

En apportant une vision d’ensemble des flux, des risques et des contraintes cliniques, il permet d’accélérer la transformation numérique tout en protégeant le cœur de métier : le soin.

La feuille de route proposée offre un cadre pragmatique pour installer durablement ce rôle et en maximiser la valeur.