Lignes directrices concernant l'évaluation de l'incidence sur la vie privée sous le régime de la Loi sur la protection des renseignements personnels sur la santé de l'Ontario

Ann Cavoukian, Ph.D.
Commissaire
Octobre 2005

Commissaire à l'information et à la protection de la vie privée / Ontario

Lignes directrices concernant l'évaluation de l'incidence sur la vie privée sous le régime de la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario

Ann Cavoukian, Ph.D.
Commissaire
Octobre 2005

Commissaire à l'information et à la protection de la vie privée / Ontario

TABLE DES MATIÈRES

1. Introduction et vue d'ensemble 4
1.1 Le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP) 4
1.2 Objet des lignes directrices concernant l'évaluation de l'incidence sur la vie privée (EIVP) 4
1.3 Qu'est-ce qu'une EIVP? 4
1.4 Avantages des EIVP 5
1.5 Méthodes d'EIVP 6
1.6 Critères à respecter pour une EIVP de haute qualité 7

2. Pour commencer 9
2.1 Êtes-vous dépositaire de renseignements sur la santé? 9
2.2 Votre système d'information, technologie ou programme est-il utilisé pour traiter des renseignements personnels sur la santé? 9
2.3 Êtes-vous un fournisseur de réseau d'information sur la santé en vertu de la *LPRPS*? 10

3. Directives sur le questionnaire 12
3.1 Structure du questionnaire 12
3.2 Champ « Remarques » ou pièces jointes 12
3.3 Gestion de la protection de la vie privée à l'échelon de l'organisme ou du projet 12
3.4 Éléments du questionnaire 13

4. Questionnaire d'évaluation de l'incidence sur la vie privée – version annotée 14
Annexe A – Modèle de questionnaire d'EIVP 27
Annexe B – Exemples de méthodes d'EIVP 37
Annexe C – Définition de « renseignements personnels sur la santé » en vertu de la *LPRPS* 38
Annexe D – Organisation de coopération et de développement économiques – Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel 39

1 INTRODUCTION ET VUE D'ENSEMBLE

1.1 Le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP)

Le gouvernement de l'Ontario a promulgué *la Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)* en vue d'assurer la protection, la confidentialité et la sécurité des renseignements personnels sur la santé de la population ontarienne dont les organismes du secteur de la santé ont la garde ou le contrôle, en régissant leur collecte, leur utilisation et leur divulgation et en exigeant que des mesures raisonnables soient prises pour en assurer la protection contre le vol, la perte et l'utilisation ou la divulgation non autorisée. Cette loi est entrée en vigueur le 1er novembre 2004. Aux termes de la *LPRPS*, le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario est responsable de surveiller la conformité à la *LPRPS*.

1.2 Objet des lignes directrices concernant l'évaluation de l'incidence sur la vie privée (EIVP)

Le CIPVP a élaboré les présentes lignes directrices concernant l'évaluation de l'incidence sur la vie privée (EIVP) pour aider les dépositaires de renseignements sur la santé à déterminer l'incidence que pourrait avoir un système d'information, une technologie ou un programme proposé [1] sur la protection des renseignements personnels sur la santé d'un particulier en vertu de la *LPRPS*. Le CIPVP recommande aux dépositaires de renseignements sur la santé qui disposent de systèmes d'information, de technologies ou de programmes importants pour le traitement des renseignements personnels sur la santé, ou qui en implantent, d'effectuer une EIVP pour identifier et réduire les risques pour la vie privée. L'EIVP est une démarche constructive dans le cadre de laquelle le dépositaire de renseignements sur la santé fait preuve de diligence raisonnable en identifiant et en réduisant les risques éventuels pour la vie privée d'un système d'information, d'une technologie ou d'un programme proposé ou existant. Cette évaluation compte désormais parmi les pratiques exemplaires de nombreux organismes du secteur de la santé dans d'autres territoires ainsi que de plusieurs dépositaires de renseignements sur la santé de l'Ontario.

Le CIPVP est conscient du fait que les dépositaires de renseignements sur la santé ne sont pas tenus de faire des EIVP en vertu de la *LPRPS*. Ceux qui s'inspirent des présentes lignes directrices pour effectuer une EIVP n'ont donc pas l'obligation d'en fournir les résultats au CIPVP pour examen aux termes de la *LPRPS*. Cependant, le CIPVP peut se servir d'une EIVP comme point de départ pour toute enquête sur une atteinte à la vie privée en vertu de cette loi.

1.3 Qu'est-ce qu'une EIVP?

Une EIVP est un outil structuré de gestion des risques qui permet d'identifier les effets réels ou éventuels d'un système d'information, d'une technologie ou d'un programme proposé ou existant sur la vie privée des particuliers, et de trouver des moyens d'atténuer ces effets. L'EIVP convient à l'évaluation des types de risques suivants :

- Les risques associés à une nouvelle technologie ou à la convergence de technologies existantes, comme un système de dossiers médicaux électroniques (DME) ou de dossiers électroniques de santé (DES);
- Les risques découlant de l'utilisation dans un nouveau contexte d'une technologie qui peut porter atteinte à la vie privée, comme l'installation d'un système de télévision en circuit fermé dans des salles d'examen médical à des fins d'éducation, ou l'enregistrement de consultations téléphoniques avec des patients;
- Les risques découlant d'un nouveau programme ou de la modification de pratiques de gestion de l'information ayant des conséquences importantes pour la vie privée, notamment une proposition d'utiliser les renseignements personnels sur la santé recueillis à des fins de traitement en vue d'élaborer une base de données à des fins de recherche, ou d'intégrer un système de DME ou de DES

1 Les termes « système d'information », « technologie » et « programme » s'entendent également des termes « application », « projet », « mécanisme », « initiative » et de tout autre terme qui désigne une démarche précise.

dans un système de prise de rendez-vous de patients;

- Les risques découlant d'anciens systèmes[2] qui ne sont pas nécessairement compatibles avec les pratiques exemplaires en matière de vie privée et de sécurité. Ces pratiques consistent notamment à vérifier l'accès aux renseignements personnels sur la santé, à accorder l'accès à ces renseignements à des utilisateurs qui en ont besoin compte tenu de leur poste, et à obliger les utilisateurs à se servir d'un nom d'utilisateur et d'un mot de passe particuliers pour accéder aux renseignements personnels sur la santé.

On a commencé à soulever la question des évaluations de l'incidence sur la vie privée dès 1989[3], et les premières lignes directrices officielles à leur sujet remontent à 1991[4]. Cependant, c'est depuis 1999 que cette pratique a commencé à se répandre, ses avantages ayant été établis et la tenue d'évaluations étant devenue obligatoire dans certaines situations. Par exemple, la *Health Information Act de l'Alberta* oblige les organismes qui comptent mettre en œuvre des pratiques administratives et des systèmes d'information aux fins de la collecte, de l'utilisation ou de la divulgation de renseignements sur la santé concernant des particuliers identifiés à fournir une EIVP au commissaire à l'information et à la protection de la vie privée de cette province, qui l'examine et fait des observations à son sujet.

1.4 Avantages des EIVP

L'EIVP comporte plusieurs avantages :

1) L'EIVP énonce les risques liés à la protection des données que les dépositaires de renseignements sur la santé sont tenus de réduire en vertu de la *LPRPS*. (Soulignons que les dépositaires de renseignements sur la santé ne sont pas tenus d'effectuer une EIVP en vertu de la LPRPS, mais qu'ils doivent prendre des mesures raisonnables dans les circonstances pour veiller à ce que les renseignements personnels sur la santé dont ils ont la garde ou le contrôle soient protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée et à ce que les dossiers qui les contiennent soient protégés contre une duplication, une modification ou une élimination non autorisée);
2) L'EIVP permet de promouvoir l'analyse systématique des questions liées à la vie privée afin de susciter un débat éclairé sur les systèmes d'information, technologies ou programmes proposés ou existants;
3) L'EIVP fait comprendre aux décideurs les risques associés à un système d'information, à une technologie ou à un programme proposé ou existant, afin qu'ils puissent éviter toute réaction négative de la part du public;
4) L'EIVP permet de déceler à l'avance les problèmes que pourrait causer un nouveau système d'information, une nouvelle technologie ou un nouveau programme, et de protéger ainsi la réputation du dépositaire de renseignements sur la santé qui compte le mettre en œuvre;
5) L'EIVP permet de tenir les proposants ou exploitants du système d'information, de la technologie ou du programme responsables de tout effet négatif éventuel sur la vie privée et des mesures à prendre pour compenser ces effets;
6) L'EIVP permet de réduire les coûts lorsqu'elle est effectuée à l'étape de l'élaboration, car il est moins coûteux d'apporter des changements pour répondre à des préoccupations en matière de vie privée, notamment en adoptant des technologies d'amélioration de la protection de la vie privée, lors de la conception et du début de la mise en œuvre, bien avant que le système, la technologie ou le programme ne soit totalement opérationnel;
7) L'EIVP constitue une source fiable de renseignements pour les dépositaires de renseignements sur la santé, les responsables de la réglementation de la protection de la

2 Un « ancien système » est une application ou un système d'information existant dans lequel un organisme a déjà investi beaucoup de temps et de ressources. Bon nombre de dépositaires de renseignements sur la santé de l'Ontario sauvegardent les renseignements personnels sur la santé des particuliers dans de tels systèmes ou applications. La plupart des nouveaux systèmes, technologies ou programmes peuvent être connectés aux anciens systèmes afin d'importer les renseignements personnels sur la santé qui s'y trouvent.

3 Voir David Flaherty, *Protecting Privacy in Surveillance Societies*, 1989, page 405.

4 Voir State of New York Public Service Commission, « Statement of Policy on Privacy in Telecommunications », 22 mars 1991, reproduit dans le mémoire du Bureau du commissaire à l'information et à la protection de la vie privée/Ontario à la Commission ontarienne des services téléphoniques intitulé *Privacy and Telecommunications*, septembre 1992.

vie privée et le public. L'EIVP doit non seulement déterminer les problèmes éventuels pour la protection de la vie privée que pourrait causer un système d'information, une technologie ou un programme proposé ou existant, mais également calmer les inquiétudes qui pourraient être soulevées à cet égard si aucune analyse crédible ou détaillée n'était effectuée;

8) Enfin, l'EIVP représente un moyen rentable pour les responsables de la réglementation de la protection de la vie privée (p. ex., les commissaires à l'information et à la protection de la vie privée) de comprendre les répercussions sur la protection des données d'un système d'information, d'une technologie ou d'un programme proposé ou existant sans qu'ils n'aient à mener eux-mêmes des études coûteuses.

1.5 Méthodes d'EIVP

Les méthodes employées pour effectuer les évaluations de l'incidence sur la vie privée varient. Certains organismes sont tenus d'adopter des méthodes précises, souvent en vertu de lois ou de politiques particulières sur la protection de la vie privée. Par exemple, le commissaire à l'information et à la protection de la vie privée de l'Alberta et le Secrétariat du Conseil de gestion de l'Ontario ont publié des lignes directrices pour aider les organismes à effectuer une EIVP. Une liste des diverses méthodes de tenue d'une EIVP figure à l'annexe B – Exemples de méthodes d'EIVP.

Les présentes lignes directrices élaborées par le CIPVP contiennent un questionnaire annoté pour les dépositaires de renseignements sur la santé qui sont assujettis à la *LPRPS*. Ce questionnaire demande deux types généraux de renseignements : ceux qui concernent les pratiques de gestion de la vie privée de l'organisme auquel appartient le dépositaire de renseignements sur la santé (10 questions) et ceux qui touchent précisément le système d'information, la technologie ou le programme (20 questions). Les politiques et procédures organisationnelles en matière de protection de la vie privée, ou leur absence, peuvent se répercuter considérablement sur la capacité du dépositaire de renseignements sur la santé de s'assurer que des systèmes d'information, technologies ou programmes précis font l'objet de mesures de protection de la vie privée. Pour cette raison, les présentes lignes directrices se concentrent non seulement sur les systèmes d'information, technologies ou programmes que le dépositaire de renseignements sur la santé décrira dans ses réponses au questionnaire, mais également sur les pratiques organisationnelles relatives aux renseignements[5] qui pourraient avoir une incidence sur la protection des renseignements personnels sur la santé de particuliers.

Les questions figurant dans les lignes directrices sont fondées sur les « pratiques exemplaires relatives aux EIVP » élaborées par des experts connus dans ce domaine, comme David Flaherty, ancien commissaire à l'information et à la protection de la vie privée de Colombie-Britannique, et Blair Stewart, commissaire adjoint à la protection de la vie privée de la Nouvelle-Zélande. En outre, la présentation et la teneur des questions[6] sont semblables à celles du questionnaire de l'EIVP produit par le commissaire à l'information et à la protection de la vie privée de l'Alberta, car on suppose que les organismes du secteur de la santé voudront, dans toute la mesure du possible, utiliser des outils qui se ressemblent d'un territoire à l'autre, d'autant plus que des renseignements personnels sur la santé seront probablement transmis de plus en plus souvent entre les provinces avec l'essor de la cybersanté [7] .

En vertu des présentes lignes directrices, les dépositaires de renseignements sur la santé doivent fournir des renseignements détaillés sur les sujets suivants :

- La gestion organisationnelle de la protection de la vie privée, y compris les politiques, les mécanismes de sécurité ainsi que la structure et l'organisation de la protection de la vie privée chez le dépositaire de renseigne-

5 Aux termes de l'article 2 de la *LPRPS*, l'expression « pratiques relatives aux renseignements », relativement à un dépositaire de renseignements sur la santé, s'entend de sa politique concernant ses actes relatifs aux renseignements personnels sur la santé, y compris a) le moment où, de façon courante, il recueille, utilise, modifie, divulgue, conserve ou élimine ces renseignements, la façon dont il le fait et les fins auxquelles il le fait; b) les mesures de précaution et pratiques d'ordre administratif, technique et matériel qu'il maintient à l'égard de ces renseignements.

ments sur la santé qui constitue le principal promoteur d'un système d'information, d'une technologie ou d'un programme proposé ou existant;

- La gestion de la protection de la vie privée dans le cadre de projets, y compris une description détaillée des éléments suivants :
    - les renseignements personnels sur la santé que traite le système d'information, la technologie ou le programme proposé ou existant;
    - les sources auprès desquelles seront obtenus ces renseignements personnels sur la santé;
    - les circonstances dans lesquelles auront lieu la collecte des renseignements personnels sur la santé;
    - le traitement des renseignements personnels sur la santé;
    - les utilisations escomptées des renseignements personnels sur la santé détenus ou produits;
    - les destinataires proposés des renseignements personnels sur la santé et l'utilisation qu'ils comptent en faire;
    - les circonstances dans lesquels auront lieu le traitement, l'utilisation et la divulgation des renseignements personnels sur la santé;
    - les mesures qui seront prises à l'égard des renseignements pour prévenir l'accès, l'utilisation, la divulgation ou la modification non autorisée et la perte;
    - les dispositions prises pour la vérification et l'application des règles.

1.6 Critères à respecter pour une EIVP de haute qualité[8]

Une EIVP de haute qualité doit contenir une description détaillée des renseignements personnels sur la santé recueillis, utilisés, divulgués et conservés au moyen du système d'information, de la technologie ou du programme proposé ou existant. L'EIVP représente en quelque sorte le portrait du système d'information, de la technologie ou du programme; elle précise pourquoi il sera ou a été mis en œuvre et comment il permet de recueillir, d'utiliser, de divulguer et de conserver des renseignements personnels sur la santé. Grâce à l'EIVP, il est possible de découvrir et de tenter de régler des problèmes précis en matière de protection de la vie privée de façon exhaustive, en se fondant sur une réflexion éclairée et des renseignements précis.

Dans ce contexte, une EIVP de haute qualité doit s'appuyer sur une perspective critique afin de mettre en évidence les risques pour la vie privée qui sont associés à un système d'information, à une technologie ou à un programme proposé ou existant. Il arrive parfois qu'une EIVP néglige certains risques pour la vie privée ou minimise leur importance par crainte de freiner les « progrès », surtout lorsqu'elle est menée par du personnel interne qui pourrait avoir un intérêt important dans la réussite de l'élaboration ou du fonctionnement du système d'information, de la technologie ou du programme du dépositaire de renseignements sur la santé. Cependant, une EIVP de haute qualité doit être fondée sur une perspective éclairée et critique afin de décrire le fonctionnement réel d'un système d'information, d'une technologie ou d'un programme proposé ou existant, les risques qu'il comporte pour la vie privée et la façon dont il serait possible de réduire ces risques. Une telle description permet sou-

6 Les lignes directrices sur les EIVP du Bureau du commissaire à l'information et à la protection de la vie privée/Ontario sont adaptées à la *LPRPS*. Celles qui émanent du commissaire à l'information et à la protection de la vie privée de l'Alberta, quant à elles, sont destinées à tous les organismes publics assujettis à la *Health Information Act* et aux lois touchant la protection de la vie privée dans le secteur public au palier municipal et provincial..

7 Le CIPVP tient à remercier Frank Work, commissaire à l'information et à la protection de la vie privée de l'Alberta, de lui avoir permis de modifier le questionnaire d'évaluation concernant l'incidence sur la vie privée qu'il a produit afin de l'adapter à la *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario.

8 La présente section s'inspire des travaux de David Flaherty, décrits dans son document inédit sur les critères d'EIVP pour Inforoute Santé du Canada Inc. (mars 2005). Le CIPVP l'en remercie.

vent de prévoir et d'éviter les incidents d'atteinte à la vie privée et d'aider les organismes de surveillance des questions touchant la protection de la vie privée (p. ex., le conseil d'administration, les cadres supérieurs ou la commissaire) de mieux comprendre les avantages et les risques de systèmes d'information, de technologies ou de programmes particuliers.

Une EIVP de haute qualité devrait également rendre compte avec exactitude des normes de protection des renseignements personnels sur la santé que doivent respecter les dépositaires de renseignements sur la santé qui sont assujettis à la *LPRPS* (ou à une autre loi, si le système d'information, la technologie ou le programme divulgue des renseignements personnels sur la santé à l'extérieur de l'Ontario). Cependant, le CIPVP souligne aussi que les dépositaires de renseignements sur la santé peuvent effectuer une EIVP pour des raisons autres que la simple conformité à la loi. Par exemple, les attentes des patients ou des clients en matière de vie privée peuvent justifier la tenue d'une EIVP, même lorsque le dépositaire de renseignements sur la santé est persuadé que son système d'information, sa technologie ou son programme est conforme à la *LPRPS*.

Pour les raisons que nous avons mentionnées plus haut, les présentes lignes directrices prévoient deux formes de réponses. Les cases à cocher permettent de répondre rapidement aux questions posées. Le champ « Remarques » permet de fournir les précisions que l'auteur de l'EIVP juge appropriées. En outre, le questionnaire comporte une colonne où il est possible d'inscrire des renvois vers des pièces jointes fournies en complément pour certaines réponses. La préparation d'une EIVP efficace et informative nécessite un dialogue entre son auteur et les promoteurs, concepteurs, développeurs et utilisateurs du système d'information, de la technologie ou du programme proposé ou existant. Les présentes lignes directrices visent à faciliter ce dialogue.

2 POUR COMMENCER

La tenue d'une EIVP est considérée comme une pratique exemplaire en matière de protection de la vie privée pour les organismes qui disposent de systèmes d'information, de technologies ou de programmes importants pour traiter des renseignements personnels, ou qui comptent en adopter. Les présentes lignes directrices sont destinées spécialement aux dépositaires de renseignements sur la santé qui sont assujettis à la *LPRPS* et qui sont dans cette situation. Pour profiter au maximum des présentes lignes directrices, vous voudrez d'abord déterminer si la *LPRPS* s'applique à votre organisme (voir la question 2.1 ci-dessous) et, deuxièmement, si le système d'information, la technologie ou le programme proposé ou existant sert ou servira au traitement de renseignements personnels sur la santé (voir la question 2.2). Enfin, vous voudrez déterminer si votre organisme compte ou non parmi ceux qui, aux termes de la *LPRPS*, doivent effectuer une EIVP (voir la question 2.3 ci-dessous).

2.1 Êtes-vous dépositaire de renseignements sur la santé?

La *LPRPS* s'applique aux dépositaires de renseignements sur la santé qui ont recueilli des renseignements personnels sur la santé le 1er novembre 2004 ou après, et à ceux qui utilisent ou divulguent des renseignements personnels sur la santé après cette date. Elle s'applique également aux personnes et aux organismes qui ne sont pas dépositaires de renseignements sur la santé mais qui ont reçu des renseignements personnels sur la santé de la part d'un dépositaire.

Question 2.1 : Êtes-vous dépositaire de renseignements sur la santé? La *LPRPS* définit un « dépositaire de renseignements sur la santé » comme étant une personne ou une organisation énumérée au paragraphe 3 (1) qui a la garde ou le contrôle de renseignements personnels sur la santé.

Parmi les exemples de dépositaires de renseignements sur la santé énumérés au paragraphe 3 (1), mentionnons les praticiens de la santé ou quiconque exploite un cabinet de groupe de praticiens de la santé qui fournissent des soins de santé, les hôpitaux, les établissements psychiatriques, les établissements de soins de longue durée, les centres d'accès aux soins communautaires, les pharmacies, les laboratoires, les services d'ambulance et les conseils de santé.

2.2 Votre système d'information, technologie ou programme est-il utilisé pour traiter des renseignements personnels sur la santé?

Les présentes lignes directrices ont pour but d'aider les dépositaires de renseignements sur la santé à identifier et à gérer les risques pour la protection de la vie privée qui sont associés à des systèmes d'information, technologies ou programmes existants qui sont utilisés pour traiter des renseignements personnels sur la santé au sens de la *LPRPS*.

Question 2.2 : Votre système d'information, technologie ou programme proposé ou existant sert-il ou servira-t-il à traiter des renseignements personnels sur la santé visés par la *LPRPS*? ? Les renseignements personnels sur la santé sont des renseignements identificatoires concernant un particulier qui se présentent sous forme verbale ou autre forme consignée si, selon le cas :

(i) ils ont trait à la santé physique ou mentale du particulier;

(ii) ils ont trait à la fourniture de soins de santé, notamment à l'identification d'une personne comme fournisseur de soins de santé;

(iii) ils constituent un programme de services au sens de la *Loi de 1994 sur les soins de longue durée*;

(iv) ils ont trait au don d'une partie du corps ou de substances corporelles;

(v) ils ont trait aux paiements relatifs aux soins de santé fournis au particulier ou à son admissibilité à ces soins;

(vi) ils sont un numéro de carte Santé;

(vii) ils permettent d'identifier le mandataire spécial d'un particulier;

(viii) ils sont un dossier qui contient l'un ou l'autre des renseignements précédents.

Les renseignements personnels sur la santé ne comprennent pas les dossiers de renseignements sur un employé ou un mandataire du dépositaire de renseignements sur la santé, à moins que ces dossiers soient tenus essentiellement pour la fourniture de soins de santé à cet employé ou mandataire. En outre, la *LPRPS* ne s'applique pas à tous les renseignements personnels sur la santé, mais uniquement à ceux qui sont (i) recueillis, utilisés ou divulgués par des dépositaires de renseignements sur la santé ou (ii) utilisés ou divulgués par des personnes qui reçoivent des renseignements personnels sur la santé de la part de dépositaires de renseignements sur la santé. Voir l'annexe C pour la définition complète de « renseignements personnels sur la santé » qui figure dans la *LPRPS*.

2.3 Êtes-vous un fournisseur de réseau d'information sur la santé en vertu de la *LPRPS*?

Le CIPVP reconnaît que la *LPRPS* n'oblige pas la tenue d'évaluations de l'incidence sur la vie privée à moins que l'organisme concerné soit un « fournisseur de réseau d'information sur la santé », qui est défini comme étant une personne (ou un organisme) « qui fournit des services à deux dépositaires de renseignements sur la santé ou plus principalement dans le but de leur permettre d'utiliser des moyens électroniques pour se divulguer entre eux des renseignements personnels sur la santé, que cette personne soit ou non mandataire de n'importe lequel d'entre eux[9] ». L'Agence des systèmes intelligents pour la santé de l'Ontario est un exemple de fournisseur de réseau d'information sur la santé au sens de la *LPRPS*.

Si vous êtes fournisseur de réseau d'information sur la santé, vous devez respecter le paragraphe 6 (3) du Règlement de l'Ontario 329/04 pris en application de la *LPRPS*, qui prévoit notamment ce qui suit :

« Le fournisseur évalue les services qui ont été fournis aux dépositaires de renseignements sur la santé concernés à l'égard des points suivants et remet à chacun d'eux une copie des résultats obtenus :

i. les menaces, la vulnérabilité et les risques qui existent en matière de protection et d'intégrité des renseignements personnels sur la santé,
ii. l'impact possible des services sur la vie privée des particuliers que concernent les renseignements. »

Le fournisseur de réseau d'information sur la santé n'est pas tenu de fournir une copie de son EIVP au CIPVP. Il doit toutefois respecter d'autres exigences figurant au paragraphe 6 (3) du Règlement 329/04 pris en application de la *LPRPS* :

- aviser chaque dépositaire de renseignements sur la santé concerné à la première occasion raisonnable s'il a eu accès à des renseignements personnels sur la santé ou en a utilisés, divulgués ou éliminés d'une façon qui n'est pas conforme au règlement;
- remettre à chaque dépositaire de renseignements sur la santé concerné une description claire des services qu'il lui fournit, y compris une description générale des mesures de précaution qui ont été mises en place pour éviter une utilisation et une divulgation non autorisées des renseignements personnels sur la santé;
- mettre à la disposition du public une description claire des services qu'il lui fournit, y compris une description générale des mesures de précaution qui ont été mises en place pour éviter une utilisation et une divulgation non autorisées, ainsi que les directives, lignes directrices et politiques qui s'appliquent à ces services;
- tenir un dossier électronique contenant tous les cas d'accès à des renseignements personnels sur la santé confiés au dépositaire de renseignements sur la santé ou de transfert de tels renseignements, et le mettre à la disposition du dépositaire;
- veiller à ce que les tiers engagés pour l'aider à fournir des services satisfont aux restrictions et aux conditions nécessaires pour lui permettre de se conformer au présent article;

9 *Loi de 2004 sur la protection des renseignements personnels sur la santé*, Règlement de l'Ontario 329/04, paragraphe 6 (2).

- Conclure avec chaque dépositaire de renseignements sur la santé un accord écrit qui décrit les services fournis ainsi que les mesures de précaution d'ordre administratif, technique et physique qui existent afin d'assurer le caractère confidentiel et la protection des renseignements, et qui exige que le fournisseur se conforme à la *LPRPS* et à son règlement d'application.

Comme nous l'avons déjà souligné, le CIPVP recommande fortement aux dépositaires de renseignements sur la santé de soumettre à une EIVP les systèmes d'information, technologies ou programmes proposés ou importants qui servent au traitement de renseignements personnels sur la santé afin d'identifier et de réduire les risques pour la vie privée, *même s'ils ne sont pas fournisseurs de réseau d'information sur la santé*, ceux-ci étant obligés de mener une EIVP en vertu de la *LPRPS*. Les présentes lignes directrices seront utiles aux dépositaires de renseignements sur la santé à cette fin.

3 DIRECTIVES SUR LE QUESTIONNAIRE

3.1 Structure du questionnaire

Si vous avez déterminé que votre organisme est dépositaire de renseignements sur la santé et que le système d'information, la technologie ou le programme proposé ou existant en question sert au traitement de renseignements personnels sur la santé au sens de la *LPRPS* (voir les sections 2.1 et 2.2 ci-dessous), vous êtes maintenant prêt à remplir le questionnaire d'EIVP.

Il y a deux types de questions dans le questionnaire. Premièrement, le dépositaire de renseignements sur la santé doit cocher des cases pour fournir l'une ou l'autre des réponses suivantes :

- « Oui »
- « En cours »
- « Non »
- « S.o./n.d. » (sans objet/non disponible)

Deuxièmement, le champ « Remarques » permet au dépositaire de renseignements sur la santé de préciser sa réponse au besoin. En outre, le questionnaire comporte une colonne où il est possible d'inscrire des renvois vers des pièces jointes fournies en complément pour certaines réponses. Il pourrait s'agir de documents sur le système d'information, la technologie ou le programme, comme une analyse de rentabilisation, le mandat du projet, les caractéristiques techniques, des extraits des manuels du système et d'entrevues avec du personnel pertinents, y compris des fournisseurs s'il y a lieu. Ces renseignements devraient être indiqués dans la colonne « Pièces jointes ». Le dépositaire de renseignements sur la santé peut se servir du champ « Remarques » ou de pièces jointes, ou encore des deux. Le questionnaire peut être rempli sur papier ou par voie électronique (voir l'annexe A – Modèle de questionnaire d'EIVP).

3.2 Champ « Remarques » ou pièces jointes

Il importe peu que vous décidiez de répondre aux questions dans le champ « Remarques » ou en joignant des pièces. Cependant, vous ne devez pas vous contenter de cocher « Oui », « Non », « En cours » ou « s.o./n.d. ». En d'autres mots, vous pouvez remplir le champ « Remarques », joindre des documents ou les deux, mais NON cocher simplement les cases sans motiver vos choix. Une EIVP bien faite doit non seulement indiquer clairement comment les renseignements personnels sur la santé visés par un système d'information, une technologie ou un programme seront recueillis, utilisés, divulgués, conservés et protégés, mais également pourquoi ils le seront par les moyens indiqués, et quelles pratiques générales de gestion de la protection de la vie privée ont été adoptées à l'échelon de l'organisme pour étayer ces choix. Dans la plupart des cas, il suffit de fournir des renseignements supplémentaires dans le champ « Remarques » ou dans un document joint pour répondre à cette exigence.

3.3 Gestion de la protection de la vie privée à l'échelon de l'organisme ou du projet

Le questionnaire est divisé en deux parties : la partie A, Gestion de la protection de la vie privée à l'échelon de l'organisme, et la partie B, Gestion de la protection de la vie privée à l'échelon du projet. La partie A porte sur l'ensemble des pratiques relatives aux renseignements du dépositaire de renseignements, alors que la partie B a trait aux caractéristiques relatives à la protection de la vie privée du système d'information, de la technologie ou du programme proposé ou existant qui fait l'objet de l'EIVP. Après que le dépositaire de renseignements sur la santé aura rempli l'ensemble du questionnaire pour un système d'information, une technologie ou un projet particulier, il suffira normalement, pour les EIVP futures, de revoir la partie A pour en maintenir l'exactitude, au lieu de la reprendre à partir de zéro.

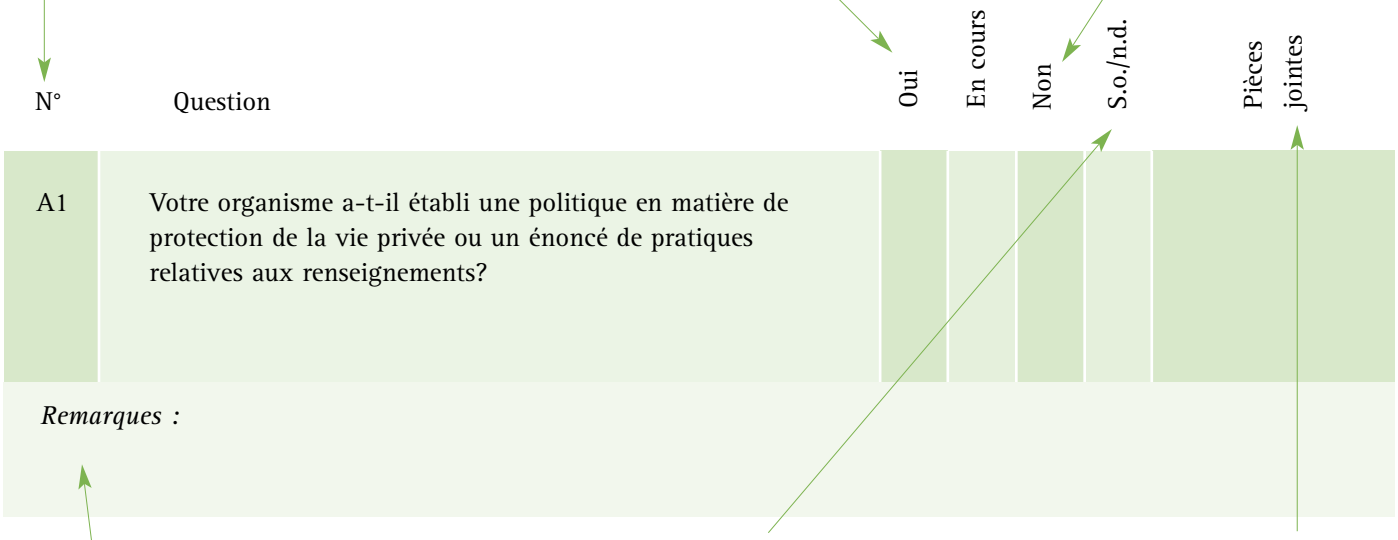
3.4 Éléments du questionnaire

Partie du questionnaire et numéro de la question.

Cochez la case de cette colonne si vous répondez « Oui », puis expliquez votre réponse dans le champ « Remarques » ou indiquez dans le champ « Pièces jointes » les documents où se trouvent des renseignements supplémentaires.

Cochez la case de cette colonne si vous êtes en voie de déterminer votre réponse. Assurez-vous d'expliquer ce choix.

Cochez la case de cette colonne si vous répondez « Non », puis expliquez votre réponse dans le champ « Remarques » ou au moyen de documents joints.



Comme nous l'avons déjà mentionné, il est important d'expliquer votre réponse dans la mesure du possible. Vous pouvez le faire dans le champ « Remarques ». Si vous utilisez la version électronique du questionnaire d'EIVP, il vous suffit de sélectionner ce champ et d'inscrire vos explications. Ce champ est d'une taille illimitée. Si vous utilisez la version sur papier, vous devrez probablement joindre des pages supplémentaires.

Cochez la case de cette colonne si la question ne s'applique pas à votre organisme ou au système d'information, à la technologie ou au programme en question, ou si les renseignements demandés ne sont pas disponibles. Assurez-vous de fournir des explications.

Indiquez dans ce champ le numéro ou l'indicatif quelconque d'une pièce jointe ou d'une partie d'une pièce jointe qui complète votre réponse. Chaque pièce jointe devrait être mentionnée au moins une fois dans le questionnaire. Le renvoi doit être précis (p. ex., indiquez le numéro de page s'il y a lieu). En règle générale, les documents joints devraient comprendre une description des pratiques relatives aux renseignements ou des politiques de protection de la vie privée de votre organisme, des déclarations publiques, des documents pertinents sur des projets (comme les mandats et des diagrammes de cheminement des données) ainsi que des extraits pertinents du plan stratégique de gestion de l'information ou de technologie de l'information (GI/TI) de votre organisme.

4 QUESTIONNAIRE D'ÉVALUATION DE L'INCIDENCE SUR LA VIE PRIVÉE (VERSION ANNOTÉE) [10]

En plus de vos réponses au questionnaire ci-dessous, votre EIVP devrait comprendre les renseignements suivants :

- Le nom du système d'information, de la technologie ou du programme qui fait l'objet de l'EIVP;
- La date à laquelle l'auteur de l'EIVP remplit le questionnaire[11] ;
- Le nom du dépositaire de renseignements sur la santé qui a la responsabilité ou le contrôle du système d'information, de la technologie ou du programme;
- Les coordonnées de l'auteur de l'EIVP, y compris ses nom, titre, adresse postale, numéros de téléphone et de télécopieur et adresse électronique. Il est particulièrement important d'inclure ces renseignements dans l'EIVP si celle-ci sera passée en revue par des intervenants de l'extérieur, comme d'autres dépositaires de renseignements sur la santé, des patients ou clients ou encore d'autres représentants de la collectivité. La personne-ressource devrait être en mesure de répondre à des questions précises sur l'EIVP ou de renvoyer le demandeur à une personne qui peut le faire.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	N'oubliez pas d'indiquer la section ou les pages pertinentes dans la colonne « Pièces jointes » quand vous joignez des documents. Pour faciliter la consultation, vous pourriez numéroter les pages de vos documents. Il est particulièrement important de le faire si des intervenants de l'extérieur passeront en revue votre EIVP, car ils seront probablement moins au fait des particularités du système d'information, de la technologie ou du programme proposé.					
	Partie A : Gestion de la protection de la vie privée à l'échelon de l'organisme Les questions de cette section ont trait à la gestion de la protection de la vie privée dans l'ensemble de votre **organisme**. Elles ne se limitent pas au système d'information, à la technologie ou au programme. Des questions précises sur le système d'information, la technologie ou le programme sont posées à la partie B.					
	Politiques et mécanismes de contrôle en matière de vie privée					
A1	Existe-t-il un plan stratégique ou un plan d'entreprise qui aborde la protection de la vie privée?					

[10] Un modèle vierge de questionnaire d'EIVP figure à l'annexe A.

[11] De l'avis de la commissaire, l'EIVP n'est jamais définitive. Elle représente un document dynamique qui devrait être mis à jour régulièrement en fonction des changements que l'on compte apporter au système d'information, à la technologie ou au programme.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	Remarques : Souvent, les dépositaires de renseignements sur la santé abordent les questions touchant la protection de la vie privée dans leurs plans de gestion de l'information ou de technologie de l'information. Certains dressent également des plans d'entreprise ou des plans stratégiques à l'échelon des sections; si ces plans abordent la protection de la vie privée, ils peuvent également être joints (p. ex., un plan d'entreprise pour un nouveau système d'information sur la santé, un nouveau service clinique, une nouvelle initiative de financement ou un nouveau programme de recherche pourrait comprendre des renseignements concernant la protection de la vie privée).					
A2	Votre organisme a-t-il établi une politique en matière de protection de la vie privée ou un énoncé de pratiques relatives aux renseignements?					
	Remarques : Contrairement à la question A1, qui porte sur les plans touchant l'ensemble de l'organisme qui comprennent des mesures de protection de la vie privée, cette question porte sur les énoncés de politiques ou de mission qui touchent particulièrement les pratiques de traitement de l'information et de protection de la vie privée de votre organisme. Ces documents sont généralement des politiques ou chartes relatives à la protection de la vie privée ou aux renseignements, et sont requis en vertu de l'article 10 de la *LPRPS*. Les documents que vise cette question s'appliquent généralement à tout l'organisme, et non à un service ou à un projet particulier.					
A3	Des politiques ou procédures de protection de la vie privée ont-elles été élaborées concernant divers aspects des activités de l'organisme?					
	Remarques : Cette question porte sur les politiques ou procédures de protection de la vie privée qui s'appliquent à des aspects précis des activités de l'organisme. Ces politiques ou procédures, le cas échéant, se distinguent généralement des politiques ou chartes de protection de la vie privée qui s'appliquent à l'ensemble de l'organisme, et que vise la question A2. Les politiques ou procédures de protection de la vie privée qui s'appliquent à des aspects précis des activités de l'organisme peuvent s'insérer dans le cadre général des politiques ou procédures visées par la question A2. Si c'est le cas, veuillez indiquer, dans le champ « Pièces jointes », où ce trouvent ces renseignements dans les documents joints.					
A4	Les politiques et procédures de protection de la vie privée mentionnées en réponse aux questions A2 et A3 respectent-elles les critères suivants? • Les renseignements personnels sur la santé sont recueillis conformément à la *LPRPS* et aux autres lois pertinentes; • Le consentement du particulier est obtenu conformément à l'article 18 de la *LPRPS*, s'il y a lieu;					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	• Une déclaration publique écrite des pratiques relatives aux renseignements de l'organisme, comprenant le nom d'une personne-ressource avec qui communiquer pour obtenir des renseignements sur la protection de la vie privée ou porter plainte, et la façon dont on peut avoir accès à un dossier de renseignements personnels sur la santé ou en demander la rectification, est mise à la disposition du public tel qu'indiqué à l'article 16 de la *LPRPS*; • Un particulier a le droit d'avoir accès aux renseignements personnels sur la santé qui le concernent et d'en demander la rectification en vertu des articles 52 à 55 de la *LPRPS*, sous réserve de certaines exceptions; • Il existe un calendrier de conservation des dossiers de renseignements personnels sur la santé indiquant la durée minimum et maximum de conservation ainsi que des procédures de destruction sécurisée de ces renseignements.					

Remarques : Cette question a trait à plusieurs aspects importants du contenu de diverses politiques ou procédures qui ont peut-être été abordées en réponse aux questions A2 et A3. Les critères précédents sont des éléments importants de la *LPRPS* et sont généralement reconnus comme étant des pratiques équitables en matière de renseignements.

A5	L'organisme prend-il des mesures de précaution d'ordre administratif, technique et matériel pour protéger les renseignements personnels sur la santé contre le vol, la perte, l'utilisation ou la divulgation non autorisée ainsi que contre la duplication, la modification ou l'élimination non autorisée en vertu de l'article 12 de la *LPRPS*?					

Remarques : Cette question vise à déterminer si votre organisme prend les mesures de précaution d'ordre administratif, physique et matériel qui sont requises pour minimiser les risques d'atteinte à la vie privée et protéger la confidentialité et l'intégrité des renseignements personnels sur la santé. Si votre organisme a élaboré un plan ou une politique de sécurité des renseignements, vous devriez en joindre une copie en réponse à cette question.

***Si votre organisme adhère à une norme reconnue de l'industrie ou du gouvernement pour assurer la sécurité des renseignements, comme la norme ISO 17799, vous devriez décrire cette norme dans vos explications et indiquer si votre organisme a obtenu la certification.*

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	Structure et organisation des mesures de protection de la vie privée					
A6	Existe-t-il une personne-ressource responsable de la protection de la vie privée dans votre organisme?					

Remarques : Si personne n'a été désigné responsable des questions touchant la protection de la vie privée dans votre organisme, cochez « Non ». Cependant, soulignons que l'article 15 de la *LPRPS* oblige les dépositaires de renseignements sur la santé à désigner une personne-ressource responsable de la protection de la vie privée. Si votre organisme en a une, vous devez préciser dans le champ « Remarques » le poste à qui est confiée la responsabilité générale des questions touchant la vie privée (p. ex., directeur général de la protection de la vie privée, directeur général de l'information).

A7	Existe-t-il un processus permettant d'informer la direction de l'organisme au sujet des questions touchant la conformité aux règles de protection de la vie privée?					

Remarques : Si une politique ou une procédure a été adoptée pour rendre compte des questions touchant la conformité aux règles de protection de la vie privée, vous devriez en joindre une copie à votre EIVP. Sinon, vous devriez indiquer le palier de direction qui serait informé d'infractions alléguées ou confirmées à la *LPRPS* ou à d'autres lois ou politiques en vigueur en matière de protection de la vie privée, ainsi que la façon dont il serait informé et le moment où cette situation lui serait signalée.

A8	Des cadres supérieurs participent-ils activement à l'élaboration, à la mise en œuvre ou à la promotion du programme de protection de la vie privée de votre organisme?					

Remarques : Si des cadres supérieurs contribuent au programme de protection de la vie privée de votre organisme, vous devriez décrire la nature de cette participation. Si votre organisme dispose des services d'une personne-ressource responsable de la protection de la vie privée, décrivez également sa situation dans la hiérarchie de l'organisme, en précisant la mesure dans laquelle elle collabore avec les cadres supérieurs.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
A9	Les employés ou mandataires qui ont accès à des renseignements personnels sur la santé dans votre organisme reçoivent-ils une formation sur la protection de la vie privée?					

Remarques : Cette question porte surtout sur la formation générale dispensée au sein de l'organisme, notamment l'orientation du nouveau personnel et la formation générale sur la *LPRPS*, mais également sur des mesures de précaution, notamment le fait d'obliger les employés ou mandataires à signer des ententes de confidentialité comme condition d'emploi. Si votre organisme n'offre aucune formation sur la protection de la vie privée, cochez « Non ». Cependant, n'oubliez pas que l'une des responsabilités de la personne-ressource en matière de protection de la vie privée de votre organisme (voir la question A6) consiste à veiller à ce que les mandataires soient bien informés de leurs obligations en vertu de la *LPRPS*. Votre EIVP devrait mentionner toute formation sur la protection de la vie privée que reçoivent les employés ou mandataires de votre organisme. Des renseignements sur la formation relative au système d'information, à la technologie ou au programme doivent être fournis en réponse à la question B15. Dans votre réponse, précisez la durée et la fréquence de la formation, les catégories d'employés ou de mandataires qui la reçoivent et la façon dont votre organisme documente le fait qu'un employé ou un mandataire l'a reçue.

A10	Des politiques et des procédures ont-elles été élaborées pour gérer les atteintes à la vie privée, notamment en ce qui concerne la notification des personnes dont la confidentialité des renseignements personnels sur la santé a été violée?					

Remarques : Cette question a trait au processus qui s'enclenche après que l'on a déterminé qu'il y a eu utilisation ou divulgation inappropriée de renseignements personnels sur la santé. Ces politiques précisent généralement les structures de rapport et de reddition de comptes dans les circonstances ainsi que les modalités de notification des particuliers dont les renseignements personnels sur la santé sont visés par l'atteinte à la vie privée. Le paragraphe 12 (2) de la *LPRPS* oblige les dépositaires de renseignements sur la santé à aviser les particuliers concernés à la première occasion raisonnable en cas de vol ou de perte de leurs renseignements personnels sur la santé ou d'accès à ceux-ci par des personnes non autorisées.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	Part B: Gestion de la protection de la vie privée à l'échelon du projet **Les questions de cette partie ont trait au système d'information, à la technologie ou au programme.**					
B1	Un sommaire du système d'information, de la technologie ou du programme proposé ou existant a-t-il été préparé, avec une description de ses exigences et de la façon dont il répond ou répondra aux besoins établis?					

Remarques : Il importe de fournir ces renseignements, qui représentent la raison d'être du système d'information, de la technologie ou du programme proposé ou existant. Ils sont généralement contenus dans la charte de projet de ce dernier ou encore dans un plan de projet, une évaluation des besoins ou un autre document expliquant pourquoi le système d'information, la technologie ou le programme a été ou sera implanté.

B2	A-t-on dressé une liste de tous les renseignements personnels sur la santé ou de toutes les données qui sont ou seront recueillis, utilisés ou divulgués par l'entremise du système d'information, de la technologie ou du programme proposé ou existant?					

Remarques : Ces renseignements sont importants parce qu'ils illustrent la portée et la nature des renseignements personnels sur la santé qui seront traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant.

B3	Des diagrammes ont-ils été tracés pour illustrer le cheminement des renseignements personnels sur la santé dans le système d'information, la technologie ou le programme proposé ou existant?					

Remarques : Il existe de nombreuses façons de préparer des diagrammes de cheminement des données, et il faut fonder son choix en partie sur la nature du système d'information, de la technologie ou du programme. Le diagramme devrait illustrer comment les renseignements personnels sur la santé sont recueillis dans le système d'information, la technologie ou le programme proposé ou existant, comment ils y circulent et comment ils sont diffusés au-delà.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B4	Des documents ont-ils été préparés en vue de préciser les personnes, postes ou catégories d'employés qui ont accès aux différents éléments ou dossiers de renseignements personnels sur la santé?					

Remarques : Ces documents sont importants pour illustrer l'application du principe fondé sur le besoin de savoir contenu dans la *LPRPS* et compléter le diagramme de cheminement des données demandé à la question B3. Dans certains cas, il pourrait être possible d'intégrer ces renseignements dans ce diagramme; si vous l'avez fait, vous devriez en prendre note dans votre réponse à la présente question et à la question B3.

B5	La collecte, l'utilisation et la divulgation de renseignements personnels sur la santé par l'entremise du système d'information, de la technologie ou du programme proposé ou existant s'appuient-elles avant tout sur le consentement du particulier ou d'un mandataire spécial autorisé?					

Remarques : En vertu de la *LPRPS*, il existe plusieurs situations où le consentement du particulier n'est pas nécessaire pour recueillir, utiliser ou divulguer des renseignements personnels sur la santé (voir les articles 36 à 50 de la *LPRPS*). Si la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé **ne s'appuient pas** sur le consentement du particulier, votre EIVP doit préciser en vertu de quoi elles sont effectuées.

B6	Avez-vous documenté les fins auxquelles seront recueillis, utilisés ou divulgués les renseignements personnels sur la santé par l'entremise du système d'information, de la technologie ou de programme?					

Remarques : Votre EIVP devrait comprendre tout document qui énonce clairement les fins auxquelles seront recueillis, utilisés ou divulgués des renseignements personnels sur la santé. Si ces documents ont été fournis en réponse à d'autres questions, vous pouvez fournir un renvoi. Cette question est associée également à la question B5, car si la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé s'appuie sur le consentement du particulier, l'alinéa 18 (1) b) de la *LPRPS* prévoit que ce consentement doit être éclairé, c'est-à-dire, comme l'indique le paragraphe 18 (5), qu'il doit être raisonnable dans les circonstances de croire que le particulier **connaît les fins** visées par la collecte, l'utilisation ou la divulgation de ses renseignements personnels sur la santé, selon le cas.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B7	Des renseignements personnels sur la santé sont-ils recueillis, utilisés, divulgués ou conservés uniquement aux fins précisées et à des fins qu'un particulier considérerait comme étant raisonnablement conformes à ces fins?					

Remarques : Si vous avez coché « Oui », vous n'aurez probablement pas à fournir de précisions. Si vous avez coché « En cours » ou « Non », vous devriez fournir des explications et décrire dans votre EIVP les mesures que vous prendrez pour vous assurer que la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé sont conformes aux fins précisées. Soulignons que le paragraphe 10 (2) de la *LPRPS* oblige les dépositaires de renseignements sur la santé à se conformer à leurs pratiques relatives aux renseignements.

B8	Les renseignements personnels sur la santé traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant seront-ils associés ou recoupés avec d'autres renseignements traités au moyen d'autres systèmes d'information, technologies ou programmes?					

Remarques : Si vous cochez « Oui » en réponse à cette question, vous devriez indiquer comment cette association ou ce recoupement sera effectué, qui a la garde du système d'information, de la technologie ou du programme qui fait l'objet de l'EIVP et pourquoi cette association ou ce recoupement est nécessaire, ainsi que les conséquences qui s'ensuivraient s'il était impossible. Aux fins du présent questionnaire, « association » s'entend de la création d'un nouveau dossier combiné à partir de deux ou plusieurs dossiers distincts de renseignements personnels sur la santé au moyen d'un identificateur, et « recoupement » s'entend de l'identification d'un dossier de renseignements personnels sur la santé au moyen de l'identificateur d'un autre dossier, sans la création d'un nouveau dossier.

B9	Les renseignements personnels sur la santé recueillis ou utilisés par l'entremise du système d'information, de la technologie ou du programme seront-ils divulgués à des personnes qui ne sont pas des employées ou des mandataires de l'organisme responsable?					

Remarques : Si vous répondez « Non » à cette question, c'est que le système d'information, la technologie ou le programme sert à traiter des renseignements personnels sur la santé aux fins internes d'un seul dépositaire de renseignements sur la santé. Il n'est pas utilisé par plusieurs dépositaires, ou les renseignements ne sont pas diffusés vers des intervenants autres que le dépositaire. Soulignons que le fournisseur peut être un **« fournisseur de réseau d'information sur la santé »** (voir la section 2.3) s'il fournit le système d'information, la technologie ou le programme essentiellement à des dépositaires qui s'en serviront pour se transmettre par voie électronique des renseignements personnels sur la santé, que ce fournisseur soit ou non un mandataire de l'un ou l'autre des dépositaires.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B10	Avez-vous pris des dispositions pour assurer la divulgation complète des fins auxquelles les renseignements personnels sur la santé seront recueillis par l'entremise du système d'information, de la technologie ou du programme?					

Remarques : La divulgation des fins auxquelles serviront les renseignements personnels sur la santé représente une mesure importante de protection de la vie privée, surtout lorsqu'il faut obtenir le consentement des particuliers, et elle est obligatoire en vertu de la *LPRPS*. Dans vos explications, vous devez préciser les mesures qui seront prises pour divulguer ces fins aux particuliers concernés par le système d'information, la technologie ou le programme (p. ex., les patients ou les clients). Aux termes de la *LPRPS*, il est possible d'obtenir un consentement éclairé (voir la question B6 plus haut) en partie en affichant ou rendant accessible un avis des fins auxquelles les renseignements personnels sur la santé seront recueillis, utilisés ou divulgués, tel que décrit au paragraphe 18 (6) de la *LPRPS*.

B11	Des produits ou un plan de communication ont-ils été élaborés pour expliquer en détail le système d'information, la technologie ou le programme aux particuliers et la façon dont les renseignements personnels sur la santé qui les concernent seront protégés?					

Remarques : Pour que les particuliers dont les renseignements personnels sur la santé seront recueillis, utilisés ou divulgués par l'entremise du système d'information, de la technologie ou du programme aient confiance dans ce dernier, il est souhaitable de les informer des mesures de précaution d'ordre technique, administratif et matériel qui seront prises afin de protéger leur vie privée et la confidentialité des renseignements personnels sur la santé qui les concernent.

B12	Le système d'information, la technologie ou le programme proposé ou existant permettra-t-il de recueillir, d'utiliser ou de divulguer des renseignements personnels sur la santé au-delà des frontières de l'Ontario?					

Remarques : La circulation transnationale de renseignements personnels sur la santé soulève un certain nombre de questions particulières en matière de vie privée, notamment l'application de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* et de la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada, la légalité des dispositions contractuelles visant à protéger la vie privée et l'équivalence des lois sur la protection de la vie privée en vigueur dans d'autres territoires. Si le système d'information, la technologie ou le programme sert au transfert international de renseignements personnels sur la santé, la situation devient encore plus complexe. Votre EIVP devrait fournir tous les renseignements nécessaires sur vos projets éventuels de transférer des renseignements personnels sur la santé entre l'Ontario et tout autre territoire. Voir également l'annexe D – Organisation de coopération et de développement économiques – Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B13	Une évaluation a-t-elle été effectuée pour déterminer les risques éventuels pour la vie privée des particuliers dont les renseignements personnels sur la santé sont recueillis, utilisés, conservés ou divulgués au moyen du système d'information, de la technologie ou du programme proposé ou existant?					

Remarques : L'EIVP comporte comme élément essentiel un examen des répercussions possibles du système d'information, de la technologie ou du programme proposé ou existant sur la vie privée des particuliers dont les renseignements personnels sur la santé pourraient être recueillis, utilisés, conservés ou divulgués. Cet examen permet de déterminer ce que pourrait être l'incidence générale sur la vie privée du système, de la technologie ou du programme. Il s'agit notamment de déterminer comment le système, la technologie ou le programme existant ou proposé pourrait influer sur la vie privée des particuliers dont les renseignements personnels sur la santé sont en jeu.

B14	Si des risques éventuels pour la vie privée ont été identifiés, des moyens d'éviter ou de réduire ces risques ont-ils été intégrés dans le système d'information, la technologie ou le programme proposé ou existant au moment de sa conception ou de sa mise en œuvre?					

Remarques : Si des risques possibles pour la vie privée sont mentionnés en réponse à la question B12 ou à d'autres questions, il faut généralement prendre des mesures précises pour les éviter ou les réduire. On pourrait notamment utiliser des technologies d'amélioration de la protection de la vie privée, réviser des formules de consentement, éclaircir ou mieux diffuser des avis sur le système d'information, la technologie ou le programme, ou encore donner une formation sur la protection de la vie privée relativement au système d'information, à la technologie ou au programme proposé ou existant. Votre EIVP devrait décrire la nature de ces mesures. Si vous l'avez déjà fait en réponse à d'autres questions, vous pouvez faire un renvoi à ces questions ou aux pièces jointes qui y sont associées. Dans votre réponse à cette question, vous devriez soulever tous les aspects mentionnés à la question B12. Si vous n'avez pris aucune mesure pour réduire les risques que vous avez relevés, justifiez votre décision dans le champ « Remarques » de cette question.

B15	Une évaluation a-t-elle été effectuée pour déterminer si d'autres dépositaires de renseignements sur la santé ont mis en œuvre un système d'information, une technologie ou un programme identique ou semblable, établir les risques pour la vie privée auxquels doivent faire face ces dépositaires et relever les mesures que ceux-ci ont prises pour éviter ou réduire ces risques?					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	Remarques : Il est utile de s'appuyer sur l'expérience d'autres dépositaires de renseignements sur la santé qui ont mis en œuvre un système d'information, une technologie ou un programme identique ou semblable pour déterminer les principaux risques et préoccupations en matière de vie privée et établir comment ces dépositaires ont résolu des difficultés particulières à ce sujet.					
B16	A-t-on demandé aux principaux intervenants de préciser s'ils considèrent les mesures de protection de la vie privée comme étant suffisantes, et de décrire l'incidence de ces mesures sur le système d'information, la technologie ou le programme proposé ou existant?					
	Remarques : Lorsqu'un système d'information, une technologie ou un programme proposé ou existant est utilisé pour traiter de grandes quantités de renseignements personnels sur la santé, ou lorsque ces renseignements sont particulièrement délicats, il est souhaitable de consulter les intervenants qui ont un intérêt dans les mesures de protection de la vie privée qui sont prises dans le cadre du projet. Si vous l'avez fait, votre EIVP devrait décrire les résultats de ces consultations.					
B17	Les utilisateurs recevront-ils une formation sur les exigences relatives à la protection des renseignements personnels sur la santé et seront-ils informés des procédures pertinentes concernant les avis à fournir en cas de vol ou de perte de renseignements ou d'accès à ceux-ci par des personnes non autorisées?					
	Remarques : Votre EIVP devrait décrire vos plans de formation concernant les mesures et politiques de protection de la vie privée et de sécurité que votre organisme a l'intention de mettre en œuvre pour le système d'information, la technologie ou le programme proposé ou existant. Vous devez informer vos mandataires de leurs obligations en matière de protection des données afin que le système d'information, la technologie ou le programme proposé ou existant soit conforme à la *LPRPS*, y compris au paragraphe 17 (3), qui oblige le mandataire d'un dépositaire de renseignements sur la santé à aviser ce dernier à la première occasion en cas de vol ou de perte de renseignements personnels sur la santé qu'il emploie en son nom ou d'accès à ceux-ci par des personnes non autorisées. Soulignons que cette question a trait à une formation précise concernant le système, la technologie ou le programme proposé ou existant; les programmes de formation plus généraux sur la protection de la vie privée devraient être décrits en réponse à la question A9.					
B18	Des politiques et procédures de sécurité visant à protéger les renseignements personnels sur la santé contre le vol, la perte, l'utilisation ou la divulgation non autorisée ainsi que la duplication, la modification ou l'élimination non autorisée ont-elle été adoptées?					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	Remarques: Votre EIVP devrait comprendre des copies des politiques et procédures liées à la gestion des renseignements personnels sur la santé en rapport avec le système d'information, la technologie ou le programme proposé ou existant. Si vous disposez de politiques et de procédures de sécurité s'appliquant à l'ensemble de votre organisme, vous devriez l'indiquer dans l'EIVP, et inscrire un renvoi à toute pièce jointe pertinente fournie en réponse à la question A5.					
B19	Des politiques ou procédures de protection de la vie privée ont-elles été élaborées concernant différents aspects de l'utilisation du système d'information, de la technologie ou du programme proposé ou existant?					
	Remarques : Cette question a trait aux politiques ou procédures de protection de la vie privée qui s'appliquent à certains aspects de l'utilisation du système d'information, de la technologie ou du programme proposé ou existant; pour des précisions, voir la question B18. Vos réponses à cette question et à la question B17 pourraient se recouper avec celles que vous avez données aux questions A3 et A4; dans ce cas, vous devriez fournir tout renvoi nécessaire dans votre EIVP.					
B20	Les politiques et procédures de protection de la vie privée mentionnées en réponse à la question B16 respectent-elles les critères suivants (dans l'affirmative, veuillez les joindre)? • Les renseignements personnels sur la santé traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant sont recueillis conformément à la *LPRPS* et aux autres lois pertinentes; • Le consentement du particulier est obtenu conformément à l'article 18 de la *LPRPS*, s'il y a lieu, relativement au système d'information, à la technologie ou au programme proposé ou existant; • Une déclaration publique écrite des fins auxquelles le système d'information, la technologie ou le programme proposé ou existant est ou sera utilisé pour recueillir, utiliser ou divulguer des renseignements personnels sur la santé est mise à la disposition du public tel qu'indiqué à l'article 16 de la *LPRPS*; • Un particulier a le droit d'avoir accès aux renseignements personnels sur la santé qui le concernent et qui sont traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant, et d'en demander la rectification en vertu des articles 52 à 55 de la *LPRPS*, sous réserve de certaines exceptions;					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	• Il existe un calendrier de conservation des dossiers de renseignements personnels sur la santé indiquant la durée minimum et maximum de conservation au moyen du système d'information, de la technologie ou du programme proposé ou existant, ainsi que des procédures de destruction sécurisée de ces renseignements.					

Remarques : Cette question a trait à plusieurs aspects importants du contenu de diverses politiques ou procédures relatives au système d'information, à la technologie ou au programme proposé ou existant qui ont peut-être été abordées en réponse à la question B17. Les critères précédents sont des éléments importants de la *LPRPS* et sont généralement reconnus comme étant des pratiques équitables en matière de renseignements.

B21	Le système d'information, la technologie ou le programme proposé ou existant permet-il de consigner les insertions, accès, modifications ou divulgations de renseignements personnels sur la santé et comprend-il une interface permettant de les vérifier pour déceler les activités non autorisées?					

Remarques : Cette question a trait à la capacité technique de contrôler les utilisations non autorisées du système d'information, de la technologie ou du programme proposé ou existant. La consignation et la vérification des activités des utilisateurs sont nécessaires pour prévenir le vol, la perte, l'utilisation ou la divulgation non autorisée ainsi que la duplication, la modification ou l'élimination non autorisée des renseignements. Si vous répondez « Oui » à cette question, vous devriez fournir une description générale de cette fonctionnalité de même que de vos procédures de vérification. Si vous répondez « Non », vous devriez expliquer pourquoi le système d'information, la technologie ou le programme proposé ou existant n'est pas doté de ces caractéristiques, et décrire les autres moyens que vous prenez ou comptez prendre pour éviter les insertions, les accès, les modifications ou les divulgations non autorisés.

B22	Des politiques et des procédures ont-elles été élaborées aux fins de l'application des règles de protection de la vie privée relativement au système d'information, à la technologie ou au programme proposé ou existant, et notamment pour remplir les engagements pris dans l'EIVP?					

Remarques : Dans vos réponses à ce questionnaire, vous prendrez certains engagements concernant le système d'information, la technologie ou le programme proposé ou existant. Vous fournirez des politiques et des procédures, et vous décrirez des mesures de sécurité. En outre, vous mentionnerez d'autres mesures de protection de la vie privée. Cette question vous demande des renseignements sur la façon dont votre organisme montrera qu'il respecte a) les exigences de la *LPRPS* et d'autres textes de loi et b) ses propres engagements. Dans votre EIVP, vous devriez décrire comment la vérification, la conformité et l'application seront assurées.

Annexe A – Modèle de questionnaire d'EIVP

Nom du système d'information, de la technologie ou du programme qui fait l'objet de l'EIVP :

Date :

Nom du dépositaire de renseignements sur la santé qui a la responsabilité ou le contrôle du système d'information, de la technologie ou du programme :

Nom de l'auteur :

Titre de l'auteur :

Adresse postale de l'auteur :

Numéro de téléphone de l'auteur :

Numéro de télécopieur de l'auteur :

Adresse électronique de l'auteur :

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes

N'oubliez pas d'indiquer la section ou les pages pertinentes dans la colonne « Pièces jointes » quand vous joignez des documents. Pour faciliter la consultation, vous pourriez numéroter les pages de vos documents. Il est particulièrement important de le faire si des intervenants de l'extérieur passeront en revue votre EIVP, car ils seront probablement moins au fait des particularités du système d'information, de la technologie ou du programme proposé.

Partie A : Gestion de la protection de la vie privée à l'échelon de l'organisme

Les questions de cette section ont trait à la gestion de la protection de la vie privée dans l'ensemble de votre organisme. Elles ne se limitent pas au système d'information, à la technologie ou au programme. Des questions précises sur le système d'information, la technologie ou le programme sont posées à la partie B.

Politiques et mécanismes de contrôle en matière de vie privée

A1	Existe-t-il un plan stratégique ou un plan d'entreprise qui aborde la protection de la vie privée?					

Remarques :

A2	Votre organisme a-t-il établi une politique en matière de protection de la vie privée ou un énoncé de pratiques relatives aux renseignements?					

Remarques :

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
A3	Des politiques ou procédures de protection de la vie privée ont-elles été élaborées concernant divers aspects des activités de l'organisme?					
Remarques :						
A4	Les politiques et procédures de protection de la vie privée mentionnées en réponse aux questions A2 et A3 respectent-elles les critères suivants? • Les renseignements personnels sur la santé sont recueillis conformément à la *LPRPS* et aux autres lois pertinentes; • Le consentement du particulier est obtenu conformément à l'article 18 de la *LPRPS*, s'il y a lieu; • Une déclaration publique écrite des pratiques relatives aux renseignements de l'organisme, comprenant le nom d'une personne-ressource avec qui communiquer pour obtenir des renseignements sur la protection de la vie privée ou porter plainte, et la façon dont on peut avoir accès à un dossier de renseignements personnels sur la santé ou en demander la rectification, est mise à la disposition du public tel qu'indiqué à l'article 16 de la *LPRPS*; • Un particulier a le droit d'avoir accès aux renseignements personnels sur la santé qui le concernent et d'en demander la rectification en vertu des articles 52 à 55 de la *LPRPS*, sous réserve de certaines exceptions; • Il existe un calendrier de conservation des dossiers de renseignements personnels sur la santé indiquant la durée minimum et maximum de conservation ainsi que des procédures de destruction sécurisée de ces renseignements.					
Remarques :						
A5	L'organisme prend-il des mesures de précaution d'ordre administratif, technique et matériel pour protéger les renseignements personnels sur la santé contre le vol, la perte, l'utilisation ou la divulgation non autorisée ainsi que contre la duplication, la modification ou l'élimination non autorisée en vertu de l'article 12 de la *LPRPS*?					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	*Remarques : **Si votre organisme adhère à une norme reconnue de l'industrie ou du gouvernement pour assurer la sécurité des renseignements, comme la norme ISO 17799, vous devriez décrire cette norme dans vos explications et indiquer si votre organisme a obtenu la certification.*					
	Structure et organisation des mesures de protection de la vie privée					
A6	Existe-t-il une personne-ressource responsable de la protection de la vie privée dans votre organisme?					
	Remarques :					
A7	Existe-t-il un processus permettant d'informer la direction de l'organisme au sujet des questions touchant la conformité aux règles de protection de la vie privée?					
	Remarques :					
A8	Des cadres supérieurs participent-ils activement à l'élaboration, à la mise en œuvre ou à la promotion du programme de protection de la vie privée de votre organisme?					
	Remarques :					
A9	Les employés ou mandataires qui ont accès à des renseignements personnels sur la santé dans votre organisme reçoivent-ils une formation sur la protection de la vie privée?					
	Remarques :					
A10	Des politiques et des procédures ont-elles été élaborées pour gérer les atteintes à la vie privée, notamment en ce qui concerne la notification des personnes dont la confidentialité des renseignements personnels sur la santé a été violée?					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
Remarques :						
	Partie B : Gestion de la protection de la vie privée à l'échelon du projet Les questions de cette partie ont trait au système d'information, à la technologie ou au programme. Description du projet					
B1	Un sommaire du système d'information, de la technologie ou du programme proposé ou existant a-t-il été préparé, avec une description de ses exigences et de la façon dont il répond ou répondra aux besoins établis?					
Remarques :						
B2	A-t-on dressé une liste de tous les renseignements personnels sur la santé ou de toutes les données qui sont ou seront recueillis, utilisés ou divulgués par l'entremise du système d'information, de la technologie ou du programme proposé ou existant?					
Remarques :						
B3	Des diagrammes ont-ils été tracés pour illustrer le cheminement des renseignements personnels sur la santé dans le système d'information, la technologie ou le programme proposé ou existant?					
Remarques :						
B4	Des documents ont-ils été préparés en vue de préciser les personnes, postes ou catégories d'employés qui ont accès aux différents éléments ou dossiers de renseignements personnels sur la santé?					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
Remarques :						
B5	La collecte, l'utilisation et la divulgation de renseignements personnels sur la santé par l'entremise du système d'information, de la technologie ou du programme proposé ou existant s'appuient-elles avant tout sur le consentement du particulier ou d'un mandataire spécial autorisé?					
Remarques :						
B6	Avez-vous documenté les fins auxquelles seront recueillis, utilisés ou divulgués les renseignements personnels sur la santé par l'entremise du système d'information, de la technologie ou de programme?					
Remarques :						
B7	Des renseignements personnels sur la santé sont-ils recueillis, utilisés, divulgués ou conservés uniquement aux fins précisées et à des fins qu'un particulier considérerait comme étant raisonnablement conformes à ces fins?					
Remarques :						
B8	Les renseignements personnels sur la santé traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant seront-ils associés ou recoupés avec d'autres renseignements traités au moyen d'autres systèmes d'information, technologies ou programmes?					
Remarques :						

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
Remarques :						
B9	Les renseignements personnels sur la santé recueillis ou utilisés par l'entremise du système d'information, de la technologie ou du programme seront-ils divulgués à des personnes qui ne sont pas des employées ou des mandataires de l'organisme responsable?					
Remarques :						
B10	Avez-vous pris des dispositions pour assurer la divulgation complète des fins auxquelles les renseignements personnels sur la santé seront recueillis par l'entremise du système d'information, de la technologie ou du programme?					
Remarques :						
B11	Des produits ou un plan de communication ont-ils été élaborés pour expliquer en détail le système d'information, la technologie ou le programme aux particuliers et la façon dont les renseignements personnels sur la santé qui les concernent seront protégés?					
Remarques :						
B12	Le système d'information, la technologie ou le programme proposé ou existant permettra-t-il de recueillir, d'utiliser ou de divulguer des renseignements personnels sur la santé au-delà des frontières de l'Ontario?					
Remarques :						

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B13	Une évaluation a-t-elle été effectuée pour déterminer les risques éventuels pour la vie privée des particuliers dont les renseignements personnels sur la santé sont recueillis, utilisés, conservés ou divulgués au moyen du système d'information, de la technologie ou du programme proposé ou existant?					
Remarques :						
B14	Si des risques éventuels pour la vie privée ont été identifiés, des moyens d'éviter ou de réduire ces risques ont-ils été intégrés dans le système d'information, la technologie ou le programme proposé ou existant au moment de sa conception ou de sa mise en œuvre?					
Remarques :						
B15	Une évaluation a-t-elle été effectuée pour déterminer si d'autres dépositaires de renseignements sur la santé ont mis en œuvre un système d'information, une technologie ou un programme identique ou semblable, établir les risques pour la vie privée auxquels doivent faire face ces dépositaires et relever les mesures que ceux-ci ont prises pour éviter ou réduire ces risques?					
Remarques :						
B16	A-t-on demandé aux principaux intervenants de préciser s'ils considèrent les mesures de protection de la vie privée comme étant suffisantes, et de décrire l'incidence de ces mesures sur le système d'information, la technologie ou le programme proposé ou existant?					
Remarques :						

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B17	Les utilisateurs recevront-ils une formation sur les exigences relatives à la protection des renseignements personnels sur la santé et seront-ils informés des procédures pertinentes concernant les avis à fournir en cas de vol ou de perte de renseignements ou d'accès à ceux-ci par des personnes non autorisées?					
Remarques :						
B18	Des politiques et procédures de sécurité visant à protéger les renseignements personnels sur la santé contre le vol, la perte, l'utilisation ou la divulgation non autorisée ainsi que la duplication, la modification ou l'élimination non autorisée ont-elle été adoptées?					
Remarques :						
B19	Des politiques ou procédures de protection de la vie privée ont-elles été élaborées concernant différents aspects de l'utilisation du système d'information, de la technologie ou du programme proposé ou existant?					
Remarques :						
B20	Les politiques et procédures de protection de la vie privée mentionnées en réponse à la question B16 respectent-elles les critères suivants (dans l'affirmative, veuillez les joindre)? • Les renseignements personnels sur la santé traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant sont recueillis conformément à la *LPRPS* et aux autres lois pertinentes;					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
	• Le consentement du particulier est obtenu conformément à l'article 18 de la *LPRPS*, s'il y a lieu, relativement au système d'information, à la technologie ou au programme proposé ou existant; • Une déclaration publique écrite des fins auxquelles le système d'information, la technologie ou le programme proposé ou existant est ou sera utilisé pour recueillir, utiliser ou divulguer des renseignements personnels sur la santé est mise à la disposition du public tel qu'indiqué à l'article 16 de la *LPRPS*; • Un particulier a le droit d'avoir accès aux renseignements personnels sur la santé qui le concernent et qui sont traités par l'entremise du système d'information, de la technologie ou du programme proposé ou existant, et d'en demander la rectification en vertu des articles 52 à 55 de la *LPRPS*, sous réserve de certaines exceptions; • Il existe un calendrier de conservation des dossiers de renseignements personnels sur la santé indiquant la durée minimum et maximum de conservation au moyen du système d'information, de la technologie ou du programme proposé ou existant, ainsi que des procédures de destruction sécurisée de ces renseignements.					
	Remarques :					
B21	Le système d'information, la technologie ou le programme proposé ou existant permet-il de consigner les insertions, accès, modifications ou divulgations de renseignements personnels sur la santé et comprend-il une interface permettant de les vérifier pour déceler les activités non autorisées?					
	Remarques :					

N°	Question	Oui	En cours	Non	S.o./n.d.	Pièces jointes
B22	Des politiques et des procédures ont-elles été élaborées aux fins de l'application des règles de protection de la vie privée relativement au système d'information, à la technologie ou au programme proposé ou existant, et notamment pour remplir les engagements pris dans l'EIVP?					
Remarques :						

Annexe B – Exemples de méthodes d'EIVP

Canada

- Commissaire à l'information et à la protection de la vie privée/Ontario, *Privacy Diagnostic Tool*; *http://www.ipc.on.ca/userfiles/page_attachments/pdt.pdf*
- Ontario, Secrétariat du Conseil de gestion, *Privacy Impact Assessment Guidelines* (juin, 2001); *http://www.gov.on.ca/MBS/english/fip/pia/*
- Ontario, Secrétariat du Conseil de gestion, *Model Cross-Jurisdictional Privacy Impact Assessment Guide* (ébauche, octobre 1999); *http://www.gov.on.ca/MBS/english/fip/pub/fed_pia.html*
- Secrétariat du Conseil du Trésor du Canada, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks* (août, 2002); *http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp*
- Office of the Information and Privacy Commissioner of Alberta, *Privacy Impact Assessment: Full Questionnaire*; *http://www.oipc.ab.ca/ims/client/upload/piaform-full.pdf*
- Alberta Medical Association, *Guide to Privacy Impact Assessments for Physicians Offices* (février, 2002).

Étranger

- Privacy Commissioner/New Zealand, *Privacy Impact Assessment Handbook* (mars, 2002, Auckland, 40 pp.); *www.privacy.org.nz/comply/pia.html*
- Département de l'Intérieur des États-Unis, *Privacy Impact Assessment and Guide* (septembre, 2002); *http://www.doi.gov/ocio/cp/Privacy%20Impact%20Assessment_9.16.02.pdf*
- Internal Revenue Service des Etats-Unis, *Model Information Technology Privacy Impact Assessment* (février, 2000); *http://www.cio.gov/documents/pia_for_it_irs_model.pdf*
- Département de la Justice des États-Unis, *Privacy Impact Assessment for Justice Information Systems* (février, 2001); *http://it.ojp.gov/initiatives/files/Privacy3.pdf*

Annexe C – Définition de « renseignements personnels sur la santé » en vertu de la *LPRPS*

L'article 4 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* définit comme suit l'expression « renseignements personnels sur la santé » :

« renseignements personnels sur la santé » s'entend de renseignements identificatoires concernant un particulier qui se présentent sous forme verbale ou autre forme consignée si, selon le cas :

(a) ils ont trait à la santé physique ou mentale du particulier, y compris aux antécédents de sa famille en matière de santé;

(b) ils ont trait à la fourniture de soins de santé au particulier, notamment à l'identification d'une personne comme fournisseur de soins de santé de ce dernier;

(c) ils constituent un programme de services au sens de la *Loi de 1994 sur les soins de longue durée* pour le particulier;

(d) ils ont trait aux paiements relatifs aux soins de santé fournis au particulier ou à son admissibilité à ces soins ou à cette assurance;

(e) ils ont trait au don, par le particulier, d'une partie de son corps ou d'une de ses substances corporelles ou découlent de l'analyse ou de l'examen d'une telle partie ou substance;

(f) ils sont le numéro de la carte Santé du particulier;

(g) ils permettent d'identifier le mandataire spécial d'un particulier.

« renseignements identificatoires » Renseignements qui permettent d'identifier un particulier ou à l'égard desquels il est raisonnable de prévoir, dans les circonstances, qu'ils pourraient servir, seuls ou avec d'autres, à en identifier un.

Les renseignements personnels sur la santé ne comprennent pas les renseignements identificatoires contenus dans un dossier dont un dépositaire de renseignements sur la santé a la garde ou le contrôle si :

(a) d'une part, les renseignements identificatoires contenus dans le dossier concernent essentiellement un ou plusieurs employés ou autres mandataires du dépositaire;

(b) d'autre part, le dossier est tenu essentiellement à une autre fin que la fourniture de soins de santé à ces employés ou autres mandataires ou d'une aide à cet égard.

Par exemple, une note d'un médecin justifiant une absence, qui se trouve dans le dossier du personnel d'une secrétaire à l'emploi d'un dépositaire de renseignements sur la santé, ne représente pas des renseignements personnels sur la santé.

Annexe D – Organisation de coopération et de développement économiques – Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

Pour des précisions, consulter le site de l'OCDE *www.oecd.om*.

Préface

Compte tenu de l'essor pris par le traitement automatique de l'information, qui permet de transmettre de vastes quantités de données en quelques secondes à travers les frontières nationales et même à travers les continents, il a fallu étudier la question de la protection de la vie privée sous l'angle des données de caractère personnel.
Des législations relatives à la protection de la vie privée ont été adoptées ou le seront prochainement dans près de la moitié des pays de l'OCDE (l'Allemagne, l'Autriche, le Canada, le Danemark, les États-Unis, la France, le Luxembourg, la Norvège et la Suède ont promulgué une législation. La Belgique, l'Espagne, les Pays-Bas et la Suisse ont établi des projets de loi) en vue de prévenir des actes considérés comme constituant des violations des droits fondamentaux de l'homme, tels que le stockage illicite de données de caractère personnel qui sont inexactes, l'utilisation abusive ou la divulgation non autorisée de ces données.

En revanche, il est à craindre que des disparités dans les législations nationales n'entravent la libre circulation des données de caractère personnel à travers les frontières; or, cette circulation s'est considérablement intensifiée au cours des dernières années et elle est appelée à se développer encore par suite de l'introduction généralisée de nouvelles technologies des ordinateurs et des télécommunications. Des restrictions imposées à ces flux pourraient entraîner de graves perturbations dans d'importants secteurs de l'économie, tels que la banque et les assurances.

C'est pourquoi, les pays Membres de l'OCDE ont jugé nécessaire d'élaborer des lignes directrices qui permettraient d'harmoniser les législations nationales relatives à la protection de la vie privée et qui, tout en contribuant au maintien de ces droits de l'homme, empêcheraient que les flux internationaux de données ne subissent des interruptions. Ces lignes directrices sont l'expression d'un consensus sur des principes fondamentaux qui peuvent être intégrés à la législation nationale en vigueur ou servir de base à une législation dans les pays qui ne sont pas encore dotés.

Les lignes directrices, qui revêtent la forme d'une recommandation du conseil de l'OCDE, ont été élaborées par un groupe d'experts gouvernementaux placé sous la présidence de M. M.D. Kirby, Président de la Commission australienne de la réforme législative. Cette recommandation a été adoptée et a pris effet le 23 septembre 1980.

Les lignes directrices sont accompagnées d'un exposé des motifs destiné à fournir des éléments d'information sur les débats et les raisonnements qui sous-tendent leur énoncé.

Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

23 septembre 1980

Le Conseil,

Vu les Articles 1 (c), 3 (a) et 5 (b) de la Convention relative à l'Organisation de Coopération et de Développement Économiques en date du 14 décembre 1960;

Reconnaissant :

que, bien que les législations et politiques nationales puissent différer, il est de l'intérêt commun des pays Membres de protéger la vie privée et les libertés individuelles et de concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information;

que le traitement automatique et les flux transfrontières de données de caractère personnel créent de nouvelles formes de relations entre pays et exigent l'instauration de règles et pratiques compatibles;

que les flux transfrontières de données de caractère personnel contribuent au développement économique et social;

que les droits internes concernant la protection de la vie privée et les flux transfrontières de données de caractère personnel sont susceptibles d'entraver ces flux transfrontières.

Résolu à favoriser la libre circulation de l'information entre les pays Membres et à éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre ces pays;

Recommande

Que les pays Membres tiennent compte, dans leur législation interne, des principes concernant la protection de la vie privée et des libertés individuelles exposés dans les lignes directrices figurant en Annexe à la présente Recommandation dont elle fait partie intégrante;

Que les pays Membres s'efforcent de supprimer ou d'éviter de créer, au nom de la protection de la vie privée, des obstacles injustifiés aux flux transfrontières des données de caractère personnel;

Que les pays Membres coopèrent pour mettre en œuvre les lignes directrices énoncées en Annexe;

Que les pays Membres conviennent dès que possible de procédures spécifiques de consultation et de coopération en vue de l'application des présentes lignes directrices

Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

Annexe à la Recommandation du Conseil du 23 septembre 1980

PREMIÈRE PARTIE : CONSIDÉRATIONS GÉNÉRALES

Définitions

1. Aux fins des présentes lignes directrices:

a) par « maître du fichier », on entend toute personne physique ou morale qui, conformément au droit interne, est habilitée à décider du choix et de l'utilisation des données de caractère personnel, que ces données soient ou non collectées, enregistrées, traitées ou diffusées par ladite personne ou par un agent agissant en son nom;

b) par « données de caractère personnel », on entend toute information relative à une personne physique identifiée ou identifiable (personne concernée);

c) par « flux transfrontière de données de caractère personnel », on entend la circulation de données de caractère personnel à travers les frontières nationales.

Champ d'application des lignes directrices

2. Les présentes lignes directrices s'appliquent aux données de caractère personnel, dans les secteurs public et privé, qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles.

3. Les présentes lignes directrices ne devraient pas être interprétées comme interdisant:

a) d'appliquer, à diverses catégories de données de caractère personnel, des mesures de protection différentes selon leur nature et le contexte dans lequel elles sont collectées, enregistrées, traitées ou diffusées;

b) d'en exclure l'application à des données de caractère personnel qui, manifestement, ne présentent aucun risque pour la vie privée et les libertés individuelles, ou

c) d'en limiter l'application au traitement automatique des données de caractère personnel.

4. Les exceptions aux principes énoncés dans les Parties Deux et Trois des présentes lignes directrices, y compris celles intéressant la souveraineté nationale, la sécurité nationale et l'ordre public, devraient être:

a) aussi peu nombreuses que possible, et
b) portées à la connaissance du public.

5. Dans le cas particulier des pays à structure fédérale, l'application des présentes lignes directrices peut être influencée par la répartition des pouvoirs dans l'État fédéral.

6. Les présentes lignes directrices devraient être considérées comme des normes minimales susceptibles d'être complétées par d'autres mesures visant à protéger la vie privée et les libertés individuelles.

PARTIE DEUX : PRINCIPES FONDAMENTAUX APPLICABLES AU PLAN NATIONAL

Principe de la limitation en matière de collecte

7. Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Principe de la qualité des données

8. Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

Principe de la spécification des finalités

9. Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

Principe de la limitation de l'utilisation

10. Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe 9, si ce n'est:

    a) avec le consentement de la personne concernée; ou
    b)) lorsqu'une règle de droit le permet.

Principe des garanties de sécurité

11. Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.

Principe de la transparence

12. Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

Principe de la participation individuelle

13. Toute personne physique devrait avoir le droit:

a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;

b) de se faire communiquer les données la concernant;
- dans un délai raisonnable;
- moyennant, éventuellement, une redevance modérée;
- selon des modalités raisonnables; et
- sous une forme qui lui soit aisément intelligible;

c) d'être informée des raisons pour lesquelles une demande quelle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet; et

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Principe de la responsabilité

14. Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

PARTIE TROIS : PRINCIPES FONDAMENTAUX APPLICABLES AU PLAN INTERNATIONAL : LIBRE CIRCULATION ET RESTRICTIONS LÉGITIMES

15. Les pays Membres devraient prendre en considération les conséquences pour d'autres pays Membres d'un traitement effectué sur leur propre territoire et de la réexportation des données de caractère personnel.

16. Les pays Membres devraient prendre toutes les mesures raisonnables et appropriées pour assurer que les flux transfrontières de données de caractère personnel, et notamment le transit par un pays Membre, aient lieu sans interruption et en toute sécurité.

17. Un pays Membre devrait s'abstenir de limiter les flux transfrontières de données de caractère personnel entre son territoire et celui d'un autre pays Membre, sauf lorsqu'un ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays Membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays Membre ne prévoit pas de protection équivalente.

18. Les pays Membres devraient éviter d'élaborer des lois, des politiques et des procédures, qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel qui iraient au-delà des exigences propres à cette protection.

PARTIE QUATRE : MISE EN ŒUVRE DES PRINCIPES A L'ECHELON NATIONAL

19. Lors de la mise en œuvre, au plan intérieur, des principes énoncés dans les Parties Deux et Trois, les pays Membres devraient établir des procédures juridiques, administratives et autres, ou des institutions pour protéger la vie privée et les libertés individuelles eu égard aux données de caractère personnel. Les pays Membres devraient notamment s'efforcer de :
    a) adopter une législation nationale appropriée ;
    b) favoriser et soutenir des systèmes d'auto-réglementation (codes de déontologie ou autres formes);
    c) permettre aux personnes physiques de disposer de moyens raisonnables pour exercer leurs droits;
    d) instituer des sanctions et des recours appropriés en cas d'inobservation des mesures mettant en œuvre les principes énoncés dans les Parties Deux et Trois, et
    e) veiller à ce que les personnes concernées ne fassent l'objet d'aucune discrimination inéquitable.

PARTIE CINQ : COOPÉRATION INTERNATIONALE

20. Les pays Membres devraient, sur demande, faire connaître à d'autres pays Membres les modalités détaillées de l'application des principes énoncés dans les présentes lignes directrices. Les pays Membres devraient également veiller à ce que les procédures applicables aux flux transfrontières de données de caractère personnel, ainsi qu'à la protection de la vie privée des libertés individuelles, soient simples et compatibles avec celles des autres pays Membres qui se confirment aux présentes lignes directrices.

21. Les pays Membres devraient établir des procédures en vue de faciliter :
    - l'échange d'informations relatives aux présentes lignes directrices ; et
    - l'assistance mutuelle lorsqu'il s'agit des questions de procédure et d'échange réciproque d'information.

22. Les pays Membres devraient s'employer à établir des principes, au plan intérieur et international, afin de déterminer le droit applicable en cas de flux transfrontières de données de caractère personnel.

Notes

Notes

Notes

Notes

Commissaire à l'information et à la protection de la vie privée / Ontario
2, rue Bloor Est, bureau 1400
Toronto (Ontario) M4W 1A8
Téléphone : 416 326-3333 ou 1 800 387-0073
Télécopieur : 416 325-9195
ATS : 416 325-7539
Site Web : www.ipc.on.ca
Courriel : info@ipc.on.ca