Feuille de route relative au partage et à la gouvernance des données dans le cadre d'un « nouveau projet »

[outil 3 complétant le modèle d'entente de partage de données élaboré par BLG]

La présente feuille de route fournit aux membres des équipes Santé Ontario (ESO) un cadre pratique pour la planification de projets collaboratifs nécessitant la mise en place de nouvelles modalités de partage de données en vertu du modèle d'entente de partage de données (EPD) et, corrélativement, de la Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS). Elle ne constitue pas une liste d'exigences obligatoires, mais un outil conçu pour orienter la réflexion et accroître les chances de réussite d'un projet. Elle ne remplace pas l'EPD.

La technologie permet l'intégration, mais ce sont les personnes qui la rendent possible — les fournisseurs de soins primaires coordonnant des soins longitudinaux dans divers milieux, les cliniciens œuvrant au-delà des frontières organisationnelles, les professionnels de la protection de la vie privée assurant une gestion responsable des données, le personnel des technologies de l'information concevant et maintenant les systèmes, les dirigeants engageant les ressources et le leadership nécessaires, et les patients accordant leur confiance à leur équipe de soins quant à l'utilisation de leurs renseignements.

La mesure ultime du succès n'est ni la sophistication technologique ni la perfection en matière de protection de la vie privée. Il s'agit plutôt de l'amélioration des soins offerts aux patients et aux familles desservis par l'ESO, les membres étant en mesure d'agir comme une maison de santé efficace et comme coordonnateurs de ces soins.

Afin de soutenir cet objectif, la feuille de route est structurée autour des cinq phases suivantes, chacune étant conçue pour aider les membres des ESO à passer, de manière délibérée et responsable, du concept initial à un partage de données durable à l'échelle du système.

Instructions: Cliquez sur le lien ci-dessous correspondant à la phase ou à la sous-phase qui répond le mieux à vos besoins, ou parcourez l'ensemble du document pour consulter les cinq phases ainsi que la conclusion. Des notes relatives au présent outil provenant de BLG et de RISE, de même qu'une proposition de citation, figurent dans un encadré à la fin du document.

- Conclusion

Ensemble, ces cinq phases offrent aux membres des ESO une feuille de route pratique et adaptable pour faire progresser les soins intégrés grâce à un partage responsable des données, fondé sur une gouvernance solide, soutenu par la technologie et, ultimement, porté par des personnes qui travaillent de concert afin d'améliorer les résultats pour les patients.

PHASE 1: Fondements du projet et alignement de la gouvernance

1.1 Définition initiale de la portée du projet

- Objectif : Établir des paramètres clairs pour le projet ainsi que les exigences relatives au partage des données.
- Activités clés :
  - Définir le service intégré ou le parcours de soins nécessitant un partage de données
  - Déterminer précisément les données à partager
  - Évaluer si le projet soutient la capacité des fournisseurs de soins primaires à offrir des soins complets et continus, et cerner les lacunes en information en soins primaires et dans d'autres secteurs qui seront comblées
  - Déterminer si le projet concerne des communautés, des patients ou des données autochtones, et établir si les principes de souveraineté des données autochtones s'appliquent
  - Cartographier l'état actuel des échanges de données et les lacunes des systèmes
  - Décrire les risques cliniques et opérationnels associés à l'absence de partage des données
  - Documenter les résultats attendus pour les patients ainsi que les gains d'efficience pour le système
- Livrable : **Charte de projet** comprenant la justification clinique et opérationnelle ainsi que les risques liés à l'inaction.

1.2 Mobilisation de la haute direction

- Objectif : Obtenir l'engagement des dirigeants des organisations composant la structure de gouvernance de l'ESO.
- Messages clés à l'intention de la haute direction :
  - Alignement stratégique : En quoi ce projet contribue à l'avancement des soins intégrés et aux objectifs de performance de l'ESO
  - Équilibre des risques : Comparaison entre les risques associés au partage des données et les risques liés à la fragmentation des soins et aux lacunes informationnelles
  - Responsabilité partagée : Délimitation claire des rôles, des responsabilités et des considérations relatives à la responsabilité juridique
  - Engagement des ressources : Investissements requis en matière de technologies, de formation et de gestion du changement
  - Partenariat avec les peuples autochtones : Si le projet concerne des communautés ou des données autochtones, assurer une mobilisation significative des dirigeants autochtones et le respect des principes de souveraineté des données dès la conception du projet
  - Avantage concurrentiel : En quoi l'intégration des données positionne l'ESO favorablement en vue de futurs financements et partenariats
  - Renforcement des soins primaires : En quoi ce projet consolide les soins primaires comme fondement des soins intégrés en offrant un accès opportun aux évaluations spécialisées, aux événements hospitaliers, aux services communautaires et à toute autre information nécessaire à la gestion longitudinale des patients
- Activités :

- Présenter la charte de projet au Conseil de collaboration ou à l'instance équivalente
- Désigner un promoteur de niveau exécutif pour chaque organisation participante
- Mettre sur pied un comité directeur doté d'un pouvoir décisionnel, en tirant parti, dans la mesure du possible, des structures de gouvernance et des comités existants
- Obtenir un accord de principe afin d'explorer des modalités de partage de données
- Si des communautés autochtones sont concernées, mobiliser les dirigeants autochtones afin de déterminer les modalités appropriées de participation à la gouvernance et le pouvoir décisionnel

- Livrable : **Document d'aval de la haute direction** désignant les promoteurs et le comité directeur.

Phase 2: Conception de l'architecture technique et juridique

2.1 Décision relative à l'architecture des systèmes

- Objectif : Déterminer l'approche technique applicable au partage des données.
- Étapes :
  - Étape 1 : Évaluation de l'état actuel des technologies – Cartographier les systèmes existants pertinents au sein de l'ensemble des organisations participantes, en tenant compte notamment :
    - des systèmes actuels contenant des données pertinentes pour le projet ;
    - de l'interopérabilité entre les systèmes existants ;
    - de l'âge et de l'état du cycle de vie des systèmes ;
    - de la capacité d'accueil d'utilisateurs supplémentaires.
  - Étape 2 : Évaluation des options d'architecture technique
    - Option A : **Exploitation d'un système existant unique (extension du système)**
      - Description : Une organisation étend l'accès à son système existant à d'autres membres de l'ESO.
      - Exemple de cas d'utilisation : Un hôpital étend l'accès à son DME à une équipe de santé familiale et aux services de soins à domicile pour des patients communs inscrits à un programme de soins complexes.
    - Option B : **Acquisition d'un nouveau système partagé (achat d'une nouvelle technologie)**
      - Description : Les membres de l'ESO procèdent conjointement à l'acquisition et à la mise en œuvre d'un nouveau système destiné à un usage partagé.
      - Exemple de cas d'utilisation : L'ESO acquiert une nouvelle plateforme de coordination des soins permettant la tenue de conférences de cas interorganisationnelles et l'élaboration de plans de soins partagés.
    - Option C : **Interconnexion de plusieurs systèmes existants (interopérabilité)**
      - Description : Mise en place de connexions d'échange de données entre les systèmes existants des organisations.
      - Exemple de cas d'utilisation : Le DME d'un hôpital échange des résultats de laboratoire et des sommaires de congé avec le DME d'un centre de santé communautaire et le système clinique d'un établissement de soins de longue durée au moyen d'un moteur d'intégration partagé.
- Activités :
  - Mobiliser le ou la responsable du numérique de la région de Santé Ontario afin d'assurer l'alignement avec les priorités de Santé Ontario
  - Mobiliser les responsables des TI de chaque organisation dans le cadre des séances de conception de l'architecture
  - Tenir des démonstrations de fournisseurs pour les options de nouveaux systèmes (le cas échéant)
  - Élaborer les exigences d'intégration et procéder à une évaluation de faisabilité
  - Analyser le coût total d'acquisition pour chaque option (projection sur cinq ans)
  - Mettre à l'essai une preuve de concept technique pour l'approche privilégiée

- Livrable : **Recommandation relative à l'architecture technique** comprenant un échéancier de mise en œuvre, un budget et une évaluation des risques.

2.2 Rôles et responsabilités organisationnels

- Objectif : Définir clairement et attribuer les rôles organisationnels applicables au dispositif de partage des données.
- Rôles — Tout dispositif de partage des données au sein d'une ESO peut comporter les rôles suivants :
  1) **Organisations membres**
     - Description : Toutes les organisations membres de l'ESO participant au dispositif de partage des données. Elles sont dépositaires de leurs données et en assument la responsabilité principale. Elles peuvent notamment inclure :
       - Dépositaires de renseignements sur la santé (DRS) : hôpitaux, établissements de soins de longue durée, centres de santé communautaires, équipes de santé familiale, etc.
       - Organisations non dépositaires de renseignements personnels sur la santé : organismes communautaires, fournisseurs de logements, organismes de services sociaux, etc.
     - Distinction importante :
       - Les DRS sont assujettis à la LPRPS et ont des obligations légales spécifiques ;
       - Les organisations non dépositaires ont des obligations limitées en vertu de la LPRPS, mais doivent respecter des obligations équivalentes ;
       - Les DRS et les organisations non dépositaires ont tous l'obligation d'exercer une surveillance à l'égard des fournisseurs de réseaux d'information sur la santé (FRIS).
     - Responsabilités des organisations membres : Chaque organisation membre demeure responsable de ses propres obligations en matière de protection de la vie privée, même lorsqu'elle a recours à un membre gestionnaire et à un FRIS.
  2) **Fournisseur de réseau d'information sur la santé (FRIS)**
     - Définition : Le FRIS est défini en lien avec les dépositaires de renseignements sur la santé visés par la LPRPS qui détiennent et exploitent l'infrastructure technique permettant le partage des données.
     - Qui peut agir à titre de FRIS :
       - Option A : **Organisation membre de l'ESO**
         - Une organisation membre de l'ESO détient, héberge et exploite directement l'infrastructure technologique ;
         - Le service des TI de l'organisation gère les serveurs, la sécurité, l'accès des utilisateurs et le soutien technique ;
         - Cette organisation membre est le FRIS au sens de la LPRPS.
       - Option B : **Fournisseur externe**
         - Un fournisseur externe (ex. : fournisseur de logiciels infonuagiques, fournisseur de services gérés) exploite l'infrastructure technologique en vertu d'un contrat ;
         - Le fournisseur offre un service aux organisations membres de l'ESO à titre de FRIS ;
         - Exemples courants : fournisseurs de DME infonuagiques, fournisseurs de plateformes de coordination des soins, exploitants de moteurs d'intégration.
  3) **Membre gestionnaire**
     - Définition : Le membre gestionnaire est une organisation membre de l'ESO qui gère la relation avec un FRIS et qui est responsable envers l'ensemble des autres organisations membres de l'ESO de veiller à ce que le FRIS exerce ses activités efficacement et respecte les exigences en matière de protection de la vie privée, de sécurité et de prestation de services.
     - Importance de ce rôle — Lorsqu'une ESO a recours à un FRIS (qu'il s'agisse d'une organisation membre ou d'un fournisseur externe), une entité doit :

        - détenir le contrat et gérer la relation ;
        - surveiller la performance et la conformité du FRIS ;
        - s'assurer que les mesures de protection de la vie privée et de sécurité sont adéquates ;
        - agir à titre d'entité responsable envers les autres organisations membres de l'ESO.
    - Le membre gestionnaire peut assumer ce rôle.
    - Point clé : Le membre gestionnaire n'est pas le FRIS (sauf si l'organisation membre exploite également directement l'infrastructure). Il gère et supervise le FRIS pour le compte de l'ensemble des organisations membres de l'ESO.
4) **Autorité de gouvernance autochtone** (le cas échéant)
    - Définition : Lorsqu'un projet concerne des données relatives à des communautés autochtones ou à des patients membres de communautés autochtones, l'autorité de gouvernance autochtone pertinente (Première Nation, Nation métisse, organisation inuite ou organisation autochtone de santé) peut exercer un pouvoir de gouvernance quant à la collecte, à l'utilisation, au partage et à la gestion de ces données.
    - Principes de souveraineté des données autochtones — La souveraineté des données autochtones reconnaît le droit des peuples autochtones de gouverner la collecte, la protection, l'utilisation et le partage des données concernant leurs communautés et leurs membres. Elle est guidée par les principes suivants (les principes « PCAP ») :
        - Propriété, contrôle, accès et possession, ou principes « PCAP »
            - Propriété : les Premières Nations sont collectivement propriétaires de leurs connaissances culturelles, de leurs données et de leurs renseignements.
            - Contrôle : les Premières Nations ont le droit d'orienter tous les aspects de la recherche et de la gestion de l'information qui les concernent.
            - Accès : les Premières Nations doivent pouvoir accéder aux données qui les concernent et déterminer les modalités selon lesquelles d'autres peuvent y accéder.
            - Possession : le contrôle physique des données permet aux Premières Nations d'affirmer et de protéger leur propriété.
        - Inuit Qaujimajatuqangit
        - Principes de recherche éthique métisse
        - Avantage collectif, autorité de contrôle, responsabilité et éthique, ou principes « CARE », élaborés par la Global Indigenous Data Alliance afin de veiller à ce que les principes voulant que les données soient faciles à trouver, accessibles, interopérables et réutilisables, ou principes « FAIR », respectent les droits des peuples autochtones.

- Activités :
    - Déterminer qui, le cas échéant, agira à titre de FRIS et/ou de membre gestionnaire ;
    - Documenter les responsabilités et les obligations spécifiques associées à chaque rôle ;
    - Confirmer la compréhension et l'acceptation, par chaque organisation participante, du rôle qui lui est attribué.
- Livrable : **Matrice d'attribution des rôles** comprenant les engagements organisationnels.

2.3 Élaboration du cadre juridique

- Objectif : Mettre en place des ententes juridiquement conformes régissant le partage des données et assurant la protection de l'ensemble des parties.
- Ententes à envisager :
    - Entre les membres — Entente de partage des données (EPD) visant à établir :
        - les participants au partage ;
        - les rôles (ex. : FRIS, membre gestionnaire) ;
        - les finalités du partage et la portée des services ;

        - les utilisations permises et les obligations des parties.
    - Avec le FRIS (le cas échéant) — Entente de services portant sur l'infrastructure technique :
        - annexes relatives à la protection de la vie privée et à la sécurité ;
        - clauses de responsabilité et d'indemnisation ;
        - dispositions relatives à la résiliation et à la portabilité des données.
- Activités :
    - Mobiliser les conseillers juridiques et responsables de la protection de la vie privée des organisations participantes ;
    - Rédiger des modèles d'ententes conformes aux exigences de la LPRPS ;
    - Déterminer les modifications requises aux règlements administratifs ou aux politiques existantes.
- Livrable : **Entente juridique appropriée** encadrant le partage des données.

Phase 3: Évaluation des risques

3.1 Identification exhaustive des risques

- Objectif : Recenser et documenter l'ensemble des risques significatifs associés tant à la mise en œuvre qu'à l'absence de mise en œuvre de l'entente de partage de données.
- Éléments à considérer :
    - Risques liés à la mise en place d'un nouveau partage de données :
        - non-respect de certaines exigences précises de la LPRPS ;
        - non-conformité aux dix principes relatifs aux pratiques équitables en matière d'information ;
        - non-respect des principes de souveraineté des données autochtones, pouvant entraîner des préjudices pour les communautés autochtones, une perte de confiance ou une utilisation inappropriée des données autochtones ;
        - scénarios prévisibles d'atteintes à la vie privée ;
        - risques liés à la qualité et à la disponibilité des données ;
        - interruptions de service ou défaillances techniques ;
        - ambiguïté des rôles et responsabilités.
    - Risques liés à l'absence de partage des données :
        - occasions manquées d'intervention précoce ;
        - incidents liés à la sécurité des patients découlant d'une information incomplète ;
        - dédoublement inutile d'examens ou de procédures ;
        - retards dans la prestation des soins et expérience patient insatisfaisante ;
        - perpétuation de soins fragmentés pour les patients autochtones, qui peuvent déjà être confrontés à des obstacles systémiques à l'accès à des services intégrés et culturellement sécuritaires ;
        - inadéquation avec les attentes en matière de soins intégrés.
- Activités :
    - Tenir des ateliers d'identification des risques réunissant des parties prenantes des domaines de la protection de la vie privée, du droit, des technologies de l'information et du milieu clinique ;
    - Examiner des projets comparables de partage de données afin d'en tirer des leçons.
- Livrable : **Registre des risques** comprenant une évaluation de la probabilité et de l'impact pour les scénarios de partage et de non-partage des données.

3.2 Planification du traitement des risques / des mesures d'atténuation

- Objectif : Élaborer des stratégies complètes pour traiter les risques identifiés au moyen de mesures de traitement appropriées
- Éléments à considérer
  - Examiner les options de traitement des risques (éviter, atténuer, transférer, accepter) et élaborer un plan comprenant notamment les éléments suivants :
    - Clauses d'indemnisation et autres dispositions prévues aux ententes juridiques
    - Assurance
    - Plan de formation et de communication
    - Plan de supervision du FRIS/fournisseur
    - Protocole d'intervention en cas d'incident
    - Communications destinées aux clients/patients (ex. : formulaires de consentement, décharge de responsabilité)
- Activités :
  - Évaluer les options de traitement pour chaque risque figurant au registre des risques
  - Attribuer les responsabilités liées à la mise en œuvre et au suivi de chaque mesure de contrôle
  - Documenter la justification des risques qui seront acceptés
  - Consulter les courtiers en assurance quant à l'adéquation de la couverture d'assurance
- Livrable : **Plan de traitement et d'atténuation des risques** précisant les mesures de contrôle et les responsabilités associées

3.3 Mise en place d'assurances additionnelles appropriées

- Objectif : Valider les mesures d'atténuation des risques prévues et cerner toute lacune au moyen d'une évaluation objective
- Options :
  - Évaluation des facteurs relatifs à la vie privée (EFVP)
  - Évaluation générale de la sécurité / des menaces et des risques
  - Évaluations de sécurité spécialisées
  - Réalisées à l'interne ou par un tiers
- Fondements de l'évaluation :
  - Entente de partage des données
  - Entente avec le FRIS / fournisseur
  - Registre des risques
  - Plan de traitement et d'atténuation des risques
  - Politiques et procédures opérationnelles
- Activités :
  - Déterminer le type et la portée appropriés de l'évaluation en fonction du profil de risque, en s'appuyant sur les structures de gouvernance existantes et les autres comités, ainsi que sur la consultation d'experts en la matière
  - Retenir les services d'évaluateurs qualifiés, internes ou externes
  - Réaliser l'évaluation et documenter les constats
  - Prendre connaissance des résultats de l'évaluation et documenter la réponse organisationnelle
- Livrable : **Rapport(s) d'évaluation** faisant état des lacunes relevées, accompagné(s) d'une documentation précisant les responsabilités liées à la correction des lacunes et des faiblesses identifiées

Phase 4: Mise en œuvre

4.1 Mobilisation des parties prenantes et respect de la souveraineté des données autochtones

- Objectif : Susciter l'adhésion et répondre aux préoccupations de l'ensemble des parties prenantes afin d'assurer une mise en œuvre harmonieuse
- Principales parties prenantes :
  - **Personnel clinique**
    - Comprendre les changements aux flux de travail et les gains d'efficience
    - Répondre aux préoccupations liées à l'ajout de tâches de documentation ou à l'accès aux systèmes
    - Mettre en évidence les améliorations en matière de sécurité des patients et de qualité des soins
    - Mobiliser des personnes championnes dans la conception et les essais
  - **Réseaux de soins primaires (RSP) et gestionnaires de cabinets de soins primaires**
    - Les RSP devraient être impliqués dans la conception des flux de travail liés à l'inscription, aux processus de consentement et à l'acheminement de l'information
    - Les gestionnaires de cabinets au sein des RSP sont souvent responsables de la gestion des accès aux systèmes, de l'impression des rapports et du classement des documents
    - Peuvent faire face à une charge de travail accrue lors de la mise en œuvre en l'absence de ressources additionnelles
    - Ont besoin de processus clairs pour la gestion des nouveaux flux d'information
    - Nécessitent une formation sur les nouveaux systèmes, tout en disposant souvent de peu de temps hors du comptoir d'accueil
  - **Personnel responsable de la protection de la vie privée et de la gestion de l'information**
    - Répondre aux préoccupations au moyen de mécanismes de contrôle robustes
    - Reconnaître l'augmentation de la charge de travail pendant la phase de mise en œuvre
  - **Personnel des technologies de l'information et équipes techniques**
    - Évaluer la capacité organisationnelle et les besoins en ressources
    - Être impliqués dans la planification de l'intégration avec les fournisseurs
    - Planifier le soutien et la maintenance continus
    - Répondre aux préoccupations liées à la complexité des systèmes
  - **Patients, familles et proches aidants**
    - Communiquer les bénéfices des soins intégrés
    - Expliquer le partage des données et les mesures de protection de la vie privée
    - Offrir, lorsque pertinent, des mécanismes de retrait (« option de retrait »)
    - Recueillir des rétroactions sur l'expérience vécue
  - **Communautés et leadership autochtones**
    - Engager une collaboration précoce et significative, non pas à titre de simple consultation, mais comme un véritable partenariat
    - Respecter les processus de gouvernance et les échéanciers autochtones (qui peuvent différer des échéanciers institutionnels)
    - Reconnaître les préjudices historiques et la méfiance actuelle à l'égard des systèmes de données en santé
- Activités :
  - Mobiliser la direction de l'ESO ainsi que le personnel technique au sein d'un comité de planification, en tirant parti, dans la mesure du possible, des structures de gouvernance et des comités existants
  - Élaborer et mettre à l'essai le plan
- Livrable : **Plan de gestion du changement** comprenant un calendrier de communications et des activités d'engagement des parties prenantes

4.2 Programme de formation et de développement des compétences

- Objectif : Rassurer les dépositaires de renseignements sur la santé (DRS) quant au fait que le personnel (y compris celui des organisations non dépositaires sans supervision directe) possède les compétences nécessaires pour traiter adéquatement les renseignements personnels sur la santé
- Exemple de programme de formation :
  - Module 1 : Fondements de la protection de la vie privée (tout le personnel)
  - Module 2 : Partage des données dans un contexte de soins intégrés (tout le personnel)
  - Module 3 : Formation propre aux systèmes (utilisateurs finaux)
  - Module 4 : Protection de la vie privée et sécurité pour le personnel des organisations non dépositaires (organisations non DRS)
  - Module 5 : Protection avancée de la vie privée pour les gestionnaires et responsables (leadership)
- Considérations :
  - **Modalités de prestation de la formation**
    - Approche hybride : apprentissage en ligne pour les contenus de base, formation en présentiel pour l'utilisation des systèmes
    - Achèvement obligatoire de la formation avant l'octroi des accès aux systèmes
    - Évaluation des compétences (questionnaire ou mises en situation)
    - Exigence de formation de mise à jour annuelle
    - Ressources à la demande et aide-mémoire opérationnels
  - **Contraintes propres aux cabinets de soins primaires**
    - Les médecins et infirmières ont difficilement la possibilité de s'absenter de leur pratique pour des formations d'une demi-journée
    - Le roulement du personnel administratif peut être élevé, ce qui nécessite une capacité de formation continue
    - Les cabinets présentent des niveaux très variables de maîtrise des dossiers médicaux électroniques, allant d'utilisateurs très avancés à des utilisateurs de base
    - La plupart des cabinets de soins primaires ne disposent pas de personnel TI sur place
  - **Garanties de compétence pour le personnel non DRS**
    - Test de compétence préalable à l'octroi de l'accès, avec note de passage minimale
    - Observation et validation par un superviseur lors des premières utilisations
    - Surveillance accrue durant les 90 premiers jours (revues des journaux d'accès)
    - Mesures correctives immédiates en cas d'incident de confidentialité
  - **Dossiers de formation et suivi de la conformité**
    - Registre de formation centralisé ou registres tenus par les organisations membres
    - Suivi des taux de complétion et analyses liées à la formation
    - Plan pour le traitement des cas de non-complétion
- Activités :
  - Élaborer le matériel de formation pour chacun des modules
  - Créer les outils d'évaluation des compétences et définir les critères de réussite
  - Mettre en place la plateforme de diffusion de la formation (système de gestion de l'apprentissage)
  - Planifier les séances de formation pour l'ensemble du personnel avant la mise en production
  - Établir un système de suivi de la complétion et de conservation des dossiers
- Livrable : **Programme de formation**, plan de déploiement et outils d'évaluation des compétences

Phase 5: Mise en production

5.1 Mise en œuvre du projet pilote

- Objectif : Tester le système de partage de données dans un environnement contrôlé afin de valider les fonctionnalités, les flux de travail et les mécanismes de contrôle avant le déploiement complet.
- Approche pilote
  - Sélection de 1 à 2 sites représentant différents types d'organisations (ex. : un DRS et un organisme non-DRS)
  - Portée limitée (programme précis ou population de patients ciblée)
  - Soutien et surveillance intensifs
  - Collecte structurée de rétroaction
- Critères de réussite du projet pilote
  - Le système fonctionne conformément aux exigences
  - L'intégration aux flux de travail permet des gains de temps ou des améliorations de la qualité
  - Les mesures de protection de la vie privée et de sécurité fonctionnent efficacement
  - Le personnel démontre sa compétence et sa satisfaction
  - Aucun incident majeur ni atteinte à la vie privée
  - La rétroaction des patients est positive
- Activités
  - Rencontres quotidiennes (« caucus ») durant la première semaine
  - Réunions hebdomadaires du groupe de travail
  - Suivi et résolution des enjeux en temps réel
  - Audit des journaux d'accès et des modes d'utilisation
  - Collecte de rétroaction qualitative auprès du personnel et des patients
  - Ajustement des outils de formation et de soutien
- Décision de déploiement : Décision de poursuite/arrêt prise par le comité directeur à la suite de l'examen des résultats du projet pilote, avant le déploiement élargi.
- Livrable : **Rapport d'évaluation du projet pilote** comprenant des recommandations.

5.2 Déploiement complet

- Objectif : Déployer le système de partage de données auprès de l'ensemble des organisations participantes de façon contrôlée et progressive.
- Approche de déploiement par organisation
  - Séquençage fondé sur le niveau de préparation, la complexité et les priorités stratégiques
  - Intervalle minimal de deux semaines entre le déploiement dans chaque organisation
  - Maintien du soutien au site pilote pendant le déploiement
- Liste de vérification de l'état de préparation au déploiement (par organisation)
  - Ententes juridiques signées
  - Infrastructure technique testée et validée
  - Ensemble du personnel ayant complété la formation requise
  - Mesures de protection de la vie privée et de sécurité en place
  - Flux de travail documentés et communiqués
  - Exigences en matière de gouvernance des données autochtones respectées (le cas échéant), y compris tout protocole propre à la communauté et les processus d'approbation requis
  - Ressources de soutien identifiées et disponibles
  - Communications de mise en production transmises au personnel et aux patients
  - Plan de retour en arrière préparé
- Soutien lors de la mise en production

- Super-utilisateurs sur place pendant la première semaine
  - Heures prolongées du service d'assistance
  - Breffages quotidiens à la haute direction
  - Processus d'escalade des enjeux en temps réel
  - Célébration et reconnaissance des jalons atteints
- Activités :
  - Confirmer l'état de préparation de chaque organisation à l'aide de la liste de vérification
  - Réaliser les activités de mise en production conformément au calendrier de déploiement
  - Surveiller la performance du système et l'expérience des utilisateurs durant les premières semaines
  - Offrir un soutien intensif et résoudre rapidement les enjeux
  - Documenter les leçons apprises et ajuster l'approche pour les organisations subséquentes
- Livrable : **Calendrier de déploiement** et plan de soutien à la mise en production

Conclusion

Cette feuille de route constitue un cadre adaptable et non une prescription rigide. Le contexte de chaque équipe Santé Ontario (ESO) est unique. Les présentes phases et outils doivent être utilisés comme point de départ et adaptés aux besoins cliniques propres à chaque situation, aux relations organisationnelles en place, à l'environnement technologique, ainsi qu'aux ressources disponibles.

Facteurs clés de réussite :

1. Équilibrer les perspectives de risque : Mettre en balance les risques liés au partage des données avec ceux découlant de soins fragmentés.
2. [illegible]es relations : Les ententes juridiques sont nécessaires, mais la confiance et une communication soutenue sont essentielles.
3. Concevoir dans une optique de durabilité : S'assurer que les rôles de fournisseur de réseau d'information sur la santé (FRIS) et d'agent sont viables à long terme.
4. Prioriser la formation : Un personnel compétent constitue la meilleure protection de la vie privée.
5. Commencer de façon ciblée : Procéder à un projet pilote à portée limitée avant d'élargir le déploiement.
6. Surveiller et ajuster : Utiliser les données pour soutenir une amélioration continue.
7. Respecter la souveraineté des données autochtones : Lorsque des communautés autochtones sont concernées, reconnaître leur droit inhérent de gouverner les données concernant leurs peuples et veiller à établir un véritable partenariat et non une simple consultation.

En définitive, le succès repose non seulement sur la technologie, mais sur l'action concertée des personnes et des structures de gouvernance, travaillant ensemble pour permettre des soins intégrés qui améliorent les résultats pour les patients et leurs familles au sein de l'ESO.

Rappel important de BLG : La présente feuille de route vise à faciliter les discussions internes et la prise de décision. Elle ne constitue pas un avis juridique. Les organisations sont invitées à consulter des conseillers juridiques et des experts en protection de la vie privée qualifiés lors de la planification d'un projet de partage de données. Les facteurs pertinents peuvent varier selon le contexte propre à chaque organisation, les modalités envisagées et l'évolution des orientations réglementaires.