

Ententes d'échange de renseignements personnels entre gouvernements

Lignes directrices sur les pratiques exemplaires

TABLE DES MATIÈRES

A. Introduction	3
A1. Objet	3
A2. Structure	3
A3. Raison d'être	3
A4. Historique	3
A5. Utilisateurs prévus	4
A6. Mode d'emploi	4
A7. Sommaire des pratiques exemplaires	5
B. En quoi consistent les ententes d'échange de renseignements personnels?	8
B1. Est-il obligatoire de conclure une EERP?	8
B2. Avantages	8
B3. Catégories	8
B4. Lignes directrices provinciales sur les EERP	9
B5. EERP types	9
B6. Entrepreneurs	9
C. Six pratiques exemplaires	11
Première pratique exemplaire : Recensement des besoins et des facteurs de risque	12
1.1 En quoi consistent les renseignements personnels?	12
1.2 Êtes-vous habilité à échanger des renseignements personnels?	12
1.2.1 Habilitation	13
1.2.2 Consentement et avis	13
1.2.3 Communication obligatoire de renseignements	13
1.3 Quand la transmission s'impose	14
1.4 Justification de l'EERP	14
1.5 Évaluation préliminaire des risques	15
1.5.1 Scénarios à risque élevé	15
1.5.2 EERP de caractère délicat	15
1.5.3 Transmission internationale	16
1.5.4 Mesures de sécurité	17
1.5.5 Transmission par l'expéditeur	17

Deuxième pratique exemplaire : Examen de stratégies de substitution 18

- 2.1 Rapports sommaires 18
- 2.2 Information rendue anonyme 18
- 2.3 Données agrégées 18

Troisième pratique exemplaire : Évaluation des risques. 19

- 3.1 Exécution d'une évaluation des facteurs relatifs à la vie privée (EFVP) ... 19
- 3.2 Rapports publics et communications 19
- 3.3 Consultation des spécialistes en protection de la vie privée et sécurité et des avocats-conseils de votre organisme 19
- 3.4 Consultation du conseiller en protection de la vie privée de votre administration 19

Quatrième pratique exemplaire : Documentation de la décision 21

- 4. Consigner la décision 21

Cinquième pratique exemplaire : Établissement d'une EERP 22

- 5.1 Mode d'emploi du modèle 22
- 5.2 Organe de surveillance 22
- 5.3 Approbation officielle ou écrite de l'EERP 22
- 5.4 Dix principes 22
- 5.5 Langage clair 22
- 5.6 Modèle d'entente d'échange de renseignements personnels 23

Sixième pratique exemplaire : Contrôle et suivi 29

- 6. Surveillance et suivi 29

ANNEXES 30

- ANNEXE A : Lois sur la protection de la vie privée applicables au secteur public du Canada 30
- Annexe B : Contexte international 32
- Annexe C : Modèles d'EFVP et documents de référence 34
- Annexe D : Autorités responsables de la protection de la vie privée au Canada 35
- Annexe E : Risques d'entrave à la vie privée 36

A. Introduction

A1. Objet

Il incombe aux administrations publiques de protéger les renseignements personnels dont ils ont la garde et dont ils sont responsables.

Les présentes lignes directrices (les « lignes directrices ») énoncent les pratiques exemplaires en matière d'ententes d'échange de renseignements personnels (EERP) entre gouvernements au Canada.

A2. Structure

Les lignes directrices énumèrent six pratiques exemplaires d'importance qui constituent les étapes du processus décisionnel, allant du recensement des besoins à la surveillance des ententes.

A3. Raison d'être

À l'instar de la plupart des économies de la planète, l'économie canadienne dépend de plus en plus du transfert international d'information, appelé « flux de données transfrontière ». Une part importante des données transmises est composée de renseignements personnels. À défaut de mesures de protection adéquates, il y a risque de préjudice au caractère privé et à la sécurité des renseignements personnels.

Le cas échéant, les violations peuvent être contraires aux lois canadiennes. De plus, elles peuvent être lourdes de conséquences pour les ministères : perte de la confiance du public, plaintes et enquêtes ultérieures et, dans certains cas, perte de financement continu d'un programme ou d'un service.

Au cours d'une vérification récente importante du flux de données transfrontière à l'Agence des services frontaliers du Canada, la commissaire fédérale à la protection de la vie privée, Jennifer Stoddart, a conclu qu'il existe de nombreux moyens à prendre pour mieux gérer les risques qui menacent les renseignements personnels et accroître la transparence, le contrôle et la responsabilisation.

Le rapport complet peut être consulté à

http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_f.asp.

Les lignes directrices proposent des stratégies qui réduisent au minimum ou éliminent les menaces aux renseignements personnels et à la sécurité dans le cadre d'ententes d'échange de renseignements personnels.

De plus, elles les normalisent afin que tous les ordres de gouvernement au Canada puissent éviter le travail redondant et traiter les ententes avec célérité et efficacité.

A4. Historique

Les autorités canadiennes responsables de la protection de la vie privée et de l'information sont sensibles de longue date aux risques posés par le flux de données transfrontière, particulièrement à destination de l'étranger, où les lois d'autres pays peuvent avoir préséance.

Les propos de David Loukidelis, commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, traduisent de façon générale le point de vue du milieu gouvernemental de la protection de la vie privée :

« *Les compétences sont soumises à des limites territoriales réelles qui menacent la capacité des autorités chargées de la protection des données d'intervenir dans le contexte du flux international de données transfrontière.* » [Traduction]

(Citation tirée de *Transborder Data Flows and Privacy – An Update on Work in Progress*, février 2006)

En réponse à une enquête que le Commissaire à la protection de la vie privée a commandé d'EKOS Research Associates en mars 2005, 85 % des répondants canadiens se sont dits quelque peu préoccupés ou très préoccupés par le transfert de renseignements personnels à des gouvernements étrangers par des organismes gouvernementaux canadiens.

Consulter les résultats du sondage à l'adresse :

http://www.privcom.gc.ca/information/survey/2005/ekos_f.asp.

Cette même année, les participants à la conférence annuelle du lac Carling ont convenu de la nécessité de formuler conseils et normes sur le flux de données transfrontière. Pour répondre à la situation, le Conseil des DPI du secteur public, auquel siègent des représentants des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales, a approuvé le financement nécessaire pour établir des consignes à l'usage de toutes les administrations publiques du Canada.

Par conséquent, le sous-comité de la protection des renseignements personnels du Conseil a élaboré les présentes lignes directrices.

A5. Utilisateurs prévus

Quiconque est responsable de consultations, d'un programme ou d'un service gouvernemental, ou de l'élaboration ou de la gestion d'un tel programme, dans des circonstances telles que des renseignements personnels sont susceptibles d'être communiqués à une administration autre ou le sont effectivement, serait bien avisé de consulter les présentes lignes directrices. Les utilisateurs visés comprennent les bureaux de DPI, les conseillers en protection de la vie privée et les gestionnaires de programmes et de services.

A6. Mode d'emploi

Les lignes directrices énoncent des pratiques exemplaires en matière d'échange de renseignements personnels entre gouvernements, mais elles ne doivent pas être utilisées isolément.

Avant d'envisager de conclure une entente, vous devez invariablement consulter les conseillers en protection de la vie privée et les avocats-conseils de votre organisme afin de recenser, d'examiner et de prendre en considération toutes lois et politiques susceptibles de se répercuter sur des questions de protection de la vie privée et de sécurité. De plus, toute

entente doit être soumise à l'examen et à l'approbation des spécialistes précités.

A7. Sommaire des pratiques exemplaires

Le texte qui suit résume les six pratiques exemplaires que les lignes directrices décrivent à grands traits.

Pratiques 1 à 3 : Les trois premières pratiques exemplaires s'appliquent **avant** la conclusion d'une entente d'échange de renseignements personnels (EERP).

Première pratique exemplaire : Recensement des besoins et des facteurs de risque

Conditions obligatoires : Vous ne devez envisager de communiquer des renseignements personnels dont vous avez la charge que si les deux conditions suivantes sont remplies :

- vous possédez le pouvoir légal nécessaire;
- il existe un besoin clair et justifiable de communiquer l'information pendant la période en cours.

Parmi les autres conditions importantes figurent :

- les mesures de protection de l'information, par exemple l'emplacement des bases de données et le mode de transmission;
- la consultation d'avocats-conseils et d'experts en protection de la vie privée, aux diverses étapes allant de l'ébauche de l'EERP à la mise en œuvre et au suivi;
- la justification de l'EERP par l'explication des motifs précis de la communication et des renseignements particuliers à communiquer.

Les pratiques exemplaires accessoires suivantes, entre autres, sont à signaler :

- obtenir le consentement des intéressés et leur communiquer un avis;
- limiter au minimum le volume de renseignements personnels recueillis;
- recueillir, utiliser et divulguer des renseignements personnels en respectant le principe que seules les personnes qui en ont véritablement besoin doivent en avoir connaissance;
- faire en sorte que l'expéditeur transmette l'information au destinataire et éviter que celui-ci la retire de la source;
- effectuer une évaluation préliminaire des risques.

(La section 1.5 présente des exemples de scénarios qui posent des risques importants, tandis que l'annexe E énumère des risques courants qui menacent les renseignements personnels.)

Deuxième pratique exemplaire : Examen de stratégies de substitution

La communication de renseignements personnels est une solution de dernier ressort à cause des risques intrinsèques qu'elle pose pour les renseignements visés. Il faut se demander s'il n'est pas possible de réaliser les objectifs du programme ou du service sans divulguer de renseignements personnels. Voici des solutions de rechange possibles :

- fournir un résumé de l'information et ne pas révéler l'identité des personnes concernées;
- rendre les données anonymes;
- fournir des données agrégées, par exemple une fourchette d'âges plutôt que des âges particuliers.

Troisième pratique exemplaire : Évaluation des risques

Examiner en détail les risques d'entrave à la vie privée en utilisant les outils recommandés, notamment les suivants :

- une évaluation des facteurs relatifs à la vie privée (EFVP) qui mesure le respect non seulement des normes juridiques établies mais des principes universels de protection des renseignements personnels **(l'annexe C énumère les lignes directrices de l'EFVP)**;
- la planification des communications, y compris la présentation de rapports au public;
- la consultation de spécialistes en protection de la vie privée et sécurité et d'avocats-conseils du ministère de même que de l'autorité en matière de protection de la vie privée de l'administration publique dont vous relevez (par exemple un commissaire ou un ombudsman).

Pratiques exemplaires 4 à 6 : Les pratiques exemplaires suivantes s'appliquent **après** que vous avez décidé de conclure une EERP.

Quatrième pratique exemplaire : Documentation de la décision

Une pratique exemplaire consiste à consigner la décision d'aller de l'avant, afin de la justifier et de décrire à grands traits un plan d'atténuation des risques. La documentation doit inclure une justification, une analyse coûts-avantages, une évaluation des facteurs relatifs à la vie privée et un plan d'atténuation de tous les risques. Assurez-vous que l'EERP repose sur de solides pratiques de gestion de l'information.

Cinquième pratique exemplaire : Établissement d'une EERP

Voici des pratiques exemplaires à appliquer pour établir une EERP :

- nommer un conseil de surveillance composé de membres du ministère qui connaissent les questions de protection de la vie privée et de sécurité et qui sont en mesure d'offrir des conseils et un soutien;
- soumettre chaque EERP à l'examen et à l'approbation de spécialistes en protection de la vie privée et d'avocats-conseils;
- rédiger les EERP en langage clair afin de garantir que tous les termes sont expliqués à fond.

Votre EERP devrait comprendre les éléments clés suivants :

- l'identité, les rôles et les responsabilités des parties;
- l'information divulguée et recueillie et le motif dans chaque cas;
- la fréquence des échanges et la durée de l'information échangée;
- le fondement juridique de la divulgation et de la collecte de l'information;
- les méthodes de transmission et de stockage de l'information et les mesures de sécurité prises;
- la marche à suivre en cas d'entrave à la vie privée ou à la sécurité;
- les restrictions à la collecte, à l'utilisation, à la divulgation et à la conservation d'information;
- des mesures visant à garantir l'exactitude de l'information;
- l'indemnisation prévue;
- la surveillance de la conformité.

(Le modèle à la section 5.6 vous invite à inclure des précisions correspondant à vos circonstances.)

Sixième pratique exemplaire : Contrôle et suivi

Le contrôle de l'efficacité de l'entente est une pratique exemplaire. Il consiste en des pistes de vérification, des autoévaluations, des vérifications, des systèmes de vérification, des certificats d'assurance et des techniques de mesure concernant les engagements pris par son gouvernement aux termes de l'entente.

B. En quoi consistent les ententes d'échange de renseignements personnels?

Une entente d'échange de renseignements personnels entre gouvernements, appelée ci-après simplement « EERP », stipule les modalités de collecte, d'utilisation et de divulgation de renseignements personnels entre administrations publiques.

Trois priorités

Si vous consentez à révéler des renseignements personnels à une administration publique, une EERP vous invite à reconnaître trois exigences prioritaires :

- le ou les motifs pour lesquels le destinataire utilisera l'information;
- le fondement juridique de la transmission et de la collecte d'information;
- un engagement à respecter le caractère privé de l'information et à en assurer la sécurité, et la garantie que l'expéditeur sera informé d'avance de l'intention du destinataire de divulguer l'information d'une manière non conforme aux modalités de l'EERP.

B1. Est-il obligatoire de conclure une EERP?

Une loi ou une politique peut exiger l'établissement d'une EERP. Dans le cas contraire, le recours à une EERP est quand même fortement recommandé, car il s'agit d'un instrument pratique et efficace de gestion des risques.

Les commissaires à la protection de la vie privée ou le public peuvent considérer la décision de renoncer à une EERP comme le signe d'une insouciance à l'égard de la protection de la vie privée.

B2. Avantages

L'EERP offre un certain nombre d'avantages qui favorisent son utilisation en tant que pratique exemplaire. Il s'agit notamment des suivants :

- la clarification des droits et des obligations des parties;
- le respect des lois et des politiques en vigueur;
- l'établissement de responsabilités en matière de garde et de contrôle de l'information;
- l'établissement de restrictions aux catégories ou au volume d'information partagée et aux motifs du partage;
- l'établissement de protocoles qui prévoient des procédures à appliquer en cas de difficulté.

La cinquième pratique exemplaire, « Établissement d'une EERP », précise le détail de l'élaboration d'une EERP et prévoit des dispositions sur la protection de la vie privée.

B3. Catégories

Transmissions répétées : L'EERP qui vise des transmissions répétées de renseignements personnels au cours d'une période donnée est la plus répandue, car elle évite aux parties de devoir conclure une entente distincte pour chaque transmission.

Transmission unique : Les parties peuvent opter pour une EERP ponctuelle si elles souhaitent transmettre de l'information une seule fois.

Transmission unidirectionnelle : L'entente unidirectionnelle prévoit la transmission d'information d'un organisme gouvernemental à un autre. L'une des parties divulgue des renseignements personnels, que l'autre recueille.

Transmission bidirectionnelle : L'entente bidirectionnelle prévoit la communication réciproque de renseignements personnels. Une partie gouvernementale divulgue des renseignements personnels à une autre pour des raisons particulières. Le destinataire en fait autant en communiquant des renseignements personnels qu'il possède concernant les mêmes personnes ou d'autres.

Mise en garde : En règle générale, les EERP doivent être bilatérales et viser à la fois la partie qui divulgue de l'information et celle qui la reçoit. Une des fonctions de l'EERP est de préciser le fondement juridique qui autorise une partie à recueillir et à divulguer de l'information, les motifs auxquels elle doit servir, l'information exacte requise et les mesures de sécurité particulières dont elle sera l'objet. L'EERP multilatérale engendre le risque de traiter des questions susmentionnées en des termes inutilement vagues ou généraux, de telle sorte que les dispositions s'appliqueraient globalement à toutes les parties.

B4. Lignes directrices provinciales sur les EERP

Certaines provinces ont adopté des lignes directrices sur les EERP qui répondent à leurs propres circonstances.

Colombie-Britannique : [Privacy Guide for Personal Information Exchange Agreements](#)

Alberta : [Guide for Developing Personal Information Sharing Agreements](#)

Ontario : [Model Data Sharing Agreement \(1995\)](#)

Vous voudrez peut-être consulter votre propre bureau d'accès à l'information et de protection de la vie privée afin de déterminer si votre administration possède des lignes directrices ou des modèles comparables.

B5. EERP types

Une EERP est en vigueur qui régit l'échange de renseignements personnels en vue de l'exécution de l'Entente Canada-Alberta sur le développement du marché du travail. Elle sert d'EERP type et peut être consultée à :

<http://www.hrsdc.gc.ca/fr/epb/lmd/lmda/alberta/pdlmdaalberta31.shtml>.

B6. Entrepreneurs

Si un entrepreneur est chargé de traiter des renseignements personnels qu'échangent des gouvernements, l'EERP doit en faire mention. Toutefois, un contrat légal distinct entre l'entreprise et l'organisme gouvernemental concerné énoncera les modalités particulières d'exercice de la fonction par l'entreprise.

Il est primordial qu'un contrat entre une administration publique et un tiers chargé de traiter de quelque façon des renseignements personnels comporte des dispositions précises énonçant le détail des responsabilités du tiers. En l'occurrence, le contrat doit préciser des limites imposées à l'utilisation que le tiers fait de l'information et aux personnes relevant du tiers autorisées à traiter l'information, des règles régissant la conservation et la sécurité de l'information et, tout particulièrement, le droit d'accès à l'information de l'organisme gouvernemental touché et l'administration du droit d'une personne à ses propres renseignements.

Par ailleurs, le contrat doit mentionner si le tiers est tenu de se conformer à la loi sur la protection de la vie privée à laquelle est tenu l'organisme gouvernemental, en sus des autres lois qui s'y appliquent. En règle générale, les organismes gouvernementaux ne peuvent impartir leurs obligations de protection de la vie privée à une tierce partie.

Il se peut que votre administration soit dotée de lois, de politiques et de lignes directrices en matière d'acquisition qui régissent les contrats à conclure avec les entreprises privées qui participent à l'échange de renseignements personnels. Par conséquent, il vous est conseillé de consulter le bureau compétent de l'accès à l'information et de protection de la vie privée pour obtenir les consignes en vigueur. Voici quelques adresses de sites Web qui pourront vous être utiles :

Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché **du Secrétariat du Conseil du Trésor du Canada :**

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/gd-do/gd-do_f.asp;

Public sector Outsourcing and Risks to Privacy **de l'Alberta :**

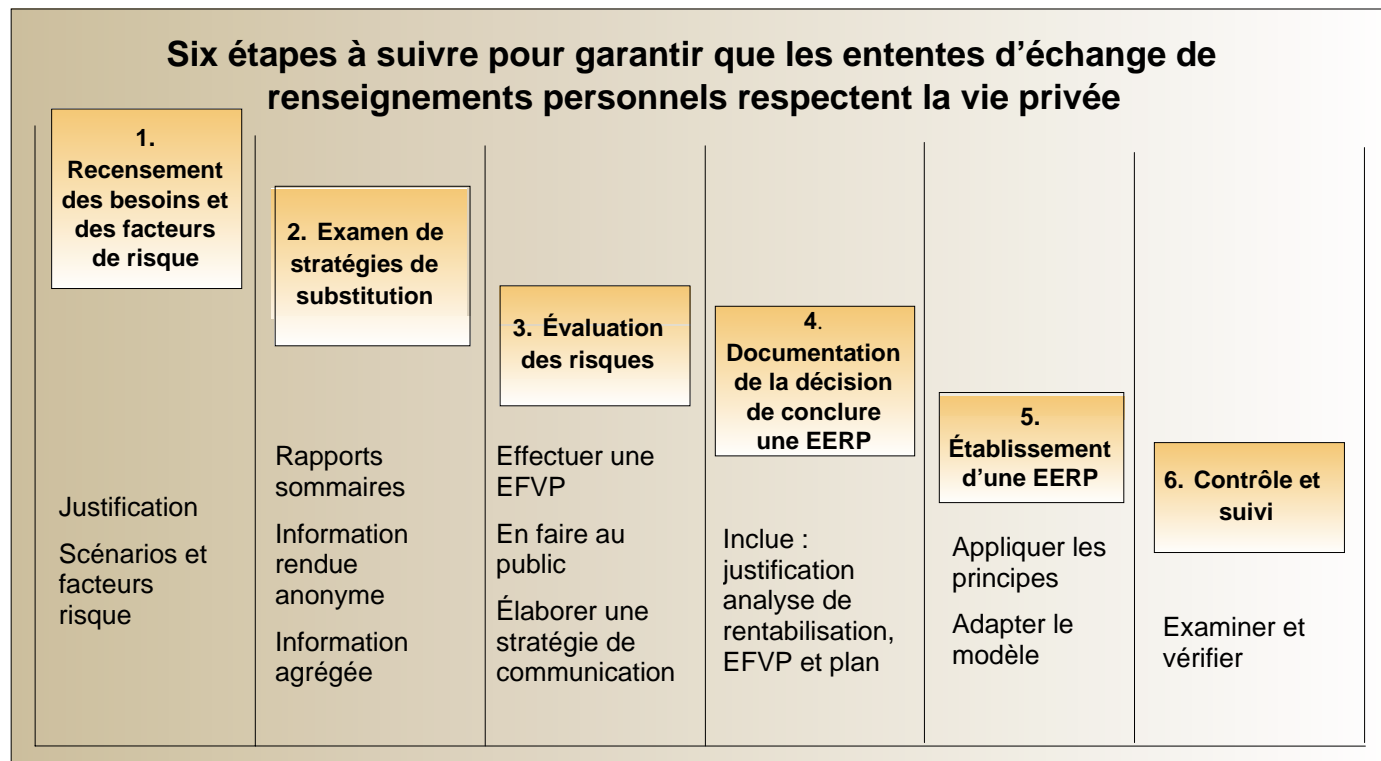
<http://www.gov.ab.ca/acn/200602/19490.pdf>;

Document de discussion provisoire de l'Alberta intitulé *Managing Contracts under the FOIP Act* (septembre 2005) :

http://www3.gov.ab.ca/foip/other_resources/publications_videos/pdf/contract_managers_guide.pdf.

C. Six pratiques exemplaires

Les six pratiques exemplaires suivantes s'étalent sur le cycle décisionnel.



lquer les

Adapter le modèle

Première pratique exemplaire : Recensement des besoins et des facteurs de risque

1.1 En quoi consistent les renseignements personnels?

La première étape consiste à déterminer si l'information susceptible d'être échangée répond à la définition de « renseignements personnels ».

La plupart des lois canadiennes définissent plus ou moins comme il suit les renseignements personnels :

En règle générale, les renseignements personnels sont des renseignements, de fait ou subjectifs, consignés ou non, sur une personne identifiable. Il s'agit de toutes catégories d'information, notamment :

- l'âge, le nom, la date de naissance, les numéros d'identification, le revenu, l'origine ethnique, le groupe sanguin;
- des opinions, des évaluations, des commentaires, la situation sociale ou des mesures disciplinaires;
- des dossiers d'employé, des documents de solvabilité ou de prêt, des dossiers médicaux et des états d'opérations.

Il vous est recommandé de consulter les lois en vigueur sur votre territoire pour obtenir la définition qui correspond à vos circonstances.

Identifiable

Si l'information échangée peut servir à identifier une personne, par exemple au moyen d'un numéro d'identification personnel, elle est considérée comme constituant des « renseignements personnels ». Il n'est pas nécessaire que de l'information contienne le nom d'une personne pour que ce soit le cas.

1.2 Êtes-vous habilité à échanger des renseignements personnels?

À cause des risques intrinsèques d'entrave à la vie privée qu'il présente, le partage de renseignements personnels doit être une solution de dernier ressort pour atteindre un objectif particulier. Il y a toujours lieu d'examiner d'abord les solutions de substitution (voir « Deuxième pratique exemplaire »).

Des renseignements personnels ne doivent être échangés que si les deux conditions suivantes sont remplies :

1. Vous êtes habilité à les échanger.
2. Il existe un besoin clair et justifiable de procéder pendant la période en cours.

(La seconde condition, celle du besoin justifiable, est examinée à la section suivante, 1.3.)

1.2.1 Habilitation

Les lois régissant un programme ou un service peuvent passer sous silence ou non la collecte ou la communication de renseignements personnels. Cependant, le fondement juridique qui autorise la prestation d'un programme ou d'un service peut comporter implicitement le pouvoir de recueillir des renseignements. Normalement, le consentement de la personne concernée ou la loi sur la vie privée en vigueur sur le territoire autoriserait la divulgation de renseignements personnels. Si le fondement juridique n'est pas clair, les fonctionnaires concernés doivent consulter les avocats-conseils de leur administration.

1.2.2 Consentement et avis

La loi ou le contrat légal en vertu duquel un programme ou un service est offert peut autoriser la communication de renseignements personnels sans le consentement de la personne concernée dans certaines circonstances.

À titre d'exemple, la quasi-totalité des lois sur la protection de la vie privée autorise l'utilisation et la communication de renseignements personnels sans le consentement de la personne concernée si elles sont conformes au motif initial pour lequel les renseignements ont été recueillis, si elles sont prescrites par une loi, si elles sont nécessaires à une procédure judiciaire ou si les renseignements doivent être archivés. Dans certains cas, les lois sur la protection de la vie privée autorisent l'utilisation et la communication de renseignements personnels aux fins d'enquêtes judiciaires, d'accords avec d'autres gouvernements, de recherches ou de situations qui offrent un avantage net au public.

Toutefois, même si la loi autorise l'utilisation ou la communication envisagée de renseignements personnels et s'il n'est pas nécessaire d'obtenir à cette fin le consentement des personnes touchées, les organismes gouvernementaux qui souscrivent à des pratiques exemplaires voudront tel consentement par souci de transparence et de responsabilisation.

À cette fin, au moment de la collecte de renseignements, la personne concernée sera informée clairement de l'utilisation qui en sera faite et, lorsqu'il s'agit d'un programme gouvernemental à participation facultative, elle sera informée que sa participation dépend de son consentement à ce que l'information soit utilisée et communiquée comme entend le faire l'administration publique concernée.

L'annexe A énumère toutes les lois canadiennes sur la protection de la vie privée ayant trait aux EERP dont traitent les présentes lignes directrices.

1.2.3 Communication obligatoire de renseignements

Dans certaines circonstances, par exemple une épidémie, la communication de renseignements personnels à une autre administration peut être obligatoire. La *Loi sur la quarantaine* (2005) est un exemple de loi fédérale qui impose la communication de renseignements personnels sur la santé aux autorités provinciales de la santé.

1.3 Quand la transmission s'impose

D'autres administrations sont susceptibles de demander à l'organisme gouvernemental dont vous relevez d'avoir accès à des renseignements personnels dont vous avez la garde. Dans d'autres circonstances, vous pouvez formuler pareille demande, ou votre organisme peut se situer au nombre de ceux qui constatent un besoin commun.

Dans tous les cas, la transmission de renseignements personnels ne doit être envisagée que lorsqu'un besoin clair se manifeste pendant la période en cours. Il ne suffit pas de souhaiter obtenir des renseignements, de prévoir un besoin éventuel ou de juger que des renseignements soient susceptibles d'être utiles à l'avenir.

La communication de renseignements personnels par un organisme gouvernemental à un autre n'est « nécessaire » que lorsque l'organisme destinataire en a besoin pour administrer un programme ou un service gouvernemental légitime, et, le cas échéant, seul le volume minimal de renseignements nécessaires à cette fin doit être transmis.

Seul le minimum nécessaire de renseignements personnels doit être recueilli, utilisé et communiqué. Les renseignements ne doivent être fournis qu'à des personnes qui en ont véritablement besoin, et le degré d'anonymat le plus rigoureux possible doit être respecté.

Voici des exemples de situations dans lesquelles un besoin se manifeste.

Responsabilité : Il peut être nécessaire de communiquer des renseignements personnels afin d'apprécier l'exactitude d'information sur des particuliers ou d'évaluer l'admissibilité à un programme ou un service.

Programmes mixtes et accords bilatéraux : Si votre ministère participe à un programme mixte ou à un accord bilatéral avec une administration autre, il peut être nécessaire d'échanger des renseignements personnels aux fins de la prestation du programme ou du service prévu.

Demande d'un client : Par commodité, des clients peuvent demander que leurs renseignements personnels soient communiqués à d'autres administrations pour éviter de devoir fournir plusieurs fois la même information.

1.4 Justification de l'EERP

L'exécution d'une analyse coûts-avantages ou d'une analyse de rentabilisation représente une pratique avantageuse pour justifier la nécessité d'échanger des renseignements personnels, car elle permet :

- de décrire les risques ou les conséquences possibles de renoncer au partage d'information;
- d'expliquer pourquoi il est nécessaire de transmettre des renseignements personnels en ce moment;
- de préciser l'information à communiquer et l'usage exact qu'en fera le destinataire;
- d'expliquer pourquoi l'information doit comprendre des données nominatives;
- de donner les raisons pour lesquelles les renseignements personnels doivent être recueillis indirectement, s'il y a lieu, et d'expliquer les avantages du partage des

données en question par rapport au recours à d'autres moyens de réaliser les mêmes objectifs;

(Voir « Deuxième pratique exemplaire : Examen de stratégies de substitution ».)

- de préciser le fondement juridique sur lequel s'appuieront la partie qui divulgue l'information et celle qui la reçoit.

Si votre objectif concerne la réduction des coûts :

- évaluez les sommes susceptibles d'être recouvrées ou économisées grâce à la divulgation ou à la réception de renseignements personnels en vertu de l'entente. Par exemple, la cessation de prestations auxquelles le bénéficiaire est inadmissible peut occasionner des économies qui n'auraient pu être réalisées à défaut du partage de renseignements;
- pesez les avantages financiers et les risques constatés pour la vie privée.

1.5 Évaluation préliminaire des risques

Après avoir déterminé que l'information répond à la définition de « renseignements personnels », obtenu l'autorisation de la communiquer et confirmé la nécessité de ce faire, vous devez évaluer les risques d'entrave à la vie privée avant de conclure une EERP.

1.5.1 Scénarios à risque élevé

Les administrations publiques voudront peut-être se prévaloir d'un test d'atteinte à la vie privée qui prend en compte trois critères liés réciproquement :

- le caractère délicat des renseignements personnels, y compris la question de savoir s'ils sont détaillés ou extrêmement personnels (comme des renseignements sur la santé) et le contexte dans lequel ils ont été recueillis;
- la question de savoir s'il est raisonnable de croire que la personne qui a fourni les renseignements s'attendrait à ce qu'ils soient utilisés aux fins prévues;
- le préjudice susceptible d'être causé par la divulgation illicite des renseignements ou leur usage abusif, y compris le risque de vol d'identité ou d'accès par des gouvernements étrangers.

1.5.2 EERP de caractère délicat

Renseignements personnels sur la santé (dossiers médicaux) : Les dossiers médicaux renferment parfois certains renseignements qui n'ont pas trait directement à l'état de santé de la personne concernée, notamment de l'information sur les antécédents familiaux, l'usage de substances illicites, les tendances suicidaires, le comportement sexuel ou la teneur de conversations avec des professionnels de la santé. Le dossier médical d'une personne peut déterminer son admissibilité à certaines formes d'assurance-santé et influencer les occasions d'études ou d'emploi qui s'offrent à elle.

NOTA : L'Alberta, la Saskatchewan, le Manitoba et l'Ontario ont adopté des lois distinctes sur l'information en santé. (Les adresses des sites Web pertinents sont énumérées à l'annexe A.)

Enquête judiciaire (casiers judiciaires) : Les administrations publiques doivent parfois partager des renseignements personnels à l'appui d'enquêtes criminelles. Les destinataires en ont besoin dans certains cas pour porter des accusations, entamer des poursuites en justice ou expulser des personnes de leur territoire. Pareils renseignements sont considérés comme extrêmement délicats, car ils concernent fréquemment la vie intime des personnes visées. De plus, au moment de la communication, aucune accusation n'aura encore été prouvée.

Documents financiers : L'information sur l'impôt, la solvabilité, les assurances et d'autres renseignements de caractère financier peuvent être considérés comme délicats à cause des conséquences qu'est susceptible de provoquer leur consultation par des personnes non autorisées.

Si l'accès à des renseignements personnels à des fins autres que celles auxquelles ils sont destinés est susceptible de porter préjudice à la personne visée, il serait considéré comme posant un « risque élevé ».

1.5.3 Transmission internationale

Si l'administration publique dont vous relevez souhaite transmettre des renseignements personnels à une administration publique étrangère, la situation présentera un risque élevé d'entrave à la vie privée. Il en est ainsi parce que les lois du pays destinataire peuvent primer les lois canadiennes. Quantité de pays de la planète adoptent des lois antiterroristes qui peuvent l'emporter sur le droit à la protection de la vie privée des particuliers. Par conséquent, les renseignements personnels sur les Canadiens acheminés à l'étranger peuvent être consultés à l'insu des personnes concernées et sans leur consentement.

Les risques sont également élevés du fait qu'il n'existe aucun moyen pratique d'obliger une partie récalcitrante à l'étranger de respecter les modalités d'un contrat ou de la contraindre à renoncer à l'accès à de l'information ou au contrôle qu'elle exerce sur cette dernière.

Des renseignements personnels ne doivent être communiqués qu'à des pays qui se sont engagés à les protéger. Même si c'est le cas, ce n'est pas tâche facile de démêler les tenants et aboutissants de lois étrangères sur la protection de la vie privée et des exceptions qu'elles prévoient.

Il est recommandé de vérifier indépendamment les garanties données par une partie qui désire obtenir des renseignements personnels.

L'annexe B offre de plus amples précisions sur les échanges internationaux.

1.5.4 Mesures de sécurité

Les mesures de protection de l'information sont d'importance capitale pour contrer le risque d'entrave à la vie privée. Parmi ces mesures figurent l'emplacement des bases de données, les méthodes de stockage, les méthodes de transmission, le recours à la technologie et le personnel responsable.

Veillez consulter votre politique de sécurité et les responsables du domaine pour connaître les mesures et les procédures de sécurité en vigueur au sein de votre administration, notamment celles qui s'appliquent à vos circonstances particulières.

À titre d'exemple, le gouvernement du Canada exige des ministères qu'ils utilisent des techniques de chiffrement ou des méthodes de protection autres homologuées ou approuvées par le Centre de la sécurité des télécommunications (CST) pour transmettre par voie électronique en toute sécurité de l'information classifiée ou de catégorie « Protégé C ». Les ministères doivent chiffrer les renseignements des catégories « Protégé A » ou « Protégé B » si les résultats d'une évaluation des menaces et des risques en indiquent la nécessité. Toutefois, ils doivent chiffrer l'information de catégorie « Protégé B » avant de la transmettre par Internet ou par le biais d'un réseau sans fil.

La sécurité ne se limite pas aux seules mesures techniques et matérielles. Des mesures de protection administratives sont également possibles, par exemple le fait de restreindre l'accès à des renseignements qu'aux personnes autorisées, à celles qui se sont engagées par écrit à respecter la sécurité des renseignements et la vie privée des personnes concernées et aux gestionnaires et employés autres sensibilisés à la sécurité et formés aux pratiques et procédures connexes.

Comme des mesures rigoureuses de protection de la sécurité déterminent le respect de la vie privée, l'EERP doit en tenir compte obligatoirement.

1.5.5 Transmission par l'expéditeur

L'information que vous communiquez à d'autres parties doit être acheminée par vous et non récupérée par le destinataire. S'il est décidé qu'il y a lieu de communiquer de l'information ou des données et s'il existe le fondement juridique nécessaire à cette fin, le destinataire ne doit pas être autorisé à accéder à la base de données qui contient les renseignements personnels dont vous avez la garde. Vous devez plutôt transmettre l'information ou les données à l'administration destinataire de la façon, au moment et à la date prévus par l'entente.

Deuxième pratique exemplaire : Examen de stratégies de substitution

Éviter de transmettre des renseignements personnels est un moyen prioritaire à prendre pour réduire énormément ou éliminer le risque d'entrave à la vie privée.

Dans le document qu'il a écrit sur un modèle d'échange de renseignements personnels, Tom Wright, ancien commissaire à l'information et à la protection de la vie privée de l'Ontario, avait ceci à dire : « La communication de renseignements personnels entre deux organismes est contraire à deux principes fondamentaux de la protection des données : les renseignements personnels doivent être recueillis directement auprès de la personne concernée; ils doivent servir uniquement aux fins pour lesquelles ils ont été recueillis (à quelques exceptions près). » [Traduction]

Les méthodes suivantes sont des solutions de substitution à la communication de renseignements personnels.

2.1 Rapports sommaires

Un sommaire de l'information contenue dans une base de données ou un répertoire peut parfois répondre aux objectifs d'un projet. Plutôt que d'identifier des personnes, le sommaire présente des résultats, par exemple le nombre de personnes qui habitent une région particulière.

2.2 Information rendue anonyme

Des renseignements personnels sont purgés de toute information nominative s'ils sont modifiés de telle sorte que l'identité de la personne concernée ne peut être décelée au moyen d'une méthode raisonnablement prévisible. Le plus souvent, sont supprimés, par exemple, le nom, l'âge et d'autres renseignements qui, ensemble, peuvent révéler une identité. Les données doivent être modifiées de telle façon qu'il est impossible de les remanier afin d'en tirer une identité ou qu'il n'existe aucun moyen raisonnable de le faire.

(Source de la définition : Institut canadien d'information sur la santé, *Le respect de la vie privée et confidentialité de l'information sur la santé à l'ICIS*, http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=RC_10_F)

2.3 Données agrégées

Données agrégées s'entend d'information à laquelle il a été donné un caractère général et qu'il est impossible de rattacher à un particulier. Citons l'exemple d'une fourchette d'âges plutôt que les âges précis de personnes. Le recours à cette forme de données est un excellent moyen d'éliminer le risque d'entrave à la vie privée. Il y a toujours lieu de se demander s'il est possible de réaliser l'objectif visé au moyen de données agrégées avant de conclure que la divulgation de renseignements personnels est indiquée.

Troisième pratique exemplaire : Évaluation des risques

Les risques pour la vie privée doivent être appréciés de façon systématique et exhaustive au moyen d'une évaluation des facteurs relatifs à la vie privée (EFVP) et d'une évaluation de la menace et des risques (EMR).

Les instruments et les procédures qui suivent se sont révélés des moyens efficaces d'évaluer les risques.

3.1 Exécution d'une évaluation des facteurs relatifs à la vie privée (EFVP)

L'un des meilleurs moyens d'apprécier le degré de risque est d'effectuer une évaluation des facteurs relatifs à la vie privée (EFVP), qui fait appel à une liste de contrôle exhaustive.

L'EFVP mesure le respect non seulement des normes juridiques établies, ce qui représente une pratique minimale acceptable, mais également des principes universels de protection de la vie privée.

Certaines administrations publiques canadiennes imposent l'exécution d'une EFVP dans certaines circonstances, par exemple au moment de la révision d'un programme ou d'un service gouvernemental.

L'annexe C énumère des modèles d'EFVP, des documents de référence et des ressources utiles. L'annexe E énumère des exemples de risques courants pour la vie privée.

3.2 Rapports publics et communications

L'autorité en vertu de laquelle vous partagez des renseignements personnels peut vous obliger à faire rapport publiquement de l'EERP que vous avez conclue.

Même si la présentation d'un rapport public n'est pas obligatoire, l'élaboration d'un plan de communications aux fins de toute EERP est affaire de pratique exemplaire. Le plan doit tenir compte de la sensibilité du public à la transmission de renseignements personnels et du besoin de transparence.

3.3 Consultation des spécialistes en protection de la vie privée et sécurité et des avocats-conseils de votre organisme

Votre organisme gouvernemental dispose peut-être de ses propres experts en protection de la vie privée et sécurité et avocats-conseils, et vous devez les consulter invariablement avant d'élaborer ou d'établir une EERP entre gouvernements.

3.4 Consultation du conseiller en protection de la vie privée de votre administration

Selon l'administration publique dont vous relevez et vos circonstances, vous pouvez être tenu par les lois ou les politiques en vigueur de consulter le commissaire ou l'ombudsman compétent à la protection de la vie privée.

Même si la consultation n'est pas obligatoire, cela tient d'une pratique exemplaire de consulter le spécialiste de votre administration en conseils et recherche sur la protection de la vie privée, à plus forte raison si l'EERP envisagée présente un degré de risque élevé.

L'autorité à consulter au gouvernement fédéral est le Commissaire à la protection de la vie privée. L'autorité correspondante de nombreuses administrations canadiennes est le commissaire compétent à l'information et à la protection de la vie privée. Le titre et l'autorité peuvent varier d'un territoire à l'autre. *L'annexe D propose des liens conduisant aux responsables de la protection de la vie privée des différentes régions du Canada.*

Quatrième pratique exemplaire : Documentation de la décision

4. Consigner la décision

Si, après avoir examiné des stratégies de substitution (deuxième pratique exemplaire) et effectué une évaluation des risques (troisième pratique exemplaire), vous décidez de la nécessité de partager des renseignements personnels, vous seriez bien avisé de coucher par écrit la décision.

La documentation justifie la décision d'échanger des renseignements personnels et décrit un plan d'atténuation des risques. Elle devrait inclure, outre une justification, une analyse coûts-avantages, une évaluation des facteurs relatifs à la vie privée et un plan d'atténuation de tous les risques.

La documentation devrait également énumérer les étapes à suivre en cas de violation de la sécurité.

Une pratique exemplaire d'importance capitale consiste à appliquer des pratiques efficaces de gestion de l'information tout au long du cycle de vie de l'EERP (schématisation, conception, mise en œuvre, suivi) à l'appui de la prise de décisions en connaissance de cause. N'oubliez pas que, à défaut de bonnes pratiques de gestion de l'information qui garantissent la description écrite de tous les aspects des ententes, vous aurez peine à assurer le suivi des ententes ou à les surveiller étroitement. Il en résultera des rapports lacunaires sur l'ampleur du partage de renseignements personnels et, par conséquent, votre organisme ne pourra constater si l'activité est bien gérée et conforme aux conditions en vigueur.

Cinquième pratique exemplaire : Établissement d'une EERP

La présente section propose un modèle d'EERP. Votre administration possède peut-être son propre modèle qui correspond à vos circonstances.

5.1 Mode d'emploi du modèle

Insérez les dispositions pertinentes à l'endroit indiqué et, au besoin, adaptez le texte à vos propres circonstances. Le modèle est complet, mais il n'englobe pas nécessairement toutes les conditions que vous voulez inclure dans votre entente.

5.2 Organe de surveillance

La mise sur pied de l'organe de surveillance de l'établissement d'une EERP tient d'une pratique exemplaire. Il s'agit d'un groupe ou comité au sein de votre organisme qui connaît bien les questions de protection de la vie privée et de sécurité et qui est en mesure d'offrir des consignes d'orientation et autres.

5.3 Approbation officielle ou écrite de l'EERP

Ne manquez pas de soumettre chaque EERP à l'examen et à l'approbation de vos conseillers en protection de la vie privée et avocats-conseils. De plus, le fondé de pouvoir compétent de chacune des parties doit approuver par écrit ou autrement l'EERP.

5.4 Dix principes

Le contenu du modèle d'EERP répond aux dix principes de protection de la vie privée du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, la norme canadienne reconnue. Il s'agit des suivants :

1. Responsabilité
2. Détermination des fins de la collecte des renseignements
3. Consentement
4. Limitation de la collecte
5. Limitation de l'utilisation, de la communication et de la conservation
6. Exactitude
7. Mesures de sécurité
8. Transparence
9. Accès aux renseignements personnels
10. Possibilité de porter plainte à l'égard du non-respect des principes

5.5 Langage clair

Chaque EERP doit être rédigée en langage clair et aisément compréhensible. Expliquez toutes les expressions et les abréviations pour éviter toute confusion.

5.6 Modèle d'entente d'échange de renseignements personnels

Nota : La plupart des ententes d'échange de renseignements entre administrations publiques canadiennes font l'objet de protocoles d'entente plutôt que de contrats, car les administrations publiques n'ont pas recours aux tribunaux pour trancher des différends.

S'il existe un accord fédéral-provincial plus vaste qui engendre un programme ou un service intergouvernemental, l'accord devrait comprendre des dispositions générales sur l'échange de renseignements, sous réserve de la conclusion d'une entente particulière entre les parties.

1.0 Titre de l'entente

[Insérer le titre]

2.0 Parties à l'entente

La présente entente est conclue entre [nom de la partie] et [nom de la partie].

3.0 Rôles et responsabilités

Chaque partie à la présente entente (l'« entente ») assume la responsabilité des actes de ses employés, agents et entrepreneurs relatifs à l'utilisation, à la divulgation et à la destination des renseignements personnels visés par la présente entente.

3.1 Expéditeur : [Nom de la partie et renseignements sur la personne-ressource] est la partie qui divulgue des renseignements personnels aux termes de la présente entente.

3.2 Destinataire : [Nom de la partie et renseignements sur la personne-ressource] est la partie qui recueille (reçoit) des renseignements personnels aux termes de la présente entente.

(S'il s'agit d'une entente réciproque, les deux parties peuvent divulguer et recueillir des renseignements, et le libellé ci-dessus doit être modifié en conséquence.)

3.3 Entrepreneurs : *(s'il y a lieu)* L'entreprise privée ou les entreprises privée suivantes sont chargées par contrat d'assurer la transmission des données visées par la présente entente.

[Préciser la partie qui a conclu un contrat avec chaque entreprise, le nom de chaque entreprise, les numéros de contrat et les lois sur la protection de la vie privée qui régissent l'information dont les entreprises contractantes ont la garde. À noter que les lois qui s'appliquent à l'organisme gouvernemental peuvent également s'appliquer aux situations dans lesquelles le gouvernement fait appel à un fournisseur par voie de contrat. Une administration publique ne peut céder par contrat ses obligations légales.]

3.4 Mécanisme de règlement des différends, renvoi à des hauts fonctionnaires ou à un médiateur : Si une question visée par la présente entente suscite un problème ou un désaccord ou si elle est contestée, les parties s'en remettent à la procédure suivante : [description du mécanisme de règlement des différends, par exemple renvoi à des hauts

fonctionnaires des deux parties et possibilité pour les parties d'adresser la question à un médiateur tiers impartial].

3.5 Responsabilité des coûts : Chaque partie assume les coûts qu'elle engage dans le contexte de la présente entente.

4.0 Objet

La présente entente a pour objet d'autoriser la divulgation de renseignements personnels par [nom de l'expéditeur] à [nom du destinataire] aux fins suivantes : [préciser les fins pour lesquelles les renseignements sont transmis]. Elle a aussi pour objet d'assurer la protection des renseignements susmentionnés.

(S'il s'agit d'une entente réciproque ou multipartite, répéter l'alinéa précédent, selon le cas.)

4.1 Détermination des renseignements personnels : La présente entente prévoit la divulgation et la collecte des renseignements personnels suivants. (Décrire les renseignements personnels à communiquer et énumérer les champs de données dont le contenu sera transmis. Ne pas oublier d'énumérer chaque champ de données ou dossier client destiné à chacune des fins mentionnées à l'article 4.0.)

Exemple de liste de champs de données

La partie A divulguera à la partie B le contenu des champs de données suivants de chaque dossier client du programme [nom du programme] aux fins de [préciser les fins].

- Nom
- Identificateur du client
- Adresse
- Date de naissance
- Prestations reçues

La partie B divulguera à la partie A le contenu des champs de données suivants de chaque dossier client du programme [nom du programme] aux fins de [préciser les fins].

- Nom
- Identificateur du client
- Adresse
- Date de naissance

(Si les listes de champs de données ou de dossiers clients sont longues, elles peuvent figurer en annexe.)

4.2 Fréquence et durée : Les renseignements personnels visés par la présente entente ne seront transmis qu'à la fréquence nécessaire et les transmissions n'auront lieu qu'au cours d'une période fixe, selon les besoins. La fréquence prévue est [insérer périodicité] et la durée prévue est [insérer date ou préciser qu'il s'agit de la durée du programme ou du service]. [S'il s'agit d'une entente de longue durée, les parties doivent quand même prévoir une période d'effet de durée limitée, mais elle peut comporter au besoin une disposition qui en autorise la reconduction.]

4.3 Fins accessoires : L'utilisation de renseignements personnels à des fins accessoires est interdite sauf si la personne concernée y consent ou si les lois en vigueur l'autorisent.

4.4 Utilisation par des tiers : Le destinataire ne peut communiquer à un tiers les renseignements qu'il reçoit aux termes de la présente entente sans le consentement écrit préalable de l'expéditeur, selon la loi qui s'applique au sein de votre administration publique, y compris les lois sur l'accès et le respect de la vie privée, ou toute autre loi pertinente.

4.5 Consentement de consultation : Les deux parties consentent de se consulter dans l'éventualité d'une demande d'accès à l'information (AI) ou d'une demande formulée en vertu de liberté d'accès à l'information (LAI).

5.0 Autorisation

[Nom de l'expéditeur] confirme qu'il est autorisé à divulguer les renseignements personnels décrits dans l'entente à [nom du destinataire], aux fins énoncées à l'article 4, en vertu de [titre et article particuliers de la loi].

[Nom du destinataire] confirme qu'il est autorisé à recueillir les renseignements personnels décrits dans l'entente auprès de [nom de l'expéditeur], aux fins énoncées à l'article 4, en vertu de [nom et article particuliers de la loi].

6.0 Méthode de transmission

Les renseignements personnels visés par la présente entente seront transmis par les modes sécuritaires suivants : [préciser les modes de transmission techniques et physiques des renseignements personnels, par exemple bandes informatiques, chiffrement, protection par mot de passe et autres].

7.0 Sécurité des renseignements personnels

7.1 Confirmation de la sécurité des renseignements personnels : Les deux parties sont responsables de la sécurité et de l'intégrité des renseignements personnels qui leur sont confiés aux termes de la présente entente, et elles s'engagent à les protéger contre l'accès, la divulgation, l'utilisation, la modification et la suppression accidentels ou non autorisés.

7.2 Protection administrative, technique et physique : Les renseignements personnels visés par la présente entente feront l'objet des mesures de protection administratives, techniques et physiques suivantes. [Énumérer toutes les mesures de protection administratives, techniques et physiques à mettre en œuvre pour assurer la confidentialité des renseignements, notamment pour en prévenir l'utilisation et la divulgation.]

7.3 Lois et politiques en matière de sécurité : Les renseignements personnels visés par la présente entente seront recueillis, divulgués, utilisés, conservés, détruits et déclassés de façon sûre, conformément aux lois, politiques de sécurité, lignes directrices et directives applicables à chaque partie.

[Lois et politiques en matière de protection de la vie privée et de sécurité] s'appliquent à [nom de l'expéditeur].

[Lois et politiques en matière de protection de la vie privée et de sécurité] s'appliquent à [nom du destinataire].

Exemple : Les principales lois et politiques canadiennes pertinentes sont : [loi autorisant le programme ou le service], la *Loi sur la protection des renseignements personnels*, la *Loi sur l'accès à l'information*, la *Loi sur la Bibliothèque et les Archives du Canada*, la Politique sur la protection des renseignements personnels, la Politique sur l'accès à l'information, la Politique du gouvernement sur la sécurité et la Politique sur la gestion de l'information gouvernementale.

7.4 Prévention de nouveaux manquements : En cas de consultation, de divulgation, d'utilisation, de modification ou de suppression accidentel ou non autorisé de renseignements personnels, la partie chargée d'en assurer la sécurité prendra immédiatement toute mesure raisonnable pour empêcher que le manquement se répète et en avisera immédiatement l'autre partie.

7.5 Vérification des mesures de sécurité : Les parties conviennent que l'expéditeur a toute discrétion pour vérifier les procédures de sécurité et de confidentialité du destinataire, sous réserve de la protection raisonnable de telles procédures.

7.6 Réaction à une entrave à la vie privée ou à la sécurité : Les parties conviennent que l'expéditeur peut, à la réception d'un avis d'accès, de divulgation, d'utilisation, de modification ou de suppression accidentel ou non autorisé, à son gré, résilier la présente entente immédiatement et demander que les renseignements personnels déjà divulgués lui soient retournés. Les parties doivent adopter un plan d'avis aux personnes dont les renseignements ont été divulgués, en cas d'entrave à la vie privée ou à la sécurité.

7.7 Déclassement des renseignements à la résiliation de l'entente : Lorsque la présente entente est résiliée, les renseignements personnels visés par elle seront déclassés, de telle sorte que les personnes concernées ne puissent être identifiées à la suite du déclassement. Les renseignements seront déclassés [c'est-à-dire retournés à l'expéditeur ou détruits par le destinataire], conformément aux lois et aux politiques énumérées à l'article 7.2.

7.8 Déclassement pour d'autres motifs : Des renseignements personnels peuvent être retournés ou déclassés, moyennant le consentement écrit des parties, pour des motifs autres que la résiliation de la présente entente.

8.0 Limitation de la collecte, de l'utilisation, de la divulgation et de la conservation

8.1 Consentement à la limitation des fins auxquelles les renseignements sont destinés : Les renseignements personnels visés par la présente entente ne seront pas recueillis (reçus), utilisés, divulgués ou conservés à des fins autres que celles que prévoit la présente entente, sauf si la personne concernée y consent ou si les lois en vigueur l'autorisent.

8.2 Avis d'identification : Sauf si la loi l'autorise, aucun effort ne sera engagé en vue d'identifier les personnes dont l'identité a été supprimée des données. Si un destinataire partie à la présente entente est autorisé en vertu des lois dont il relève à identifier une personne, il doit d'abord en informer l'expéditeur et lui en demander l'autorisation.

9.0 Transparence, accès individuel et possibilité de porter plainte pour cause de non-respect

Chaque partie convient, relativement aux renseignements personnels dont elle a le contrôle, de répondre aux demandes des personnes qui désirent recevoir leurs renseignements personnels ou les faire modifier conformément à [titre de la loi]. Chaque partie convient d'informer l'autre partie de la demande et de la correction de renseignements. De plus, chaque partie convient de respecter les modifications apportées à des renseignements personnels par l'autre partie.

10.0 Exactitude

Chaque partie déploiera des efforts raisonnables pour assurer l'intégralité, l'exactitude et l'opportunité des renseignements visés par la présente entente. Les parties conviennent qu'elles ne peuvent garantir l'exactitude des renseignements visés par la présente entente et que, par conséquent, elles ne seront pas tenues pour responsables de tout préjudice subi par l'autre partie par suite de la divulgation ou de l'utilisation de tout renseignement imprécis, incomplet ou périmé, mais chaque partie s'efforcera de corriger toute inexactitude et veillera au respect du droit d'une personne d'accéder à ses renseignements personnels et de les corriger (voir 9.0).

11.0 Indemnisation

[Partie A] indemnifiera [partie B], ses représentants et ses employés des dommages, coûts, pertes ou dépenses que l'un ou plusieurs d'entre eux peuvent subir et des réclamations, actions, poursuites en justice ou autres procédures contre un ou plusieurs d'entre eux consécutivement à une blessure ou une perte causée ou présumée être causée par les actes ou omissions de [partie A], de ses représentants et de ses employés, en rapport avec l'exécution de la présente entente ou attribuable à son exécution.

[Partie B] indemnifiera [partie A], ses représentants et ses employés des dommages, coûts, pertes ou dépenses que l'un ou plusieurs d'entre eux peuvent subir et des réclamations, actions, poursuites en justice ou autres procédures contre un ou plusieurs d'entre eux consécutivement à une blessure ou une perte causée ou présumée être causée par les actes ou omissions de [partie B], de ses représentants et de ses employés, en rapport avec l'exécution de la présente entente ou attribuable à son exécution.

Chaque partie convient d'informer l'autre partie de toute réclamation, action, poursuite en justice ou procédure se rapportant à la gestion des renseignements visés par la présente entente. Chaque partie doit, à ses frais et à la demande raisonnable de l'autre partie, diriger la défense contre toute réclamation, action, poursuite en justice ou procédure et toutes négociations en vue de leur règlement ou participer à telles défense ou négociations, mais une partie ne sera pas tenue d'indemniser l'autre partie ou une autre personne indemnisée du règlement d'une réclamation, d'une action, d'une poursuite en justice ou d'une procédure autre sauf si la partie y a consenti par écrit avant le règlement.

12.0 Contrôle du respect

Les parties examineront, séparément ou solidairement et à des intervalles réguliers, les pratiques et les procédures décrites dans la présente entente afin de confirmer le respect des lois qui y sont mentionnées. [Nota : Préciser si un examen doit comprendre une inspection sur les lieux.] Chaque partie fournira les résultats de ses examens à l'autre partie, moyennant une demande écrite.

Les parties prendront, par ailleurs, les mesures indiquées pour assurer l'actualité de la présente entente et tenir un registre de tous cas particuliers de divulgation des renseignements personnels recueillis aux termes de la présente entente.

Les parties reconnaissent, de plus, que la présente entente est assujettie à des vérifications de conformité, des enquêtes et des examens effectués par le commissaire fédéral, provincial ou territorial compétent, un autre fonctionnaire autorisé ou un tiers compétent.

13.0 Modifications

La présente entente peut être modifiée moyennant le consentement écrit des représentants désignés de chaque partie.

14.0 Disposition générales

(Insérer, au besoin, d'autres clauses qui ne sont pas contraires au fondement juridique auquel se reporte chacune des parties. Les clauses peuvent traiter, notamment, de questions particulières comme le flux international de données.)

15.0 Signatures, dates de signature et annexes pertinentes

(L'article comprend les nom, titre et signature des représentants compétents de l'expéditeur et du destinataire de même que la date de la présente entente. Veiller à ce qu'un signataire de niveau suffisant représentant chaque partie signe la présente entente.)

Sixième pratique exemplaire : Contrôle et suivi

6. Surveillance et suivi

Le contrôle de l'efficacité de l'entente tient d'une pratique exemplaire. Le contrôle se présente sous forme de pistes de vérification de TI, d'autoévaluations, de vérifications, de systèmes de vérification et de techniques de mesure dont sont l'objet les engagements pris par votre administration publique aux termes de l'entente.

Dans des circonstances normales, vous ne vous chargeriez pas de vérifier les activités et les responsabilités de l'autre partie; vous vous en remettiez plutôt à l'engagement qu'elle a pris dans l'entente de se conformer à leur structure juridique et stratégique. Une autre solution consiste à obtenir la confirmation du respect des obligations au moyen de l'échange périodique des résultats d'autoévaluations et de certificats de conformité pendant la durée de l'entente. Toutefois, l'EERP doit prévoir le droit de faire enquête sur des questions intéressant l'autre partie si vous le jugez utile et le droit de résilier l'entente si vous n'êtes pas satisfait des résultats de l'enquête.

Fait à noter, le contrôle même peut poser un risque pour la vie privée s'il n'est pas effectué correctement. Assurez-vous que l'équipe responsable du contrôle possède les qualités et l'autorisation voulues et que les mesures de protection appliquées aux renseignements personnels sont également appliquées au contrôle de l'entente.

Enfin, ne manquez pas d'examiner régulièrement vos dossiers de l'EERP afin de confirmer que cette dernière repose sur des documents complets, précis et à jour et que vous appliquez des pratiques sûres de gestion de l'information (p. ex. en décrivant par écrit tout cas de divulgation).

ANNEXES

ANNEXE A : Lois sur la protection de la vie privée applicables au secteur public du Canada

Territoire	Secteur public	Santé	Municipalité
Alberta	<u><i>Freedom of Information and Protection of Privacy Act</i></u>	<u><i>Health Information Act</i></u>	
Colombie-Britannique	<u><i>Freedom of Information and Protection of Privacy Act</i></u>		
Manitoba	<u><i>Freedom of Information and Protection of Privacy Act</i></u>	<u><i>Personal Health Information Act</i></u>	
Nouveau-Brunswick	<u><i>Loi sur la protection des renseignements personnels</i></u>		
Terre-Neuve	<u><i>Access to Information and Protection of Privacy Act</i></u>		
Territoires du Nord-Ouest	<u><i>Access to Information and Protection of Privacy Act</i></u>		
Nouvelle-Écosse	<u><i>Freedom of Information and Protection of Privacy</i></u>		
Nunavut	Voir T. N.-O.		
Ontario	<u><i>Loi sur l'accès à l'information et la protection de la vie privée</i></u>	<u><i>Loi de 2004 sur la protection des renseignements personnels sur la santé</i></u>	<u><i>Loi sur l'accès à l'information municipale et la protection de la vie privée</i></u>

Territoire	Secteur public	Santé	Municipalité
Île-du-Prince-Édouard	<u><i>Freedom of Information and Protection of Privacy Act</i></u>		
Québec	<u><i>Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels</i></u>		
Saskatchewan	<u><i>Freedom of Information and Protection of Privacy Act</i></u>	<u><i>The Health Information Act</i></u>	<u><i>Local Authority Freedom of Information and Protection of Privacy Act</i></u>
Yukon	<u><i>Access to Information and Protection of Privacy Act</i></u>		
Gouvernement du Canada	<u><i>Loi sur la protection des renseignements personnels</i></u>		

Annexe B : Contexte international

Si votre administration publique désire transmettre des renseignements personnels à un gouvernement étranger, la situation est généralement considérée comme posant d'importants risques pour la vie privée. Cela s'explique du fait que les lois étrangères peuvent avoir préséance sur les lois canadiennes.

Des pays de par le monde adoptent des lois antiterroristes susceptibles de l'emporter sur le droit des particuliers à la protection de la vie privée. Cela signifie que des renseignements personnels sur des Canadiens acheminés à l'étranger peuvent être consultés à leur insu et sans leur consentement.

Les risques sont grands, de plus, car il n'existe aucune façon pratique d'assurer le respect d'une entente ou d'avoir de nouveau accès à de l'information que possède une partie récalcitrante à l'étranger ou d'en reprendre le contrôle.

Le pays partage-t-il les valeurs et les principes canadiens?

Des renseignements personnels ne doivent être communiqués qu'à des pays qui se sont engagés à les protéger. Même si c'est le cas, ce n'est pas tâche facile de saisir les tenants et aboutissants des lois étrangères sur la protection de la vie privée et de leurs exceptions.

Il est recommandé de vérifier indépendamment les garanties données par la partie qui souhaite recevoir des renseignements personnels.

Les processus et les questions d'importance dont traite le présent document peuvent également servir à l'établissement d'ententes internationales portant sur des renseignements personnels. Il est important de consulter des avocats-conseils et des spécialistes en matière de protection de la vie privée à toutes les étapes de l'élaboration d'une entente.

Clauses de protection d'ententes internationales

Même si des lois étrangères peuvent primer une clause qui interdit à un gouvernement étranger de consulter des renseignements personnels à des fins autres que celles que prévoit une entente, vous devez néanmoins envisager de l'inclure dans l'entente en tant que mesure de protection.

Pareilles clauses pourraient être formulées comme suit :

« L'accès aux renseignements personnels visés par la présente entente par une partie qui n'y est pas désignée ou à des fins qui n'y sont pas prévues est rigoureusement interdit. »

Lois provinciales influant sur le flux international de renseignements : Votre administration publique peut avoir adopté des lois qui limitent les endroits auxquels des renseignements personnels peuvent être transmis.

Par exemple, l'article 30 de la *Freedom of Information and Protection of Privacy Act* de la Colombie-Britannique, sous réserve de certaines circonstances, limite au territoire canadien le stockage de renseignements personnels et l'accès à ces derniers.

Voir à ce propos : http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm#section30.

Mise en garde : À cause de la nature complexe de l'activité, les lignes directrices n'offrent aucun libellé type concernant le flux international de données. Lorsque vous envisagez de conclure une entente internationale, consultez les lois sur la protection de la vie privée aussi bien que les avocats-conseils et les spécialistes en protection de la vie privée de votre administration publique.

Annexe C : Modèles d'EFVP et documents de référence

Gouvernement du Canada	Colombie-Britannique	Alberta	Saskatchewan	Manitoba	Ontario
<p>Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée – Cadre de gestion des risques d'entrave à la vie privée</p> <p>Modèle du rapport d'EFVP</p> <p>Outil d'apprentissage en ligne pour l'EFVP</p>	<p>Privacy Impact Assessment Process</p> <p>NOTA : L'article 69 de la FOIPA exige une EFVP.</p>	<p>Privacy Impact Assessments</p>	<p>Privacy Impact Assessments (PDF)</p>	<p>The Privacy Compliance Tool</p>	<p>Privacy Impact Assessment Guidelines</p> <p>Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act (PDF)</p>

Annexe D : Autorités responsables de la protection de la vie privée au Canada

Le site Web du Commissaire à la protection de la vie privée du Canada renvoie aux bureaux et aux organismes gouvernementaux provinciaux et territoriaux responsables de la protection de la vie privée :

http://www.privcom.gc.ca/information/comms_f.asp.

Au **gouvernement du Canada**, trois organismes s'occupent de la question :

- le Secrétariat du Conseil du Trésor, en ce qui concerne la *Loi sur la protection des renseignements personnels* et les directives en matière de politique. Les rapports de mise en œuvre et les avis connexes peuvent être consultés sur le site Web suivant du SCT : http://www.tbs-sct.gc.ca/gos-sog/atip-aiprp/index_f.asp. Les politiques peuvent être consultées à l'adresse : <http://www.tbs-sct.gc.ca>;
- Industrie Canada, en ce qui a trait aux lois fédérales sur la protection de la vie privée applicables au secteur privé (la *Loi sur la protection des renseignements personnels et les documents électroniques*), à l'adresse http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00003f.html;
- Justice Canada, à l'adresse <http://canada.justice.gc.ca/>.

Le Commissaire à la protection de la vie privée du Canada est un agent fédéral du Parlement qui exerce un rôle de surveillance des deux lois fédérales sur la protection de la vie privée : <http://www.privcom.gc.ca/>.

Annexe E : Risques d'entrave à la vie privée

Voici certains des risques courants d'entrave à la vie privée que posent les ententes d'échange de renseignements personnels.

Fondement juridique inexistant ou douteux : L'incapacité de déterminer le fondement clair d'un programme de collecte, d'utilisation ou de divulgation de renseignements personnels suscite des préoccupations profondes.

Profilage ou appariement de données : Regroupement de renseignements personnels non liés entre eux et provenant de diverses sources pour constituer de nouveaux renseignements sur une personne ou utilisation d'information sur les préférences et les habitudes d'une personne pour en tracer le profil.

Surveillance des opérations : Observation ou suivi de l'interaction d'une personne avec un ou plusieurs programmes ou services. La situation débouche normalement sur l'établissement de nouveaux renseignements personnels qui décrivent l'expérience globale qu'a une personne d'un ou de plusieurs programmes.

Identification de personnes : Pour qu'une personne ait droit à des services gouvernementaux, le bénéficiaire est généralement tenu de s'identifier et d'authentifier son identité par souci de gestion des risques pour la sécurité. Il existe des risques de surveillance là où l'utilisation d'identificateurs ou de systèmes d'identification communs facilite le partage de données, le profilage ou la surveillance des opérations. La nature et le nombre des éléments de données nécessaires pour confirmer l'identité d'une personne doivent être étalonnés en fonction du niveau de confiance nécessaire à l'exécution de l'opération.

Mesures de sécurité insuffisantes : Non-respect des normes des contrôles électroniques ou physiques de la sécurité ou des normes de sécurité de transmission, telles normes de chiffrement. Des études ont montré qu'entre 70 et 80 % des accès illicites à des bases de données sont attribuables à des personnes autorisées à accéder aux réseaux qui y conduisent, possédant des codes d'accès aux bases de données et ayant une connaissance de la valeur des données qu'elles souhaitent exploiter.

Utilisation ou divulgation d'information à des fins accessoires : Les objectifs de l'EERP, l'utilisation faite de l'information ou sa divulgation dépassent les fins initiales pour lesquelles elle a été recueillie.