

Outil d'évaluation de l'impact sur la vie privée



OMBUDSMAN DU
MANITOBA

Partie 1 : Résumé du programme ou de l'activité

Qui?

Nom du projet

Nom du ministère, de la division ou du secteur de programme

Nom(s) des représentants du projet

Énumérez les entités externes susceptibles de participer

Quoi?

Résumé du nouveau programme, service, logiciel ou changement :

Expliquez le nouveau programme, service ou changement et notamment son état actuel.

Raisons d'être, buts et objectifs

Décrivez ce que vous essayez d'accomplir avec le nouveau programme, service ou changement. Par exemple : améliorer les services à la clientèle, améliorer l'efficacité, mieux protéger la vie privée, simplifier les processus.

Décrivez le type d'application

Identifiez et décrivez les types d'applications et de plateformes et les entités externes impliquées dans le flux de renseignements (collecte, utilisation et communication).

Pourquoi?

Expliquez pourquoi vous adoptez le nouveau programme, service ou changement et décrivez-en les avantages.

Où?

Où le flux de données se produit-il? En ligne, en personne, sur papier, au Manitoba, au Canada ou aux États-Unis?

Quand?

Indiquez les dates importantes, notamment les échéances du projet, les étapes principales, les calendriers de mise en oeuvre, les paramètres du contrat.

Partie 2 : Décrivez la portée

1. Décrivez le flux de renseignements (médicaux) personnels

Décrivez la façon dont les renseignements circuleront au sein de l'organisation, notamment leur communication (renseignements fournis à l'extérieur de l'organisation). Cette section doit comporter une brève description (écrite ou visuelle) de la circulation des renseignements (médicaux) personnels dans le système, depuis la collecte jusqu'à l'utilisation au sein de l'organisation, ainsi que la communication (échange) à l'extérieur de l'organisation (le cas échéant). Consultez l'Annexe B pour voir un exemple de tableau de flux de données.

1. Qui gère et utilise le système, et qui y a accès?

Indiquez qui est responsable de la gestion du système. Indiquez aussi qui sont les utilisateurs prévus du système au sein de l'organisation et quel(s) lien(s) ils ont avec le nouveau programme, service ou changement.

2. Existe-t-il des liens avec d'autres systèmes?

Expliquez les liens éventuels avec d'autres programmes ou services. Par exemple, les données seront-elles recueillies d'autres systèmes et(ou) partagées avec d'autres systèmes? Veuillez indiquer le calendrier d'activités et expliquer si des liens sont prévus dans l'avenir mais ne vont pas être établis dans l'immédiat.

3. Envisagez-vous d'apporter des améliorations au système dans l'avenir?

Le système sera-t-il élargi pour inclure un plus grand nombre d'utilisateurs? Est-ce que le contrat de nouveau service ou système inclut une série de mises à niveau?

4. D'autres utilisations des renseignements sont-elles envisagées pour l'avenir?

Avez-vous envisagé des utilisations secondaires pour les renseignements (médicaux) personnels contenus dans le système, notamment la recherche ou l'analyse? On entend par utilisation secondaire des renseignements toute utilisation qui diffère de la raison pour laquelle les renseignements ont été recueillis en premier lieu.

Partie 3 : Collecte, utilisation et communication des renseignements (médicaux) personnels

1. Autorité en matière de collecte, d'utilisation et de communication des renseignements (médicaux) personnels

Indiquez la disposition précise de la loi, du règlement ou de la politique habilitante qui vous autorise à recueillir, à utiliser et à communiquer des renseignements (médicaux) personnels. Il peut notamment s'agir de la LAIPVP, de la LRMP ou de la législation habilitante de l'organisation. Veuillez indiquer l'autorité qui vous est accordée pour :

- La collecte
- L'utilisation
- La communication

2. Catégories de renseignements (médicaux) personnels qui seront recueillis, utilisés et(ou) communiqués

i. Remplissez le tableau (voir l'exemple à l'Annexe C)

Énumérez les renseignements (médicaux) personnels qui seront recueillis et expliquez brièvement l'utilisation qui en sera faite ainsi que leur communication éventuelle. Les renseignements (médicaux) personnels peuvent être classés selon les catégories énoncées à l'Annexe D.

ii. Expliquez les processus de décision et d'approbation concernant la collecte, l'utilisation et la communication des renseignements

Expliquez brièvement le processus de décision et d'approbation qui régit la collecte, l'utilisation et la communication des renseignements (médicaux) personnels dans le système. Par exemple, comment la direction participe-t-elle au processus de décision?

3. Source et exactitude des renseignements (médicaux) personnels

Expliquez brièvement qui fournit des renseignements (médicaux) personnels à votre programme. Par exemple, est-ce que c'est la personne concernée ou une autre source comme un ministère ou un membre de la famille?

Comment veillez-vous à ce que les renseignements obtenus soient exacts? Comment veillez-vous à ce que les renseignements restent exacts et puissent être mis à jour?

4. Énoncés de notification

Veillez fournir un modèle de l'(des) énoncé(s) de notification dont vous vous servez pour informer les particuliers au sujet de la collecte, de l'utilisation et de la communication de leurs renseignements (médicaux) personnels, de votre autorité légale et de vos coordonnées en cas de questions. Indiquez si, selon vous, des changements doivent être apportés ou si les énoncés doivent être mis à jour.

Si les données sont détenues et(ou) gérées à l'extérieur de votre organisation et(ou) dans un autre ressort [par exemple, lorsqu'une organisation recueille des renseignements (médicaux) personnels qui vont directement à une compagnie aux États-Unis pour y être détenus et gérés], veuillez indiquer si vous avez l'intention d'aviser les particuliers au sujet de l'endroit où leurs données sont stockées et de quelle façon vous pensez le faire. Cela ne concerne pas les situations où le transfert de renseignements (médicaux) personnels s'effectue de façon habituelle.

Partie 4 : Droits d'accès des particuliers

En vertu de la LAIPVP et de la LRMP, les particuliers ont le droit de :

- demander à avoir accès à leurs renseignements (médicaux) personnels détenus par un organisme public ou un dépositaire, et à en obtenir une copie;
- demander qu'une correction soit apportée à ces renseignements.

Capacité de donner à un particulier accès à ses renseignements (médicaux) personnels détenus sous forme électronique ou sur papier

Expliquez la façon dont vous donnerez aux particuliers accès à leurs renseignements (médicaux) personnels, y compris la façon dont vous leur fournirez des copies s'ils en demandent.

Décrivez la façon dont vous corrigerez les renseignements (médicaux) personnels d'un particulier si cela est nécessaire.

Partie 5 : Vie privée et mesures de sécurité

1. Garanties

i. Garanties administratives

Décrivez les politiques, procédures et lignes directrices internes qui s'appliquent à ce programme, service ou système.

Expliquez comment les politiques, procédures ou lignes directrices protègent la vie privée et établissent des normes de sécurité.

Si le service ou le système inclut des renseignements médicaux personnels, décrivez la façon dont les séances d'orientation sur la LRMP et la signature d'engagements de non-divulgaration en vertu de la LRMP seront gérées.

Décrivez toute autre entente supplémentaire de confidentialité qui est en place en matière de sécurité.

Décrivez le processus prévu en cas d'atteinte à la vie privée ou à la sécurité.

ii. Garanties techniques

Le système sera-t-il utilisé par des utilisateurs internes (le personnel) et(ou) des utilisateurs externes (participants au programme)?

Le système pourra-t-il prévoir des profils et des mots de passe pour tous les utilisateurs en fonction de leur rôle?

Si des utilisateurs externes ont accès au système, décrivez le processus de validation de l'identité qui sera utilisé.

Comment les renseignements (médicaux) personnels sont-ils recueillis auprès des particuliers? (sur papier, sous forme électronique, les deux).

Comment les renseignements (médicaux) personnels sont-ils utilisés, communiqués et transportés à l'intérieur du ministère, de la direction ou du secteur de programme?

Comment les renseignements (médicaux) personnels sont-ils communiqués à l'extérieur de l'organisation?

iii. Vérification du système

Est-ce que le niveau de sensibilité des renseignements (médicaux) personnels dans le système exige la vérification du système?

Est-ce que le système est doté d'une fonction de vérification? Dans l'affirmative, décrivez.

Des vérifications seront-elles prévues régulièrement pour détecter les atteintes à la vie privée et à la sécurité?

Qui effectuera les vérifications et qui en assurera le suivi?

2. Emplacement des renseignements (médicaux) personnels

Décrivez où seront détenus les documents sur papier ou sous forme électronique. Par exemple, bureaux ou serveurs sur place, installations de stockage et(ou) serveurs hors-site.

- i. Documents sur papier
- ii. Documents sous forme électronique

3. Est-ce que des renseignements (médicaux) personnels seront stockés par des organisations à l'extérieur du Manitoba? Du Canada?

Décrivez l'emplacement des renseignements (médicaux) personnels.

Si des renseignements (médicaux) personnels sont stockés à l'extérieur du Manitoba ou du Canada, veuillez donner les motifs.

4. Conservation et destruction des documents

Des calendriers de conservation des documents sont-ils en place pour l'organisation?

Les calendriers prévoient-ils la conservation et la destruction des documents à la fois sur papier et sous forme électronique?

Est-ce que l'organisation surveille la conservation des documents pour veiller au respect des calendriers?

Quels sont le plan et la méthode prévus pour la destruction des documents sur papier et sous forme électronique?

5. Gestionnaires de l'information

Aux termes de la LAIPVP et de la LRMP, une organisation doit conclure un accord avec un gestionnaire de l'information si elle communique des renseignements (médicaux) personnels à cette personne (un tiers externe à l'organisation) pour que celle-ci les traite, les stocke ou les détruise, ou bien pour qu'elle fournisse à l'organisation des services de gestion de l'information ou de technologie de l'information.

Si votre programme ou activité exige que vous fassiez appel à un gestionnaire de l'information, expliquez comment l'accord écrit protégera les renseignements (médicaux) personnels contre des risques tels que l'accès, l'utilisation, la communication, la destruction ou la modification non autorisés.

Quelle est la durée de l'accord?

L'accord sera-t-il examiné par un avocat?

Partie 6 : Résumé et résultats de l'EIVP

Procéder à une EIVP consiste principalement à identifier et à diminuer les risques pour la vie privée. Pour vous aider dans cette tâche, la liste de vérification suivante énonce les renseignements à inclure dans votre résumé.

- Une description de la proposition, notamment les objectifs, les parties concernées, le calendrier et les principales étapes, les besoins de ressources, les avantages pour l'organisation ou le public et toute obligation pertinente au sujet de la protection de la vie privée (lois, politiques et procédures applicables).
- Les risques qui ont été identifiés en matière de vie privée.
- Les incidences possibles de ces risques sur les particuliers.
- La probabilité que ces risques se concrétisent.
- Une description des propositions ou plans éventuels susceptibles d'éliminer ou de réduire les risques pour la vie privée.
- L'identification de tous les risques résiduels (auxquels les options proposées ne peuvent remédier) et les implications probables de ces risques résiduels sur la réaction du public, le succès du projet et autres intérêts de l'organisation.
- Une indication pour déterminer si l'impact sur la vie privée est proportionnel aux résultats attendus.

Autres commentaires :

Présentés à : [représentant chargé de l'accès à l'information et de la protection de la vie privée]

Présentés par :

Date :