

15 DECEMBRE 2025



# REGISTRE DES RISQUES

IDENTIFICATION, EVALUATION ET SUIVI DES RISQUES PROJET

Louis ZEPHIR  
MEDHEAD

## 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

## Table des matières

Synthèse exécutive.....	3
Statistiques clés .....	3
Points d'attention.....	3
Méthodologie d'évaluation .....	4
Échelle de probabilité.....	4
Échelle d'impact .....	4
Interprétation du score .....	4
Vue d'ensemble des risques.....	5
Matrice des risques.....	6
Fiches de risques détaillées .....	7
Plan d'action prioritaire .....	10
Actions immédiates (Q1 2026).....	10
6.2 Actions court terme (Q2-Q3 2026).....	10
Processus de gestion des risques .....	11
Identification .....	11
Évaluation .....	11
Suivi .....	11
Responsabilités.....	11

# Synthèse exécutive

Ce registre recense les risques identifiés pour le projet de Preuve de Concept du système d'allocation de lits d'urgence MedHead. Chaque risque est évalué selon sa probabilité et son impact, avec un plan de mitigation associé.

## Statistiques clés

Par Status		Par Niveau de risque	
Ouvert	4	Critique (15-25)	5
Surveillé	2	Élevé (10-14)	5
Mitigé	5	Moyen (6-9)	1
Accepté	1	Faible (1-5)	1
<b>TOTAL</b>	<b>12</b>	<b>TOTAL</b>	<b>12</b>

## Points d'attention

- **4 risques ouverts** nécessitent une action immédiate dans le cadre de la Phase 1 de la feuille de route.
- Le risque R003 (Sécurité) présente le score le plus élevé (20/25) et est prioritaire.
- **5 risques ont été mitigés** grâce aux mesures prises pendant le développement de la PoC.

# Méthodologie d'évaluation

Les risques sont évalués selon deux dimensions : la probabilité d'occurrence et l'impact sur le projet. Le score final est le produit de ces deux facteurs.

## Échelle de probabilité

Niveau	Valeur	Description
Très basse	1	Très peu probable (< 10%)
Basse	2	Peu probable (10-25%)
Moyenne	3	Possible (25-50%)
Haute	4	Probable (50-75%)
Très haute	5	Quasi certain (> 75%)

## Échelle d'impact

Niveau	Valeur	Description
Négligeable	1	Impact minimal, facilement absorbable
Faible	2	Impact limité, perturbation mineure
Moyen	3	Impact significatif, ajustements nécessaires
Élevé	4	Impact majeur sur les délais ou la qualité
Critique	5	Impact sur la viabilité du projet ou la sécurité patient

## Interprétation du score

- **Score 15-25 (Critique)** : Action immédiate requise, escalade au comité de pilotage
- **Score 10-14 (Élevé)** : Plan de mitigation prioritaire, suivi hebdomadaire
- **Score 6-9 (Moyen)** : Surveillance régulière, mitigation planifiée
- **Score 1-5 (Faible)** : Surveillance périodique, acceptation possible

# Vue d'ensemble des risques

ID	Risque	Prob.	Impact	Score	Status
R001	Performance insuffisante en temps réel	Moyenne	Critique	15	Mitigé
R002	Absence de mécanismes de résilience	Haute	Élevé	16	Ouvert
R003	Authentification basique insuffisante	Haute	Critique	20	Ouvert
R004	Manque d'observabilité	Moyenne	Élevé	12	Ouvert
R005	Architecture synchrone non extensible	Moyenne	Élevé	12	Accepté
R006	Intégrité des données de référence NHS	Basse	Moyen	4	Mitigé
R007	Résistance au changement des équipes hospitalières	Moyenne	Élevé	12	Surveillé
R008	Scalabilité pour 2000 hôpitaux	Moyenne	Critique	15	Surveillé
R009	Non-conformité RGPD	Basse	Critique	10	Mitigé
R010	Indisponibilité de la base de données	Moyenne	Critique	15	Ouvert
R011	Dérive du périmètre (scope creep)	Moyenne	Moyen	9	Mitigé
R012	Dépendance à des bibliothèques vulnérables	Moyenne	Élevé	12	Mitigé

## Matrice des risques

La matrice ci-dessous positionne chaque risque selon sa probabilité (axe vertical) et son impact (axe horizontal).

	Négligeable (1)	Faible (2)	Moyen (3)	Élevé (4)	Critique (5)
Très haute (5)					
Haute (4)				R002	R003
Moyenne (3)			R011	R004, R005, R007, R012	R001, R008, R010
Basse (2)			R006		R009
Très basse (1)					

### Légende des couleurs :

- Critique (15-25)
- Élevé (10-14)
- Moyen (6-9)
- Faible (1-5)

# Fiches de risques détaillées

## R001 - Performance insuffisante en temps réel

Catégorie	Technique	Score	15/25
Probabilité	Moyenne	Status	Mitigé
Impact	Critique	Responsable	Architecte technique

### Description :

Le système ne répond pas dans les délais requis (< 1 seconde) sous charge normale ou en pic de demandes.

### Plan de mitigation :

Tests de performance continus, optimisation des requêtes SQL, mise en cache, indexation appropriée.

## R002 - Absence de mécanismes de résilience

Catégorie	Technique	Score	16/25
Probabilité	Haute	Status	Ouvert
Impact	Élevé	Responsable	Équipe développement

### Description :

La PoC ne dispose pas de circuit breakers, retry policies ou fallback en cas de défaillance des systèmes auxiliaires.

### Plan de mitigation :

Phase 1 de la feuille de route : implémenter Resilience4j avec circuit breakers sur tous les appels externes.

## R003 - Authentification basique insuffisante

Catégorie	Sécurité	Score	20/25
Probabilité	Haute	Status	Ouvert
Impact	Critique	Responsable	Architecte sécurité

### Description :

L'authentification actuelle ne respecte pas les standards NHS (OAuth2/OpenID Connect).

### Plan de mitigation :

Phase 1 : mise en place OAuth2/JWT, intégration future avec NHS Identity.

## R004 - Manque d'observabilité

Catégorie	Opérationnel	Score	12/25
Probabilité	Moyenne	Status	Ouvert
Impact	Élevé	Responsable	Équipe SRE

### Description :

Absence de monitoring centralisé, métriques et distributed tracing pour le diagnostic des incidents.

### Plan de mitigation :

Phase 3 : déploiement Prometheus/Grafana et Jaeger pour le tracing distribué.

## R005 - Architecture synchrone non extensible

Catégorie	Technique	Score	12/25
Probabilité	Moyenne	Status	Accepté
Impact	Élevé	Responsable	Architecte solution

### Description :

L'architecture actuelle ne supporte pas le modèle événementiel requis pour l'intégration avec le lac de données.

### Plan de mitigation :

Phase 2 : intégration Apache Kafka pour le bus d'événements. Accepté pour la PoC.

## R006 - Intégrité des données de référence NHS

Catégorie	Données	Score	4/25
Probabilité	Basse	Status	Mitigé
Impact	Moyen	Responsable	Data owner

### Description :

Les données de spécialités NHS peuvent évoluer et diverger du référentiel officiel.

### Plan de mitigation :

Processus de synchronisation mensuelle avec le référentiel NHS Digital. Validation à l'import.

## R007 - Résistance au changement des équipes hospitalières

Catégorie	Projet	Score	12/25
Probabilité	Moyenne	Status	Surveillé
Impact	Élevé	Responsable	Chef de projet

### Description :

Les utilisateurs finaux peuvent rejeter le nouveau système par habitude ou méfiance.

### Plan de mitigation :

Phase 4 (Pilote) : accompagnement au changement, formation, feedback utilisateur, ambassadeurs.

## R008 - Scalabilité pour 2000 hôpitaux

Catégorie	Technique	Score	15/25
Probabilité	Moyenne	Status	Surveillé
Impact	Critique	Responsable	Architecte technique

### Description :

L'architecture actuelle n'a pas été validée pour le volume national (2000 hôpitaux, 200 000 lits).

### Plan de mitigation :

Phase 5 : tests de charge à grande échelle, architecture Kubernetes auto-scaling, optimisation.

## R009 - Non-conformité RGPD

Catégorie	Conformité	Score	10/25
Probabilité	Basse	Status	Mitigé
Impact	Critique	Responsable	DPO

**Description :**

Risque de traitement non conforme des données patients dans les environnements de test.

**Plan de mitigation :**

Utilisation exclusive de données anonymisées ou fictives. Pas de données patients réelles en PoC.

**R010 - Indisponibilité de la base de données**

<b>Catégorie</b>	Opérationnel	<b>Score</b>	15/25
<b>Probabilité</b>	Moyenne	<b>Status</b>	Ouvert
<b>Impact</b>	Critique	<b>Responsable</b>	DBA / SRE

**Description :**

Point unique de défaillance (SPOF) avec une seule instance PostgreSQL.

**Plan de mitigation :**

Phase 1 : mise en place d'un cluster PostgreSQL répliqué avec failover automatique.

**R011 - Dérive du périmètre (scope creep)**

<b>Catégorie</b>	Projet	<b>Score</b>	9/25
<b>Probabilité</b>	Moyenne	<b>Status</b>	Mitigé
<b>Impact</b>	Moyen	<b>Responsable</b>	Chef de projet

**Description :**

Ajout de fonctionnalités non prévues retardant la livraison de la PoC.

**Plan de mitigation :**

Gouvernance stricte, backlog priorisé, validation des changements par le comité d'architecture.

**R012 - Dépendance à des bibliothèques vulnérables**

<b>Catégorie</b>	Technique	<b>Score</b>	12/25
<b>Probabilité</b>	Moyenne	<b>Status</b>	Mitigé
<b>Impact</b>	Élevé	<b>Responsable</b>	Équipe développement

**Description :**

Les dépendances Maven peuvent contenir des CVE non corrigées.

**Plan de mitigation :**

OWASP Dependency-Check intégré au pipeline CI/CD, mise à jour régulière des dépendances.

# Plan d'action prioritaire

Les actions suivantes sont prioritaires pour réduire l'exposition aux risques critiques et élevés.

## Actions immédiates (Q1 2026)

1. [R003] Implémenter OAuth2/JWT et préparer l'intégration NHS Identity
2. [R002] Ajouter Resilience4j avec circuit breakers sur tous les appels externes
3. [R010] Mettre en place le cluster PostgreSQL avec réPLICATION
4. [R004] Déployer la stack d'observabilité Prometheus/Grafana

## Actions court terme (Q2-Q3 2026)

5. [R005] Intégrer Apache Kafka pour l'architecture événementielle
6. [R007] Lancer le programme d'accompagnement au changement pour le pilote
7. [R008] Réaliser les tests de charge à grande échelle

# Processus de gestion des risques

## Identification

Les risques peuvent être identifiés par tout membre de l'équipe projet. Ils sont soumis via le formulaire dédié et examinés lors de la revue hebdomadaire.

## Évaluation

Chaque risque est évalué par l'architecte solution et le chef de projet selon la méthodologie décrite en section 2.

## Suivi

- **Revue hebdomadaire** : Point sur les risques ouverts et les actions en cours
- **Comité mensuel** : Revue complète du registre avec le comité de pilotage
- **Escalade immédiate** : Pour tout nouveau risque critique (score  $\geq 15$ )

## Responsabilités

Rôle	Responsabilités
Chef de projet	Maintien du registre, coordination des actions, reporting
Architecte solution	Évaluation technique, définition des mitigations
Propriétaire du risque	Suivi et mise en œuvre du plan de mitigation
Comité de pilotage	Validation des risques critiques, arbitrage, décisions