2025

MedHead

Evaluation de conformité

Système d'allocation de lits d'urgence (POC)

LOUIS ZEPHIR

PHASE G - GOUVERNANCE DE LA MISE EN ŒUVRE

Table des matières

Historique

Auteur	Remarques	Date	n° version
Louis ZEPHIR	Création du documents, début de rédaction	01/12/2025	1.0
Louis ZEPHIR	Mise à jour, correction orthographe	03/01/2026	*1.1*

Auteurs

Auteur	Fonction	Contact
Louis ZEPHIR	Architecte Logiciel	louis.zephir@medhead.fr

Introduction

Ce document présente l'évaluation de conformité de la Preuve de Concept (PoC) du système d'allocation de lits d'urgence par rapport aux principes architecturaux définis par le consortium MedHead.

Cette évaluation s'inscrit dans la phase G (Gouvernance de la mise en œuvre) du cycle ADM TOGAF et vise à démontrer que la PoC respecte les exigences métier et techniques établies.

Objectif de l'évaluation

L'objectif est de vérifier l'alignement de la PoC avec les 14 principes architecturaux regroupés en trois catégories : principes métier (A1-A4), principes informatiques (B1-B6), et principes méthodologiques (C1-C4).

Périmètre

Cette évaluation couvre le système d'allocation de lits d'urgence, incluant l'API REST, le modèle de données (Hospital, Specialty, Bed), et le pipeline CI/CD associé.

Synthèse de la conformité

Le tableau ci-dessous présente une vue d'ensemble du niveau de conformité pour chaque principe architectural.

Conforme	Partielle	Taux global
11/14	**3/14**	**79%**

ID	Principe	Conformité
A1	Primauté des principes	**Conforme**
A2	Maximiser les avantages pour l'entreprise	**Conforme**
A3	Conformité aux lois et règlements	**Conforme**
A4	Adhésion au serment d'Hippocrate	**Conforme**
B1	Continuité des activités des systèmes critiques	**Partielle**
B2	Clarté grâce à une séparation fine des préoccupations	**Conforme**
B3	Intégration et livraison continues	**Conforme**
B4	Tests automatisés précoces et complets	**Conforme**
B5	Sécurité shift-left	**Partielle**
B6	Extension par fonctionnalités pilotées par événements	**Partielle**
C1	Personnalisation de l'ADM TOGAF 10	**Conforme**
C2	Référentiel d'architecture centralisé	**Conforme**
C3	Normes reconnues pour les meilleures pratiques	**Conforme**
C4	Culture de learning avec PoC	**Conforme**

Évaluation des principes d'architecture métier

Principe A1 : Primauté des principes

Statut : Conforme

Évaluation : La PoC respecte l'ensemble des principes architecturaux définis par le consortium. Toutes les décisions de conception ont été prises en conformité avec les directives établies.

Preuves : *Documentation complète des choix architecturaux, revue de conformité réalisée avant chaque livraison.*

Principe A2 : Maximiser les avantages pour l'entreprise

Statut : Conforme

Évaluation : Le système d'allocation de lits vise à améliorer les soins aux patients en optimisant le placement dans les hôpitaux selon leurs spécialités et disponibilités.

Preuves : *API REST permettant une allocation optimale basée sur la localisation, la spécialité requise et la disponibilité des lits.*

Principe A3 : Conformité aux lois et règlements

Statut : Conforme

Évaluation : La PoC utilise des données fictives/anonymisées conformément aux recommandations RGPD. L'architecture permet l'intégration future avec les systèmes d'identité NHS.

Preuves : *Aucune donnée patient réelle utilisée, architecture prête pour l'intégration OpenID Connect.*

Principe A4 : Adhésion au serment d'Hippocrate

Statut : Conforme

Évaluation : Le système priorise la rapidité d'allocation pour les urgences vitales. L'algorithme minimise le temps de transport tout en garantissant l'accès aux soins appropriés.

Preuves : *Tests de performance démontrant des temps de réponse < 1 seconde pour l'allocation d'urgence.*

Évaluation des principes d'architecture informatique

Principe B1 : Continuité des activités des systèmes critiques

Statut : Partielle

Évaluation : L'architecture microservices permet la tolérance aux pannes. Les mécanismes de failover et la redondance complète nécessitent une implémentation en production.

Preuves : *Architecture découplée, gestion des erreurs implémentée. Recommandation: ajouter circuit breaker et retry patterns pour la production.*

Recommandations : Implémenter Resilience4j pour les circuit breakers, configurer la réplication de base de données.

Principe B2 : Clarté grâce à une séparation fine des préoccupations

Statut : Conforme

Évaluation : Architecture hexagonale respectée avec séparation claire entre domaine, application et infrastructure. Chaque service a une responsabilité unique.

Preuves : *Structure de packages: domain/, application/, infrastructure/. Tests unitaires isolés par couche.*

Principe B3 : Intégration et livraison continues

Statut : Conforme

Évaluation : Pipeline CI/CD opérationnel avec build automatique, exécution des tests et génération des rapports à chaque commit.

Preuves : *Configuration Jenkins/GitHub Actions, rapports de tests automatisés, déploiement automatique sur environnement de test.*

Principe B4 : Tests automatisés précoces et complets

Statut : Conforme

Évaluation : Couverture de tests complète selon la pyramide des tests: unitaires, intégration, E2E. Tests BDD pour les scénarios métier.

Preuves : *Rapports de couverture > 80%, scénarios Cucumber pour les critères d'acceptation, tests de performance JMeter.*

Principe B5 : Sécurité shift-left

Statut : Partielle

Évaluation : Validation des entrées implémentée, authentification prévue. Audit de sécurité complet recommandé avant production.

Preuves : *Validation des DTOs, préparation pour OAuth2/JWT.*

Recommandations : Effectuer un audit OWASP, implémenter le rate limiting, ajouter les tests de pénétration.

Principe B6 : Extension par fonctionnalités pilotées par événements

Statut : Partielle

Évaluation : L'architecture est prête pour l'event-driven. L'intégration avec un bus d'événements (Kafka) est documentée mais non implémentée dans la PoC.

Preuves : *Modèle de domaine avec événements définis, interfaces pour publication d'événements.*

Recommandations : Intégrer Apache Kafka pour la publication des événements d'allocation de lits.

Évaluation des principes de méthodologie

Principe C1 : Personnalisation de l'ADM TOGAF 10

Statut : Conforme

Évaluation : Le développement suit les phases ADM pertinentes pour une PoC: Vision, Architecture métier/SI/Technique, et Gouvernance.

Preuves : *Documentation architecturale alignée sur les livrables ADM, traçabilité des décisions.*

Principe C2 : Référentiel d'architecture centralisé

Statut : Conforme

Évaluation : Tous les artefacts architecturaux sont versionnés dans un référentiel Git unique avec documentation Markdown.

Preuves : *Repository Git structuré, documentation dans /docs, diagrammes versionnés.*

Principe C3 : Normes reconnues pour les meilleures pratiques

Statut : Conforme

Évaluation : Utilisation de Spring Boot (JVM), API REST avec spécification OpenAPI, conteneurisation Docker, tests BDD.

Preuves : *swagger.yaml conforme OpenAPI 3.0, Dockerfile multi-stage, scénarios Gherkin.*

Principe C4 : Culture de learning avec PoC

Statut : Conforme

Évaluation : La PoC valide les hypothèses critiques: temps de réponse, scalabilité de l'algorithme d'allocation, modèle de données.

Preuves : *Hypothèses documentées, résultats des tests de charge, recommandations pour la production.*

Conformité RGPD

Le projet MedHead traite des données de santé, considérées comme sensibles au titre de l'Article 9 du RGPD.

Cette section détaille les mesures de conformité implémentées dans la PoC et les actions requises pour la production.

Base légale du traitement

Le traitement des données repose sur les bases légales suivantes :

- **Article 6.1.d** : Sauvegarde des intérêts vitaux (urgence médicale)
- **Article 9.2.c** : Protection des intérêts vitaux (personne incapable de consentir)
- **Article 9.2.h** : Finalités de prise en charge sanitaire

Données personnelles traitées

Conformément au principe C4 (données fictives pour les PoC), les données suivantes sont utilisées :

Catégorie	Sensibilité RGPD	Statut PoC
Données d'identification patient	Données personnelles	Fictives
Données de santé (spécialité requise)	Données sensibles (Art. 9)	Fictives
Géolocalisation (lat/long)	Données personnelles	Non stockées
Données hospitalières (lits, spécialités)	Non personnelles	Réelles
Comptes utilisateurs	Données personnelles	Fictives

Mesures techniques de protection

Mesure	Implémentation	Statut
Authentification	JWT avec expiration configurable	✅ Implémenté
Hashage mots de passe	BCrypt avec salt	✅ Implémenté
Contrôle d'accès	RBAC (ADMIN, USER, OPERATOR)	✅ Implémenté
Chiffrement en transit	HTTPS/TLS 1.3	⚠️ Production
Chiffrement au repos	PostgreSQL pgcrypto / chiffrement disque	⚠️ Production
Journalisation	Logs des accès et authentifications	✅ Implémenté

Checklist de conformité

Exigence RGPD	PoC	Production
Base légale définie	✅	✅
Minimisation des données	✅	✅
Données fictives/anonymisées pour tests	✅	N/A
Authentification et contrôle d'accès	✅	✅
Chiffrement des données	Partiel	✅ Requis
Désignation d'un DPO	N/A	✅ Requis

Analyse d'Impact (AIPD)	N/A	✅ Requis
Registre des traitements	N/A	✅ Requis

Recommandations pour la production

Actions requises avant mise en production :

- Réaliser une Analyse d'Impact (AIPD) complète - obligatoire pour les données de santé à grande échelle
- Désigner un Délégué à la Protection des Données (DPO)
- Activer le chiffrement HTTPS/TLS et le chiffrement des données au repos
- Constituer le registre des activités de traitement (Article 30)
- Implémenter les fonctionnalités d'exercice des droits (accès, portabilité, effacement)
- Définir les procédures de notification de violation (72h - Article 33)

Statut : La PoC respecte les principes RGPD applicables à un environnement de développement. L'utilisation de données fictives et les mesures de sécurité implémentées (JWT, BCrypt, RBAC) démontrent la prise en compte des exigences réglementaires dès la conception (Privacy by Design).

Recommandations

Sur la base de cette évaluation, les recommandations suivantes sont formulées pour le passage en production :

Priorité haute

- **Continuité d'activité (B1) :** Implémenter les patterns de résilience (circuit breaker, retry) avec Resilience4j et configurer la réplication de base de données.
- **Sécurité (B5) :** Réaliser un audit de sécurité OWASP, implémenter l'authentification OAuth2/JWT et ajouter le rate limiting.

Priorité moyenne

- **Architecture événementielle (B6) :** Intégrer Apache Kafka pour la publication des événements métier (allocation de lit, changement de disponibilité).
- **Observabilité :** Déployer une stack de monitoring (Prometheus/Grafana) et implémenter le distributed tracing.

Conclusion et approbation

La Preuve de Concept du système d'allocation de lits d'urgence démontre un niveau de conformité satisfaisant avec les principes architecturaux du consortium MedHead.

Avec 11 principes pleinement conformes sur 14 (79%) et 3 principes partiellement conformes, la PoC valide les hypothèses techniques critiques et fournit une base solide pour le développement du système de production.

Les écarts identifiés (B1, B5, B6) sont documentés avec des recommandations claires et n'invalident pas la démonstration de faisabilité. Ces points devront être adressés lors de la phase de mise en production.

Approbation

Nom	Rôle	Signature
Kara Trace	Membre du CA MedHead	
	Architecte PoC	