

Dossier général — Portail de déclaration des incidents de santé et sécurité d'un manufacturier (exemple fictif)

Projet : Portail de déclaration des incidents de santé et sécurité d'un manufacturier (exemple fictif)

Espace : Manufacturier — espace fictif

Version : V2 — 16 octobre 2026

Conservé par : Compte d'exemple

Statut : Résultat assisté par IA

État de la revue : résultat assisté par IA — proposition, revue critique par un second modèle et contrôles automatiques effectués ; aucune validation professionnelle.

Résultat assisté par IA — proposition, revue critique et contrôles automatiques ; non validé par un professionnel ; ne constitue ni une estimation validée ni une offre de prix. Analyse assistée par des fournisseurs d'IA établis aux États-Unis.

Contenu du dossier

- Besoin et objectifs
- Recommandation
- Périmètre et éléments cadrés
- Exclusions
- Hypothèses
- Architecture et flux
- Registre des décisions d'architecture
- Scénario présenté et alternatives

Effort, budgets et récurrent

- Limites, hypothèses de prix et inconnues
- Risques et dépendances
- Délai
- Prochaines décisions
- État de la revue IA et réserves
- Références et versions

Besoin et objectifs

Remplacer les formulaires papier et le chiffrier partagé par un portail interne de déclaration, d'enquête et de suivi des incidents, quasi-accidents et situations dangereuses, dans quatre usines.

Le manufacturier compte 1 200 employés dans quatre usines. Les déclarations se font sur papier et dans un chiffrier partagé, jugé insuffisant. Le portail traite des coordonnées, des renseignements de santé et des dossiers d'employés. Les données doivent rester au Canada (politique interne). L'équipe TI interne exploitera la solution selon ses normes d'hébergement infonuagique et de journalisation. Le client est au Québec : la Loi 25 et la loi sur les renseignements de santé et de services sociaux sont à considérer. Trois intégrations sont prévues (annuaire, ressources humaines, progiciel de gestion) et trois ans d'historique doivent être repris. L'échéance est dans l'année ; le budget n'est pas arrêté.

Recommandation

Portail web sur mesure de déclaration et de suivi des incidents, hébergé dans une région canadienne selon les normes de votre équipe TI — Application web adaptative construite sur mesure : formulaire de déclaration avec photos, flux d'enquête et de mesures correctives avec relances, avis automatique des événements graves, droits d'accès par rôle et par donnée sensible, préparation des déclarations réglementaires et tableau de bord. Elle s'appuie sur des services gérés (identité fédérée avec l'annuaire, stockage chiffré de fichiers, envoi de courriels, base de données gérée qui porte aussi la file des traitements différés, journalisation centralisée) et sur trois intégrations (annuaire, ressources humaines, progiciel de gestion). Elle est livrée avec une chaîne de déploiement automatisée, de la documentation technique et un transfert à l'équipe TI.

Le besoin est propre au client : flux d'enquête par superviseur, avis de gravité et visibilité restreinte des renseignements médicaux. Il est lié à trois systèmes existants et à des normes d'hébergement imposées. La référence « acheter ou construire » (non vérifiée) a pour choix par défaut de construire, et rien dans le dossier ne la fait dévier : l'achat d'un produit du marché est examiné à part, comme approche non retenue. La volumétrie est modeste (100 à 1 000 opérations par mois pour 1 200 employés) et la réalisation est confiée à une petite équipe ; un monolithe modulaire (hypothèse, référence non vérifiée) est plus simple à exploiter pour une équipe TI interne que des services séparés. Les données de santé et d'employés justifient des contrôles d'accès par objet, un chiffrement, un second facteur pour tout rôle qui voit des renseignements protégés, un journal d'audit et des vérifications selon les références OWASP (Top 10, ASVS, API) ; l'identité passe par la fédération avec l'annuaire. La région canadienne respecte la politique de territoire. Une région hors Québec appelle l'examen des

facteurs relatifs à la vie privée avant toute communication de renseignements hors du Québec (Loi 25), à faire par vous.

Conditions :

- Les normes d'hébergement et de journalisation de votre équipe TI sont communiquées avant la conception technique.
- Des environnements d'essai et un interlocuteur sont fournis pour l'annuaire, les ressources humaines et le progiciel de gestion.
- L'annuaire peut imposer un second facteur aux rôles qui voient les renseignements de santé.
- Le chiffrier des trois dernières années est livré tôt, avec une personne de l'entreprise pour valider la correspondance des données.
- Un responsable de la protection des renseignements personnels et un responsable du service de santé et sécurité sont désignés pour valider les rôles, les seuils de gravité et les règles de conservation.
- Pour tenir une échéance ou un budget qui seraient fixés, les leviers sont de phaser le périmètre (par exemple tableau de bord ou reprise de l'historique en second temps), de lancer un pilote dans une usine ou de renforcer l'équipe.

Périmètre inclus

Code	Nature	Élément	État
E-1	Objectif	Remplacer le papier et le chiffrier par un portail unique	à confirmer
E-2	Exigence	Déclaration par tout employé, sur poste ou téléphone	à confirmer
E-3	Exigence	Enquête du superviseur et mesures correctives avec relances	à confirmer
E-4	Exigence	Avis immédiat pour les événements graves	à confirmer
E-5	Exigence	Accès restreint aux renseignements médicaux et à l'identité des blessés	à confirmer
E-6	Exigence	Préparation des déclarations obligatoires à l'organisme de réglementation	à confirmer
E-7	Exigence	Tableau de bord par usine et par mois	à confirmer
E-8	Exigence	Ouverture de session par l'annuaire de l'entreprise	à confirmer
E-9	Exigence	Employés et supérieurs issus du système de ressources humaines	à confirmer
E-10	Exigence	Usines et départements issus du progiciel de gestion	à confirmer

Code	Nature	Élément	État
E-11	Exigence	Reprise de trois ans de déclarations du chiffrier	à confirmer
E-12	Contrainte	Exploitation par l'équipe TI selon ses normes d'hébergement et de journalisation	à confirmer
E-13	Contrainte	Données au Canada	à confirmer
E-14	Contrainte	Exigence de territoire : politique interne, sans obligation externe	à confirmer
E-15	Contrainte	Données de santé, d'identification et d'employés : protection renforcée	à confirmer
E-16	Contrainte	Budget non arrêté	à confirmer
E-17	Contrainte	Échéance dans l'année	à confirmer
E-18	Exigence	Sécurité applicative, chiffrement et journal d'audit des accès sensibles	à confirmer
E-19	Exigence	Disponibilité du portail	à confirmer
E-20	Exigence	Dépôt et gestion des photos et pièces jointes	à confirmer
E-21	Exigence	Notifications par courriel ou par message	à confirmer
E-22	Exigence	Accessibilité des écrans visée au niveau AA, vérifiée sur les parcours essentiels	à confirmer
E-23	Hypothèse	Application web adaptée au téléphone, sans application native	à confirmer
E-24	Hypothèse	Volumétrie : environ 1 200 employés, 1 000 déclarations par mois retenues	à confirmer
E-25	Hypothèse	Comptes fournis par l'annuaire ; rôles et droits construits dans le portail	à confirmer
E-26	Hypothèse	Aucun logiciel de santé et sécurité existant à conserver	à confirmer
E-27	Hypothèse	Rythme de réalisation de base : une personne à temps plein	à confirmer
E-28	Hypothèse	Durées minimales de calendrier pour la recette et la stabilisation	à confirmer

E-29 figure à la section « Exclusions ».

E-30 figure à la section « Exclusions ».

E-31 figure à la section « Exclusions ».

Exclusions

- E-29 — Dépôt des déclarations à l'organisme de réglementation
- E-30 — Formation des utilisateurs et supports qui leur sont destinés
- E-31 — Conseil juridique ou réglementaire

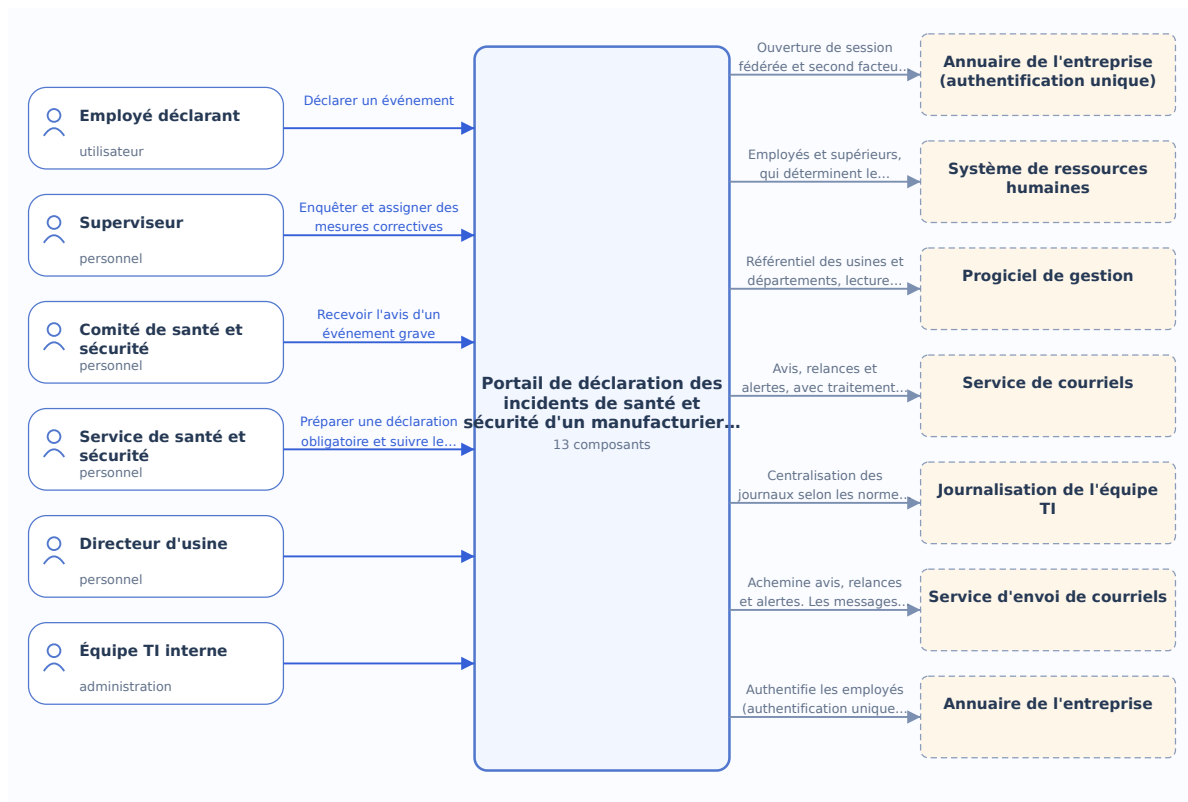
Principales hypothèses

- Application web adaptée au téléphone, sans application native
- Volumétrie : environ 1 200 employés, 1 000 déclarations par mois retenues
- Comptes fournis par l'annuaire ; rôles et droits construits dans le portail
- Aucun logiciel de santé et sécurité existant à conserver
- Rythme de réalisation de base : une personne à temps plein
- Durées minimales de calendrier pour la recette et la stabilisation

Architecture proposée

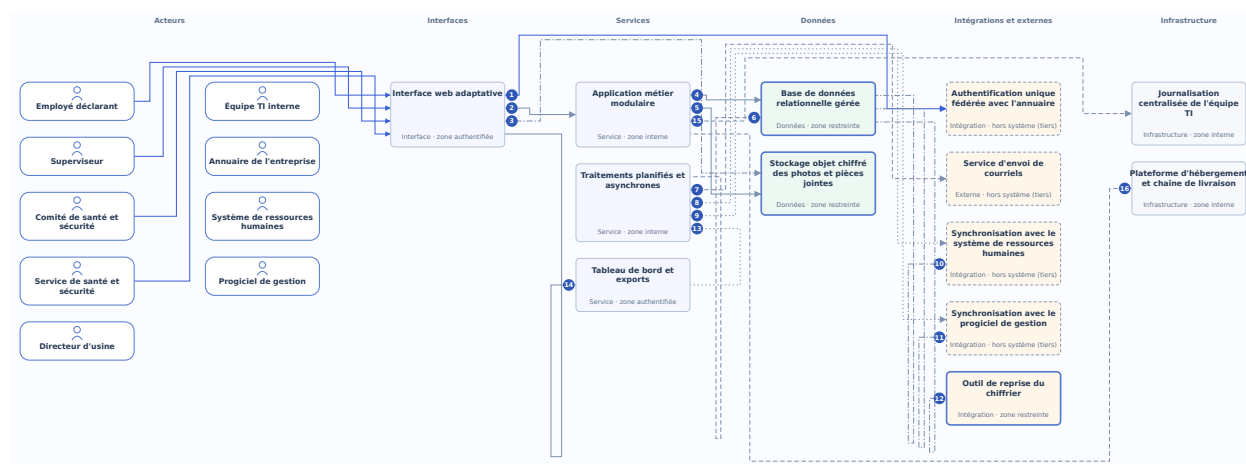
Application web adaptative construite sur mesure : formulaire de déclaration avec photos, flux d'enquête et de mesures correctives avec relances, avis automatique des événements graves, droits d'accès par rôle et par donnée sensible, préparation des déclarations réglementaires et tableau de bord. Elle s'appuie sur des services gérés (identité fédérée avec l'annuaire, stockage chiffré de fichiers, envoi de courriels, base de données gérée qui porte aussi la file des traitements différés, journalisation centralisée) et sur trois intégrations (annuaire, ressources humaines, progiciel de gestion). Elle est livrée avec une chaîne de déploiement automatisée, de la documentation technique et un transfert à l'équipe TI.

Vue d'ensemble



Composants et flux

Traits : appel (plein), événement (tirets), traitement planifié (pointillés), fichier (tiret-point), action d'une personne (bleu). Contour épais : zone restreinte ; contour pointillé : hors système.



Composants

Composant	Nature	Responsabilité
Interface web adaptative	Interface	Formulaire de déclaration (photos, lieu, personnes, gravité), écrans d'enquête, de mesures correctives, de préparation des déclarations réglementaires et tableau de bord. Utilisable sur poste et sur téléphone, sans mode hors ligne ni application native. Photos prises par le navigateur sans enregistrement dans la galerie lorsque possible. Niveau AA des règles WCAG 2.2 visé en hypothèse, vérifié sur les parcours essentiels.
Application métier modulaire	Service	Une application déployée d'un bloc, en modules aux frontières explicites : déclaration, enquête, mesures et relances, gravité et avis, droits d'accès, préparation réglementaire. Applique les droits par rôle, par usine, par dossier et par champ (renseignements médicaux et identité des blessés), valide les entrées et les fichiers, écrit le journal d'audit.
Authentification unique fédérée avec l'annuaire	Intégration	Ouverture de session par l'annuaire de l'entreprise. Le portail ne gère aucun mot de passe. Second facteur porté par l'annuaire pour les administrateurs et pour tout rôle qui voit les champs protégés (superviseurs, comité, service de santé et sécurité). Expiration et révocation des sessions.
Base de données relationnelle gérée	Données	Stockage transactionnel des dossiers, mesures, référentiels, journal d'audit applicatif et file des traitements différés (l'avis d'un événement grave s'écrit dans la même transaction que l'événement). Chiffrée au repos, en région canadienne, avec la protection de base de l'hébergeur (restauration à un instant donné) et migrations de schéma versionnées.
Stockage objet chiffré des photos et pièces jointes	Données	Conserve les fichiers hors de la base, en région canadienne, chiffrés, sans accès public. Téléchargement par liens signés de courte durée, émis seulement si l'utilisateur a le droit de voir le dossier. Les métadonnées et les droits restent en base. Protection de base de l'hébergeur, sans archivage distinct.
Traitements planifiés et asynchrones	Service	Lit la file en base : envoi des avis et courriels avec reprise sur échec, relance des mesures en retard. Exécute les synchronisations nocturnes des référentiels, le calcul des agrégats du tableau de bord et la purge selon la durée de conservation. Aucune file de messages externe.

Composant	Nature	Responsabilité
Service d'envoi de courriels	Externe	Achemine avis, relances et alertes. Les messages ne contiennent ni renseignement médical ni identité des blessés : seulement un lien vers le portail, où les droits s'appliquent. Hypothèse : le courriel est le seul canal ; le message texte reste une alternative, jamais un envoi doublé.
Synchronisation avec le système de ressources humaines	Intégration	Importe les employés et leur supérieur (qui détermine le superviseur destinataire), gère les arrivées, départs et changements, signale les employés sans supérieur.
Synchronisation avec le progiciel de gestion	Intégration	Importe les usines et départements comme référentiels en lecture seule ; conserve les anciens codes pour ne pas casser l'historique.
Outil de reprise du chiffrier	Intégration	Traitement ponctuel : lecture de trois ans de déclarations (environ 36 000 lignes en hypothèse, à confirmer par le chiffrier), nettoyage, correspondance avec les employés, usines et départements, chargement avec rapport d'écarts et rejeu. Supprimé ou verrouillé après la bascule.
Tableau de bord et exports	Service	Agrégats par usine et par mois : nombre d'événements, gravité, mesures en retard, délai moyen de fermeture. Fiche de synthèse exportable par événement déclarable. Respecte les droits : aucune identité ni donnée médicale dans les agrégats.
Journalisation centralisée de l'équipe TI	Infrastructure	Reçoit les journaux techniques et d'audit (connexions, consultations des champs sensibles, changements de droits) dans le format et la destination des normes de l'équipe TI. Les journaux ne contiennent pas de contenu médical.
Plateforme d'hébergement et chaîne de livraison	Infrastructure	Hébergement infonuagique en région canadienne selon les normes de l'équipe TI : environnements séparés, plusieurs zones d'une même région, infrastructure décrite par du code, déploiement automatisé avec retour arrière, secrets hors du code, suivi des dépendances, surveillance et alertes.

Flux

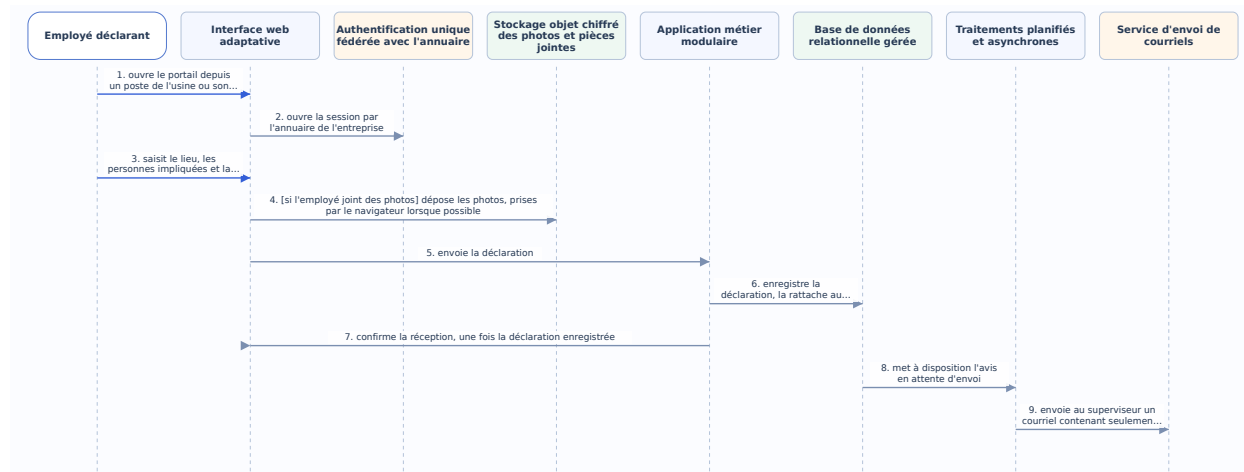
N°	De	Vers	Mode	Échange
1	Interface web adaptative	Authentification unique fédérée avec l'annuaire	action d'une personne	L'employé ouvre une session par l'annuaire ; le portail reçoit une identité vérifiée, avec second facteur pour les rôles qui voient les champs protégés.

N°	De	Vers	Mode	Échange
2	Interface web adaptative	Application métier modulaire	appel	Déclarations, enquêtes, mesures et consultations, toutes soumises au contrôle d'accès.
3	Interface web adaptative	Stockage objet chiffré des photos et pièces jointes	fichier	Dépôt des photos et pièces jointes par liens signés de courte durée, après contrôle du type et de la taille.
4	Application métier modulaire	Base de données relationnelle gérée	appel	Lecture et écriture des dossiers et du journal d'audit ; l'avis d'un événement grave ou d'une mesure est inscrit dans la file en base, dans la même transaction.
5	Application métier modulaire	Stockage objet chiffré des photos et pièces jointes	appel	Émission des liens signés et enregistrement des métadonnées.
6	Base de données relationnelle gérée	Traitements planifiés et asynchrones	événement	Les traitements lisent la file en base : avis immédiat, relances, envois en attente.
7	Traitements planifiés et asynchrones	Service d'envoi de courriels	événement	Avis immédiat au comité et au directeur d'usine, relances des mesures en retard, avec reprise sur échec.
8	Traitements planifiés et asynchrones	Synchronisation avec le système de ressources humaines	traitement planifié	Synchronisation quotidienne des employés et supérieurs.
9	Traitements planifiés et asynchrones	Synchronisation avec le progiciel de gestion	traitement planifié	Synchronisation quotidienne des usines et départements.
10	Synchronisation avec le système de ressources humaines	Base de données relationnelle gérée	fichier	Mise à jour des employés et du rattachement hiérarchique.
11	Synchronisation avec le progiciel de gestion	Base de données relationnelle gérée	fichier	Mise à jour des référentiels d'usines et de départements.
12	Outil de reprise du chiffrer	Base de données relationnelle gérée	fichier	Chargement ponctuel des trois ans d'historique, rapport d'écarts à valider par le client.
13	Traitements planifiés et asynchrones	Tableau de bord et exports	traitement planifié	Calcul des agrégats mensuels par usine.
14	Tableau de bord et exports	Interface web adaptative	appel	Affichage du tableau de bord et téléchargement des fiches de synthèse pour le service de santé et sécurité.
15	Application métier modulaire	Journalisation centralisée de l'équipe TI	événement	Envoi des journaux d'audit et techniques vers l'outil central de l'équipe TI.
16	Plateforme d'hébergement et chaîne de livraison	Application métier modulaire	événement	Déploiement automatisé vers des environnements séparés, avec retour arrière.

Parcours utilisateurs

Déclarer un événement — Employé déclarant

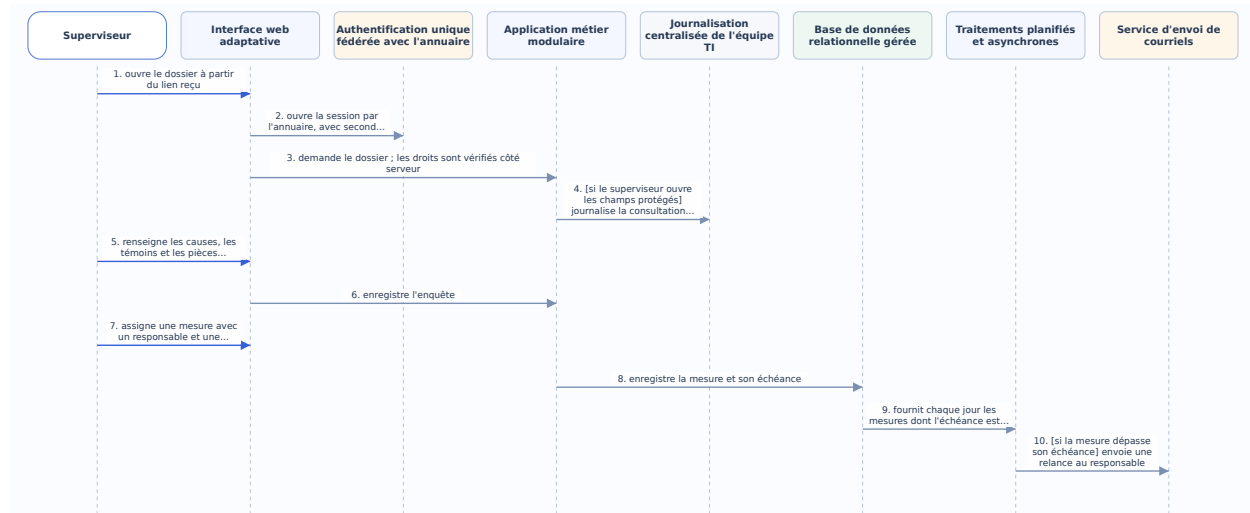
But : Déclarer rapidement un événement avec photos, lieu, personnes et gravité perçue, et être sûr qu'il est bien reçu par son superviseur.



- 1. Employé déclarant → Interface web adaptative : ouvre le portail depuis un poste de l'usine ou son téléphone
- 2. Interface web adaptative → Authentification unique fédérée avec l'annuaire : ouvre la session par l'annuaire de l'entreprise
- 3. Employé déclarant → Interface web adaptative : saisit le lieu, les personnes impliquées et la gravité perçue
- 4. Interface web adaptative → Stockage objet chiffré des photos et pièces jointes : dépose les photos, prises par le navigateur lorsque possible
- 5. Interface web adaptative → Application métier modulaire : envoie la déclaration
- 6. Application métier modulaire → Base de données relationnelle gérée : enregistre la déclaration, la rattache au superviseur et inscrit l'avis au superviseur dans la même écriture
- 7. Application métier modulaire → Interface web adaptative : confirme la réception, une fois la déclaration enregistrée
- 8. Base de données relationnelle gérée → Traitements planifiés et asynchrones : met à disposition l'avis en attente d'envoi
- 9. Traitements planifiés et asynchrones → Service d'envoi de courriels : envoie au superviseur un courriel contenant seulement un lien vers le dossier

Enquêter et assigner des mesures correctives — Superviseur

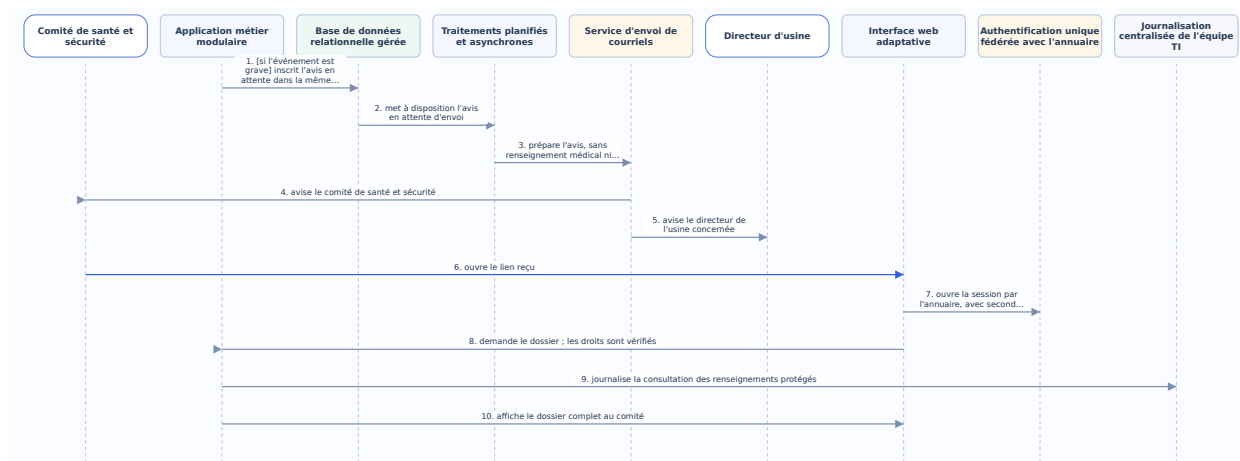
But : Mener l'enquête dans le portail, assigner des mesures avec responsable et échéance, et voir les retards relancés automatiquement.



- 1. Superviseur → Interface web adaptative : ouvre le dossier à partir du lien reçu
- 2. Interface web adaptative → Authentification unique fédérée avec l'annuaire : ouvre la session par l'annuaire, avec second facteur
- 3. Interface web adaptative → Application métier modulaire : demande le dossier ; les droits sont vérifiés côté serveur
- 4. Application métier modulaire → Journalisation centralisée de l'équipe TI : journalise la consultation des renseignements médicaux et de l'identité des blessés
- 5. Superviseur → Interface web adaptative : renseigne les causes, les témoins et les pièces jointes
- 6. Interface web adaptative → Application métier modulaire : enregistre l'enquête
- 7. Superviseur → Interface web adaptative : assigne une mesure avec un responsable et une échéance
- 8. Application métier modulaire → Base de données relationnelle gérée : enregistre la mesure et son échéance
- 9. Base de données relationnelle gérée → Traitements planifiés et asynchrones : fournit chaque jour les mesures dont l'échéance est dépassée
- 10. Traitements planifiés et asynchrones → Service d'envoi de courriels : envoie une relance au responsable

Recevoir l'avis d'un événement grave — Comité de santé et sécurité

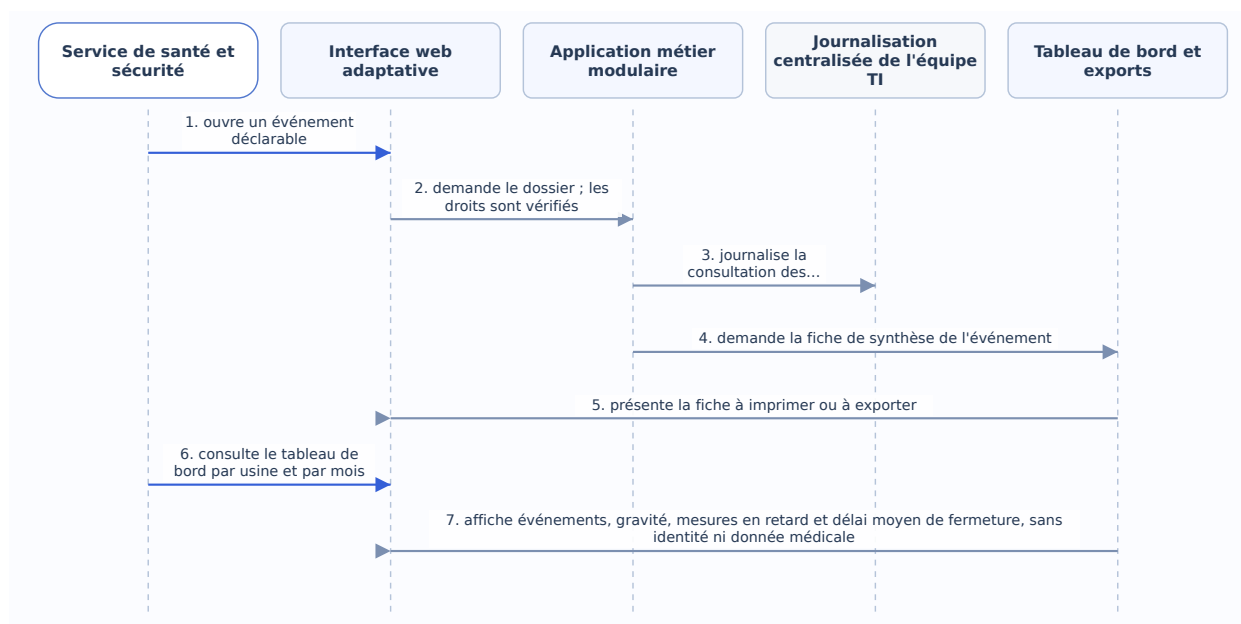
But : Être averti sans délai d'un événement grave et consulter le dossier avec les droits appropriés.



- 1. Application métier modulaire → Base de données relationnelle gérée : inscrit l'avis en attente dans la même écriture que l'événement
- 2. Base de données relationnelle gérée → Traitements planifiés et asynchrones : met à disposition l'avis en attente d'envoi
- 3. Traitements planifiés et asynchrones → Service d'envoi de courriels : prépare l'avis, sans renseignement médical ni identité, avec un lien
- 4. Service d'envoi de courriels → Comité de santé et sécurité : avise le comité de santé et sécurité
- 5. Service d'envoi de courriels → Directeur d'usine : avise le directeur de l'usine concernée
- 6. Comité de santé et sécurité → Interface web adaptative : ouvre le lien reçu
- 7. Interface web adaptative → Authentification unique fédérée avec l'annuaire : ouvre la session par l'annuaire, avec second facteur
- 8. Interface web adaptative → Application métier modulaire : demande le dossier ; les droits sont vérifiés
- 9. Application métier modulaire → Journalisation centralisée de l'équipe TI : journalise la consultation des renseignements protégés
- 10. Application métier modulaire → Interface web adaptative : affiche le dossier complet au comité

Préparer une déclaration obligatoire et suivre les indicateurs — Service de santé et sécurité

But : Obtenir une fiche de synthèse à reporter à l'organisme de réglementation et suivre les résultats par usine et par mois.



- 1. Service de santé et sécurité → Interface web adaptative : ouvre un événement déclarable
- 2. Interface web adaptative → Application métier modulaire : demande le dossier ; les droits sont vérifiés
- 3. Application métier modulaire → Journalisation centralisée de l'équipe TI : journalise la consultation des renseignements protégés
- 4. Application métier modulaire → Tableau de bord et exports : demande la fiche de synthèse de l'événement
- 5. Tableau de bord et exports → Interface web adaptative : présente la fiche à imprimer ou à exporter
- 6. Service de santé et sécurité → Interface web adaptative : consulte le tableau de bord par usine et par mois
- 7. Tableau de bord et exports → Interface web adaptative : affiche événements, gravité, mesures en retard et délai moyen de fermeture, sans identité ni donnée médicale

Garanties de fonctionnement

- Une déclaration confirmée n'est jamais perdue ni enregistrée deux fois — comment : La confirmation n'est affichée qu'après l'écriture durable du dossier, qui inclut l'avis au superviseur. Le formulaire porte un identifiant unique créé à l'ouverture ; une contrainte d'unicité sur cet identifiant, par déclarant, empêche un doublon si l'employé renvoie. Les photos sont rattachées au dossier après leur dépôt. — si le résultat d'un tiers est inconnu : Si la réponse est perdue (réseau d'usine, téléphone), l'employé peut renvoyer : le portail retrouve le dossier par son identifiant et ne le recrée pas. Une photo déposée sans dossier rattaché est signalée et purgée plus tard, jamais exposée. — composants : Interface web adaptative, Application métier

modulaire, Base de données relationnelle gérée, Stockage objet chiffré des photos et pièces jointes (retenu)

- L'avis d'un événement grave n'est jamais perdu en silence — comment : L'avis est inscrit dans la file d'envoi, en base, dans la même transaction que l'événement grave. Les traitements planifiés lisent cette file et reprennent l'envoi sur échec, avec une clé par événement et par destinataire pour éviter les envois en double. L'avis ne contient qu'un lien, sans renseignement sensible. Le même mécanisme porte l'avis au superviseur à chaque déclaration. — si le résultat d'un tiers est inconnu : Si le service de courriels ne répond pas ou si l'accusé est perdu, l'envoi passe à l'état « à vérifier » : il n'est pas déclaré échoué ni réussi. Après les reprises, le service de santé et sécurité est alerté pour joindre le comité et le directeur par un autre moyen. Un doublon éventuel est toléré, car il ne contient rien de sensible. — composants : Application métier modulaire, Base de données relationnelle gérée, Traitements planifiés et asynchrones, Service d'envoi de courriels (hypothèse)
- Chaque mesure en retard est relancée sans harcèlement ni oubli — comment : Le traitement planifié relit les mesures en retard et enregistre chaque relance avant de l'envoyer. Une contrainte d'unicité par mesure et par palier de relance empêche d'envoyer deux fois la même relance si le traitement est rejoué. — si le résultat d'un tiers est inconnu : Si le résultat de l'envoi est inconnu, la relance reste « à vérifier » et sera constatée au prochain passage ; le tableau de bord montre la mesure en retard, de sorte qu'une relance manquée ne cache pas le retard. — composants : Traitements planifiés et asynchrones, Base de données relationnelle gérée, Service d'envoi de courriels (hypothèse)
- Une synchronisation incomplète ne remplace jamais les employés et les usines connus — comment : Chaque import est appliqué par identifiant d'employé ou d'usine, sans créer de doublon s'il est rejoué. Un fichier ou une réponse incomplète (volume anormalement bas) est refusé en bloc ; les employés sans supérieur sont signalés ; les anciens codes sont conservés. — si le résultat d'un tiers est inconnu : Si l'export arrive en retard, en double ou tronqué, le portail garde les données de la veille, journalise l'écart et prévient l'équipe TI. Les départs ne sont désactivés qu'après confirmation par un import complet. — composants : Synchronisation avec le système de ressources humaines, Synchronisation avec le progiciel de gestion, Traitements planifiés et asynchrones, Base de données relationnelle gérée (hypothèse)
- La reprise du chiffrier peut être rejouée sans doublons ni perte silencieuse — comment : Chaque ligne du chiffrier garde son identifiant d'origine, unique dans le portail, ce qui rend le chargement rejouable. Un rapport d'écarts liste les lignes rejetées ou non rapprochées des employés, usines et départements, à valider par l'entreprise avant la bascule. — si le résultat d'un tiers est inconnu : Une ligne dont le rapprochement est incertain est placée « à vérifier » et chargée seulement après décision d'une personne de l'entreprise ; un chargement interrompu se reprend sans effacer ce qui a été validé. — composants : Outil de reprise du chiffrier, Base de données relationnelle gérée (hypothèse)

Données

Composant	Zone	Données conservées
Interface web adaptative	zone authentifiée	Déclarations en saisie, Photos en transfert, Aucune donnée conservée sur l'appareil au-delà de la session
Application métier modulaire	zone interne	Déclarations, enquêtes, mesures, Rôles et rattachements aux usines, Renseignements de santé et identités (champs protégés)
Authentification unique fédérée avec l'annuaire	hors système (tiers)	Identité et attributs de l'employé, Jetons de session
Base de données relationnelle gérée	zone restreinte	Déclarations et enquêtes, Mesures correctives, Employés, supérieurs, usines, départements, Journal d'audit, File des messages à envoyer, Historique repris du chiffrier
Stockage objet chiffré des photos et pièces jointes	zone restreinte	Photos d'événements, Pièces jointes d'enquête
Traitements planifiés et asynchrones	zone interne	Messages à envoyer (lus en base), Journaux d'exécution
Service d'envoi de courriels	hors système (tiers)	Adresse du destinataire, Objet et lien d'un dossier
Synchronisation avec le système de ressources humaines	hors système (tiers)	Employés, courriels, supérieurs, usine de rattachement
Synchronisation avec le progiciel de gestion	hors système (tiers)	Usines, Départements
Outil de reprise du chiffrier	zone restreinte	Déclarations historiques, Rapport de correspondance et de rejets
Tableau de bord et exports	zone authentifiée	Agrégats mensuels par usine, Fiches de synthèse réglementaires
Journalisation centralisée de l'équipe TI	zone interne	Journaux techniques, Journaux d'accès aux renseignements sensibles
Plateforme d'hébergement et chaîne de livraison	zone interne	Configuration des environnements, Secrets, Protection de base de l'hébergeur

Intégrations

Intégration	Objectif
Annuaire de l'entreprise (authentification unique)	Ouverture de session fédérée et second facteur de tous les rôles qui voient les champs protégés, ainsi que des administrateurs. Protocole standard et licence du second facteur supposés, à confirmer.
Système de ressources humaines	Employés et supérieurs, qui déterminent le superviseur destinataire. Mode d'accès supposé : export planifié ou interface documentée.
Progiciel de gestion	Référentiel des usines et départements, lecture seule. Mode d'accès supposé : export planifié ou interface documentée.
Service de courriels	Avis, relances et alertes, avec traitement en région canadienne à vérifier avant le choix.
Journalisation de l'équipe TI	Centralisation des journaux selon les normes imposées.

Contraintes

- Toutes les données, fichiers, sauvegardes, journaux et services auxiliaires sont traités en région canadienne (politique interne ; variante hors Canada non proposée sans votre accord).
- Une région hors Québec appelle l'examen des facteurs relatifs à la vie privée de la Loi 25 avant toute communication de renseignements, à mener par vous.
- Hébergement, journalisation et exploitation suivent les normes de l'équipe TI, non encore communiquées ; l'architecture est suspendue à ces normes.
- Chiffrement en transit et au repos ; secrets hors du code ; dépendances suivies.
- Contrôles de sécurité structurés par l'OWASP Top 10:2025, l'ASVS 5.0.0 (niveau visé à confirmer) et l'OWASP API Security 2023, sans conformité présumée. Un test d'intrusion indépendant reste une variante chiffrée à part, hors enveloppe.
- Loi 25 et loi sur les renseignements de santé et de services sociaux à considérer ; application de la seconde selon le statut de l'entreprise, à confirmer.
- Durée de conservation paramétrable et destruction en fin de conservation, à définir avec votre responsable de la protection des renseignements personnels.
- Sauvegardes : protection de base de l'hébergeur (environ 35 jours, région canadienne) en attendant votre réponse sur la conservation et la restauration ; aucun archivage à long terme.
- Disponibilité supposée 24 h sur 7 sur plusieurs zones d'une même région canadienne, sans reprise multirégion.
- Aucune IA dans la solution : le dossier n'en demande pas. Le dépôt à l'organisme de réglementation reste manuel et hors du portail.
- Seuls les employés authentifiés par l'annuaire accèdent au portail ; aucune page publique ni compte local.

Rôles : déclarant, superviseur, comité de santé et sécurité, service de santé et sécurité, directeur d'usine, administrateur technique. Le contrôle se fait côté serveur, par fonction et par objet, jamais seulement dans l'interface.

- Renseignements médicaux et identité des blessés : visibles des seuls superviseurs concernés, du comité et du service de santé et sécurité. Chaque consultation est journalisée.
- Un déclarant voit ses propres déclarations ; un superviseur voit celles de son équipe ; un directeur d'usine voit les agrégats et les événements graves de son usine, sans les champs protégés.
- Un second facteur, porté par l'annuaire, est exigé de tout rôle qui voit les champs protégés (superviseurs, comité, service de santé et sécurité) et des administrateurs.
- Les fichiers ne sont jamais exposés par une adresse publique permanente.
- Les environnements d'essai ne contiennent aucune donnée réelle sans masquage.
- Les accès d'administration technique sont séparés des rôles applicatifs et journalisés.

Limites de l'architecture proposée

- Juridiction du client : Québec. Lois de protection des renseignements personnels à considérer : Loi 25 (Commission d'accès à l'information du Québec) ; renseignements de santé : Loi sur les renseignements de santé et de services sociaux (Commission d'accès à l'information du Québec) — nommées d'après le registre de Linuen ; ce n'est ni un avis juridique ni une conformité.
- 17 décisions d'architecture (DA-1, DA-2, DA-3, DA-4, DA-5, DA-6, DA-7, DA-8, DA-9, DA-10, DA-11, DA-12, DA-13, DA-14, DA-15, DA-16, DA-17) : proposées par l'analyse et maintenues à la revue critique, à confirmer avec vous avant la réalisation.

Où l'IA intervient

La solution proposée n'emploie pas l'IA.

Pistes d'IA, non comprises dans la solution

L'analyse a repéré ces fonctions où l'IA pourrait aider. Vous ne les avez pas demandées : elles ne sont ni dans la solution ni dans le budget. Vous pouvez les explorer dans « Scénarios alternatifs ».

- Proposer une catégorie et une cause pour le texte libre des trois ans de déclarations du chiffrier à la reprise. (appel d'un modèle de langage) — Réduit le nettoyage manuel d'un texte libre hétérogène et rend l'historique comparable dans le tableau de bord. — risque : Classement faux pris pour acquis ; renseignements de santé et noms envoyés à un fournisseur, avec lieu d'inférence canadien exigé et examen de

confidentialité préalable. — données transmises : Texte libre des descriptions et causes des déclarations historiques, avec masquage des noms et des renseignements médicaux avant l'envoi. — ordre de grandeur : Opération ponctuelle : quelques dizaines d'heures de mise en place et de validation, coût d'usage faible pour environ 36 000 lignes.

- Résumer un dossier d'enquête (causes, témoins, mesures) pour le comité et le service de santé et sécurité. (appel d'un modèle de langage) — Gain de temps de lecture et de préparation des fiches de synthèse réglementaires. — risque : Résumé inexact sur un document à portée réglementaire ; exposition de renseignements médicaux et d'identités ; relecture humaine obligatoire. — données transmises : Contenu du dossier d'enquête, dont des renseignements de santé et d'identification, à masquer avant tout envoi. — ordre de grandeur : Quelques dizaines d'heures plus garde-fous de données ; coût d'usage faible pour moins de 1 000 dossiers par mois.
- Repérer des causes et des situations dangereuses récurrentes dans le texte libre des déclarations de toutes les usines. (appel d'un modèle de langage) — Aide la prévention en rendant visibles des tendances que les comptes du tableau de bord ne montrent pas. — risque : Regroupements trompeurs ; données sensibles traitées chez un fournisseur ; à utiliser comme aide à l'analyse, non comme décision. — données transmises : Descriptions d'événements sans noms ni renseignements médicaux, après masquage. — ordre de grandeur : Piste d'une phase ultérieure : effort modéré et coût d'usage faible à ce volume.

Détails techniques

Avec quoi la solution est construite, et où elle est hébergée. Chaque choix porte son statut : retenu lorsque le dossier l'arrête, hypothèse lorsqu'il a simplement servi au chiffage, à confirmer lorsqu'il dépend d'une réponse attendue. Un choix marqué hypothèse n'engage personne ; il indique ce qui a été supposé pour produire les chiffres.

Outils de programmation

Couche	Choix	Statut	Pourquoi ce choix pour ce dossier
Langage et exécution	Langage typé répandu, exécuté côté serveur (hypothèse : TypeScript sur Node.js, version à support long terme)	hypothèse	Un seul langage pour le serveur et l'interface adaptative. Technologie répandue et bien documentée, que votre équipe TI peut reprendre pour l'exploitation.

Couche	Choix	Statut	Pourquoi ce choix pour ce dossier
Cadriciel applicatif	Cadriciel web en modules, déployé comme une seule application (monolithe modulaire)	hypothèse	Volumétrie modeste (100 à 1 000 opérations par mois, 1 200 employés), règles transactionnelles (enquêtes, mesures, droits par champ) et une seule unité à exploiter pour l'équipe TI. Référence d'architecture à valider.
Interface utilisateur	Interface web adaptative, sans application native ni mode hors ligne ; niveau AA des règles WCAG 2.2 visé	à confirmer	Les employés déclarent depuis un poste d'usine ou un téléphone : le web adaptatif évite magasin d'applications et gestion de parc mobile. Photos prises par le navigateur, sans copie dans la galerie lorsque possible, pour limiter les renseignements de santé hors du portail. Le niveau AA est vérifié par contrôles automatisés et essais manuels (clavier, lecteur d'écran) sur les parcours essentiels, sans audit externe.
Base de données	Base relationnelle transactionnelle gérée (hypothèse : PostgreSQL), chiffrée au repos, en région canadienne, haute disponibilité sur plusieurs zones	hypothèse	Dossiers, mesures, référentiels synchronisés, journal d'audit et agrégats sont structurés. Les contraintes d'intégrité et les migrations versionnées servent aussi la reprise de trois ans de chiffrier. Elle porte également la file des traitements différés.
Stockage de fichiers	Stockage objet chiffré, sans accès public, en région canadienne, liens signés de courte durée	hypothèse	Photos et pièces jointes liées à des dossiers sensibles : l'accès suit les droits du dossier. La région canadienne respecte votre politique de territoire. Protection de base de l'hébergeur, sans archivage distinct.
File de tâches de fond	File de traitements adossée à la base et tâches planifiées de l'application, avec reprise sur échec	hypothèse	L'avis d'un événement grave s'inscrit dans la même transaction que l'événement, puis est lu par les tâches d'envoi : aucun avis perdu. Volumes modestes et une seule application, d'où l'absence de courtier de messages distinct. Couvre relances, synchronisations nocturnes, agrégats et purge.
Authentification	Authentification unique fédérée avec l'annuaire de l'entreprise (hypothèse : OpenID Connect ou SAML), second facteur porté par l'annuaire	à confirmer	Le portail ne gère aucun mot de passe. Le second facteur s'applique aux administrateurs et à tout rôle qui voit les champs protégés : superviseurs, comité, service de santé et sécurité. Protocole offert et licence du second facteur à confirmer. Rôles et droits par champ construits dans le portail.

Couche	Choix	Statut	Pourquoi ce choix pour ce dossier
Courriel et notifications	Service d'envoi de courriels transactionnels traitant au Canada (fournisseur à choisir)	à confirmer	Avis, relances et alertes sans renseignement médical ni identité des blessés, seulement un lien vers le portail. Région de traitement à vérifier à cause de la politique de territoire. Le message texte reste une alternative, jamais un envoi doublé.
Observabilité	Journaux structurés et alertes envoyés vers l'outil central de journalisation de l'équipe TI	à confirmer	La journalisation selon vos normes est imposée. Les journaux d'audit (consultations de champs sensibles, changements de droits) et techniques ne contiennent aucun contenu médical. Format et destination à confirmer.
Intégration continue	Dépôt de code avec revue des changements, construction reproductible, suivi des dépendances, déploiement automatisé avec retour arrière	à confirmer	Données de santé et exigence de sécurité : secrets hors du code, dépendances suivies, mise en production approuvée manuellement. La plateforme exacte suit les normes de l'équipe TI.
Tests	Tests unitaires et d'intégration automatisés, tests des droits par rôle et par objet, analyse statique, vérifications d'accessibilité automatisées et manuelles, revue de sécurité structurée par l'OWASP	hypothèse	Le risque principal est l'accès aux renseignements médicaux et à l'identité des blessés : les tests d'autorisation par champ et par dossier ont priorité. Références : OWASP Top 10:2025, ASVS 5.0.0 (niveau à confirmer) et API Security 2023, sans conformité présumée.
Outillage de développement	Infrastructure décrite par du code pour l'essai et la production	à confirmer	Les environnements doivent être reproductibles par l'équipe TI qui exploitera la solution. L'outil exact dépend de ses normes.

- Langage typé répandu, exécuté côté serveur (hypothèse : TypeScript sur Node.js, version à support long terme) — écarté : Java ; C# (.NET) ; Python
- Cadriciel web en modules, déployé comme une seule application (monolithe modulaire) — écarté : Services séparés ; Plateforme de formulaires sans code
- Interface web adaptative, sans application native ni mode hors ligne ; niveau AA des règles WCAG 2.2 visé — écarté : Application mobile native ; Application web progressive avec mode hors ligne
- Base relationnelle transactionnelle gérée (hypothèse : PostgreSQL), chiffrée au repos, en région canadienne, haute disponibilité sur plusieurs zones — écarté : Base NoSQL

documentaire ; Base relationnelle commerciale selon les normes de l'équipe TI

- Stockage objet chiffré, sans accès public, en région canadienne, liens signés de courte durée — écarté : Fichiers dans la base ; Stockage objet d'un autre hébergeur canadien ; Partage de fichiers de l'entreprise
- File de traitements adossée à la base et tâches planifiées de l'application, avec reprise sur échec — écarté : Courtier de messages dédié ; Orchestrateur de flux dédié
- Authentification unique fédérée avec l'annuaire de l'entreprise (hypothèse : OpenID Connect ou SAML), second facteur porté par l'annuaire — écarté : Comptes locaux avec second facteur ; Fournisseur d'identité tiers en intermédiaire
- Service d'envoi de courriels transactionnels traitant au Canada (fournisseur à choisir) — écarté : Serveur de courriel de l'entreprise ; Messages texte (variante chiffrée à part)
- Journaux structurés et alertes envoyés vers l'outil central de journalisation de l'équipe TI — écarté : Outil de journalisation propre au projet ; Service de surveillance de l'hébergeur
- Dépôt de code avec revue des changements, construction reproductible, suivi des dépendances, déploiement automatisé avec retour arrière — écarté : Déploiement manuel scripté ; Chaîne imposée par l'équipe TI
- Tests unitaires et d'intégration automatisés, tests des droits par rôle et par objet, analyse statique, vérifications d'accessibilité automatisées et manuelles, revue de sécurité structurée par l'OWASP — écarté : Tests manuels seulement ; Test d'intrusion indépendant (ligne de dépenses dédiée, voir notes)
- Infrastructure décrite par du code pour l'essai et la production — écarté : Configuration manuelle des environnements

Hébergement

Modèle d'hébergement : Infonuagique gérée (plateforme) (à confirmer)

Catégorie de fournisseur : Grand fournisseur infonuagique avec région canadienne et services gérés (calcul, base, stockage objet), selon les normes de l'équipe TI ; chiffage sur l'hypothèse d'Azure, région Canada Central

Conservation des données : Canada

Environnements : Développement (local ou éphémère) · Essai (données masquées) · Production

Sauvegardes et rétention : Protection de base de l'hébergeur : restauration à un instant donné de la base sur environ 35 jours et protection du stockage objet, en région canadienne. Aucun service de sauvegarde distinct ni archivage à long terme. Restauration de la base et des fichiers vérifiée avant la mise en service. Conservation à confirmer avec vous.

Reprise après incident : Hypothèse : service 24 h sur 7 sur plusieurs zones d'une

même région canadienne, sans reprise multirégion. Perte de données maximale d'environ une heure et interruption de quelques heures, à confirmer. Une seconde région canadienne est une variante chiffrée à part.

Services d'hébergement chiffrés

Ces lignes sont celles de l'estimation : elles figurent déjà dans les dépenses du dossier, initiales et récurrentes.

Service	Périodicité	Montant par période
Hébergement de production en région canadienne (application et base de données à haute disponibilité)	Mensuelle	804,00 CAD
Environnement d'essai (préproduction) en région canadienne	Mensuelle	339,00 CAD
Stockage chiffré des photos et pièces jointes	Mensuelle	2,16 CAD
Trafic sortant (consultation des photos et pièces jointes)	Mensuelle	3,60 CAD
Surveillance, alertes et conservation des journaux techniques et d'audit	Mensuelle	35,00 CAD
Sauvegardes et conservation des sauvegardes	Mensuelle	0,00 CAD
Services imposés par les normes de votre équipe TI (coffre de secrets et de clés de chiffrement)	Mensuelle	25,00 CAD
Protection de base de l'hébergeur : sauvegardes gérées de la base (restauration à un instant donné) et protection des fichiers, comprises dans l'hébergement — activation	Une fois	0,00 CAD
Sous-domaine interne et certificat géré de la plateforme — activation	Une fois	0,00 CAD
Reprise après sinistre : haute disponibilité sur plusieurs zones d'une même région, sans seconde région — activation	Une fois	0,00 CAD

- Politique de territoire interne : la région canadienne vaut pour la base, les fichiers, les sauvegardes, les journaux et le service de courriels. Aucune variante hors Canada sans votre accord.
- Une communication de renseignements hors du Québec appelle l'examen des facteurs relatifs à la vie privée de la Loi 25, à mener par vous.
- Vos normes d'hébergement et de journalisation ne sont pas connues : hébergeur, journalisation et chaîne de livraison sont des hypothèses de chiffrage.
- Aucun nom de produit n'est engagé : PostgreSQL, Node.js et Azure sont des hypothèses, à confirmer avec Linuen et votre équipe TI.

Le test d'intrusion indépendant fait l'objet d'une ligne de dépenses dédiée ; son inclusion dans l'enveloppe se confirme avec vous.

- Aucun paiement, moteur de recherche ni composant d'IA : le dossier n'en demande pas.

Registre des décisions d'architecture

Chaque décision d'architecture du dossier est consignée au format MADR (Markdown Architectural Decision Records) : son contexte, les options envisagées, la décision, ses conséquences, ses hypothèses, les vérifications prévues et les références d'architecture sur lesquelles elle s'appuie.

Décisions proposées par l'analyse et maintenues à la revue critique : elles orientent l'architecture chiffrée et se confirment avec vous avant la réalisation.

DA-1 — Construire un portail sur mesure plutôt qu'acheter ou adapter un produit

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	partiellement couverte par les références citées

Décision type : Décision type — acheter ou construire : application sur mesure, plateforme du marché adaptée, ou logiciel complet acheté — option retenue : Construire une application sur mesure, appuyée sur des services gérés

Contexte

Flux d'enquête par superviseur, avis de gravité et visibilité restreinte des renseignements médicaux, liés à trois systèmes existants et aux normes imposées par l'équipe TI.

- E-1 — Remplacer le papier et le chiffrier par un portail unique
- E-3 — Enquête du superviseur et mesures correctives avec relances
- E-5 — Accès restreint aux renseignements médicaux et à l'identité des blessés
- E-26 — Aucun logiciel de santé et sécurité existant à conserver
- Q-10 — Existe-t-il, en plus du papier et du chiffrier, un logiciel du marché de santé et sécurité en service que vous voulez conserver, interfacer ou remplacer ?

Options envisagées

- Acheter un logiciel complet et adapter le processus à l'outil — Pourrait couvrir le besoin courant, mais son hébergement en région canadienne, ses rôles fins sur les champs médicaux et ses intégrations avec vos trois systèmes sont à vérifier ; aucun produit n'a été comparé dans ce dossier.
- Adapter une plateforme du marché avec quelques composants spécifiques — Piste valable pour le formulaire et le flux, mais la restriction par champ et les normes d'hébergement imposées limitent la marge ; non chiffrée ici.

Décision

Construire une application sur mesure, appuyée sur des services gérés. Aucune déclaration contraire du client ni avantage démontré d'un produit du marché ne justifie de dévier du choix par défaut. L'examen d'un logiciel de santé et sécurité du marché reste possible à part, comme approche non retenue.

Conséquences

- Compromis : Contrôle total des droits et de l'hébergement contre un coût de réalisation et une maintenance à la charge de l'équipe TI.
- Risque : Un produit du marché existant pourrait couvrir l'essentiel du besoin à moindre coût et rester non examiné.

Hypothèses

- Aucun logiciel de santé et sécurité en service à conserver.
- La fiche de décision type est non vérifiée : son choix par défaut est cité comme hypothèse.

Vérifications prévues

- Confirmer avec vous si un produit du marché a déjà été évalué ou écarté.
- Si la réponse sur l'outil existant change, revoir le périmètre d'intégration.

Références

- Décision type — acheter ou construire : application sur mesure, plateforme du marché adaptée, ou logiciel complet acheté (v1 — référence à vérifier)

DA-2 — Une seule application structurée en modules plutôt que des services séparés

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — style d'architecture : monolithe modulaire, microservices ou assemblage de services gérés — option retenue : Monolithe modulaire

Contexte

Petite équipe de réalisation, volumétrie modeste (100 à 1 000 opérations par mois), exploitation par une équipe TI interne.

- E-24 — Volumétrie : environ 1 200 employés, 1 000 déclarations par mois retenues
- E-27 — Rythme de réalisation de base : une personne à temps plein
- E-12 — Exploitation par l'équipe TI selon ses normes d'hébergement et de journalisation
- E-1 — Remplacer le papier et le chiffrier par un portail unique

Options envisagées

- Microservices — Une seule équipe et un domaine encore mouvant ; la charge d'exploitation serait disproportionnée pour votre équipe TI.
- Assemblage de services gérés autour d'un noyau léger — Aucun produit ne couvre l'essentiel du flux d'enquête ; les services gérés servent seulement aux fonctions périphériques (courriel, stockage, base).

Décision

Monolithe modulaire : modules déclaration, enquête, mesures et relances, gravité et avis, droits d'accès, préparation réglementaire, avec une base partagée et des traitements asynchrones internes. Les frontières de modules sont documentées pour permettre une extraction ultérieure.

Conséquences

- Compromis : Simplicité d'exploitation et transactions locales contre mise à l'échelle sélective.
- Risque : Les modules peuvent se mélanger avec le temps.

Hypothèses

- La charge reste modeste ; aucune mise à l'échelle particulière n'est requise.
- La fiche de style d'architecture est non vérifiée.

Vérifications prévues

- Revoir si les normes de l'équipe TI imposent un style de déploiement différent.

Références

- Décision type — style d'architecture : monolithe modulaire, microservices ou assemblage de services gérés (v3 — référence à vérifier)
- Monolithe modulaire — une application déployée d'un bloc, structurée en modules (v2)

DA-3 — Authentification unique par l'annuaire, avec second facteur pour tout rôle qui voit les champs protégés

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — authentification : comptes intégrés à l'application, fournisseur d'identité géré ou annuaire de l'organisation — option retenue : Authentification unique par l'annuaire de l'organisation

Contexte

Utilisateurs tous employés, déjà présents dans l'annuaire ; authentification unique demandée ; superviseurs, comité et service de santé et sécurité voient des renseignements de santé.

- E-8 — Ouverture de session par l'annuaire de l'entreprise
- E-25 — Comptes fournis par l'annuaire ; rôles et droits construits dans le portail
- E-18 — Sécurité applicative, chiffrement et journal d'audit des accès sensibles
- E-5 — Accès restreint aux renseignements médicaux et à l'identité des blessés
- Exigence de qualité : Sécurité
- Q-2 — Comment accéder à l'annuaire (protocole d'authentification unique), au système de ressources humaines et au progiciel de gestion (interface, fichier d'export, fréquence) ? L'annuaire peut-il imposer un second facteur aux superviseurs, au comité et au service de santé et sécurité (licence comprise) ? Pouvez-vous fournir des environnements d'essai et un interlocuteur pour chacun ?

Options envisagées

- Comptes gérés par l'application, second facteur pour les rôles sensibles — Choix par défaut des fiches pour des populations externes ; ici, les employés sont dans l'annuaire, et des comptes propres dupliqueraient l'identité et sa révocation. Retenu

seulement si l'annuaire ne peut pas offrir le second facteur (environ + 10 à 30 h).

- Fournisseur d'identité géré (OpenID Connect) — Utile pour unifier plusieurs applications ou des exigences avancées ; n'apporte rien tant que l'annuaire remplit le rôle.

Décision

Authentification unique par l'annuaire de l'organisation. Le portail ne gère aucun mot de passe. Le second facteur, porté par l'annuaire, est exigé des administrateurs et de tout rôle qui voit les champs protégés (superviseurs, comité, service de santé et sécurité), soit une centaine de comptes ; l'expiration et la révocation des sessions s'appuient aussi sur l'annuaire. Seuls les rôles applicatifs et le rattachement aux usines sont construits dans le portail. La licence du second facteur est à confirmer avec vous.

Conséquences

- Compromis : Dépendance à la disponibilité et à la configuration de l'annuaire contre aucun mot de passe à protéger.
- Compromis : Friction d'usage du second facteur pour environ cent comptes, contre une protection des données de santé.
- Risque : Le protocole d'accès à l'annuaire est supposé standard ; une interface propriétaire augmenterait l'effort.
- Risque : Une licence de second facteur à acquérir serait à votre charge.

Hypothèses

- L'annuaire peut imposer un second facteur à ces rôles.
- La fiche d'authentification est non vérifiée ; la règle d'identité l'est.

Vérifications prévues

- Confirmer le protocole, l'environnement d'essai et l'interlocuteur de l'annuaire.
- Vérifier que chaque rôle qui voit un champ protégé est soumis au second facteur.
- Vérifier l'expiration et la révocation des sessions selon le niveau ASVS visé, à confirmer.

Références

- Décision type — authentification : comptes intégrés à l'application, fournisseur d'identité géré ou annuaire de l'organisation (v2 — référence à vérifier)
- Authentification et gestion des identités — NIST SP 800-63-4 (v2)
- Exigences de vérification de sécurité applicative — OWASP ASVS (v2)

DA-4 — Hébergement de la chaîne complète dans une région canadienne

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — lieu d'hébergement des données : au Québec, au Canada ou ailleurs, selon la nature des données — option retenue : Hébergement au Canada, région canadienne vérifiée

Contexte

Données de santé, d'identification et d'employés ; exigence de territoire « Au Canada » déclarée comme politique interne ; client au Québec.

- E-13 — Données au Canada
- E-14 — Exigence de territoire : politique interne, sans obligation externe
- E-15 — Données de santé, d'identification et d'employés : protection renforcée
- Exigence de qualité : Résidence des données
- Exigence de qualité : Confidentialité et renseignements personnels
- Q-1 — Quelles sont les normes d'hébergement infonuagique et de journalisation de votre équipe TI (fournisseur et région approuvés, environnements, format et destination des journaux, gestion des secrets, correctifs) ?

Options envisagées

- Hébergement au Québec, chaîne complète — Respecterait aussi la politique ; non exigé. Variante chiffrable si votre équipe TI ou votre responsable de la protection des renseignements personnels la préfère, car elle évite l'examen des facteurs relatifs à la vie privée pour une communication hors du Québec.
- Hébergement hors du Canada — Contraire à la politique interne ; écartée, non proposée sans votre accord.

Décision

Hébergement au Canada, région canadienne vérifiée, pour la base, les fichiers, les sauvegardes, les journaux et les services auxiliaires (courriel inclus). Aucune obligation légale ou contractuelle de résidence au Québec n'est déclarée, donc le choix par défaut s'applique. Le fournisseur et la région exacts découlent des normes de votre équipe TI, non communiquées.

Conséquences

- Compromis : Choix de fournisseurs plus restreint contre protection des renseignements de santé et d'employés.
- Risque : Une région hors Québec appelle l'examen des facteurs relatifs à la vie privée de la Loi 25, à mener par vous.
- Risque : Un sous-traitant (courriel) pourrait traiter hors du Canada.

Hypothèses

- Loi 25 à considérer ; application de la loi sur les renseignements de santé et de services sociaux selon le statut de l'entreprise, à confirmer. Aucune conformité n'est présumée.
- La fiche d'hébergement est non vérifiée.

Vérifications prévues

- Vérifier la région de traitement de chaque service auxiliaire, sauvegardes et journaux inclus.
- Faire valider par votre responsable de la protection des renseignements personnels l'examen préalable.

Références

- Décision type — lieu d'hébergement des données : au Québec, au Canada ou ailleurs, selon la nature des données (v3 — référence à vérifier)
- Classification, chiffrement et résidence des données (v2)
- Renseignements personnels au Canada et au Québec — Loi 25, LPRPDE, principes des autorités sur l'IA (v1)

DA-5 — Base de données relationnelle pour les dossiers, mesures et journal d'audit

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — stockage principal des données : base relationnelle, base documentaire ou stockage clé-valeur géré — option retenue : Base de données relationnelle

Contexte

Données structurées et liées (déclarations, enquêtes, mesures, employés, usines), intégrité nécessaire, tableau de bord et exports.

- E-3 — Enquête du superviseur et mesures correctives avec relances
- E-7 — Tableau de bord par usine et par mois
- E-11 — Reprise de trois ans de déclarations du chiffrier
- E-24 — Volumétrie : environ 1 200 employés, 1 000 déclarations par mois retenues
- Q-7 — L'exclusion « backup » du dossier vise-t-elle les sauvegardes ? Quelle durée de conservation des sauvegardes et quelle capacité de restauration attendez-vous pour des dossiers contenant des renseignements de santé ?

Options envisagées

- Base documentaire — Les dossiers sont liés (employé, supérieur, usine, mesures) ; les relations et transactions priment.
- Stockage clé-valeur géré — Aucun débit ni cache mesuré ne le justifie à ce volume.

Décision

Base relationnelle gérée, chiffrée au repos, en région canadienne, avec la protection de base de l'hébergeur (restauration à un instant donné, environ 35 jours) et des migrations de schéma versionnées. Aucun service de sauvegarde distinct ni archivage à long terme, conformément à l'exclusion du dossier lue ainsi en attendant votre réponse. Les agrégats du tableau de bord sont calculés dans la même base, sans stockage complémentaire.

Conséquences

- Compromis : Cohérence et rapports simples contre mise à l'échelle des écritures, sans objet à ce volume.
- Compromis : Protection de base seulement : une corruption détectée après environ 35 jours ne serait plus restaurable.
- Risque : Restauration jamais éprouvée : à vérifier avant la mise en service.
- Risque : Durée de conservation des renseignements de santé non fixée ; la protection de base peut être trop courte.

Hypothèses

- L'exclusion « backup » du dossier est lue comme visant un service de sauvegarde distinct ou un archivage long terme, à confirmer.
- La fiche de stockage principal est non vérifiée.

Vérifications prévues

- Confirmer avec vous la portée de l'exclusion, la durée de conservation et la restauration attendue.
- Exécuter un test de restauration avant la bascule.

Références

- Décision type — stockage principal des données : base relationnelle, base documentaire ou stockage clé-valeur géré (v2 — référence à vérifier)
- Base relationnelle transactionnelle comme stockage principal (v2)

DA-6 — Photos et pièces jointes dans un stockage objet chiffré, hors de la base

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — fichiers déposés ou produits : stockage objet, base de données ou disque du serveur — option retenue : Stockage objet, hors de la base

Contexte

Photos et pièces jointes d'événements et d'enquêtes, avec droits alignés sur le dossier et résidence canadienne.

- E-20 — Dépôt et gestion des photos et pièces jointes
- E-2 — Déclaration par tout employé, sur poste ou téléphone
- E-13 — Données au Canada
- Exigence de qualité : Résidence des données
- Q-7 — L'exclusion « backup » du dossier vise-t-elle les sauvegardes ? Quelle durée de conservation des sauvegardes et quelle capacité de restauration attendez-vous pour des dossiers contenant des renseignements de santé ?

Options envisagées

- Dans la base de données — Les photos prises sur téléphone sont volumineuses et leur nombre croît.
- Disque du serveur d'application — Fichiers durables et sensibles ; le disque ne convient qu'aux fichiers temporaires.

Décision

Stockage objet, hors de la base, en région canadienne, sans accès public, chiffré, avec liens signés de courte durée émis seulement si l'utilisateur a le droit de voir le dossier. Métadonnées et droits en base. Le contrôle du type réel et de la taille précède le dépôt. La protection de base du stockage est distincte de celle de la base ; une restauration conjointe est vérifiée avant la mise en service, sans archivage distinct. Le fournisseur reste une hypothèse selon vos normes d'hébergement.

Conséquences

- Compromis : Coût faible et capacité extensible contre une restauration à coordonner avec la base.
- Risque : Photos montrant des personnes blessées : sensibles comme les champs médicaux, à traiter selon les mêmes droits.
- Risque : Restauration base et fichiers incohérente.

Hypothèses

- Pas de photos à migrer depuis le chiffrier (à confirmer).
- La fiche de stockage de fichiers est non vérifiée.

Vérifications prévues

- Tester l'expiration des liens et le refus d'accès hors droits.
- Confirmer la politique de conservation des photos avec votre responsable.

Références

- Décision type — fichiers déposés ou produits : stockage objet, base de données ou disque du serveur (v2 — référence à vérifier)
- Stockage objet pour les fichiers et documents (v1)
- Stockage objet compatible S3 (OVHcloud — région canadienne Beauharnois confirmée) (v2)

DA-7 — Contrôle d'accès côté serveur par rôle, usine, dossier et champ sensible

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Contexte

Seuls les superviseurs, le comité et le service de santé et sécurité voient les renseignements médicaux et l'identité des blessés ; données de santé et d'employés.

- E-5 — Accès restreint aux renseignements médicaux et à l'identité des blessés
- E-15 — Données de santé, d'identification et d'employés : protection renforcée
- E-18 — Sécurité applicative, chiffrement et journal d'audit des accès sensibles
- Exigence de qualité : Sécurité
- Exigence de qualité : Confidentialité et renseignements personnels
- Q-8 — Comment définit-on un événement « grave », et quels sont les cas particuliers de rôles (déclaration visant le superviseur lui-même, absence du superviseur, déclaration confidentielle) ?
- Q-5 — Quels renseignements de santé précis sont saisis (nature des blessures, soins, arrêts de travail), qui est le responsable de la protection des renseignements personnels, et pour quelle durée les dossiers sont-ils conservés ?
- Q-12 — Souhaitez-vous un test d'intrusion indépendant avant la mise en service, ou un niveau de vérification applicative précis (par exemple exigé par votre équipe TI) ?

Options envisagées

- Contrôle par rôle seulement, au niveau des écrans — Insuffisant : l'autorisation par objet et par champ doit être serveur pour éviter l'accès par appel direct.
- Chiffrement applicatif de chaque champ médical — Variante plus forte que la demande ; à chiffrer à part si votre équipe TI ou la gouvernance l'exige.
- Test d'intrusion indépendant avant la mise en service — Variante chiffrée à part, hors de l'enveloppe ; à retenir si vos normes internes l'exigent.

Décision

Autorisation à moindre privilège appliquée côté serveur, par fonction et par objet : un déclarant voit ses déclarations, un superviseur celles de son équipe, un directeur d'usine les agrégats et les événements graves de son usine sans champs protégés. Les champs médicaux et l'identité des blessés sont filtrés à la lecture, exclus des agrégats, des courriels et des journaux techniques. Chaque consultation de champ protégé est journalisée. Environnements d'essai sans donnée réelle non masquée. Vérifications automatisées et revue de sécurité incluses, niveau ASVS visé à confirmer ; un test d'intrusion indépendant est une variante chiffrée à part, hors de l'enveloppe présentée.

Conséquences

- Compromis : Effort de conception et de tests de sécurité contre réduction du risque d'incident de confidentialité.
- Compromis : Sans test indépendant, la vérification repose sur des contrôles de l'équipe de réalisation.
- Risque : Cas de rôles non définis (déclaration visant le superviseur, absence) pouvant exposer ou bloquer un dossier.
- Risque : Une erreur de filtre sur un champ protégé échapperait aux contrôles automatisés.

Hypothèses

- Échelle de gravité fixe à quatre niveaux ; supérieur suivant en cas de conflit ou d'absence.
- Aucune conformité n'est présumée ; les listes OWASP structurent les vérifications.

Vérifications prévues

- Tests d'autorisation par objet et par champ pour chaque rôle, y compris appels directs aux interfaces.
- Revue du journal d'audit par un responsable désigné.
- Confirmer le niveau de vérification applicative visé et le recours à un test indépendant.

Références

- Risques applicatifs de référence — OWASP Top 10 (édition 2025) (v2)
- Exigences de vérification de sécurité applicative — OWASP ASVS (v2)
- Sécurité intégrée à la conception (piliers Well-Architected) (v2)
- Classification, chiffrage et résidence des données (v2)

DA-8 — Usage sur téléphone par l'interface web adaptative, sans application native

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — application mobile : site adaptatif, application Web progressive ou native — option retenue : Site Web adaptatif, sans application

Contexte

Déclaration depuis un poste d'usine ou un téléphone ; photos de blessures ou de lieux ; aucun mode hors ligne exigé ni magasin d'applications demandé.

- E-23 — Application web adaptée au téléphone, sans application native
- E-2 — Déclaration par tout employé, sur poste ou téléphone
- E-22 — Accessibilité des écrans visée au niveau AA, vérifiée sur les parcours essentiels
- Q-9 — Les employés utiliseront-ils leur téléphone personnel ou un appareil fourni, un accès web suffit-il, et les avis passent-ils par courriel ou par message texte (selon le choix) ?

Options envisagées

- Application Web progressive installable — Utile pour des notifications poussées ou un hors-ligne court ; aucun n'est demandé. Variante possible si les usines ont des zones sans réseau.
- Native multiplateforme (une base de code) — Magasin, capteurs ou hors-ligne prolongé non exigés ; coût et maintenance supplémentaires, à chiffrer à part.

Décision

Site web adaptatif sans application. La prise de photo passe par le navigateur du téléphone, sans enregistrement dans la galerie de l'appareil lorsque c'est possible, avec une consigne d'usage pour les appareils personnels. Les avis passent par courriel, donc aucune notification mobile n'est requise. Accessibilité : niveau AA des règles WCAG 2.2 visé en hypothèse, vérifié par des contrôles automatisés et des essais manuels (clavier, lecteur d'écran) sur les parcours essentiels, sans audit externe.

Conséquences

- Compromis : Moindre coût et déploiement unique contre expérience moins riche et aucune saisie hors réseau.
- Compromis : Le niveau AA demande des vérifications dès la conception, contre un public élargi.
- Risque : Zones d'usine sans couverture : la déclaration ne serait pas possible sur le moment.
- Risque : Adoption faible si les appareils ne sont pas disponibles.
- Risque : Une copie de photo de blessure peut rester dans la galerie d'un téléphone personnel, hors des droits d'accès du portail, si la capture sans enregistrement n'est pas possible sur l'appareil.

Hypothèses

- Les employés disposent d'un navigateur récent sur poste ou téléphone.
- La fiche mobile est non vérifiée.
- Niveau AA à confirmer avec vous.

Vérifications prévues

- Confirmer les appareils, personnels ou fournis, et la couverture réseau dans les quatre usines.
- Essais de prise de photo sur les modèles courants, dont l'absence de copie dans la galerie.
- Contrôles d'accessibilité automatisés et essais manuels sur la déclaration, l'enquête et la consultation.

Références

- Décision type — application mobile : site adaptatif, application Web progressive ou native (v1 — référence à vérifier)
- Accessibilité des sites et applications Web — WCAG 2.2 et standard québécois SGQRI 008 3.0 (v2)

DA-9 — Avis et relances par courriel, sans renseignement sensible dans le message

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — notifications aux utilisateurs : courriel transactionnel, texto, notification mobile ou messages dans l'application — option retenue : Courriel transactionnel par un service spécialisé

Contexte

Avis immédiat des événements graves, relances des mesures en retard, notifications demandées par courriel ou message.

- E-4 — Avis immédiat pour les événements graves
- E-21 — Notifications par courriel ou par message
- E-3 — Enquête du superviseur et mesures correctives avec relances
- Q-9 — Les employés utiliseront-ils leur téléphone personnel ou un appareil fourni, un accès web suffit-il, et les avis passent-ils par courriel ou par message texte (selon le choix) ?

Options envisagées

- Texto par une passerelle — Pertinent pour l'urgence d'un événement grave auprès de personnes sans courriel de poste ; ajoute un fournisseur et un récurrent. Variante à chiffrer si vous la reprenez.
- Notification mobile (push) — Requiert une application installée, non retenue.
- Messages dans l'application — Les superviseurs ne sont pas connectés en continu ; insuffisant pour un avis immédiat.

Décision

Courriel transactionnel par un service spécialisé, avec reprise sur échec et région de traitement canadienne à vérifier. Le message contient seulement un lien vers le portail, où les droits s'appliquent : aucun renseignement médical ni identité des blessés. Le message texte reste une alternative, jamais un envoi doublé.

Conséquences

- Compromis : Simplicité et traçabilité contre un délai de lecture non garanti pour un avis urgent.
- Risque : Un avis grave non lu à temps ; la fiabilité de livraison du courriel dépend du fournisseur.
- Risque : Fournisseur de courriel traitant hors du Canada.

Hypothèses

- Tous les destinataires d'avis ont un courriel professionnel dans l'annuaire ou les ressources humaines.
- La fiche de notifications est non vérifiée.

Vérifications prévues

- Confirmer la région de traitement du service de courriels.
- Définir avec vous le délai de livraison attendu pour un avis grave.

Références

- Décision type — notifications aux utilisateurs : courriel transactionnel, texto, notification mobile ou messages dans l'application (v2 — référence à vérifier)
- Renseignements personnels au Canada et au Québec — Loi 25, LPRPDE, principes des autorités sur l'IA (v1)

DA-10 — Échanges planifiés avec les ressources humaines et le progiciel de gestion

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	partiellement couverte par les références citées

Décision type : Décision type — intégration avec les systèmes existants : API synchrone, échange asynchrone, fichiers planifiés ou saisie manuelle — option retenue : Échange de fichiers planifié

Contexte

Employés, supérieurs, usines et départements viennent de systèmes tiers ; données de référence qui changent lentement ; mode d'accès inconnu.

- E-9 — Employés et supérieurs issus du système de ressources humaines
- E-10 — Usines et départements issus du progiciel de gestion
- Q-2 — Comment accéder à l'annuaire (protocole d'authentification unique), au système de ressources humaines et au progiciel de gestion (interface, fichier d'export, fréquence) ? L'annuaire peut-il imposer un second facteur aux superviseurs, au comité et au service de santé et sécurité (licence comprise) ? Pouvez-vous fournir des environnements d'essai et un interlocuteur pour chacun ?
- Exigence de qualité : Sécurité

Options envisagées

- API documentée et versionnée, appel synchrone — Choix par défaut, mais le portail doit rester utilisable si le système tiers est lent ou hors ligne ; la copie locale évite ce couplage.
- Saisie manuelle assumée (repli) — Les superviseurs dépendent de la hiérarchie à jour ; la saisie manuelle serait fragile pour 1 200 employés.

Décision

Synchronisation quotidienne planifiée, en lecture seule, des deux référentiels, par export de fichier ou par interface documentée interrogée en lot selon ce que chaque système offre. Le portail garde une copie locale, conserve les anciens codes, signale les employés sans supérieur et valide toute donnée reçue. Les appels exposés ou consommés suivent l'authentification par appel et les quotas de la règle API.

Conséquences

- Compromis : Découplage et résilience contre des données jusqu'à une journée de retard.
- Risque : Interface absente ou propriétaire, environnements d'essai tardifs.
- Risque : Départs ou changements de supérieur non reflétés avant la synchronisation suivante, avec mauvais routage possible d'un dossier.

Hypothèses

- Les deux systèmes fournissent un export ou une interface documentée.
- L'annuaire est traité à part (authentification unique).

Vérifications prévues

- Obtenir pour chaque système le mode d'accès, la fréquence permise, un environnement d'essai et un interlocuteur.
- Définir la règle de repli quand le supérieur est inconnu.

Références

- Décision type — intégration avec les systèmes existants : API synchrone, échange asynchrone, fichiers planifiés ou saisie manuelle (v2 — référence à vérifier)
- Intégrations par API explicites et contrats versionnés (v3)
- Sécurité des API — OWASP API Security Top 10 (2023) (v1)

DA-11 — Relances, avis et synchronisations par une file de traitements adossée à la base

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	partiellement couverte par les références citées

Décision type : Décision type — traitements différés : en ligne seulement, file de traitements en base ou courtier de messages dédié — option retenue : File de traitements adossée à la base de données

Contexte

Envoi d'avis avec reprise sur échec, relances des mesures en retard, synchronisations nocturnes, calcul des agrégats, purge.

- E-4 — Avis immédiat pour les événements graves
- E-3 — Enquête du superviseur et mesures correctives avec relances

E-9 — Employés et supérieurs issus du système de ressources humaines

- E-7 — Tableau de bord par usine et par mois
- Exigence de qualité : Disponibilité

Options envisagées

- Pendant la requête, sans file — Les appels au courriel et aux systèmes tiers peuvent échouer ou être lents ; les relances et synchronisations sont planifiées.
- Courtier de messages dédié — Aucun débit élevé ni plusieurs consommateurs ; composant supplémentaire à exploiter et à payer sans gain à ce volume.

Décision

File de traitements adossée à la base de données, sans service de file distinct, avec tâches planifiées, reprise sur échec et journalisation d'exécution. Un avis grave est inscrit dans la même transaction que l'événement, pour ne pas être perdu. Les volumes sont modestes et une seule application produit et consomme les tâches.

Conséquences

- Compromis : Simplicité et cohérence transactionnelle contre un débit limité, sans objet ici.
- Risque : Tâche échouée sans alerte : un avis grave non envoyé passerait inaperçu.

Hypothèses

- Environ 1 000 déclarations par mois au plus.
- La fiche des traitements différés est non vérifiée.

Vérifications prévues

- Alerte sur toute tâche d'avis en échec ou en attente au-delà d'un délai à fixer avec vous.

Références

- Décision type — traitements différés : en ligne seulement, file de traitements en base ou courtier de messages dédié (v2 — référence à vérifier)

DA-12 — Une seule organisation, cloisonnée par usine seulement au niveau des droits

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — plusieurs organisations dans une même solution : base partagée cloisonnée, base par organisation ou instance par client — option retenue : Une seule organisation (pas de modèle multi-organisations)

Contexte

Une entreprise unique répartie dans quatre usines ; directeurs d'usine et superviseurs limités à leur périmètre.

- E-1 — Remplacer le papier et le chiffrier par un portail unique
- E-5 — Accès restreint aux renseignements médicaux et à l'identité des blessés
- E-10 — Usines et départements issus du progiciel de gestion
- E-25 — Comptes fournis par l'annuaire ; rôles et droits construits dans le portail

Options envisagées

- Base (ou schéma) par organisation — Les usines appartiennent à la même organisation ; l'isolement physique ajouterait des coûts sans exigence documentée.

Décision

Aucun modèle multi-organisations : une seule base et un seul déploiement. L'usine est un attribut de rattachement qui sert aux droits et au tableau de bord, sans isolement physique par usine.

Conséquences

- Compromis : Simplicité et agrégats entre usines faciles contre aucun isolement physique entre usines.
- Risque : Une erreur de filtre par usine exposerait des dossiers d'une autre usine ; à couvrir par des tests.

Hypothèses

- Aucune filiale ni usine d'une autre entité juridique ne s'ajoute.
- La fiche des locataires est non vérifiée.

Vérifications prévues

- Tests d'accès entre usines pour chaque rôle.

Références

- Décision type — plusieurs organisations dans une même solution : base partagée cloisonnée, base par organisation ou instance par client (v2 — référence à vérifier)
- Multi-locataire — modèles de partage des ressources entre clients (v2)

DA-13 — Journaux d'audit et techniques envoyés vers l'outil central de l'équipe TI

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	partiellement couverte par les références citées

Contexte

Normes de journalisation imposées, accès aux renseignements médicaux à tracer, exploitation par une équipe TI interne.

- E-12 — Exploitation par l'équipe TI selon ses normes d'hébergement et de journalisation
- E-18 — Sécurité applicative, chiffrement et journal d'audit des accès sensibles
- Q-1 — Quelles sont les normes d'hébergement infonuagique et de journalisation de votre équipe TI (fournisseur et région approuvés, environnements, format et destination des journaux, gestion des secrets, correctifs) ?
- Exigence de qualité : Sécurité

Options envisagées

- Journalisation propre au portail seulement — Contraire aux normes imposées et aux pratiques de détection centralisée.

Décision

Journal d'audit applicatif (connexions, consultations de champs protégés, changements de droits) enregistré en base et transmis, avec les journaux techniques, vers l'outil central dans le format et la destination des normes de l'équipe TI. Les journaux ne contiennent aucun contenu médical. Une surveillance avec alertes sur les échecs de tâches et les accès anormaux est prévue ; les responsabilités d'exploitation sont à répartir avec votre équipe selon les fonctions du cadre de cybersécurité cité (gouverner, protéger, détecter, répondre, restaurer).

Conséquences

- Compromis : Intégration aux normes TI contre dépendance à un format non connu.
- Risque : Normes non communiquées : format, rétention et destination peuvent changer l'effort (environ + 20 à 80 h).
- Risque : Journaux conservés trop longtemps contenant des identifiants personnels.

Hypothèses

- Les journaux sont envoyés vers un outil central exportable.
- Durée de conservation des journaux à fixer avec votre équipe.

Vérifications prévues

- Obtenir les normes de journalisation avant la conception.
- Tester qu'une consultation de champ protégé produit une entrée d'audit.

Références

- Excellence opérationnelle et observabilité (v2)
- Cadre de cybersécurité NIST CSF 2.0 — fonctions de gouvernance (v1)
- Risques applicatifs de référence — OWASP Top 10 (édition 2025) (v2)

DA-14 — Disponibilité 24 h sur 7 par plusieurs zones d'une même région canadienne, sans reprise multirégion

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	partiellement couverte par les références citées

Contexte

Disponibilité exigée sans cible chiffrée ; usines possiblement en continu (quarts de nuit) ; protection des données à préciser.

- E-19 — Disponibilité du portail
- Q-6 — Quelles plages de service (usines en continu, quarts de nuit) et quelle durée d'interruption et de perte de données maximale tolérez-vous ?
- Q-7 — L'exclusion « backup » du dossier vise-t-elle les sauvegardes ? Quelle durée de conservation des sauvegardes et quelle capacité de restauration attendez-vous pour des dossiers contenant des renseignements de santé ?
- Exigence de qualité : Disponibilité
- E-13 — Données au Canada

Options envisagées

- Reprise dans une seconde région canadienne — Plus forte que la demande ; environ + 20 à 60 h et un récurrent plus élevé, à retenir si la cible l'exige.
- Une seule zone — Écarté : une panne de zone interromprait les déclarations.

Décision

Hypothèse unique : service 24 h sur 7. Services gérés répartis sur plusieurs zones d'une même région canadienne, protection de base de l'hébergeur avec une restauration vérifiée avant la mise en service, déploiement avec retour arrière. Interruption maximale de quelques heures et perte de données d'une heure au plus sont des hypothèses. Une seconde région canadienne est une variante à chiffrer.

Conséquences

- Compromis : Coût d'infrastructure modéré contre une tolérance limitée aux pannes régionales.
- Risque : Une cible plus stricte que l'hypothèse exigerait de revoir l'infrastructure.
- Risque : Dépendance à la disponibilité de l'annuaire pour la connexion.

Hypothèses

- Cible chiffrée non déclarée ; hypothèses de plage 24 h sur 7, d'interruption et de perte de données ci-dessus.

Vérifications prévues

- Faire valider la cible par vos responsables d'usine.
- Répéter une restauration avant la mise en service.

Références

- Excellence opérationnelle et observabilité (v2)
- Optimisation des coûts et récurrent explicite (v2)

DA-15 — Reprise du chiffrier par un outil ponctuel avec rapport d'écarts et rejeu

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	non couverte par les références — justification propre au dossier

Contexte

Trois ans de déclarations à reprendre en partie, avec qualité et volume réels inconnus.

- E-11 — Reprise de trois ans de déclarations du chiffrier
- Q-3 — Combien de déclarations par mois le chiffrier contient-il réellement, et combien de lignes, de fichiers et de pièces jointes sur trois ans, dans quel état (colonnes uniformes, doublons, texte libre, photos) ?
- E-24 — Volumétrie : environ 1 200 employés, 1 000 déclarations par mois retenues

Options envisagées

- Saisie manuelle de l'historique — Disproportionnée pour plusieurs dizaines de milliers de lignes.
- Ne pas reprendre l'historique — Contraire à la demande ; les tendances du tableau de bord perdraient leur profondeur.

Décision

Outil de reprise ponctuel : lecture du chiffrier, nettoyage, correspondance nominale avec les employés, usines et départements, chargement par lots avec rapport d'écarts à valider par votre équipe, rejeu possible, puis verrouillage après la bascule. Les cas non rapprochés restent identifiés, sans invention de lien. Photos non reprises par hypothèse.

Conséquences

- Compromis : Historique exploitable contre effort de nettoyage et validation par votre équipe.
- Risque : Noms non rapprochables, doublons, texte libre : une part de l'historique pourrait rester non reprise ou à valider manuellement.
- Risque : Données de santé dans le chiffrier : l'outil et les copies de travail doivent respecter la région canadienne et être détruits.

Hypothèses

- Environ 36 000 lignes (1 000 déclarations par mois sur 36 mois), même hypothèse que le dimensionnement du stockage et des envois ; structure régulière.
- Hypothèse non appuyée par une fiche de référence.

Vérifications prévues

- Obtenir un échantillon du chiffrier et son nombre de lignes réel avant la conception de la reprise.
- Valider le rapport d'écarts avec le service de santé et sécurité avant la bascule.

Références

Aucune référence d'architecture citée ; la décision repose sur une justification propre au dossier.

DA-16 — Chaîne de livraison automatisée avec environnements séparés et déploiement contrôlé

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Contexte

Application sur mesure exploitée par l'équipe TI, données sensibles, exigence de sécurité et normes d'hébergement imposées.

- E-12 — Exploitation par l'équipe TI selon ses normes d'hébergement et de journalisation
- E-18 — Sécurité applicative, chiffrement et journal d'audit des accès sensibles
- Exigence de qualité : Sécurité
- Q-1 — Quelles sont les normes d'hébergement informatique et de journalisation de votre équipe TI (fournisseur et région approuvés, environnements, format et destination des journaux, gestion des secrets, correctifs) ?

Options envisagées

- Déploiement manuel sans automatisation — Non reproductible et sujet aux erreurs sur un système de santé et sécurité.

Décision

Code revu avant fusion, tests automatisés sur les demandes de fusion, construction reproductible, inventaire et suivi des dépendances, secrets hors du code, infrastructure décrite par du code, trois environnements séparés et déploiement en production déclenché manuellement après approbation, avec retour arrière. Le niveau de garantie de la chaîne est une hypothèse à confirmer avec votre équipe.

Conséquences

- Compromis : Mise en place initiale de la chaîne contre des livraisons sûres et réversibles.
- Risque : Chaîne sans responsable après le transfert ; dépendance compromise ou abandonnée.

Hypothèses

- Votre équipe TI peut prescrire ou fournir l'outillage de chaîne ; à confirmer.

Vérifications prévues

- Désigner un responsable de la chaîne et des mises à jour de dépendances côté TI.

Références

- Livraison continue et chaîne d'approvisionnement logicielle — DORA, SLSA, NIST SSDF (v2)
- Risques applicatifs de référence — OWASP Top 10 (édition 2025) (v2)

DA-17 — Aucune IA générative dans la solution

Statut	Date	Couverture
Proposée par l'IA, à confirmer avec vous	16 octobre 2026	couverte par les références citées

Décision type : Décision type — fonction d'IA générative : aucune, appel d'un modèle par API, recherche augmentée sur des documents, ou agent outillé — option retenue : Aucune IA générative (règles explicites ou recherche classique)

Contexte

Le besoin se décrit par des règles explicites ; données de santé et d'employés sous résidence canadienne.

- E-4 — Avis immédiat pour les événements graves
- E-5 — Accès restreint aux renseignements médicaux et à l'identité des blessés
- E-15 — Données de santé, d'identification et d'employés : protection renforcée
- Exigence de qualité : Confidentialité et renseignements personnels

Options envisagées

- Appel d'un modèle de langage par API, tâche bornée et sortie structurée — Possible pour résumer ou classer, mais aucune fonction demandée ne l'exige ; transmettre des renseignements de santé à un fournisseur ajouterait des garde-fous et un examen de confidentialité.

Décision

Aucune IA générative. Le seuil de gravité, le routage au superviseur, les relances et les agrégats reposent sur des règles stables. Les pistes d'IA sont présentées à part, non retenues et non chiffrées.

Conséquences

- Compromis : Comportement prévisible et périmètre simple contre l'absence d'aide à la lecture du texte libre.
- Risque : Aucun risque propre à l'IA ; l'analyse du texte libre reste manuelle.

Hypothèses

- Le client n'a pas demandé de fonction d'IA.

Vérifications prévues

- Revoir si une fonction d'IA est ajoutée : garde-fous et lieu d'inférence canadien à documenter.

Références

- Décision type — fonction d'IA générative : aucune, appel d'un modèle par API, recherche augmentée sur des documents, ou agent outillé (v2)
- Garde-fous d'une fonction d'IA générative — données, qualité, coût, repli (v2)

Scénario présenté et alternatives

Scénario présenté : Scénario initial (construire) — scénario exploré, non retenu

Approches examinées

Les approches considérées avant de retenir celle qui est chiffrée. Une approche « à vérifier » ne l'a pas été : ses fonctions, ses intégrations et ses coûts restent à confirmer avant d'en faire une option.

Approche	Statut	Ordre de grandeur	Motif
Portail web sur mesure hébergé en région canadienne, selon les normes de votre équipe TI (construction)	retenue et chiffrée	610 à 1 205 h classiques · 42 665,50 CAD à 128 882,50 CAD	Le besoin est propre : enquête par superviseur, avis de gravité, visibilité restreinte des renseignements médicaux, trois intégrations et normes d'hébergement imposées. Les postes chiffrant cette approche.

Approche	Statut	Ordre de grandeur	Motif
Achat et paramétrage d'un logiciel du marché de santé et sécurité au travail (achat et paramétrage)	à vérifier	250 à 550 h classiques · 20 895,15 CAD à 45 969,33 CAD	Aucun produit n'est nommé ni vérifié. À vérifier : hébergement au Canada, droits d'accès par champ pour les renseignements médicaux, avis de gravité, relances, tableau de bord, intégrations aux trois systèmes, reprise du chiffrier, coût d'abonnement pour 1 200 employés. — ne couvre pas : Droits d'accès fins sur la santé et l'identité des blessés, selon le produit ; Fiche de synthèse adaptée à l'organisme de réglementation ; Synchronisation avec les ressources humaines et le progiciel, si absente de série ; Reprise du chiffrier selon les formats d'import offerts
Produit du marché pour le flux d'incidents, avec modules sur mesure pour accès, avis et intégrations (hybride)	à vérifier	380 à 750 h classiques · 31 760,63 CAD à 62 685,45 CAD	Réduit la construction du flux de base, mais dépend d'un produit exposant des interfaces ouvertes et hébergé au Canada. À vérifier : limites de personnalisation, coût des licences, cohérence avec les normes de votre équipe TI. — ne couvre pas : Règles d'accès sur les données de santé hors des capacités du produit ; Tableau de bord propre à vos indicateurs ; Fiche réglementaire adaptée
Première version réduite (déclaration, enquête, mesures, avis, droits), puis tableau de bord, fiche réglementaire et historique en second temps (première version réduite)	possible	550 à 850 h classiques · 45 969,33 CAD à 71 043,51 CAD	Même socle, mêmes intégrations et mêmes contrôles d'accès, mais le tableau de bord, la fiche réglementaire et la reprise des trois ans sont reportés. Levier si l'échéance dans l'année ou un budget à fixer l'exigent ; le report ne retire ni sécurité ni confidentialité. — ne couvre pas : Tableau de bord par usine et par mois en première version ; Reprise de l'historique du chiffrier au démarrage ; Fiche de synthèse pour les déclarations réglementaires au démarrage

Ordre de grandeur des autres approches : leurs heures de réalisation classique au coût moyen d'une heure de référence de ce dossier (83,58 CAD) — une comparaison, pas un devis.

Effort, enveloppe de services et coûts

Montants en CAD, horizon de 12 mois. Les bornes basse / centrale / haute sont des scénarios de planification, non un intervalle de confiance ; l'enveloppe n'est pas un devis ferme.

Résultat	Basse	Centrale	Haute
Effort (heures)	313,3 h	524,1 h	951,25 h
Enveloppe de services	42 665,50 CAD	71 294,25 CAD	128 882,50 CAD

Résultat	Basse	Centrale	Haute
Coût total client sur l'horizon	76 630,62 CAD	105 259,37 CAD	162 847,62 CAD

Dépenses initiales : 18 500,00 CAD

Récurrent mensuel indicatif : 1 288,76 CAD

Récurrent sur l'horizon : 15 465,12 CAD

- Montants hors taxes. TPS et TVQ applicables selon le statut fiscal du client et la nature des prestations.
- Convention du récurrent annuel : toute période entamée sur l'horizon est comptée entière.
- 21 % du budget (22 147,12 CAD sur 105 259,37 CAD) repose sur des hypothèses que vos réponses peuvent confirmer — voir « À préciser ensemble ».
- Budget recommandé à autoriser : entre 88 125,21 CAD et 187 274,76 CAD, environ 121 048,28 CAD (scénario central plus une provision pour imprévus de 15 788,91 CAD, soit 15 %)
- Une estimation faite à ce stade comporte une marge : le montant final dépend de ce qui reste à préciser et de vos choix.
- La provision suit la part du budget à confirmer : 10 % jusqu'à 15 %, 15 % jusqu'à 40 %, 20 % au-delà.
- Sans l'accélération supposée par le mode de réalisation : 114 750,00 CAD d'enveloppe de services et 26 semaines.
- Échéance déclarée au questionnaire : dans l'année (52 semaines). Délai calculé : 21 semaines : l'échéance est tenue au rythme retenu.

Coût total de possession

Résultat	Basse	Centrale	Haute
Coût total (construction, dépenses initiales et récurrent sur l'horizon)	76 630,62 CAD	105 259,37 CAD	162 847,62 CAD

Hypothèse de réalisation

Mode : Réalisation assistée par l'IA. Réalisation assistée par des outils d'IA de développement, par une équipe qui les emploie au quotidien, sous la supervision de développeurs. Les heures de chaque poste sont estimées pour une réalisation classique, puis multipliées par un facteur publié selon la nature du travail ; le dossier montre les deux.

Facteur = heures retenues ÷ heures de réalisation classique, par nature de travail et par borne (basse / centrale / haute).

Nature de travail	Facteurs (b / c / h)	Base	Source et date
Code standard (écrans, formulaires, CRUD, API internes, logique courante)	0,30 / 0,40 / 0,60	Hypothèse d'une équipe rompue aux outils d'IA sur une application neuve : au-delà des essais en entreprise publiés (0,79-0,81), en deçà du cas isolé de Peng 2023 (0,44) pour la valeur haute.	Peng et al. 2023, arXiv 2302.06590 ; Cui, Demirer et al., Management Science 2025 ; décision de Linuen du 27 septembre 2026, 2026-09-27
Tests automatisés et documentation	0,25 / 0,35 / 0,55	Artefacts les plus générables ; même hypothèse d'équipe que le code standard.	Extrapolation des facteurs du code standard ; décision de Linuen du 27 septembre 2026, 2026-09-27
Infrastructure et déploiement	0,50 / 0,65 / 0,85	Configuration largement générée ; les pièges propres à chaque fournisseur demeurent.	Jugement structuré ; décision de Linuen du 27 septembre 2026, 2026-09-27
Migration et reprise de données	0,55 / 0,70 / 0,90	Les scripts s'accélèrent, la compréhension des données existantes beaucoup moins.	Jugement structuré ; décision de Linuen du 27 septembre 2026, 2026-09-27
Intégration avec l'existant et les tiers	0,65 / 0,80 / 1,00	Zone du ralentissement mesuré par METR 2025 : inconnues et attentes de tiers, accélération limitée.	METR, juillet 2025, arXiv 2507.09089 ; décision de Linuen du 27 septembre 2026, 2026-09-27
Analyse, cadrage, conception	0,70 / 0,80 / 0,95	Temps dominé par les échanges et les décisions humaines ; rédaction et variantes accélérées.	Jugement structuré ; décision de Linuen du 27 septembre 2026, 2026-09-27
Coordination, validation client, formation	1,00 / 1,00 / 1,00	Calendriers de personnes ; la politique compte déjà 5 jours de validation par jalon.	Politique de chiffrage de la plateforme (boucle de validation client par jalon), 2026-09-27
Sécurité, revue et assurance qualité	1,00 / 1,00 / 1,10	Plus de code généré = plus à relire (Faros 2025 : revue +91 % ; DORA 2024-2025 : stabilité en baisse).	Faros AI 2025 ; DORA 2024 et 2025 ; Denisov-Blanch (Stanford) 2025, 2026-09-27

Borne	Référence	Retenue
Basse		610 h
Centrale		853 h
Haute		1205 h

- 6 facteurs reposent sur un jugement, sans mesure dédiée : Code standard (écrans, formulaires, CRUD, API internes, logique courante), Tests automatisés et documentation, Infrastructure et déploiement, Migration et reprise de données, Intégration avec l'existant et les tiers, Analyse, cadrage, conception.
- Si l'accélération ne se matérialisait pas, l'enveloppe de services serait de 114 750,00 CAD au lieu de 71 294,25 CAD, et le délai de 26 semaines au lieu de 21 (scénario central).

Postes d'effort

Cod e	Poste	Nature de travail	Référence (b / c / h)	Facteur (b / c / h)	Retenue (b / c / h)	À confirmer	Comment ce chiffre est établi
P-1	Cadrage et spécification fonctionnelle	Analyse, cadrage, conception	26 / 36 / 46 h	0,70 / 0,80 / 0,95	18,2 / 28,8 / 43,7 h	—	Décomposition : ateliers (10 h), rédaction de la spécification (16 h), maquettes des écrans clés (6 h), validation et corrections (4 h).
P-2	Conception technique, modèle de données et plan de sécurité	Analyse, cadrage, conception	28 / 40 / 50 h	0,70 / 0,80 / 0,95	19,6 / 32 / 47,5 h	—	Décomposition : modèle de données et droits (14 h), intégrations et reprise (8 h), sécurité et audit (8 h), alignement sur les normes TI et revue (10 h).
P-3	Socle d'hébergement, environnements et chaîne de livraison	Infrastructure et déploiement	40 / 60 / 100 h	0,50 / 0,65 / 0,85	20 / 39 / 85 h	dépend de Q-1	Scénario : base gérée (10 h), stockage et chiffrement (8 h), infrastructure en code (16 h), chaîne de livraison (14 h), surveillance et journalisation (12 h) ; fourchette élargie car les normes sont inconnues.
P-4	Déclaration d'événements avec photos, sur poste et téléphone	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	54 / 70 / 96 h	0,30 / 0,40 / 0,60	16,2 / 28 / 57,6 h	—	Décomposition : modèle et API (14 h), formulaire adaptatif accessible (22 h), photos, capture et liens signés (19 h), listes et détail (10 h), validations (5 h).

Cod e	Poste	Nature de travail	Référence (b / c / h)	Facteur (b / c / h)	Retenue (b / c / h)	À confirmer	Comment ce chiffre est établi
P-5	Enquête du superviseur, mesures correctives et relances	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	47 / 62 / 84 h	0,30 / 0,40 / 0,60	14,1 / 24,8 / 50,4 h	—	Décomposition : enquête (20 h), mesures et échéances (16 h), flux et statuts (10 h), traitement planifié des relances (10 h), historique (6 h).
P-6	Droits d'accès par champ et journal d'audit des données sensibles	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	40 / 55 / 72 h	0,30 / 0,40 / 0,60	12 / 22 / 43,2 h	—	Décomposition : modèle de rôles et rattachements (10 h), contrôle par objet et par champ (18 h), journal d'audit (12 h), conservation et purge (8 h), exigence du second facteur et sessions (7 h).
P-7	Avis immédiat des événements graves et notifications par courriel	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	20 / 28 / 36 h	0,30 / 0,40 / 0,60	6 / 11,2 / 21,6 h	—	Décomposition : file en base et reprise (8 h), règles de gravité et destinataires (7 h), gabarits (5 h), intégration du service de courriels (8 h).
P-8	Tableau de bord par usine et par mois	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	25 / 35 / 45 h	0,30 / 0,40 / 0,60	7,5 / 14 / 27 h	—	Décomposition : requêtes et agrégats (12 h), calcul planifié (6 h), écrans et graphiques (12 h), droits et tests de cohérence (5 h).
P-9	Préparation des déclarations réglementaires (fiche de synthèse)	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	14 / 20 / 28 h	0,30 / 0,40 / 0,60	4,2 / 8 / 16,8 h	—	Décomposition : sélection des champs (4 h), gabarit PDF (8 h), export tableau (4 h), droits et essais (4 h).

Cod e	Poste	Nature de travail	Référence (b / c / h)	Facteur (b / c / h)	Retenue (b / c / h)	À confirmer	Comment ce chiffre est établi
P-10	Intégration de l'annuaire (authentification unique)	Intégration avec l'existant et les tiers	20 / 30 / 50 h	0,65 / 0,80 / 1,00	13 / 24 / 50 h	dépend de Q-2	Scénario : configuration de la fédération (10 h), association des identités et rôles (8 h), sessions et second facteur (6 h), essais avec l'équipe TI (6 h).
P-11	Synchronisation avec le système de ressources humaines	Intégration avec l'existant et les tiers	24 / 35 / 60 h	0,65 / 0,80 / 1,00	15,6 / 28 / 60 h	dépend de Q-2	Scénario : lecture de la source (8 h), correspondance et mise à jour (12 h), cas de départs et changements (7 h), rapport d'écarts et rejeu (8 h).
P-12	Synchronisation avec le progiciel de gestion (usines et départements)	Intégration avec l'existant et les tiers	16 / 24 / 40 h	0,65 / 0,80 / 1,00	10,4 / 19,2 / 40 h	dépend de Q-2	Analogie avec la synchronisation RH, environ 70 % de sa charge : deux référentiels simples, sans hiérarchie ni cas de départs.
P-13	Reprise de trois ans de déclarations du chiffrier	Migration et reprise de données	40 / 56 / 100 h	0,55 / 0,70 / 0,90	22 / 39,2 / 90 h	dépend de Q-3	Scénario : profilage (10 h), règles de nettoyage et correspondance (18 h), outil de chargement par lots et rapport (14 h), répétitions (10 h), bascule (4 h).
P-14	Revue de sécurité applicative et correction des écarts	Sécurité, revue et assurance qualité	20 / 30 / 40 h	1,00 / 1,00 / 1,10	20 / 30 / 44 h	—	Décomposition : revue des droits (8 h), analyse automatisée et dépendances (6 h), essais manuels ciblés (10 h), corrections (6 h).

Cod e	Poste	Nature de travail	Référence (b / c / h)	Facteur (b / c / h)	Retenue (b / c / h)	À confirm er	Comment ce chiffre est établi
P-15	Tests automatisés, essais d'accessibilité et campagne d'ensemble	Tests automatisés et documentation	48 / 67 / 86 h	0,25 / 0,35 / 0,55	12 / 23,45 / 47,3 h	—	Analogie : environ 20 % des heures de réalisation applicative (déclaration, enquête, droits, avis, tableau de bord, fiche), plus 13 h d'accessibilité (automatisation 4 h, essais manuels 9 h).
P-16	Recette avec le client et traitement des anomalies	Coordination, validation client, formation	20 / 30 / 40 h	1,00 / 1,00 / 1,00	20 / 30 / 40 h	—	Décomposition : scénarios (8 h), accompagnement de deux cycles (14 h), suivi des anomalies (8 h).
P-17	Mise en production et configuration de l'environnement	Infrastructure et déploiement	16 / 24 / 32 h	0,50 / 0,65 / 0,85	8 / 15,6 / 27,2 h	—	Décomposition : configuration de production (8 h), essai de restauration (6 h), répétition de bascule (4 h), bascule et vérifications (6 h).
P-18	Documentation et transfert à l'équipe TI	Tests automatisés et documentation	22 / 31 / 41 h	0,25 / 0,35 / 0,55	5,5 / 10,85 / 22,55 h	—	Décomposition : guide d'exploitation (12 h), architecture et sécurité (8 h), guide d'administration (5 h), deux séances de transfert (6 h).
P-19	Gestion de projet et coordination	Coordination, validation client, formation	60 / 80 / 105 h	1,00 / 1,00 / 1,00	60 / 80 / 105 h	—	Ratio de 10 à 15 % appliqué aux postes de réalisation, de tests et de mise en service du même dossier.

Cod e	Poste	Nature de travail	Référence (b / c / h)	Facteur (b / c / h)	Retenue (b / c / h)	À confirmer	Comment ce chiffre est établi
P-20	Stabilisation après la mise en service	Code standard (écrans, formulaires, CRUD, API internes, logique courante)	30 / 40 / 54 h	0,30 / 0,40 / 0,60	9 / 16 / 32,4 h	—	Analogie : environ 7 % des heures de réalisation applicative, étalées sur au moins quatre semaines.

Taux appliqués et heures par rôle

Taux de référence pour l'évaluation : ils convertissent les heures en dollars et n'engagent personne ; un mandat de réalisation se négocie à part.

Rôle	Taux de référence	Basse	Centrale	Haute
Analyste d'affaires / chargé de projet	140,00 CAD	38,2 h	58,8 h	83,7 h
Analyste qualité / développeur	115,00 CAD	32 h	53,45 h	91,3 h
Architecte technique	165,00 CAD	19,6 h	32 h	47,5 h
Chargé de projet	140,00 CAD	60 h	80 h	105 h
Développeur / support applicatif	120,00 CAD	9 h	16 h	32,4 h
Développeur back-end	130,00 CAD	32,1 h	58 h	115,2 h
Développeur back-end / analyste données	135,00 CAD	33,7 h	61,2 h	133,8 h
Développeur back-end / intégration	130,00 CAD	39 h	71,2 h	150 h
Développeur back-end/front-end	130,00 CAD	16,2 h	28 h	57,6 h
Rédacteur technique / architecte	150,00 CAD	5,5 h	10,85 h	22,55 h
Spécialiste infrastructure / DevOps	150,00 CAD	28 h	54,6 h	112,2 h

Dépenses du projet

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-1	Hébergement de production en région canadienne (application et base de données à haute disponibilité)	Mensuelle	804,00 CAD	9 648,00 CAD	—	Référence centrale : 2 × App Service P1 v3 (245,28 \$ US) + PostgreSQL 2 vCore en haute disponibilité (288,50 \$ US) + 128 Go doublés (32,38 \$ US) = 566,16 \$ US × 1,4196 = 804 \$ CA par mois (prix Azure lus le 2026-10-16). Aucun écart de la référence : charge modeste (1 000 déclarations par mois, pointe ×3) et disponibilité indispensable, d'où la base en haute disponibilité.
D-2	Environnement d'essai (préproduction) en région canadienne	Mensuelle	339,00 CAD	4 068,00 CAD	—	Référence centrale : App Service P1 v3 (122,64 \$ US) + PostgreSQL B2ms (108,04 \$ US) + 64 Go (8,10 \$ US) = 238,78 \$ US × 1,4196 = 339 \$ CA par mois (prix Azure lus le 2026-10-16). Aucun écart de la référence.
D-3	Stockage chiffré des photos et pièces jointes (prix hypothèse)	Mensuelle	2,16 CAD	25,92 CAD	dépend de Q-3	Calcul : 6 Go par mois (volumétrie) × 12 mois × 0,03 \$ par Go-mois = 2,16 \$ par mois. Prix unitaire posé par hypothèse, sans tarif consulté. — formule : 6 (Nouveau stockage de pièces jointes par mois (Go)) × 12 (Mois cumulés après un an d'exploitation) × 0,03 CAD (Prix du stockage objet par Go-mois (CAD)) = 2,16 CAD

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-4	Trafic sortant (consultation des photos et pièces jointes) (prix hypothèse)	Mensuelle	3,60 CAD	43,20 CAD	dépend de Q-9	Calcul : $6 \text{ Go} \times 5 \text{ consultations} \times 0,12 \$ \text{ par Go} = 3,60 \$$ par mois. Le trafic sortant n'est pas compris dans la référence d'hébergement. — formule : $6 \text{ (Nouveau stockage de pièces jointes par mois (Go))} \times 5 \text{ (Consultations moyennes de chaque fichier)} \times 0,12 \text{ CAD (Prix du trafic sortant par Go (CAD))} = 3,60 \text{ CAD}$
D-5	Surveillance, alertes et conservation des journaux techniques et d'audit (prix hypothèse)	Mensuelle	35,00 CAD	420,00 CAD	dépend de Q-1	Calcul : $1\,000 \text{ déclarations} \times 0,01 \text{ Go} \times 3,50 \$ \text{ par Go} = 35 \$$ par mois ; volume de journaux et prix posés par hypothèse, sans tarif consulté. — formule : $1\,000 \text{ (Déclarations par mois)} \times 0,01 \text{ (Journaux produits par déclaration (Go))} \times 3,50 \text{ CAD (Prix d'ingestion et de conservation par Go (CAD))} = 35,00 \text{ CAD}$
D-6	Sauvegardes et conservation des sauvegardes	Mensuelle	0,00 CAD	0,00 CAD	dépend de Q-7	La référence d'hébergement de production (Azure, lue le 2026-10-16) couvre la base avec 128 Go doublés ; la sauvegarde gérée est comprise jusqu'à la taille du stockage provisionné selon l'offre du fournisseur, à vérifier. — montant nul : compris dans D-1

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-7	Test d'intrusion indépendant avant la mise en production	Une fois	18 500,00 CAD	18 500,00 CAD	—	Milieu de la bande publiée de 12 000 à 25 000 \$ CA pour une application à plusieurs rôles (Stingrai, publiée le 2026-06-05, lue le 2026-10-15). Aucun écart de la référence : six rôles, renseignements de santé et d'employés, mais une seule application web et trois intégrations en lecture.
D-8	Conseil juridique ou réglementaire (Loi 25, renseignements de santé)	Une fois	0,00 CAD	0,00 CAD	—	Exclusion déclarée par le client au questionnaire d'ouverture (hors-périmètre : formation, conseil juridique ou réglementaire). — montant nul : coût possible laissé hors de l'enveloppe présentée, à prévoir par vous
D-9	Maintenance et support après la mise en service	Mensuelle	0,00 CAD	0,00 CAD	—	Réponse déclarée au questionnaire d'ouverture : l'exploitation et la maintenance reposent sur le service informatique du client. — montant nul : sans objet dans ce dossier
D-10	Fournisseur d'identité et authentification	Mensuelle	0,00 CAD	0,00 CAD	—	Écart de la référence : le dossier fédère l'annuaire existant au lieu d'un service payant (Auth0, tarifs lus le 2026-10-16, de 497 à 2 271 \$ par mois pour 5 000 à 10 000 utilisateurs). — montant nul : sans objet dans ce dossier

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-11	Envoi des courriels d'avis et de relance (prix hypothèse)	Mensuelle	5,00 CAD	60,00 CAD	dépend de Q-9	Calcul : 5 000 courriels × 0,001 \$ = 5 \$ par mois ; prix unitaire posé par hypothèse, sans tarif consulté. — formule : 5 000 (Courriels de notification par mois) × 0,001 CAD (Prix par courriel envoyé (CAD)) = 5,00 CAD
D-12	Dépôt de code, intégration continue et suivi des dépendances (prix hypothèse)	Mensuelle	75,00 CAD	900,00 CAD	dépend de Q-1	Calcul : 3 postes × 25 \$ par mois = 75 \$ par mois ; nombre de postes et prix posés par hypothèse, sans tarif consulté.
D-13	Licences logicielles renouvelables	Mensuelle	0,00 CAD	0,00 CAD	—	Approche du dossier : application construite sur mesure ; les services de plateforme sont facturés dans l'hébergement (référence Azure lue le 2026-10-16). — montant nul : sans objet dans ce dossier
D-14	Frais d'ouverture de compte et de mise en place des services	Une fois	0,00 CAD	0,00 CAD	dépend de Q-1	Les tarifs publics de l'hébergeur lus le 2026-10-16 (API de prix Azure) ne comportent que des prix de consommation, sans frais d'ouverture. — montant nul : sans objet dans ce dossier

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-15	Nom de domaine et certificats de sécurité	Mensuelle	0,00 CAD	0,00 CAD	dépend de Q-1	Accès réservé aux employés authentifiés par l'annuaire (description) ; les certificats gérés de l'hébergeur n'ont pas de frais pour un sous-domaine, selon le fonctionnement courant des services d'hébergement d'applications. — montant nul : sans objet dans ce dossier
D-16	Thème graphique et composants d'interface	Une fois	0,00 CAD	0,00 CAD	—	Application interne à usage fonctionnel ; le travail d'interface est chiffré dans les postes de déclaration et de tableau de bord. — montant nul : sans objet dans ce dossier
D-17	Configuration des services tiers (annuaire, courriel, référentiels)	Une fois	0,00 CAD	0,00 CAD	—	Ces tâches figurent aux postes de travail du dossier (mise en production, intégrations de l'annuaire, des ressources humaines et du logiciel) ; les trois systèmes appartiennent au client. — montant nul : compris dans P-17
D-18	Frais externes de reprise des données du chiffrier	Une fois	0,00 CAD	0,00 CAD	dépend de Q-3	Environ 36 000 lignes supposées (1 000 déclarations par mois × 36 mois, volumétrie du dossier), traitées par scripts ; le travail est au poste « reprise du chiffrier ». — montant nul : compris dans P-13

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-19	Matériel (postes, tablettes, bornes)	Une fois	0,00 CAD	0,00 CAD	dépend de Q-9	Description : déclaration depuis un poste de l'usine ou le téléphone de l'employé ; approche en application web adaptative. — montant nul : sans objet dans ce dossier
D-20	Production de contenu (textes, images, vidéos)	Une fois	0,00 CAD	0,00 CAD	—	Description : formulaires, enquêtes, mesures et tableau de bord ; formation et supports aux utilisateurs exclus du cadrage. — montant nul : sans objet dans ce dossier
D-21	Usage de modèles d'intelligence artificielle	Mensuelle	0,00 CAD	0,00 CAD	—	Architecture du dossier : aucun composant ne porte de rôle d'IA, et la description ne mentionne aucune fonction d'IA. — montant nul : sans objet dans ce dossier
D-22	Services imposés par les normes de votre équipe TI (coffre de secrets et de clés de chiffrement) (prix hypothèse)	Mensuelle	25,00 CAD	300,00 CAD	dépend de Q-1	Forfait de 25 \$ par mois posé par hypothèse pour deux coffres (essai et production) de faible volume d'opérations ; aucun tarif consulté. Il chiffre une inconnue plutôt que de la laisser à zéro.
D-23	Protection de base de l'hébergeur : sauvegardes gérées de la base (restauration à un instant donné) et protection des fichiers, comprises dans l'hébergement — activation (prix hypothèse)	Une fois	0,00 CAD	0,00 CAD	dépend de Q-7	La référence d'hébergement de production (Azure, lue le 2026-10-16) compte 128 Go doublés ; la sauvegarde gérée est comprise jusqu'à cette taille selon l'offre, à vérifier.

Code	Dépense	Périodicité	Montant par période	Sur l'horizon	À confirmer	Comment ce chiffre est établi
D-24	Sous-domaine interne et certificat géré de la plateforme — activation (prix hypothèse)	Une fois	0,00 CAD	0,00 CAD	dépend de Q-1	Accès réservé aux employés authentifiés par l'annuaire (description) ; les certificats gérés d'un hébergeur n'ont pas de frais pour un sous-domaine, selon le fonctionnement courant de ces services.
D-25	Reprise après sinistre : haute disponibilité sur plusieurs zones d'une même région, sans seconde région — activation (prix hypothèse)	Une fois	0,00 CAD	0,00 CAD	dépend de Q-6	Aucune cible de disponibilité n'est déclarée ; le scénario repose sur la redondance multizone déjà chiffrée (prix Azure lus le 2026-10-16).

Calcul du 16 octobre 2026 — chiffres du calcul retenu à la revue ; aucune valeur inventée lorsque tout est inconnu.

Volumétrie retenue

Grandeur	Valeur retenue	À confirmer	Comment ce chiffre est établi
Déclarations d'événements par mois	1 000 déclarations par mois	hypothèse à confirmer	Borne haute de l'intervalle déclaré (100 à 1 000 opérations par mois), retenue par prudence et lue comme des déclarations, soit 12 000 par an ; cette valeur unique alimente la reprise, le stockage et les courriels. — déclaré : de 100 à 1 000 ; borne haute de l'intervalle déclaré, retenue pour le dimensionnement — à confirmer
Employés pouvant déclarer un événement	1 200 employés	—	Description : 1 200 employés dans quatre usines, tous déclarants ; cohérent avec l'intervalle de 500 à 5 000 du questionnaire. — déclaré : de 500 à 5 000 ; donnée fournie
Facteur de pointe sur le volume de déclarations	3 multiple de la moyenne horaire	hypothèse à confirmer	Scénario : déclarations concentrées en fin de quart et après un événement marquant, soit 3 fois la moyenne. — hypothèse — à confirmer

Grandeur	Valeur retenue	À confirmer	Comment ce chiffre est établi
Croissance annuelle du volume de déclarations	0,1 par an (fraction)	hypothèse à confirmer	Hypothèse de 10 % par an : meilleur signalement des quasi-accidents après le passage du papier au portail ; effectif stable. — hypothèse — à confirmer
Usines à couvrir	4 usines	—	Description : employés répartis dans quatre usines. — donnée fournie
Taille moyenne d'une photo après compression	3 Mo par photo	hypothèse à confirmer	Photo de téléphone courante de 2 à 4 Mo ; 3 Mo retenus, sans compression côté serveur. — hypothèse — à confirmer
Nouveau stockage de pièces jointes par mois	6 Go par mois	hypothèse à confirmer	Calcul : 1 000 déclarations × 2 photos × 3 Mo = 6 000 Mo, soit environ 6 Go par mois, soit environ 72 Go par an. — dérivée d'une donnée fournie
Lignes d'historique du chiffrier à reprendre (trois ans)	36 000 lignes	hypothèse à confirmer	Calcul : 1 000 déclarations par mois retenues × 36 mois = 36 000 lignes, sans pièces jointes ; même hypothèse que les volumes mensuels. — dérivée d'une donnée fournie
Utilisateurs à droits élargis (superviseurs, comité, santé et sécurité, directeurs)	100 utilisateurs	hypothèse à confirmer	Calcul : environ 1 superviseur pour 12 employés, soit 100, comités, service de santé et sécurité et directeurs inclus ; ils voient les champs protégés et portent le second facteur. — hypothèse — à confirmer
Courriels de notification par mois	5 000 courriels par mois	hypothèse à confirmer	Calcul : 1 000 déclarations par mois × 5 courriels par déclaration = 5 000 par mois. — dérivée d'une donnée fournie
Photos jointes par déclaration	2 photos par déclaration	hypothèse à confirmer	Scénario : une photo du lieu et une de la situation ou de l'équipement, prises au téléphone, pour chaque déclaration. — hypothèse — à confirmer
Notifications courriel par déclaration	5 courriels par déclaration	hypothèse à confirmer	Scénario : avis au superviseur, accusé au déclarant, 1 à 2 affectations de mesures, 1 relance ; l'avis de gravité est rare et compté dans la marge. — hypothèse — à confirmer

Ce qui ferait bouger le budget

Facteur	Hypothèse retenue	Alternative	Impact	Effet sur le délai
Mode d'accès aux trois systèmes existants	Annuaire fédéré par protocole standard avec second facteur offert pour les rôles qui voient des renseignements de santé ; ressources humaines et logiciel par export planifié ou interface documentée, avec environnements d'essai.	Une ou deux interfaces propriétaires ou absentes, à construire sur mesure ; environnements d'essai tardifs ; second facteur à gérer par le portail.	+ 30 à 100 h pour les interfaces ; + 10 à 30 h pour le second facteur géré par le portail · Proportionnel aux heures, au taux publié du rôle d'intégration ; licence de second facteur en plus si elle est à acquérir	+ 1 à 3 semaines
Normes d'hébergement et de journalisation de l'équipe TI	Région canadienne d'un grand fournisseur infonuagique, trois environnements, journaux exportables vers l'outil central.	Normes imposant un socle, des contrôles ou des outils propres à l'entreprise.	+ 20 à 80 h · Heures au taux du rôle infrastructure, plus un effet possible sur le récurrent d'hébergement	+ 0,5 à 2 semaines
Volume et qualité du chiffrier à reprendre	Environ 36 000 lignes (1 000 déclarations par mois sur 36 mois) à structure régulière, sans pièces jointes, correspondance par nom.	Structure irrégulière, doublons, texte libre ou photos à reprendre ; ou, à l'inverse, quelques milliers de lignes seulement si le rythme réel est plus bas.	+ 20 à 70 h si irrégulier ou avec pièces jointes ; – 10 à – 25 h si quelques milliers de lignes · Proportionnel aux heures, au taux publié du rôle de données ; stockage et envois ajustés au volume réel	+ 0,5 à 2 semaines, ou – 0,5 semaine

Facteur	Hypothèse retenue	Alternative	Impact	Effet sur le délai
Cible de disponibilité et conservation des sauvegardes	Service 24 h sur 7 sur plusieurs zones d'une même région canadienne, sans reprise dans une seconde région ; protection de base de l'hébergeur d'environ 35 jours.	Reprise dans une seconde région canadienne, ou conservation plus longue des renseignements de santé avec essais de restauration récurrents.	+ 20 à 60 h pour la seconde région ; + 10 à 30 h pour la conservation longue · Heures au taux infrastructure, plus environ + 400 à 800 \$ par mois de récurrent pour la seconde région (hypothèse) ; stockage proportionnel à la durée de conservation	+ 0,5 à 1,5 semaine
Format imposé de la déclaration réglementaire	Fiche de synthèse exportable, que le service de santé et sécurité reporte à la main.	Reproduction du formulaire officiel ou export dans un format structuré imposé.	+ 15 à 50 h · Proportionnel aux heures, au taux publié du rôle de développement	+ 0,5 à 1,5 semaine

Ce qui n'est pas compris

- contenus et médias — Les libellés d'interface et les gabarits d'avis sont dans la réalisation. Textes de procédures, images et vidéos sont à fournir par vous.
- référencement — Portail interne derrière authentification : aucun référencement public.
- traduction — Français seulement. Une seconde langue ajouterait environ 15 à 40 h.
- formation — Exclue par vous, y compris guides et aide-mémoire. Le transfert technique à l'équipe TI est compris dans la documentation et le transfert.
- conseil juridique ou réglementaire — Exclu par vous. Le portail est conçu selon la nature des données ; la Loi 25 et la loi sur les renseignements de santé sont à considérer, sans conformité attestée.
- support après stabilisation — Quatre semaines de stabilisation comprises. Ensuite, l'exploitation revient à votre équipe TI ; aucun contrat de support n'est chiffré.
- évolutions fonctionnelles — Hors périmètre : application native, mode hors ligne, messages texte, dépôt automatisé à l'organisme, règles de routage configurables,

reprise multirégion, archivage à long terme.

Compris dans l'évaluation : reprise de données historiques, accessibilité, licences tierces.

Hypothèses de consommation et de prix, postes non chiffrés et limites

Les heures sont des scénarios de planification (basse / centrale / haute), sans signification probabiliste. Tout poste entre dans les totaux : l'incertitude s'exprime par la largeur de la fourchette et par la base écrite de chaque chiffre, jamais par un retrait du total. Les lignes qui reposent sur une hypothèse à confirmer sont marquées comme telles, avec la question dont elles dépendent, et la part du budget qu'elles représentent est indiquée.

- Prix d'essai ou hypothèses (non référencés) : D-3, D-4, D-5, D-11, D-12, D-22, D-23, D-24, D-25.
- Les heures retenues supposent une réalisation assistée par des outils d'IA de développement : les facteurs appliqués sont des hypothèses déclarées, dont 6 reposent sur un jugement, sans mesure dédiée. La section « Hypothèse de réalisation » dit ce que vaudrait le dossier si l'accélération ne se matérialisait pas.
- Les frais prélevés par votre prestataire de paiement sur vos ventes ne sont pas compris dans cette estimation.

Risques et dépendances utiles à la décision

- Les normes d'hébergement et de journalisation de l'équipe TI ne sont pas connues. Elles pourraient imposer un fournisseur, des services ou des contrôles différents des hypothèses. — Heures d'infrastructure et récurrent à réviser (environ + 20 à 80 h) ; la conception technique ne peut pas être figée avant leur réception.
- Les modes d'accès à l'annuaire, aux ressources humaines et au progiciel sont supposés (fédération standard, exports planifiés). Une interface absente ou propriétaire, ou des environnements d'essai tardifs, sont possibles. — Intégrations plus longues (environ + 30 à 100 h) et risque de décalage du calendrier, car ces systèmes appartiennent à des tiers.
- Le second facteur est porté par l'annuaire pour les administrateurs et pour les rôles qui voient les champs protégés (environ une centaine de comptes). L'annuaire pourrait ne pas l'offrir à ces comptes, ou sa licence pourrait être à acquérir. — Second facteur géré par le portail (environ + 10 à 30 h) ou licence récurrente à ajouter ; sans lui, des comptes ayant accès à des données de santé se connecteraient sans second facteur.

Le volume réel du chiffrier est inconnu. Le dossier retient 1 000 déclarations par mois (environ 36 000 lignes sur trois ans) ; une « opération » peut aussi désigner une enquête ou une mesure. La qualité est inconnue : doublons, noms non rapprochables, texte libre, photos éventuelles. — Volume réel plus faible : environ – 10 à – 25 h sur la reprise et stockage réduit. Structure irrégulière ou pièces jointes : environ + 20 à 70 h, avec validation manuelle par l'entreprise d'une partie de l'historique.

- Fuite ou accès abusif aux renseignements médicaux et à l'identité des blessés (contrôle d'accès incomplet, lien de fichier partagé, contenu sensible dans un courriel d'avis). — Incident de confidentialité à gérer au sens de la Loi 25, atteinte aux employés et à la confiance dans le portail. Mesures prévues : contrôle côté serveur par champ, liens signés, avis sans contenu médical, second facteur, journal d'audit, vérifications et revue de sécurité.
- Aucun test d'intrusion indépendant n'est dans l'enveloppe ; il est chiffré en variante. Le niveau de vérification applicative visé reste une hypothèse. — Des failles pourraient n'être trouvées qu'après la mise en service. Si votre équipe TI l'exige, le coût du prestataire s'ajoute, plus les correctifs.
- Le statut de l'entreprise au regard de la loi sur les renseignements de santé et de services sociaux n'est pas établi, ni la durée de conservation ni le responsable de la protection des renseignements personnels. — Les obligations de conservation, de destruction et de gouvernance pourraient s'ajouter (environ + 10 à 40 h). Le conseil juridique est hors périmètre : cette détermination vous revient.
- Le service de courriels, ou tout autre sous-traitant, pourrait traiter des données hors du Canada. Une région hors Québec appelle l'examen des facteurs relatifs à la vie privée. — Choix de fournisseur restreint ; sans service canadien, un autre canal ou fournisseur est à retenir. Les avis sans renseignement sensible réduisent le risque.
- Aucune cible de disponibilité n'est fixée alors qu'elle est indispensable. L'hypothèse retenue est un service 24 h sur 7 sur plusieurs zones d'une région ; des usines en continu pourraient exiger davantage. — Reprise dans une seconde région canadienne : environ + 20 à 60 h et hausse du récurrent d'infrastructure.
- L'exclusion « backup » du dossier semble issue du mot « reprise » du chiffrier, non d'un refus de sauvegarde. Le portail s'appuie sur la protection de base de l'hébergeur (environ 35 jours), sans service de sauvegarde distinct, ce qui est court si la durée de conservation des renseignements de santé est plus longue. — Une perte ou une corruption détectée tardivement pourrait ne plus être restaurable. Conservation plus longue ou essais de restauration récurrents : environ + 10 à 30 h et récurrent de stockage accru.
- Le seuil de gravité, les cas de rôles (déclaration visant le superviseur, absence) et le format des déclarations réglementaires restent à définir. — Règles de routage plus complexes ou reproduction d'un formulaire officiel : environ + 10 à 50 h chacun ; un avis mal calibré peut être manqué ou noyer le comité.
- Les photos de blessures ou de lieux prises avec un téléphone personnel peuvent laisser une copie dans la galerie, hors du portail et hors des droits d'accès. La capture

par le navigateur sans enregistrement n'est pas possible sur tous les appareils. — Renseignements de santé hors du périmètre contrôlé, avec risque d'incident de confidentialité. Atténuation : capture par le navigateur lorsque possible et consigne claire ; appareils fournis ou application native à chiffrer à part.

- Le niveau d'accessibilité AA est une hypothèse vérifiée par des contrôles automatisés et des essais manuels sur les parcours essentiels, sans audit externe ni attestation. — Un niveau plus élevé, un audit externe ou des écrans supplémentaires à vérifier augmenteraient les heures de réalisation et de tests ; l'attente d'une conformité attestée ne serait pas tenue.
- Les employés d'usine peuvent avoir un accès limité à un poste ou à un téléphone, ou refuser d'utiliser leur appareil personnel ; le portail n'a ni application native ni mode hors ligne. — Adoption plus faible des déclarations ; une application native ou des bornes dédiées seraient à chiffrer à part. La formation, hors périmètre, pèse aussi sur l'adoption.

Limites de l'approche retenue :

- Aucune application mobile native ni mode hors ligne : l'usage sur téléphone passe par l'interface web adaptative.
- Le dépôt à l'organisme de réglementation reste fait par une personne, hors du portail.
- La formation des utilisateurs, leurs guides et aide-mémoire, et le conseil juridique ou réglementaire sont exclus.
- Les lois à considérer (Loi 25, loi sur les renseignements de santé et de services sociaux) sont nommées sans conformité attestée ; l'application de la seconde reste à confirmer selon votre statut.
- Le niveau de vérification applicative visé est une hypothèse ; un test d'intrusion indépendant est une variante chiffrée à part, hors de l'enveloppe présentée.
- Le niveau AA d'accessibilité est visé en hypothèse avec vérifications automatisées et essais manuels ; aucun audit externe ni attestation.
- Aucun service de sauvegarde distinct ni archivage à long terme : seule la protection de base de l'hébergeur est supposée, en attendant votre réponse sur la conservation.
- Une région québécoise, une reprise multirégion ou un service de messages texte sont des variantes, non retenues par défaut.
- La reprise du chiffrier est partielle ; la qualité des données historiques peut limiter ce qui se charge automatiquement.

Délai

21 semaines depuis le démarrage (15 à 29 semaines).

Hypothèse de capacité : 1,00 personne(s) à 40,00 h productives par semaine, plus une coordination à temps partiel.

Dont 4 semaine(s) de délais externes non compressibles.

Le délai compte 3 semaine(s) d'attente incompressible (Recette, Stabilisation) : une fenêtre d'observation ou un cycle ne raccourcissent pas avec l'effort.

Rythmes possibles

Rythme	Équipe	Délai	Effort	Enveloppe de services
Rapide	3 personnes	13 semaines	576,51 h	78 423,68 CAD
Équilibré	2 personnes	14 semaines	550,31 h	74 858,96 CAD
Économe	1 personne	21 semaines	524,1 h	71 294,25 CAD

Le même travail (524,1 h), réparti sur plus ou moins de personnes. Linuen Studio le calcule à partir des postes et de leurs dépendances : un poste est tenu par une personne à la fois et ne commence qu'une fois ses préalables terminés. La plus longue chaîne de postes dépendants (189,6 h) fixe le délai le plus court possible : au-delà de l'équipe « Rapide », une personne de plus ne l'accélérerait pas.

Chaque personne supplémentaire ajoute 5 % d'heures de coordination (au plus 30 %) : une équipe plus grande va plus vite et coûte un peu plus. Hypothèse : 40 h productives par personne et par semaine.

Valeurs centrales ; délais externes et attentes incompressibles compris (7 semaines). Le délai annoncé plus haut est celui de l'hypothèse de capacité du dossier.

Phases ramenées par l'application dans la proportion de l'effort retenu (heures retenues ÷ heures de référence, basse / centrale / haute : 0,51 / 0,61 / 0,79). Les délais externes ne bougent pas.

Phase	Référence (b / c / h)	Retenue (b / c / h)	Jalon
Cadrage	0,75 / 1 / 1,3 sem.	0,4 / 0,6 / 1 sem.	Spécification fonctionnelle validée : échelle de gravité, rôles, champs de santé, contenu de la fiche réglementaire.
Conception	0,8 / 1,1 / 1,4 sem.	0,4 / 0,7 / 1,1 sem.	Conception technique et plan de sécurité revus avec l'équipe TI, alignés sur ses normes d'hébergement et de journalisation.

Phase	Référence (b / c / h)	Retenue (b / c / h)	Jalon
Réalisation	8,3 / 11,4 / 15,7 sem.	4,3 / 7 / 12,4 sem.	Déclaration, enquête, mesures, avis, droits d'accès, tableau de bord et fiche réglementaire livrés en environnement d'essai ; revue de sécurité et essais d'accessibilité faits.
Intégrations	2,7 / 3,9 / 6,7 sem.	1,4 / 2,4 / 5,3 sem.	Annuaire, ressources humaines et progiciel raccordés ; reprise du chiffrier répétée avec rapport d'écarts validé.
Recette	2 / 2 / 3 sem.	2 / 2 / 2,4 sem.	Deux cycles de recette terminés par le service de santé et sécurité, les superviseurs et l'équipe TI ; anomalies bloquantes corrigées. — durée minimale 2 sem.
Mise en production	1,1 / 1,6 / 2,1 sem.	0,6 / 1 / 1,7 sem.	Production configurée, restauration essayée, bascule faite, documentation remise et transfert à l'équipe TI réalisé.
Stabilisation	4 / 4 / 5 sem.	4 / 4 / 4 sem.	Au moins quatre semaines de suivi après la mise en service ; anomalies corrigées, relances et synchronisations réglées. — durée minimale 4 sem.

- Normes d'hébergement et de journalisation de l'équipe TI : 2 semaine(s) — Les normes doivent être communiquées avant la conception technique ; sans elles, la conception et le socle d'hébergement ne peuvent pas être arrêtés. Fourchette de 1 à 3 semaines.
- Environnements d'essai et interlocuteurs : annuaire, ressources humaines, progiciel : 3 semaine(s) — Ouverture des accès et fourniture de données d'essai par les propriétaires des trois systèmes. À demander dès le cadrage pour qu'ils courent pendant la réalisation. Fourchette de 2 à 5 semaines. (en parallèle du travail, non ajouté au délai)
- Livraison du chiffrier et validation des correspondances par le client : 2 semaine(s) — Le chiffrier doit être livré tôt et une personne de l'entreprise doit valider les correspondances de la reprise ; l'attente court pendant la réalisation. (en parallèle du travail, non ajouté au délai)
- Validation de la spécification par le service de santé et sécurité et le responsable de

la protection des renseignements personnels : 1 semaine(s) — Boucle de validation client avant la conception : échelle de gravité, champs de santé, durée de conservation.

- Fenêtre de changement de l'équipe TI pour la mise en production : 1 semaine(s) — Le processus de changement de l'équipe TI peut imposer une fenêtre de bascule planifiée. Fourchette de 0 à 2 semaines.

Ce délai est un plan de réalisation sous hypothèse de capacité, non un engagement de livraison.

À préciser ensemble

Écart de fourchette (haute – basse) qui dépend de chaque réponse, classé par écart en jeu. Une réponse qui sort de l'hypothèse retenue peut déplacer une ligne au-delà de ses bornes : voir « Ce qui ferait bouger le budget ».

Question	Réponse retenue (hypothèse)	Lignes concernées	Écart en jeu (haute – basse)
Q-1 — Quelles sont les normes d'hébergement infonuagique et de journalisation de votre équipe TI (fournisseur et région approuvés, environnements, format et destination des journaux, gestion des secrets, correctifs) ?	Région canadienne d'un grand fournisseur infonuagique, environnements de développement, d'essai et de production, journaux envoyés vers l'outil central de l'équipe TI.	P-2, P-3, P-17, D-2, D-5, D-9, D-12, D-14, D-15, D-21, D-22, D-24	17 233,50 CAD + 5 688,00 CAD de dépenses sur l'horizon
Q-2 — Comment accéder à l'annuaire (protocole d'authentification unique), au système de ressources humaines et au progiciel de gestion (interface, fichier d'export, fréquence) ? L'annuaire peut-il imposer un second facteur aux superviseurs, au comité et au service de santé et sécurité (licence comprise) ? Pouvez-vous fournir des environnements d'essai et un interlocuteur pour chacun ?	Fédération standard avec l'annuaire, second facteur déjà offert pour ces rôles ; synchronisation quotidienne par export ou interface documentée pour les ressources humaines et le progiciel.	P-10, P-11, P-12, D-10, D-17	14 430,00 CAD + 0,00 CAD de dépenses sur l'horizon
Q-3 — Combien de déclarations par mois le chiffrier contient-il réellement, et combien de lignes, de fichiers et de pièces jointes sur trois ans, dans quel état (colonnes uniformes, doublons, texte libre, photos) ?	Environ 36 000 lignes (1 000 par mois sur 36 mois), structure régulière, sans pièces jointes ; correspondance nominale avec les employés par nom.	P-13, D-3, D-18	9 180,00 CAD + 25,92 CAD de dépenses sur l'horizon
Q-5 — Quels renseignements de santé précis sont saisis (nature des blessures, soins, arrêts de travail), qui est le responsable de la protection des renseignements personnels, et pour quelle durée les dossiers sont-ils conservés ?	Champs de santé limités (blessure, arrêt de travail) ; conservation paramétrable, purge sur demande.	P-6, D-7, D-8	4 056,00 CAD + 18 500,00 CAD de dépenses sur l'horizon

Question	Réponse retenue (hypothèse)	Lignes concernées	Écart en jeu (haute – basse)
Q-4 — Quel organisme reçoit les déclarations obligatoires, quels formulaires ou formats exige-t-il, et le portail doit-il produire un document à reporter ou un fichier structuré ?	Une fiche de synthèse exportable (PDF et tableau) par événement déclarable, que le service de santé et sécurité reporte à la main.	P-9, D-13	1 701,00 CAD + 0,00 CAD de dépenses sur l'horizon
Q-6 — Quelles plages de service (usines en continu, quarts de nuit) et quelle durée d'interruption et de perte de données maximale tolérez-vous ?	Service 24 h sur 7 à zones multiples dans une région ; interruption maximale de quelques heures ; perte de données maximale d'une heure.	D-1, D-25	9 648,00 CAD de dépenses sur l'horizon
Q-7 — L'exclusion « backup » du dossier vise-t-elle les sauvegardes ? Quelle durée de conservation des sauvegardes et quelle capacité de restauration attendez-vous pour des dossiers contenant des renseignements de santé ?	Exclusion lue comme visant un service de sauvegarde distinct ou un archivage long terme ; protection de base de la base et des fichiers sur environ 35 jours, restauration vérifiée une fois avant la mise en service.	D-6, D-23	0,00 CAD de dépenses sur l'horizon
Q-8 — Comment définit-on un événement « grave », et quels sont les cas particuliers de rôles (déclaration visant le superviseur lui-même, absence du superviseur, déclaration confidentielle) ?	Échelle de gravité fixe à quatre niveaux ; le supérieur hiérarchique suivant prend le dossier en cas d'absence ou de conflit.	P-1, P-5, P-8	10 921,50 CAD
Q-9 — Les employés utiliseront-ils leur téléphone personnel ou un appareil fourni, un accès web suffit-il, et les avis passent-ils par courriel ou par message texte (selon le choix) ?	Accès web adaptatif sans application native ; photos prises par le navigateur sans enregistrement dans la galerie lorsque possible ; avis et relances par courriel.	P-4, P-7, D-4, D-11, D-19	7 410,00 CAD + 103,20 CAD de dépenses sur l'horizon
Q-12 — Souhaitez-vous un test d'intrusion indépendant avant la mise en service, ou un niveau de vérification applicative précis (par exemple exigé par votre équipe TI) ?	Pas de test d'intrusion indépendant dans l'enveloppe ; variante chiffrée à part.	P-14	2 760,00 CAD
Q-10 — Existe-t-il, en plus du papier et du chiffrier, un logiciel du marché de santé et sécurité en service que vous voulez conserver, interfacé ou remplacer ?	Aucun produit existant ; le papier et le chiffrier sont les seuls outils remplacés.	conditionne le périmètre entier (aucune ligne isolée)	conditionne le périmètre entier (aucune ligne isolée)
Q-11 — L'interface doit-elle être offerte en d'autres langues que le français, et existe-t-il une date ferme de mise en service (par exemple liée à une échéance réglementaire ou à un audit) ?	Interface en français seulement ; pas de date ferme au-delà de l'année.	D-16, D-20	0,00 CAD de dépenses sur l'horizon

État de la revue IA et réserves

État de la revue : résultat assisté par IA — proposition, revue critique par un second modèle et contrôles automatiques effectués ; aucune validation professionnelle.

La revue automatique a porté sur l'intégralité du périmètre présenté (31 éléments).

- défaut démontré (proposition) : La dépense « Test d'intrusion indépendant avant la mise en production » chiffre un test d'intrusion indépendant à 18 500 \$. Pourtant, trois sections disent le contraire : les limites de l'approche (« la vérification indépendante n'est pas incluse »), le poste P-14 (« Vérification indépendante non incluse ») et la pile de tests (« Test d'intrusion externe (variante chiffrée à part) »). — Vous ne pouvez pas savoir si le test d'intrusion fait partie de l'enveloppe présentée. Le total et le périmètre de sécurité sont ambigus. — modifié dans la révision : Le test d'intrusion indépendant est maintenant présenté partout comme une variante chiffrée à part, hors de l'enveloppe présentée. Cela figure dans les limites de l'approche, dans l'exigence de sécurité (E-18), dans la note de couverture, dans le poste de revue de sécurité (« test d'intrusion indépendant ... hors de ce poste »), dans la décision de contrôle d'accès (avec une alternative dédiée) et dans le risque correspondant. Une nouvelle question, Q-12, vous demande si vous le souhaitez ou si vos normes l'exigent. Par défaut, la vérification se limite aux contrôles automatisés et à la revue de sécurité de la réalisation.
- défaut démontré (proposition) : Au calendrier, la phase de stabilisation annonce « Quatre semaines de suivi » (minimum de 4 semaines), mais affiche 1,3 semaine en valeur centrale et 1,7 en valeur haute. La recette a un minimum de 2 semaines pour deux cycles, mais sa valeur basse est de 1,7 semaine. Une fenêtre d'observation et un cycle de validation ont été dérivés des heures. — La durée calculée est sous-estimée d'au moins 2,7 semaines sur la stabilisation, et la recette peut être planifiée sous son propre minimum. — modifié dans la révision : Une hypothèse explicite (E-28) fixe des durées minimales de calendrier : recette d'au moins 2 semaines (deux cycles de validation) et stabilisation d'au moins 4 semaines de suivi, quelles que soient les heures. Elle est reprise dans la couverture, dans les hypothèses et les références du poste de recette (au moins deux semaines) et dans le poste de stabilisation (au moins quatre semaines de calendrier, heures étalées sur cette durée). Les durées de phase dérivées des heures ne peuvent donc plus passer sous ces minima.
- défaut démontré (besoin E-24) : Deux hypothèses de volume se contredisent. Les dépenses retiennent 1 000 déclarations par mois, soit 12 000 par an. La reprise suppose 3 000 lignes pour trois ans, « hypothèse de 1 000 déclarations par an ». Au rythme mensuel retenu, trois ans donneraient environ 36 000 lignes. Par ailleurs, une déclaration par mois pour 1 200 employés reste à confirmer : une « opération » peut aussi désigner une enquête ou une mesure. — Le poste de reprise ou les dépenses liées au volume (stockage, journaux, courriels) reposent sur un volume faux d'un facteur 10 à 12. — modifié dans la révision : Une seule hypothèse est retenue partout : 1 000 déclarations par mois (12 000 par an), soit environ 36 000 lignes à reprendre

sur trois ans. Elle figure dans E-24, E-11, le composant de reprise, la couverture, la décision de reprise (alternative « plusieurs dizaines de milliers de lignes ») et le poste de reprise du chiffrier, dont les heures passent à 40 / 56 / 100 h avec une base de 36 000 lignes. La mention « 1 000 par an » est retirée. La question Q-3 demande désormais le nombre réel de déclarations par mois et de lignes du chiffrier ; elle précise qu'une « opération » peut aussi désigner une enquête ou une mesure. La réponse resserrera la reprise, le stockage et les envois ensemble.

- défaut démontré (décision Relances, avis et synchronisations par une file de traitements adossée à la base) : La décision retient une file de traitements adossée à la base : l'avis grave est inscrit dans la même transaction que l'événement. La pile technique retient plutôt une « file de messages gérée ». Ce service distinct n'apparaît ni parmi les composants ni dans les dépenses. — Avec une file gérée séparée, la garantie « L'avis d'un événement grave n'est jamais perdu en silence » (écriture dans la même transaction) n'est plus tenue, et un récurrent reste non chiffré. — modifié dans la révision : La file adossée à la base est retenue partout, sans service de file distinct. Dans l'architecture, la base de données porte la file des messages à envoyer et le flux base → traitements planifiés est ajouté ; les traitements planifiés précisent « aucune file de messages externe ». La décision dit « sans service de file distinct », les postes d'infrastructure et d'avis graves parlent de file en base, et la conception technique intègre la file en base. L'avis grave s'écrit ainsi dans la même transaction que l'événement, et aucun service de file n'est à ajouter.
- défaut démontré (décision Authentification unique par l'annuaire de l'entreprise, sans compte propre au portail) : La décision limite le second facteur au service de santé et sécurité et aux administrateurs. Or les superviseurs et le comité voient aussi les renseignements médicaux, et les limites d'accès comme la volumétrie (100 rôles privilégiés) les comptent parmi les rôles privilégiés. — Environ une centaine de comptes ayant accès à des données de santé pourraient se connecter sans second facteur. — modifié dans la révision : Le second facteur, porté par l'annuaire, est étendu aux administrateurs et à tout rôle qui voit les champs protégés : superviseurs, comité et service de santé et sécurité (environ une centaine de comptes). Cela apparaît dans l'exigence de sécurité, la décision d'authentification (tradeoffs, vérifications), le composant d'annuaire, les limites d'accès, les postes de droits d'accès et d'intégration de l'annuaire, la couverture et la justification de l'approche. La question Q-2 demande si l'annuaire peut l'imposer à ces rôles, licence comprise, et un risque est ajouté : un second facteur géré par le portail coûterait environ + 10 à 30 h, ou une licence récurrente s'ajouterait. Cette licence est à confirmer avec vous.
- défaut démontré (décision Usage sur téléphone par l'interface web adaptative, sans application native) : La décision et la pile visent le niveau AA comme hypothèse. Les exclusions écartent pourtant tout audit et tout correctif liés à une norme d'accessibilité, et aucun poste ne prévoit d'essais d'accessibilité. — L'engagement sur le niveau AA n'est ni chiffré ni vérifiable, ce qui peut créer une attente que la livraison ne tiendra pas. — modifié dans la révision : Le niveau AA (WCAG 2.2) est conservé en hypothèse et chiffré. Une exigence E-22 est ajoutée, avec une couverture partielle : aucun audit externe ni attestation. Les heures passent à 54 / 70

/ 96 h pour la déclaration et à 47 / 62 / 84 h pour l'enquête, pour concevoir des écrans accessibles. Le poste de tests passe à 48 / 67 / 86 h, dont 13 h de vérifications automatisées et d'essais manuels (clavier, lecteur d'écran) sur la déclaration, l'enquête et la consultation. La décision d'accès web et un risque décrivent ces limites. Le niveau reste à confirmer avec vous.

- information manquante (proposition) : Le risque sur l'exclusion « backup » demande une décision, mais aucune question n'y correspond. La dépense de sauvegarde suppose une conservation par défaut de quelques jours, ce qui est court pour des renseignements de santé dont la durée de conservation n'est pas fixée. — Une perte ou une corruption détectée tardivement pourrait ne plus être restaurable, et l'exclusion du dossier reste ambiguë. — modifié dans la révision : La question essentielle Q-7 est ajoutée : l'exclusion « backup » vise-t-elle les sauvegardes, et quelle durée de conservation et capacité de restauration attendez-vous pour des dossiers de santé ? Par défaut, on suppose la protection de base de l'hébergeur (environ 35 jours, région canadienne), sans archivage long terme ni service distinct, avec une restauration vérifiée avant la mise en service. L'alternative est de + 10 à 30 h et un récurrent de stockage accru. La question est reliée aux décisions de base de données, de stockage de fichiers et de disponibilité, et au risque sur l'exclusion « backup ». Le poste d'infrastructure et celui de mise en production en tiennent compte.
- défaut démontré (poste P-18) : Ce poste inclut un « aide-mémoire pour les utilisateurs ». La dépense Production de contenu (textes, images, vidéos) affirme qu'aucun guide n'est produit, et la formation est exclue. — Le périmètre de la documentation destinée aux utilisateurs est flou, à la limite de la formation exclue. — modifié dans la révision : L'aide-mémoire pour les utilisateurs est retiré du poste de documentation et de transfert, qui ne couvre plus que la documentation technique (exploitation, architecture, administration, restauration) et les séances de transfert à l'équipe TI : 22 / 31 / 41 h, avec un guide d'administration seul. L'exclusion de la formation (E-30) nomme maintenant aussi les guides et aide-mémoire destinés aux utilisateurs, ce que reprennent les limites de l'approche, la couverture et le contenu du poste. Le périmètre est donc cohérent avec la formation exclue.
- risque (décision Usage sur téléphone par l'interface web adaptative, sans application native) : Si les employés prennent les photos de blessures ou de lieux avec leur téléphone personnel, une copie peut rester dans la galerie de l'appareil, hors du portail et hors des droits d'accès. — Des renseignements de santé pourraient se retrouver hors du périmètre contrôlé, avec un risque d'incident de confidentialité. — modifié dans la révision : La capture de photo par le navigateur, sans enregistrement dans la galerie lorsque c'est possible, avec une consigne d'usage pour les appareils personnels, est ajoutée à l'hypothèse web adaptatif, au composant d'interface, à la décision d'accès mobile (avec un essai d'absence de copie dans la galerie), au poste de déclaration (54 / 70 / 96 h) et à la couverture. Un risque dédié est ajouté : cette capture n'est pas possible sur tous les appareils, avec des appareils fournis ou une application native en atténuation, à chiffrer à part. La question Q-9 demande si les téléphones sont personnels ou fournis ; cela reste à confirmer avec vous.

défaut démontré (besoin E-19) : L'exigence suppose un service continu sur les heures d'exploitation des usines. La réponse par défaut de Q-6 suppose un service 24 h sur 7. — La cible retenue pour dimensionner l'hébergement et la surveillance est ambiguë. — modifié dans la révision : Une seule hypothèse est retenue partout : service 24 h sur 7, car les quarts de nuit sont possibles, sur plusieurs zones d'une même région canadienne et sans reprise multirégion. Elle figure dans l'exigence E-19, la couverture, la décision de disponibilité, les contraintes d'architecture, les hypothèses du poste d'infrastructure et la réponse par défaut de la question Q-6. La cible reste à confirmer avec vous.

Références et versions

Version conservée : V2 — 16 octobre 2026 (2026-10-16T08:59:09-04:00)

Version de présentation : 1.7

Calcul : 82 — moteur 2.4

Gabarit du dossier : 1.19

Références de connaissances citées : Décision type — acheter ou construire : application sur mesure, plateforme du marché adaptée, ou logiciel complet acheté (v1 — référence à vérifier) ; Décision type — style d'architecture : monolithe modulaire, microservices ou assemblage de services gérés (v3 — référence à vérifier) ; Monolithe modulaire — une application déployée d'un bloc, structurée en modules (v2) ; Décision type — authentification : comptes intégrés à l'application, fournisseur d'identité géré ou annuaire de l'organisation (v2 — référence à vérifier) ; Authentification et gestion des identités — NIST SP 800-63-4 (v2) ; Exigences de vérification de sécurité applicative — OWASP ASVS (v2) ; Décision type — lieu d'hébergement des données : au Québec, au Canada ou ailleurs, selon la nature des données (v3 — référence à vérifier) ; Classification, chiffrement et résidence des données (v2) ; Renseignements personnels au Canada et au Québec — Loi 25, LPRPDE, principes des autorités sur l'IA (v1) ; Décision type — stockage principal des données : base relationnelle, base documentaire ou stockage clé-valeur géré (v2 — référence à vérifier) ; Base relationnelle transactionnelle comme stockage principal (v2) ; Décision type — fichiers déposés ou produits : stockage objet, base de données ou disque du serveur (v2 — référence à vérifier) ; Stockage objet pour les fichiers et documents (v1) ; Stockage objet compatible S3 (OVHcloud — région canadienne Beauharnois confirmée) (v2) ; Risques applicatifs de référence — OWASP Top 10 (édition 2025) (v2) ; Sécurité intégrée à la conception (piliers Well-Architected) (v2) ; Décision type — application mobile : site adaptatif, application Web progressive ou native (v1 — référence à vérifier) ; Accessibilité des sites et applications Web — WCAG 2.2 et standard québécois SGQRI 008 3.0 (v2) ; Décision type — notifications aux utilisateurs : courriel transactionnel, texto, notification mobile ou messages dans l'application (v2 — référence à vérifier) ; Décision type — intégration avec les systèmes existants : API synchrone, échange asynchrone, fichiers planifiés ou saisie manuelle (v2 — référence à vérifier) ; Intégrations par API explicites

et contrats versionnés (v3) ; Sécurité des API — OWASP API Security Top 10 (2023) (v1) ; Décision type — traitements différés : en ligne seulement, file de traitements en base ou courtier de messages dédié (v2 — référence à vérifier) ; Décision type — plusieurs organisations dans une même solution : base partagée cloisonnée, base par organisation ou instance par client (v2 — référence à vérifier) ; Multi-locataire — modèles de partage des ressources entre clients (v2) ; Excellence opérationnelle et observabilité (v2) ; Cadre de cybersécurité NIST CSF 2.0 — fonctions de gouvernance (v1) ; Optimisation des coûts et récurrent explicite (v2) ; Livraison continue et chaîne d'approvisionnement logicielle — DORA, SLSA, NIST SSDF (v2) ; Décision type — fonction d'IA générative : aucune, appel d'un modèle par API, recherche augmentée sur des documents, ou agent outillé (v2) ; Garde-fous d'une fonction d'IA générative — données, qualité, coût, repli (v2)

Ce document se lit hors ligne ; les liens externes éventuels ne servent qu'à approfondir une référence. Il ne remplace pas une validation professionnelle.