Analyse des Risques - Mise en place de HeelonGed

Document destiné aux clients - Trust Center
Version : 1.0
Date : 05/05/2026
Rédigé par : Patrick Paysan (HeelonGed)

Introduction

Ce document présente une **analyse des risques** liée à la mise en place de **HeelonGed** (Gestion Électronique de Documents) en interne, conformément aux exigences :

- **ISO 15189** (laboratoires de biologie médicale).
- **RGPD** (protection des données personnelles).
- **HDS** (Hébergement de Données de Santé en France, si applicable).
- **ISO 27001** (sécurité de l'information).

L'objectif est d'identifier, évaluer et mitiger les risques associés à l'utilisation de HeelonGed pour la **gestion des documents sensibles** (ex: résultats de laboratoire, procédures qualité, données patients).

---

1. Contexte et Périmètre

1.1 Périmètre de l'Analyse

Élément	Détails
Système	HeelonGed (API Rust/Axum + SQLite), version 1.0.3.
Environnement	En local ou Déploiement sur VPS (Fedora + Podman rootful).
Utilisateurs	Laboratoires de biologie médicale, personnel administratif et technique.
Données gérées	Documents qualité (SMQ), résultats de laboratoire, procédures, enregistrements d'audit.
Exigences réglementaires	ISO 15189, RGPD, HDS (si hébergement de données de santé).

1.2 Méthodologie

- **Identification des risques** : Brainstorming + retour d’expérience (REX) sur les GED.
- **Évaluation** : Matrice **Impact x Probabilité** (échelle 1 à 5).
- **Mitigation** : Mesures techniques et organisationnelles pour réduire les risques.
- **Acceptabilité** : Risque résiduel après mitigation (à valider par le client).

---

2. Identification des Risques

2.1 Risques Liés à la Sécurité des Données

ID	Risque	Description	Cause Possible	Impact Potentiel
R1	**Accès non autorisé**	Un utilisateur non autorisé accède à des documents sensibles (ex: résultats patients).	Mauvaises permissions, clés API compromises.	**Critique** : Violation RGPD, perte de confiance, sanctions légales (jusqu’à 4% du CA).
R2	**Perte de données**	Suppression accidentelle ou corruption de documents (ex: base SQLite, fichiers).	Erreur humaine, panne matérielle.	**Critique** : Perte d’informations vitales, non-conformité ISO 15189.
R3	**Fuite de données**	Fuites de documents via des vulnérabilités (ex: injection SQL, mauvaise configuration CORS).	Failles de sécurité dans l’API.	**Critique** : Sanctions RGPD, atteinte à la réputation.
R4	**Chiffrement insuffisant**	Données sensibles non chiffrées (au repos ou en transit).	Configuration incorrecte.	**Majeur** : Risque de vol de données, non-conformité HDS.
R5	**Sauvegardes défaillantes**	Échec des sauvegardes automatiques.	Script de backup non testé, espace disque insuffisant.	**Majeur** : Impossibilité de restauration, perte de données.

2.2 Risques Liés à la Disponibilité

ID	Risque	Description	Cause Possible	Impact Potentiel
R6	**Indisponibilité du service**	HeelonGed inaccessible (ex: panne serveur, attaque DDoS).	Problème réseau, saturation du serveur.	**Majeur** : Blocage des activités du laboratoire.
R7	**Corruption de la base de données**	La base SQLite (`ged.db`) est corrompue.	Arrêt brutal du conteneur Podman.	**Critique** : Perte de traçabilité, non-conformité ISO 15189.
R8	**Dépassement de la capacité**	Saturation du stockage (`STORAGE_PATH`) ou de la base de données.	Limite `MAX_UPLOAD_MB` trop élevée.	**Mineur** : Ralentissement du système.

2.3 Risques Liés à l'Intégrité

ID	Risque	Description	Cause Possible	Impact Potentiel
R9	**Modification non autorisée**	Un document est modifié sans validation (ex: procédure qualité).	Absence de workflow d'approbation.	**Majeur** : Non-conformité ISO 15189, erreurs opérationnelles.
R10	**Versionnage incorrect**	Perte de l'historique des versions d'un document.	Mauvaise utilisation de l'API.	**Majeur** : Impossibilité de rollback, non-conformité audit.
R11	**Falsification de logs**	Les logs d'audit (`audit_logs`) sont altérés.	Accès root non contrôlé.	**Critique** : Perte de traçabilité, fraude.

2.4 Risques Liés à la Conformité

ID	Risque	Description	Cause Possible	Impact Potentiel
R12	**Non-conformité ISO 15189**	HeelonGed ne répond pas aux exigences de traçabilité ou de validation.	Validation incomplète du système.	**Critique** : Perte d'accréditation COFRAC.
R13	**Non-conformité RGPD**	Données personnelles (ex: noms de patients) non protégées.	Absence de chiffrement ou de pseudonymisation.	**Critique** : Sanctions RGPD (jusqu'à 20M€ ou 4% du CA).

R14	**Non-conformité HDS**	Hébergement de données de santé sans certification HDS.	Hébergement non conforme en France.	**Critique** : Sanctions, perte de confiance.

2.5 Risques Liés à l'Utilisation

ID	Risque	Description	Cause Possible	Impact Potentiel
R15	**Erreur humaine**	Mauvaise manipulation des documents (ex: suppression accidentelle).	Formation insuffisante.	**Mineur/Majeur** : Perte de temps, restauration nécessaire.
R16	**Adoption faible**	Les utilisateurs ne adoptent pas HeelonGed (préfèrent le papier ou d'autres outils).	Manque de formation ou d'ergonomie.	**Mineur** : Baisse de productivité.
R17	**Compatibilité logicielle**	Incompatibilité avec d'autres systèmes (ex: LIMS, logiciels de paie).	Format de fichiers non standard.	**Majeur** : Blocage des processus métiers.

3. Évaluation des Risques

3.1 Matrice d'Évaluation

Échelles :

- **Impact** : 1 (Faible) → 5 (Critique).
- **Probabilité** : 1 (Très improbable) → 5 (Très probable).
- **Score de risque** = Impact × Probabilité.

Score	Niveau de Risque	Action Recommandée
1-5	Faible	Accepter (surveillance minimale).
6-12	Moyen	Mitiger si possible.
13-25	Élevé/Critique	**Mitiger impérativement**.

3.2 Évaluation par Risque

ID	Risque	Impact	Probabilité	Score	Niveau	Acceptabilité
R1	Accès non autorisé	5	3	15	Élevé	Non acceptable
R2	Perte de données	5	2	10	Moyen	À mitiger
R3	Fuite de données	5	2	10	Moyen	À mitiger
R4	Chiffrement insuffisant	4	3	12	Moyen	À mitiger
R5	Sauvegardes défaillantes	5	2	10	Moyen	À mitiger
R6	Indisponibilité	4	2	8	Moyen	À mitiger
R7	Corruption de la base	5	1	5	Faible	Acceptable
R8	Dépassement capacité	2	3	6	Moyen	À surveiller
R9	Modification non autorisée	4	3	12	Moyen	À mitiger
R10	Versionnage incorrect	4	2	8	Moyen	À mitiger
R11	Falsification de logs	5	1	5	Faible	Acceptable
R12	Non-conformité ISO 15189	5	2	10	Moyen	À mitiger
R13	Non-conformité RGPD	5	2	10	Moyen	À mitiger
R14	Non-conformité HDS	5	1	5	Faible	Acceptable*
R15	Erreur humaine	3	4	12	Moyen	À mitiger
R16	Adoption faible	2	3	6	Moyen	À surveiller
R17	Incompatibilité logicielle	3	2	6	Moyen	À surveiller

*Si HeelonGed est hébergé sur un VPS certifié HDS ou équivalent.

4. Mesures de Mitigation

4.1 Mesures Techniques

ID	Risque	Mesure de Mitigation	Responsable	Échéance	Statut
R1	Accès non autorisé	- **Authentification forte** (2FA) pour les utilisateurs. - **Clés API sécurisées** (rotation tous les 90 jours). - **Rôles stricts** (lecteur/éditeur/admin).	Admin GED	Immédiat	
R2	Perte de données	- **Sauvegardes automatiques** quotidiennes (base + fichiers). - **Test de restauration** mensuel. - **Stockage redondant** (ex: RAID ou cloud).	Admin IT	1 mois	
R3	Fuite de données	- **Chiffrement des données au repos** (AES-256). - **Chiffrement en transit** (TLS 1.3). - **Audit des accès** (logs `audit_logs`).	Admin Sécurité	2 semaines	
R4	Chiffrement insuffisant	- **Activer le chiffrement** pour les dossiers sensibles (`STORAGE_PATH`). - **Utiliser des conteneurs sécurisés** (Podman avec SELinux).	Admin IT	Immédiat	
R5	Sauvegardes défaillantes	- **Script de backup testé** (voir Annexe A). - **Alertes en cas d’échec** (email/SMS).	Admin IT	1 semaine	
R6	Indisponibilité	- **Redondance du serveur** (cluster Podman ou Kubernetes). - **Monitoring** (ex: Prometheus + Grafana).	Admin Sécurité	3 mois	
R9	Modification non autorisée	- **Workflow d’approbation** (statut `draft` → `approved`). - **Notifications** pour les modifications.	Admin Qualité	2 semaines	
R10	Versionnage	- **Formation des utilisateurs** sur	Admin GED	1 mois	

	incorrect	l'API de versionnage. - **Documentation claire** (ex: guide utilisateur).		
R12	Non-conformité ISO 15189	- **Validation complète** du système (voir Guide de Conformité). - **Audit interne** annuel.	Admin Qualité	2 mois
R13	Non-conformité RGPD	- **Anonymisation/pseudonymisation** des données patients. - **DPO désigné** pour superviser.	DPO	Immédiat
R15	Erreur humaine	- **Formation obligatoire** pour tous les utilisateurs. - **Interface intuitive** (UI/UX).	RH	1 mois

4.2 Mesures Organisationnelles

Mesure	Description	Responsable
Politique de sécurité	Rédiger une **charte d'utilisation** de HeelonGed (ex: interdiction de partager les clés API).	Admin Sécurité
Gestion des incidents	Mettre en place un **processus de signalement** des incidents (ex: formulaire dédié).	Admin Qualité
Revues de sécurité	**Audit trimestriel** des logs et des accès.	Admin Sécurité
Sensibilisation	**Campagnes de sensibilisation** régulières (ex: phishing, bonnes pratiques GED).	RH
Contrats avec les prestataires	Vérifier que les **sous-traitants** (ex: hébergeur VPS) respectent le RGPD et la HDS.	Juridique

5. Risques Résiduels

Après application des mesures de mitigation, les **risques résiduels** sont les suivants :

ID	Risque	Score Initial	Score Résiduel	Niveau Résiduel	Acceptabilité	Justification
R1	Accès non autorisé	15	5	Faible	Acceptable	Mesures : 2FA + rôles stricts + audit.

R2	Perte de données	10	3	Faible	Acceptable	Sauvegardes automatiques + tests de restauration.
R3	Fuite de données	10	4	Moyen	À surveiller	Chiffrement activé, mais risque résiduel lié aux vulnérabilités 0-day.
R6	Indisponibilité	8	6	Moyen	À surveiller	Redondance partielle (pas de cluster encore).
R12	Non-conformité ISO 15189	10	4	Moyen	À surveiller	Validation en cours, audit interne prévu.
R13	Non-conformité RGPD	10	3	Faible	Acceptable	Mesures : chiffrement + DPO + anonymisation.

6. Plan d’Action

6.1 Actions Prioritaires

Action	Responsable	Échéance	Statut	Indicateur de Suivi
Mettre en place le 2FA	Admin Sécurité	15/05/2026		% d’utilisateurs avec 2FA activé.
Tester les sauvegardes automatiques	Admin IT	20/05/2026		Rapport de test de restauration.
Chiffrer les données sensibles	Admin IT	10/05/2026		% de fichiers chiffrés.
Former les utilisateurs	RH	30/05/2026		Nombre d’utilisateurs formés.
Valider HeelonGed (ISO 15189)	Admin Qualité	30/06/2026		Rapport de validation signé.
Mettre en place un monitoring	Admin Sécurité	01/06/2026		Tableau de bord Grafana opérationnel.

6.2 Actions à Long Terme

Action	Responsable	Échéance	Statut
Déployer un cluster Podman/K8s	Admin IT	Q3 2026	
Obtenir la certification HDS	Juridique	Q4 2026	
Automatiser les audits de sécurité	Admin Sécurité	Q2 2026	

7. Annexes

Annexe A : Script de Sauvegarde Automatique

```
#!/bin/bash
# Script de sauvegarde pour HeelonGed
# À exécuter quotidiennement via cron (ex: 0 2 * * *)

# Variables
BACKUP_DIR="/srv/backups/heelonged"
DATE=$(date +%Y%m%d_%H%M%S)
DB_PATH="/srv/heelonged-backend/db/ged.db"
FILES_PATH="/srv/heelonged-backend/files"
LOG_FILE="/var/log/heelonged_backup.log"

# Créer le dossier de backup
mkdir -p $BACKUP_DIR/$DATE

# Sauvegarder la base de données
echo "[$(date)] Début de la sauvegarde de la base..." >> $LOG_FILE
podman exec heelonged-backend sh -c "sqlite3 $DB_PATH '.backup
$BACKUP_DIR/$DATE/ged.db'" 2>> $LOG_FILE
if [ $? -eq 0 ]; then
  echo "[$(date)] Sauvegarde de la base réussie." >> $LOG_FILE
else
  echo "[$(date)] ERREUR : Échec de la sauvegarde de la base." >> $LOG_FILE
  exit 1
fi

# Sauvegarder les fichiers
echo "[$(date)] Début de la sauvegarde des fichiers..." >> $LOG_FILE
cp -r $FILES_PATH $BACKUP_DIR/$DATE/files 2>> $LOG_FILE
if [ $? -eq 0 ]; then
  echo "[$(date)] Sauvegarde des fichiers réussie." >> $LOG_FILE
else
  echo "[$(date)] ERREUR : Échec de la sauvegarde des fichiers." >> $LOG_FILE
```

```
  exit 1
fi

# Compresser les sauvegardes
echo "[$(date)] Compression des sauvegardes..." >> $LOG_FILE
tar -czf $BACKUP_DIR/heelonged_backup_$DATE.tar.gz -C $BACKUP_DIR/$DATE . 2>>
$LOG_FILE

# Nettoyer les anciennes sauvegardes (> 30 jours)
echo "[$(date)] Nettoyage des sauvegardes anciennes..." >> $LOG_FILE
find $BACKUP_DIR -type d -mtime +30 -exec rm -rf {} \; 2>> $LOG_FILE

echo "[$(date)] Sauvegarde terminée avec succès." >> $LOG_FILE
```

Annexe B : Modèle de Charte d’Utilisation

```
# **Charte d’Utilisation de HeelonGed**

*À signer par tous les utilisateurs*


---

## 1. **Objet**

Cette charte définit les **règles d’utilisation** de HeelonGed pour garantir la **sécurité, la confidentialité et la conformité** des données.


---

## 2. **Engagements de l’Utilisateur**

- [ ] **Respecter les droits d’accès** : Ne pas partager ses identifiants ou clés API.

- [ ] **Utiliser HeelonGed conformément** à sa destination (gestion de documents professionnels).

- [ ] **Signaler toute anomalie** (ex: accès suspect, perte de données) à l’administrateur.

- [ ] **Respecter les règles de nommage** des fichiers (voir [Guide des Bonnes Pratiques](#)).

- [ ] **Ne pas stocker de données personnelles** non autorisées (ex: données patients sans anonymisation).


---

## 3. **Engagements de HeelonGed**

- Maintenir un **niveau de sécurité élevé** (chiffrement, sauvegardes, audits).

- **Former les utilisateurs** aux bonnes pratiques.

- **Corriger les vulnérabilités** dans les meilleurs délais.


---

## 4. **Sanctions**

Tout manquement à cette charte peut entraîner :

- La **suspension de l’accès** à HeelonGed.

- Des **actions disciplinaires** (selon le règlement interne du laboratoire).

- Des **poursuites légales** en cas de violation du RGPD ou de la HDS.


---
```

5. **Signature**

Nom : _____

Prénom : _____

Service : _____

Date : _____

Signature : _____

Annexe C : Modèle de Fiche de Signalement d’Incident

```
# **Fiche de Signalement d’Incident**

*À remplir en cas d’incident lié à HeelonGed*


---

| **Champ**               | **Valeur**                          |

|-------------------------|-------------------------------------|

| **Date/Heure**          | [AAAA-MM-JJ HH:MM]                  |

| **Signalé par**         | [Nom/Prénom]                        |

| **Service**             | [Ex: Biologie, Qualité]             |

| **Type d’incident**     | [√] Accès non autorisé <br> [√] Perte de données
<br> [√] Indisponibilité <br> [√] Autre : _______ |


---

## **Description de l’Incident**

[Décrivez précisément ce qui s’est passé.]


---

## **Impact Estimé**

- [ ] Faible (pas de conséquence majeure)

- [ ] Moyen (perturbation temporaire)

- [ ] Élevé (blocage des activités)

- [ ] Critique (perte de données, violation RGPD)


---

## **Mesures Immédiates Prises**

[Ex: Isolation du système, notification au DPO, etc.]


---

## **Preuves Associées**

- Logs (`audit_logs`) : [Oui/Non]

- Capture d’écran : [Oui/Non] (joindre si possible)

- Autres : _____
```

Transmission

- **Destinataire** : [Admin GED / DPO / Responsable Qualité]
- **Date de transmission** : [AAAA-MM-JJ]

Annexe D : Glossaire

Terme	Définition
GED	Gestion Électronique de Documents.
ISO 15189	Norme internationale pour les laboratoires de biologie médicale.
RGPD	Règlement Général sur la Protection des Données (UE).
HDS	Hébergement de Données de Santé (certification française).
2FA	Double Authentification (ex: mot de passe + code SMS).
Podman	Outil de conteneurisation (alternative à Docker).
Audit Logs	Journaux enregistrant toutes les actions sur les documents.
DPO	Délégué à la Protection des Données.
COFRAC	Comité Français d'Accréditation (organisme certificateur pour les laboratoires).

8. Conclusion

Ce document **identifie, évalue et mitige les risques** liés à la mise en place de **HeelonGed** en interne.
Les mesures proposées permettent de :

Réduire les risques critiques (accès non autorisé, perte de données).
Garantir la conformité avec l'ISO 15189, le RGPD et la HDS.
Assurer la continuité d'activité du laboratoire.

Prochaines étapes pour vos clients :

1. **Valider les risques résiduels** avec leur **DPO** et leur **responsable qualité**.
2. **Mettre en œuvre les mesures prioritaires** (2FA, sauvegardes, formation).
3. **Intégrer ce document** dans leur **Système de Management de la Qualité (SMQ)**.