Cadre décisionnel relatif aux « rôles » en matière de partage des données
[outil 4 complémentant le modèle d'entente de partage de données élaboré par BLG]

Le présent document vise à aider les membres des ESO à évaluer leur degré de préparation organisationnelle et à examiner les principaux facteurs à considérer avant d'accepter d'agir à titre de mandataire pour d'autres dépositaires de renseignements sur la santé ou à titre de fournisseur de réseau d'information sur la santé (FRIS) en vertu de la LPRPS. Il ne s'agit pas d'une liste d'exigences obligatoires, mais d'un outil conçu pour orienter et éclairer la réflexion.

Instructions: Cliquez sur l'un des liens ci-dessous pour accéder à la section qui correspond le mieux à votre besoin, ou faites défiler l'ensemble du document pour consulter les trois rôles et les principaux points de décision. Des notes relatives au présent artefact provenant de BLG et de RISE, ainsi qu'une citation proposée, figurent dans un encadré à la fin du document.

Le présent document comprend quatre sections :

1. Rôle de mandataire

Un mandataire fournit des services ou exerce des fonctions pour le compte d'un dépositaire de renseignements sur la santé (DRS), lesquels impliquent la collecte, l'utilisation, la communication ou la destruction de renseignements personnels sur la santé (RPS). Le mandataire assume des obligations prévues par la loi et le dépositaire demeure juridiquement responsable des actes du mandataire.

Évaluation de la capacité organisationnelle

- Clarté de la définition des services : Pouvons-nous définir avec précision les services que nous fournirions et les RPS auxquels nous devrions accéder ? Les limites sont-elles claires et gérables ?
- Infrastructure de sécurité : Disposons-nous de mesures de sécurité physique appropriées, de contrôles de sécurité des TI et de protocoles de confidentialité permettant de protéger les RPS selon des normes équivalentes à celles des dépositaires ?
- Expertise en sécurité des TI : Avons-nous accès à une expertise en sécurité des TI pour mettre en place les contrôles requis et répondre aux questions s'y rapportant ?
- Capacité de formation du personnel : Pouvons-nous offrir une formation complète sur la LPRPS à tout le personnel concerné ? Avons-nous les ressources nécessaires pour maintenir une sensibilisation et une conformité continues ?
- Expertise en protection de la vie privée : Avons-nous accès à une expertise en matière de protection de la vie privée pour répondre aux questions courantes, élaborer des politiques et gérer les incidents ?
- Contrôles opérationnels : Avons-nous des processus de contrôle des accès, de journalisation des audits, de destruction sécurisée et de gestion des atteintes qui satisfont aux exigences de la LPRPS ?
- Assurance de la qualité : Avons-nous des mécanismes de contrôle de la qualité pour garantir que les services sont fournis avec exactitude et fiabilité, sans compromettre l'intégrité des données ?

Considérations relatives à la relation et à l'entente

- Attentes des dépositaires : Avons-nous clairement discuté avec le ou les dépositaire(s) de ce qu'ils attendent de nous ? Ces attentes sont-elles réalistes et compatibles avec nos capacités ? Serons-nous mis en situation de réussir ?
- Modalités de l'entente : Sommes-nous à l'aise avec les modalités proposées de l'entente de mandataire, notamment la portée, la répartition des responsabilités, les droits d'audit, les dispositions relatives à la résiliation et à l'indemnisation ?
- Plusieurs dépositaires : Si nous agissons comme mandataire pour plusieurs dépositaires, est-il clair de qui nous recevrons nos directives ? Existe-t-il un risque de conflits et, le cas échéant, comment seront-ils résolus ?
- Surveillance et reddition de comptes : Sommes-nous prêts à faire l'objet d'audits de la part des dépositaires ? Pouvons-nous fournir les rapports et la transparence qu'ils exigent ?

Considérations d'affaires et stratégiques
- Proposition de valeur : L'exercice de ce rôle de mandataire crée-t-il une valeur pour notre organisation et pour l'ESO ? Contribuera-t-il à l'amélioration des soins aux patients ou de l'efficience opérationnelle ?
- Affectation des ressources : Avons-nous le temps et les ressources humaines nécessaires pour assumer ces responsabilités sans compromettre nos fonctions principales ?
- Viabilité à long terme : S'agit-il d'un projet ponctuel ou d'une relation continue ? Souhaitons-nous exercer ce rôle à long terme ?

Évaluation des risques et de la responsabilité
- Exposition en cas d'atteinte : Quelles seraient les répercussions sur notre réputation et nos relations en cas d'atteinte à la vie privée impliquant des RPS que nous traitons à titre de mandataire ?
- Limites de responsabilité : L'entente de mandataire limite-t-elle adéquatement notre responsabilité ? Disposons-nous d'une assurance couvrant nos activités à titre de mandataire ?
- Risque réglementaire : Sommes-nous à l'aise avec la possibilité de plaintes ou d'enquêtes du Commissaire à l'information à la protection de la vie privée (CIPVP) découlant de nos activités de mandataire, même si le dépositaire demeure ultimement responsable ?
- Planification de la résiliation : Si la relation de mandat prend fin, disposons-nous de plans pour le retour sécurisé ou la destruction des RPS ? Existe-t-il un processus de sortie clair ?

2. Rôle de fournisseur de réseau d'information sur la santé (FRIS)

Un FRIS exploite une infrastructure permettant aux dépositaires de renseignements sur la santé (DRS) de partager des renseignements personnels sur la santé (RPS) aux fins de la prestation de soins de santé ou de l'aide à la prestation de soins de santé.

En permettant le partage sécurisé des RPS entre les membres des ESO, un FRIS peut soutenir des soins intégrés et contribuer à l'amélioration des résultats pour les patients et leurs familles à l'échelle d'une ESO. Pour cette raison, il peut être approprié qu'un membre de l'ESO disposant d'une capacité suffisante accepte d'assumer le rôle de FRIS.

Évaluation de la capacité organisationnelle
- Infrastructure technique : Disposons-nous, ou pouvons-nous acquérir, des systèmes de TI robustes et sécurisés capables de traiter de grands volumes de données de santé sensibles, avec des mécanismes appropriés de chiffrement, de redondance et de reprise après sinistre ?

- Ressources financières : Pouvons-nous financer de manière durable les coûts initiaux de mise en place (juridiques, techniques, évaluation des facteurs relatifs à la vie privée) ainsi que les dépenses opérationnelles continues (maintenance, mises à jour de sécurité, audits, personnel) liées à l'infrastructure du réseau ?
- Expertise et dotation en personnel : Avons-nous, ou pouvons-nous recruter, du personnel possédant une expertise en informatique de la santé, en droit de la protection de la vie privée, en sécurité de l'information, en administration de réseaux et en conformité à la LPRPS ?
- Structure de gouvernance : Disposons-nous de structures de gouvernance appropriées pour superviser les activités de FRIS, notamment une surveillance par le conseil d'administration, la désignation d'un responsable de la protection de la vie privée et des cadres de reddition de comptes ?
- Gestion de la responsabilité : Avons-nous évalué notre exposition aux risques de responsabilité en cas d'atteinte à la vie privée, de défaillance des systèmes ou de problèmes liés à la qualité des données ? Avons-nous une couverture d'assurance adéquate ?
- Historique de conformité : Avons-nous des antécédents démontrés de conformité aux lois sur la protection de la vie privée et de solides pratiques en matière de sécurité de l'information ?

Considérations relatives à l'alignement stratégique et à la valeur

- Alignement avec la mission : L'exercice du rôle de FRIS est-il conforme à la mission et aux objectifs stratégiques de notre organisation ? Contribuera-t-il à l'avancement des objectifs de coordination des soins pour notre population ?
- Évaluation des besoins : Existe-t-il un besoin clair et démontré pour l'infrastructure de réseau que nous fournirions ? Avons-nous validé la demande auprès des dépositaires susceptibles d'y participer ?
- Analyse des solutions de rechange : Avons-nous examiné si des FRIS existants ou d'autres mécanismes de partage de l'information pourraient répondre plus efficacement aux besoins de l'ESO ?
- Environnement concurrentiel : Comprenons-nous qui d'autre offre des services similaires ? Qu'est-ce qui distinguerait notre offre potentielle ?
- Plan de viabilité : Disposons-nous d'un modèle financier viable à long terme ? Le réseau sera-t-il autosuffisant ou nécessitera-t-il des subventions continues ?

Facteurs relationnels et de collaboration

- Confiance et crédibilité : Avons-nous des relations solides et empreintes de confiance avec les DRS et les membres qui participeraient ? Sommes-nous perçus comme un partenaire neutre et fiable ?
- Adhésion des parties prenantes : Avons-nous obtenu l'engagement des principales parties prenantes, notamment les dépositaires, les cadres supérieurs, les conseils d'administration et les leaders cliniques ? Existe-t-il un consensus quant aux objectifs communs ?
- Pouvoir décisionnel : Les modalités de prise de décision en matière de gouvernance du réseau sont-elles claires ? Les membres participants disposent-ils d'une participation appropriée tout en nous permettant de conserver le contrôle opérationnel ?

Évaluation des risques

- Conséquences d'une atteinte : Avons-nous évalué les conséquences réputationnelles, financières et juridiques en cas d'atteinte majeure à la vie privée ou de défaillance du système sous notre responsabilité ?
- Surveillance réglementaire : Sommes-nous prêts à faire face à d'éventuelles enquêtes du CIPVP si des plaintes sont formulées concernant les activités du réseau ?
- Glissement de portée : Avons-nous des limites claires quant à ce que le réseau fera ou ne fera pas ? Pouvons-nous résister aux pressions visant à étendre la portée au-delà de nos capacités ?
- Stratégie de sortie : Si nous devions mettre fin aux services de FRIS, disposons-nous d'un plan pour la migration des données, la continuité des services et une cessation ordonnée ?

3. Rôle de membre gestionnaire

Un membre gestionnaire supervise une organisation externe (par exemple, un fournisseur de services infonuagiques) qui agit à titre de FRIS pour les membres d'une ESO. Le membre gestionnaire fournit des services de diligence raisonnable et de surveillance pour le compte des autres membres, lesquels demeurent juridiquement responsables des actes du FRIS.

Évaluation de la capacité organisationnelle

- Expertise en matière de surveillance : Disposons-nous, ou pouvons-nous accéder, à une expertise en gestion de fournisseurs, en évaluation technologique et en sécurité des TI, en audit de la protection de la vie privée et en conformité à la LPRPS afin de superviser efficacement un FRIS externe ?
- Capacité de diligence raisonnable : Pouvons-nous effectuer une diligence raisonnable initiale approfondie des candidats au rôle de FRIS, y compris des évaluations techniques, des audits de sécurité, des examens de la stabilité financière et des vérifications de références ?
- Compétences en négociation contractuelle : Disposons-nous d'une expertise juridique et en approvisionnement pour négocier des modalités favorables protégeant les intérêts des membres et assurant la conformité à la LPRPS ?
- Ressources pour la surveillance continue : Pouvons-nous consacrer le temps et les ressources nécessaires à la surveillance continue du rendement, de la conformité et des niveaux de service du FRIS ?
- Préparation à la gestion des incidents : Sommes-nous en mesure de coordonner, pour le compte des membres, la gestion des atteintes à la vie privée, des interruptions de service et des autres incidents impliquant le FRIS externe ?

Considérations relatives à l'autorité et à la gouvernance

- Mandat clair : Les autres membres nous ont-ils accordé un mandat clair pour agir en leur nom dans la sélection, la conclusion de contrats avec le FRIS externe et la supervision de celui-ci ?
- Cadre décisionnel : Existe-t-il un cadre clair quant à la manière dont les décisions concernant le FRIS seront prises ? Dans quels cas disposons-nous d'une autonomie décisionnelle et dans quels cas devons-nous consulter les membres ?
- Structure de responsabilité : Les membres comprennent-ils qu'ils demeurent responsables en vertu de la LPRPS, même si nous assurons la surveillance ? Les membres sont-ils clairs quant à leurs obligations continues ?
- Relations de reddition de comptes : Avons-nous mis en place des mécanismes clairs de reddition de comptes afin de tenir les membres informés du rendement du FRIS, des enjeux de conformité et des risques ?
- Processus de résolution des différends : Existe-t-il un processus pour résoudre les désaccords entre nous et les autres membres concernant la supervision du FRIS ou des enjeux de rendement ?
- Mobilisation des membres : Sommes-nous en mesure de mobiliser efficacement des membres diversifiés (hôpitaux, médecins, services communautaires) présentant des niveaux variables de sophistication technique et en matière de protection de la vie privée ?

Sélection et gestion des fournisseurs

- Critères de sélection : Avons-nous élaboré des critères exhaustifs pour évaluer les fournisseurs FRIS potentiels, notamment en matière de capacité technique, de sécurité, de conformité à la protection de la vie privée, de stabilité financière et d'expérience ?
- Connaissance du marché : Comprenons-nous le marché des services de FRIS, y compris les fournisseurs disponibles, les modèles de tarification courants et les normes de l'industrie ?

- Modalités contractuelles : Pouvons-nous nous assurer que les contrats comprennent des dispositions appropriées relatives à la conformité à la LPRPS, aux droits d'audit, à la notification des atteintes, aux niveaux de service, à la responsabilité, à la résiliation ainsi qu'au retour ou à la destruction des données ?
- Suivi du rendement : Avons-nous établi des indicateurs clés de rendement et des ententes sur les niveaux de service que nous pouvons réalistement surveiller et faire respecter ?
- Droits d'audit et mise en œuvre : Sommes-nous en mesure d'exercer efficacement les droits d'audit, directement ou par l'entremise de tiers qualifiés, afin de vérifier la conformité du FRIS ?
- Gestion de la relation : Pouvons-nous maintenir une relation de travail efficace avec le fournisseur FRIS qui soit à la fois collaborative et dûment à distance ?

Surveillance de la conformité et des risques

- Expertise en LPRPS : Avons-nous une compréhension suffisante des exigences de la LPRPS applicables aux FRIS afin de cerner les lacunes en matière de conformité et de tenir le fournisseur responsable ?
- Examen des évaluations des facteurs relatifs à la vie privée (EFVP) : Sommes-nous en mesure d'examiner et d'évaluer la pertinence des EFVP réalisées par le FRIS externe ou pour son compte ?
- Coordination de la réponse aux atteintes : Sommes-nous prêts à coordonner, pour le compte des membres, la réponse aux atteintes à la vie privée ou aux incidents de sécurité impliquant le FRIS externe, y compris les décisions relatives à la notification au CIPVP ?
- Évaluation et communication des risques : Pouvons-nous cerner, évaluer et communiquer en temps opportun aux membres les risques posés par le FRIS externe, de manière claire et exploitable ?

Considérations financières et d'affaires

- Structure des coûts : Avons-nous établi un modèle équitable et durable pour le recouvrement de nos coûts de surveillance ?
- Proposition de valeur : La surveillance que nous assurons apporte-t-elle une valeur suffisante pour justifier les coûts, comparativement au fait que les membres effectuent leur propre diligence raisonnable ?
- Capacité d'évolution : Si des membres additionnels souhaitent adhérer ou si les besoins des membres existants augmentent, sommes-nous en mesure d'adapter notre surveillance en conséquence ?

Considérations relatives à la responsabilité et à l'assurance

- Exposition à la responsabilité : Quelle est notre responsabilité potentielle en cas de défaillance du FRIS externe ? Sommes-nous adéquatement assurés ?
- Répartition des risques : La répartition des risques entre nous et les membres est-elle équitable et appropriée?
- Norme de diligence : Comprenons-nous la norme de diligence applicable à notre rôle de surveillance ? Avons-nous documenté notre méthodologie de surveillance et notre diligence ?

4. Principaux points de décision

Avant de s'engager dans quelque rôle que ce soit, la direction devrait s'assurer que :

- le conseil d'administration et la haute direction ont examiné la présente évaluation et appuient la décision ;
- un conseiller juridique possédant une expertise en LPRPS a examiné les ententes proposées et formulé des conseils ;
- le responsable de la protection de la vie privée ou le leader en la matière a évalué le degré de préparation et cerné les lacunes en matière de conformité ;
- la direction des TI et de la sécurité confirme la capacité technique ou dispose d'un plan pour l'atteindre (pour les rôles de FRIS et de mandataire) ;
- le responsable des finances a confirmé la viabilité des investissements requis et des coûts récurrents ;
- le responsable de la gestion des risques a évalué l'exposition à la responsabilité et confirmé que la couverture d'assurance est adéquate ;
- les autres membres de l'ESO comprennent et appuient le rôle proposé (en particulier pour le rôle de membre gestionnaire) ;
- un plan de mise en œuvre comportant des jalons clairs et des mécanismes de reddition de comptes a été élaboré ;
- il existe un consensus clair selon lequel l'exercice du rôle est conforme à la mission et à la capacité organisationnelles ; et
- le processus décisionnel et sa justification ont été documentés à des fins de référence ultérieure.

Citation proposée : BLG et RISE. Cadre décisionnel relatif aux « rôles » en matière de partage des données [outil 4 complétant le modèle d'entente de partage de données élaboré par BLG]. Hamilton : McMaster Health Forum, 2026 (sous licence de BLG).
Note de BLG et de RISE : Le présent outil doit être lu conjointement avec la note RISE suivante, laquelle fournit des liens vers le modèle d'entente de partage de données (EPD) ainsi que vers les trois autres outils de la série : Lavis JN, Moat KA, Wood B, Black L. Note RISE 37 : Soutenir le partage de données au sein des ESO grâce à un modèle d'entente et quatre outils. Hamilton : McMaster Health Forum, 2026.
Note de BLG : Les renseignements contenus dans le présent document sont de nature générale et ne constituent pas un avis juridique, un exposé exhaustif du droit ni une opinion sur quelque sujet que ce soit. Nul ne devrait agir ou s'abstenir d'agir sur la base de ces renseignements sans procéder à un examen approfondi du droit applicable à la lumière des faits propres à une situation donnée. Il est fortement recommandé de consulter un conseiller juridique pour toute question ou préoccupation particulière.
Note de RISE : RISE prépare à la fois ses propres ressources (telles que la note RISE qui présente le présent outil et les autres outils de l'EPD) afin de soutenir l'apprentissage rapide et l'amélioration continue, et offre également une « voie d'accès » structurée aux ressources préparées par d'autres partenaires et par le ministère. RISE est soutenue par une subvention du ministère de la Santé de l'Ontario versée au McMaster Health Forum. Les opinions, résultats et conclusions exprimés sont ceux de RISE et sont indépendants du ministère et de Santé Ontario. Aucune approbation par le ministère ou par Santé Ontario n'est voulue ni ne doit être inférée.