

Évaluation de la protection des renseignements personnels dans les projets du PPICS

Préparé pour

Le Bureau de la santé et l'inforoute, Santé Canada

Par **PRIVA-C™**

Rapport final

15 octobre 2002

TABLE DES MATIÈRES

| | | |
|--------|---|----|
| 1. | SOMMAIRE..... | 1 |
| 2. | MÉTHODOLOGIE | 3 |
| 3. | Évaluation de la protection des renseignements personnels dans le cadre du PPICS .. | 4 |
| 3.1. | APERÇU..... | 4 |
| 3.2. | ÉVALUATION DES ASPECTS POUR L'ENSEMBLE DES PROJETS | 4 |
| 3.2.1. | Méthodologie utilisée pour la cotation | 4 |
| 3.2.2. | Analyse de l'aspect « patient »..... | 6 |
| 3.2.3. | Analyse de l'aspect « relations humaines » | 7 |
| 3.2.4. | Analyse de l'aspect « processus » | 9 |
| 3.2.5. | Analyse de l'aspect « sécurité » | 10 |
| 3.2.6. | Analyse de l'aspect « gestion de l'information »..... | 12 |
| 3.3. | RÉDUCTION DES RISQUES ASSOCIÉS À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE PPICS | 13 |
| 3.3.1. | Réduction au moyen de leadership | 13 |

1. SOMMAIRE

En avril 2000, Santé Canada lançait le Programme des partenariats pour l'infrastructure canadienne de la santé (PPICS), un programme d'encouragement à frais partagés de deux ans qui a pour but de favoriser l'utilisation des technologies de l'information et des communications (TIC) afin d'améliorer la santé des Canadiens et les services de santé qui leur sont offerts. Les principaux secteurs visés par cette initiative sont la télésanté et les dossiers électroniques de santé. En tout, vingt-neuf projets ont été approuvés.

Afin de s'assurer que les projets sont conformes aux exigences en matière de confidentialité, Santé Canada a engagé PRIVA CTM pour que ce dernier évalue globalement cet aspect dans chacun des vingt-neuf (29) projets du PPICS.

Le présent rapport sur l'évaluation des lacunes relatives à la protection des renseignements personnels présente les résultats d'analyse de l'état actuel d'avancement de tous les projets pour que Santé Canada ait un aperçu des programmes de protection des renseignements personnels propres à ces projets. On a demandé à chacun des vingt-neuf (29) projets financés par le PPICS de répondre à une enquête sur la protection des renseignements personnels et d'être prêts à effectuer une entrevue de suivi. L'enquête est un outil d'auto-évaluation servant à évaluer les éléments liés à la confidentialité et à la sécurité dans chaque projet. Grâce à cette enquête, les gestionnaires de projets peuvent évaluer la conformité de leur projet aux lois et aux règlements applicables en ce qui concerne la protection des renseignements personnels, évaluer les moyens techniques utilisés à cet effet, examiner les politiques et les processus à ce sujet, et déterminer la conformité d'un projet aux principes du Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation (CSA). Les enquêtes ont servi à repérer les forces et les lacunes possibles des programmes de protection des renseignements personnels de chaque projet. Les résultats ont été présentés sous forme de diagramme afin d'évaluer et de cerner les tendances observables.

Les résultats pour l'ensemble des projets figurent à la rubrique Évaluation des aspects pour l'ensemble des projets, à la section 4, et comprennent les recommandations pour le PPICS en ce qui concerne les cinq secteurs touchés par la protection opérationnelle des renseignements personnels, à savoir : les patients, les relations humaines, les processus, la sécurité et la gestion de l'information. Les principales recommandations sont les suivantes :

- Efforts continus pour informer les patients des pratiques des projets en ce qui concerne le traitement de l'information
- Formation personnalisée sur la protection des renseignements personnels et la sécurité, qui doit être offerte dans chaque site
- Ressources sur la protection des renseignements personnels, disponibles sur place
- Procédures de résolution des incidents relatifs à la protection des renseignements personnels et à la sécurité
- Vérification de la sécurité ou évaluation de la menace et des risques au moins une fois par année ou chaque fois qu'un nouveau système est introduit dans le milieu actuel
- Stratégies suggérées pour gérer les risques associés à l'utilisation du télécopieur

Lorsque le présent rapport était rédigé, dix-neuf projets avaient répondu à l'enquête et treize d'entre eux avaient été interviewés. Par conséquent, ce rapport présente séparément les résultats de l'évaluation sur la confidentialité pour les projets qui ont répondu à l'enquête et fait l'objet

d'une entrevue de suivi et pour ceux qui ont seulement répondu à l'enquête. Quant aux projets pour lesquels il n'y a pas eu d'entrevue, l'évaluation des lacunes comprend les résultats (fondés sur les réponses à l'enquête), mais elle ne comporte pas de recommandations puisqu'il est difficile de formuler des recommandations pertinentes sans une entrevue pour confirmer ou clarifier les réponses.

2. MÉTHODOLOGIE

On a demandé à chacun des vingt-neuf (29) projets financés par le PPICS de répondre à une enquête sur la protection des renseignements personnels. Chaque fois qu'on recevait les réponses d'un projet, on prévoyait une entrevue de suivi afin de clarifier et d'approfondir les réponses. Selon le projet et les réponses données à l'enquête, l'entrevue pouvait durer de quelques minutes à une heure et demie. La plupart des entrevues ont pris environ une heure. Les projets qui avaient effectué une évaluation de l'incidence sur la protection des renseignements personnels n'étaient pas tenus de répondre à l'enquête; ils avaient la possibilité de faire parvenir le document de l'évaluation. Certains projets ont joint à leurs réponses des renseignements supplémentaires, comme des politiques sur la protection des renseignements personnels.

L'enquête sur la protection des renseignements personnels permet d'analyser les pratiques d'un projet à partir de cinq principaux aspects, à savoir :

- o **Patients** –la relation entre le projet et les patients.
- o **Relations humaines** –la relation entre le projet, ses employés et ses partenaires.
- o **Processus** –la manière dont le projet administre son programme de protection des renseignements personnel et de sécurité.
- o **Sécurité** – les mesures de sécurité physiques, techniques ou opérationnelles, les moyens de communications, et les bases de données qui sont utilisés pour protéger les renseignements personnels détenus ou régis par le projet.
- o **Gestion de l'information** – les pratiques du projet en ce qui concerne le traitement de l'information.

Le rapport final a été réalisé à partir d'une évaluation de tous les projets qui ont répondu à l'enquête ou qui ont fait une évaluation de l'incidence sur la protection des renseignements personnels. Un rapport individuel a été produit pour chaque projet qui a retourné l'enquête ou fait parvenir une évaluation de l'incidence. Le rapport présente une analyse des forces et des lacunes des projets en ce qui concerne chacun des cinq aspects, et un sommaire des solutions actuelles et prévues pour chaque projet (p. ex., des outils et des procédures de protection des renseignements personnels). Les recommandations sont fondées sur les mesures correctives que devrait utiliser le projet pour être conformes aux lois applicables et aux meilleures pratiques en matière de protection des renseignements personnels.

On analyse également le PPICS en général, et on formule des recommandations afin de réduire les risques associés à la protection de renseignements personnels du point de vue de la gestion de projet à Santé Canada.

3. Évaluation de la protection des renseignements personnels dans le cadre du PPICS

3.1. Aperçu

Les projets du PPICS sont de vastes projets de collaboration qui touchent les systèmes de télésanté et les dossiers de santé électroniques.

Tous les projets sont uniques et traitent de questions particulières liées à l'utilisation des renseignements concernant les patients; certains transfèrent et entreposent les renseignements des patients par voie électronique (un dossier de santé électronique), tandis que d'autres recourent à des consultations vidéo, mais n'entreposent pas les données des patients (télésanté).

La question qui se pose pour les projets faisant appel au dossier électronique de santé (DES) est qu'ils sont axés sur les renseignements recueillis et sur la personne qui y aura accès. Quant aux projets faisant appel aux consultations de télésanté, ce n'est pas tant l'accès à l'information qui pose problème, mais bien comment les séances sont organisées et s'il faut les enregistrer. L'analyse suivante tient compte de ces questions.

3.2. Évaluation des aspects pour l'ensemble des projets

3.2.1. Méthodologie utilisée pour la cotation

Afin d'évaluer les lacunes, les questions où on a répondu « Non » par opposition à « Oui » ont été cotées de manière différente, comme il est indiqué ci-dessous. Si le projet comporte des pratiques en matière de protection des renseignements personnels, il a répondu « Oui ». Les trois niveaux associés à la réponse « Oui » servent à indiquer la qualité de la pratique en fonction des meilleures pratiques.

| Réponse | Sens | Cote d'évaluation des lacunes |
|---------|--|-------------------------------|
| Non | Aucune pratique de la protection des renseignements personnels n'est en place dans le cadre du projet. | 4 |
| Oui - 1 | La pratique existe, mais elle est de qualité médiocre. | 2 |
| Oui - 2 | La pratique existe, mais elle est de qualité moyenne. | 1 |
| Oui - 3 | La pratique existe, et répond aux normes des meilleures pratiques. | 0 |

L'outil dynamique Excel applique cette échelle de cotation à chaque question posée pendant l'enquête, ce qui a permis d'obtenir une cote finale d'évaluation des lacunes pour chaque projet en fonction des réponses « Oui » et « Non ». Par exemple, un « Non » indique qu'un projet ne possède pas la pratique en matière de protection des renseignements personnels; il y a donc lacune.

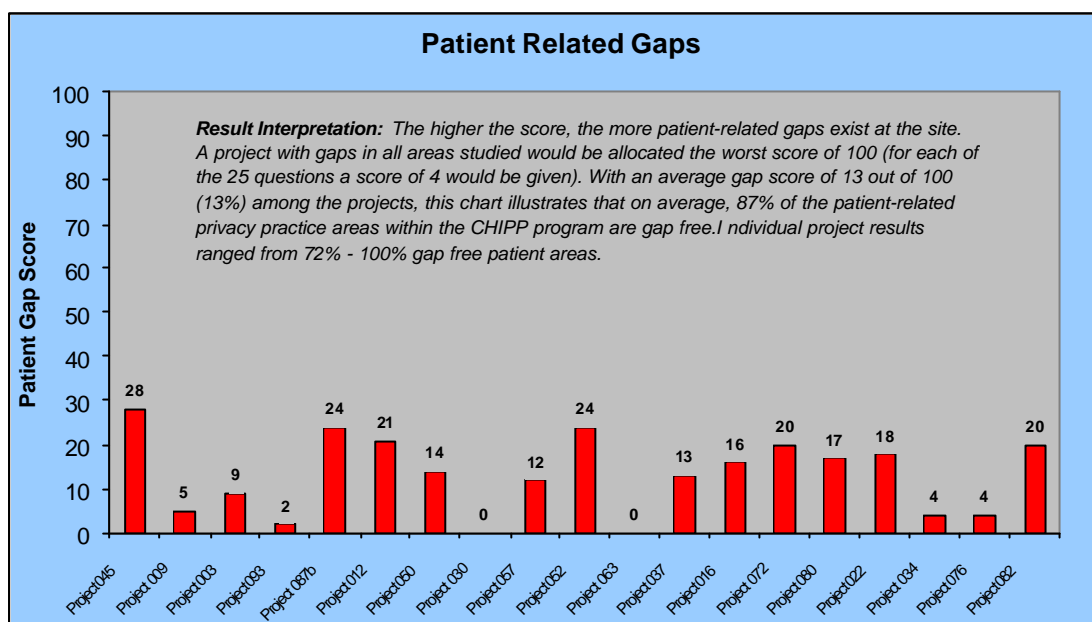
L'outil génère des graphiques en fonction des résultats obtenus pour chaque projet. Ces graphiques servent de guide pour l'analyse. Il est important de noter que l'enquête est quelque peu subjective puisque les projets peuvent utiliser divers critères d'évaluation pour déterminer si un « Oui » équivaut à un « 1 » ou à un « 2 ». Les entrevues postérieures à l'enquête visent à réduire au maximum la subjectivité. Comme les projets ne sont pas tous rendus à la même étape

de mise en oeuvre et qu'ils sont influencés de diverses façons par le milieu, tant à l'externe qu'à l'interne, il est difficile de les comparer. Par exemple, le projet 012 a répondu à de nombreuses questions en fonction des pratiques du ministère territorial de la santé et des services sociaux. Quant au projet 009, aux premières étapes de la mise en oeuvre, il n'était pas en mesure de répondre à toutes les questions. PRIVA-C™ a pris en considération les circonstances propres à chaque projet lorsqu'elle a effectué les évaluations.

Les résultats des projets qui n'ont pas été interviewés devront être examinés compte tenu du fait que les réponses n'ont pas encore été confirmées ou clarifiées. Il est à noter que le graphique suivant contient deux cotes différentes pour le projet 087. Les employés travaillant à ce projet ont mentionné qu'ils ne pouvaient pas répondre seulement à une enquête pour le projet, en raison de la diversité des volets cliniques et des sites de partenaires. Une enquête concerne le volet A du projet 087 (projet 087a) et l'autre, le volet B (projet 087b).

Remarque : Il a été impossible d'effectuer une analyse approfondie du projet 087a pour la majorité des mesures; le personnel a répondu «Non» et a mentionné qu'aucun élément supplémentaire n'a été ajouté aux politiques actuelles du site en ce qui concerne les services de télésanté. Sans une entrevue de suivi, il a été impossible d'évaluer précisément ces pratiques ou de tirer des conclusions sur les pratiques en matière de protection des renseignements personnels du projet. Par conséquent, l'évaluation suivante du projet 087 vise seulement le volet B.

3.2.2. Analyse de l'aspect « patient »



| | |
|---------------------------------------|------|
| Nombre de mesures | 25 |
| Cote moyenne d'évaluation des lacunes | 12 |
| Cote médiane | 12.5 |
| Cote la plus basse | 0 |
| Cote la plus élevée | 28 |

Résultats

En général, les projets comportent des pratiques très solides en matière de protection des renseignements personnels des patients. (Voir la section Interprétation des résultats du graphique ci-dessus.) Voici certaines de leurs forces communes :

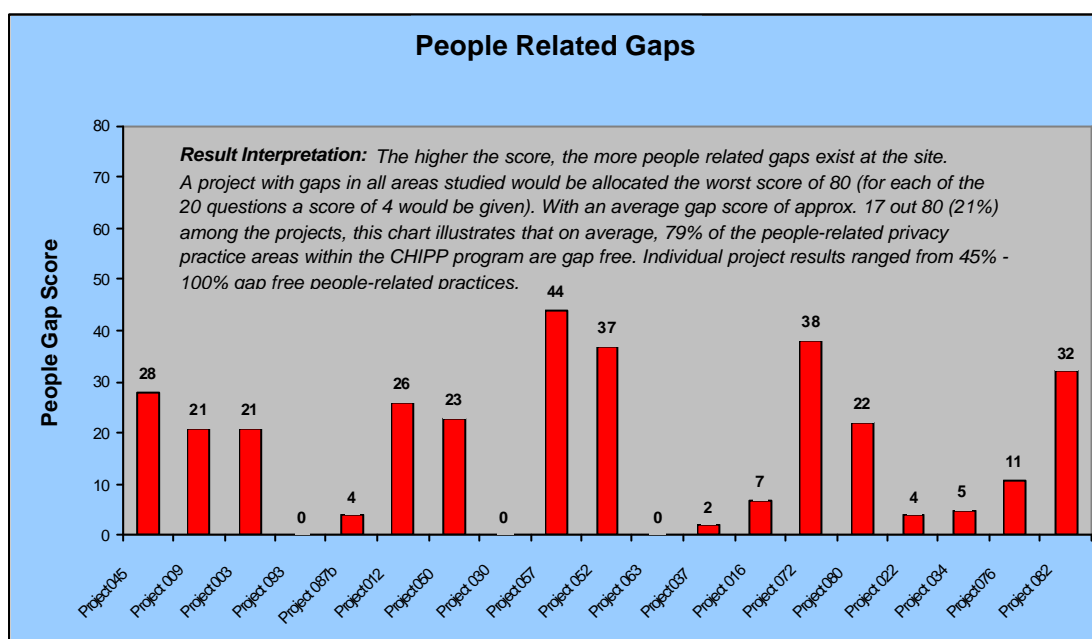
- Obtenir le consentement du patient, au besoin
- Informer le patient de l'utilisation des renseignements
- Indiquer au patient les buts de la collecte d'information
- Certains projets comportent d'excellents plans de communication publique, lesquels prévoient l'utilisation de brochures informatives et de sites Web efficaces.

Recommandations

- *Améliorer la communication aux points de collecte* – Un grand nombre de projets n'ont pas de stratégie de communication détaillée sur la protection des renseignements personnels des patients. Il est particulièrement important d'utiliser des brochures, des affiches ou des messages verbaux lors de la première collecte d'information (lorsque le patient utilise le système pour la première fois) afin d'indiquer au patient toutes les façons dont seront utilisés ou divulgués ses renseignements personnels.

- *Éducation continue* – Dans le cadre des projets, il arrive fréquemment que l'on recoure à des technologies ou à des procédures inconnues d'un grand nombre de patients. Il faut donc bien informer les patients afin de les rendre plus à l'aise avec le processus, et les assurer que leurs renseignements seront bien protégés. On recommande aux projets qui ne l'ont pas déjà fait d'utiliser leur site Web et d'autres moyens (p. ex., des brochures, des affiches) comme moyens de communication afin d'informer continuellement les patients des pratiques du projet en matière de protection des renseignements personnels.

3.2.3. Analyse de l'aspect « relations humaines »



| | |
|---------------------------------------|------|
| Nombre de mesures | 20 |
| Cote moyenne d'évaluation des lacunes | 16 |
| Cote médiane | 16.5 |
| Cote la plus basse | 0 |
| Cote la plus élevée | 38 |

Résultats

Dans l'ensemble, les projets du PPICS s'occupent bien de l'aspect « relations humaines » dans la protection des renseignements personnels. Cependant, il y a lieu d'apporter plus d'améliorations que pour l'aspect « patient ».

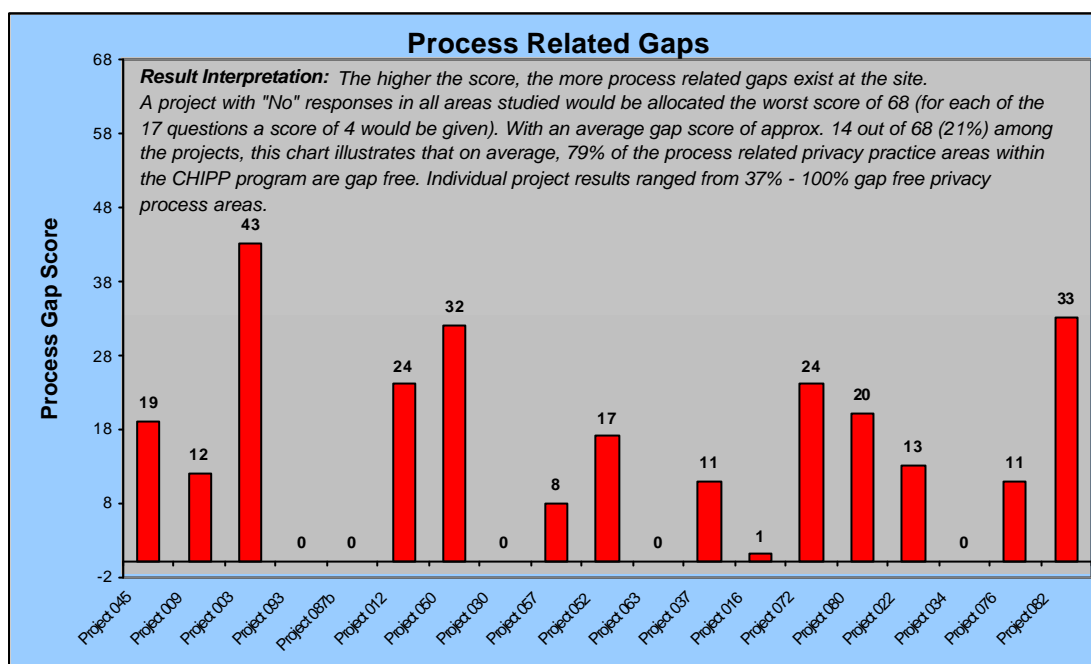
- La majorité des projets ont indiqué que la protection des renseignements personnels, la sécurité et la confidentialité sont des priorités importantes pour l'équipe de gestion principale.

- En ce qui concerne les projets qui se déroulent dans plusieurs sites éloignés, des coordonnateurs de sites ont été nommés et des gestionnaires de division supervisent les opérations relatives aux sites éloignés dont ils sont en charge.
- Tous les projets comportent des politiques quelconques de protection des renseignements personnels pour l'aspect «ressources humaines», qui sont une combinaison de ce que chaque projet utilise. Parmi les politiques communes, on compte des politiques et des procédures sur l'utilisation acceptable qui ont pour but de révoquer ou de changer les privilèges en ce qui concerne l'accès aux renseignements.
- Les projets exigent bel et bien que les renseignements personnels soient protégés lors de la passation de marchés avec des tierces parties; cependant, peu de projets vérifient et examinent activement la conformité des tierces parties aux pratiques en matière de protection des renseignements personnels.
- La plupart des projets ont nommé une personne externe (p. ex., un employé d'hôpital ou un agent régional) comme personne-ressource sur la protection des renseignements personnels pour traiter les questions ou les plaintes des patients à cet égard.

Recommandations

- *Formation personnalisée sur la protection des renseignements personnels et la sécurité, qui doit être offerte dans chaque site* – Bien que la plupart des employés du projet reçoivent à un moment ou à un autre une formation générale à ce sujet, celle-ci n'est pas générique et propre au projet. Chaque projet devrait offrir une formation axée sur ses propres préoccupations en matière de traitement de l'information et de la sécurité. De plus, on devrait y ajouter un volet spécialisé pour les employés qui traitent et qui gèrent l'information.
- *Ressources sur la protection des renseignements personnels disponibles sur place* – Il faut nommer une personne au sein du projet à qui les employés et les patients puissent communiquer leurs préoccupations ou leurs questions liées à la protection des renseignements personnels. Cette personne pourrait ensuite communiquer avec les personnes-ressources externes, au besoin. Ainsi, le processus sera normalisé et la méthode de résolution des problèmes, uniformisée.
- *Composante de protection des renseignements personnels et de sécurité, qui doit être intégrée aux fonctions* – Les descriptions de travail des employés du projet et leurs examens de rendement réguliers doivent comprendre des exigences et des responsabilités liées à la protection des renseignements personnels et à la sécurité.

3.2.4. Analyse de l'aspect « processus »



| | |
|---------------------------------------|------|
| Nombre de mesures | 17 |
| Cote moyenne d'évaluation des lacunes | 15 |
| Cote médiane | 12.5 |
| Cote la plus basse | 0 |
| Cote la plus élevée | 43 |

Résultats

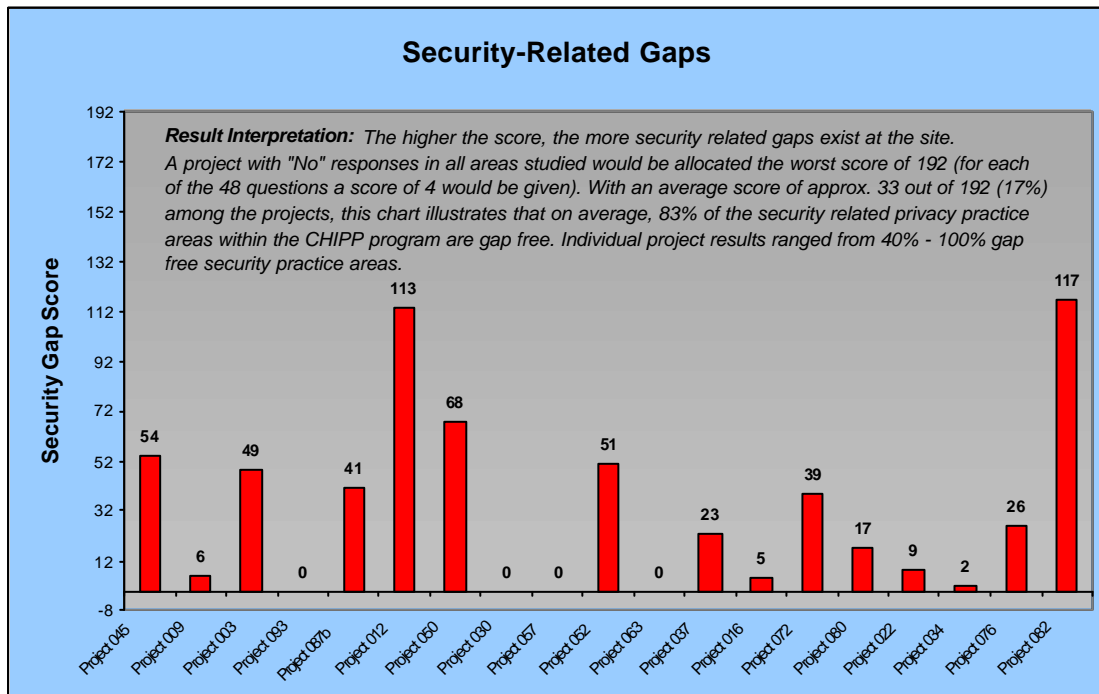
Les projets du PPICS comportent plusieurs processus solides visant à protéger l'information des patients; toutefois, ces processus ont quelques faiblesses. Donc, quelques secteurs doivent être améliorés.

- En général, les projets utilisent les politiques en matière de protection des renseignements personnels en place dans les sites où ils sont installés (le site central ou l'hôpital); des politiques particulières directement liées au projet n'ont pas été créées. (Il est à noter que le personnel des projets n'était pas certain des politiques actuellement en place dans les sites éloignés qui faisaient peut-être partie de leur projet.)
- Seuls quelques projets comptaient une personne responsable des médias de masse ou une procédure à cet égard. Dans chaque projet, une personne doit occuper la fonction de personne-ressource pour gérer les relations publiques, et tous les employés doivent transmettre les questions liées aux relations publiques à cette personne.
- Dans quatre projets seulement, une évaluation officielle de l'incidence sur la protection des renseignements personnels a été effectuée.

Recommandations

- *Politiques adaptées en matière de protection des renseignements personnels* – Il faut évaluer la pertinence des politiques actuellement utilisées par chaque site par rapport aux projets. Il faut ensuite les adapter, au besoin, afin qu'elles s'appliquent à tous les processus de traitement de l'information propres au projet.
- *Relations liées à la protection des renseignements personnels* – Une personne-ressource doit être nommée dans tous les projets; elle s'occupera de la protection des renseignements personnels et de la sécurité en ce qui concerne les questions et les demandes de renseignements des médias de masse.
- *Procédures pour les incidents liés à la protection des renseignements personnels* – Il est important que les projets élaborent un processus en vue de cerner les manquements ou les incidents relatifs à la protection des renseignements personnels et à la sécurité, et de réagir à cet égard. Ce processus doit également définir les méthodes à utiliser pour communiquer les violations aux personnes appropriées, c'est-à-dire à la personne faisant objet des données, aux autorités responsables de l'application des lois ou aux gestionnaires de projets appropriés. (Pour de plus amples renseignements, voir les recommandations pour la réduction des risques associés à la protection des renseignements personnels dans le cadre du PPICS, à la section 4.3.)
- *Exécution d'évaluations de l'incidence sur la protection des renseignements personnels* – Comme tous les projets constituent des initiatives de systèmes d'information, il faut effectuer des évaluations régulières de l'incidence sur la protection des renseignements personnels pour tous les projets.

3.2.5. Analyse de l'aspect « sécurité »



| | |
|---------------------------------------|------|
| Nombre de mesures | 48 |
| Cote moyenne d'évaluation des lacunes | 34 |
| Cote médiane | 23.5 |
| Cote la plus basse | 0 |
| Cote la plus élevée | 117 |

Résultats

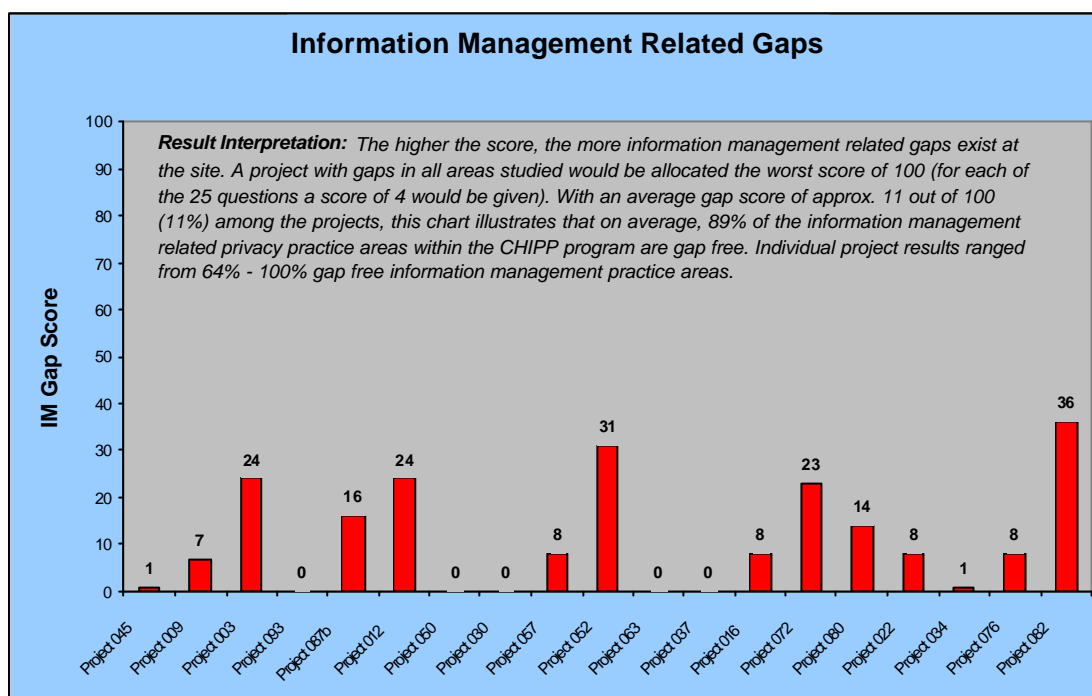
Les projets utilisent des mesures de protection dont le niveau varie afin de protéger l'information des patients.

- Les projets utilisent des réseaux sécuritaires comportant des mesures de protection, comme des pare-feu et des mécanismes de surveillance des réseaux.
- Dans l'ensemble, des mesures de sécurité physique sont en place : des zones de restriction (p. ex., salle de l'ordinateur TI principal) avec des contrôles d'accès pour les secteurs où se trouve l'équipement sensible et les données délicates.
- Dans le cadre des projets recourant à la téléconsultation, les séances sont effectuées dans des pièces insonorisées.
- Des noms d'utilisateurs et des contrôles d'accès uniques ont été mis en place afin d'accéder à tous les sites, au besoin. La plupart des projets ont effectué un inventaire des dispositifs des réseaux, des films et de l'équipement vidéo, des logiciels, du matériel de communication, et des bases de données.

Recommandations

- *Politiques sur la sécurité* – Il faut élaborer et mettre en oeuvre des politiques sur la sécurité. Dans les projets faisant appel à la téléconsultation, il faut également adapter les politiques actuelles sur la sécurité, afin de réduire les risques associés à la sécurité.
- *Copie de sauvegarde des données* – Toutes les copies de sauvegarde comportant des renseignements délicats doivent être entreposées dans des endroits sécuritaires à l'extérieur des sites.
- *Sécurité physique* – L'équipement pour les téléconsultations ou les DES doit être entreposé dans des pièces fermées à clé ou autres afin de prévenir les vols.
- *Vérification de la sécurité et évaluation de la menace et des risques* – Il faut effectuer des vérifications de la sécurité et des évaluations de la menace et des risques au moins une fois par année ou chaque fois qu'un nouveau système est introduit dans le milieu actuel.
- *Mesures de protection* – Il faut faire en sorte que les téléconsultations effectuées dans le cadre de projets soit réalisées dans des pièces sécuritaires et insonorisées.

3.2.6. Analyse de l'aspect « gestion de l'information »



| | |
|---------------------------------------|----|
| Nombre de mesures | 24 |
| Cote moyenne d'évaluation des lacunes | 12 |
| Cote médiane | 8 |
| Cote la plus basse | 0 |
| Cote la plus élevée | 31 |

Résultats

Le rendement relatif à la protection des renseignements personnels dans le secteur de la gestion de l'information est divers, mais en général très bon. Plusieurs projets doivent être grandement améliorés (en particulier, si l'on compare les résultats à ceux concernant les patients et les relations humaines; de plus, plusieurs projets ne comportent que quelques lacunes).

- La plupart des projets recourant aux DES ont une fonction de vérification et divers niveaux d'accès pour les utilisateurs déterminés par le rôle de l'utilisateur.
- Les projets qui font appel aux consultations vidéo en direct n'enregistrent pas les séances, à l'exception d'un projet où les séances sont filmées uniquement à des fins éducatives (pour former les chirurgiens).
- Certains projets n'ont pas d'inventaire des données détenues, permettant de repérer les buts principaux et secondaires de l'information.
- De nombreux projets (comme ceux recourant à la téléconsultation) communiquent l'information par télécopieur.

Recommandations

- *Politiques et procédures sur l'accès* – Tous les projets doivent avoir des politiques et des procédures pour accorder les privilèges d'accès selon les fonctions des postes et les révoquer ou les modifier s'il y a un changement dans les fonctions.
- *Lignes directrices pour la collecte* – Il faut mettre en oeuvre une politique visant l'ensemble du PPICS pour savoir quand il est approprié d'enregistrer les consultations vidéo, et d'offrir d'autres services afin que les pratiques du PPICS soient uniformes. Les lignes directrices devraient également indiquer comment informer les patients et obtenir leur consentement avant de commencer l'enregistrement.
- *Inventaire des données détenues* – Tous les projets doivent avoir un inventaire des données détenues où sont indiqués les buts principaux et secondaires de l'information.
- *Diminution des risques associés aux télécopieurs* – Les projets doivent gérer les risques associés aux télécopieurs :
 - en évitant le plus possible de les utiliser (p. ex., envoyer par courrier l'information personnelle à délai de livraison critique)
 - en programmant dans les télécopieurs les numéros utilisés régulièrement
 - en établissant des procédures de confirmation afin de veiller à ce que la télécopie soit reçue pas la partie externe (p. ex., appel pour confirmer la réception dans les cinq minutes suivant l'envoi de la télécopie)

3.3. Réduction des risques associés à la protection des renseignements personnels dans le PPICS

3.3.1. Réduction au moyen de leadership

Le Bureau de la santé et l'inforoute et les chefs de projets du PPICS assument le rôle complexe d'appuyer de nombreux projets indépendants. Le Bureau doit exercer un leadership auprès des sites en supervisant les pratiques en matière de protection des renseignements personnels. Actuellement, les sites présentent régulièrement aux chefs de projets des rapports sur l'état d'avancement de leur projet; mais il manque une orientation continue en ce qui concerne la protection des renseignements personnels. Le Bureau de la santé et l'inforoute a la possibilité de rehausser le niveau de ses relations avec les projets afin de fournir un leadership sur la protection des renseignements personnels et de réduire les risques en surveillant régulièrement les pratiques au sein des projets.

On recommande ci-dessous des moyens pour réduire l'exposition aux risques associés à la protection des renseignements personnels à Santé Canada :

Responsabilisation en matière de protection des renseignements personnels

- Établir des procédures régulières pour que les employés de Santé Canada examinent les mesures de protection des renseignements personnels. Les examens serviront à vérifier la conformité des projets aux lois fédérales et provinciales, ainsi qu'aux principes du *Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation*. (La conformité à la loi faisait partie des exigences obligatoires dans les propositions de projets originales.)

Application des mesures de la protection des renseignements personnels

- Les employés de Santé Canada doivent également faire en sorte que le personnel clé de chaque projet reçoit les rapports ci-joints sur l'évaluation des lacunes en matière de protection des renseignements personnels et qu'il les comprend bien, de sorte que des mesures puissent être prises pour combler les lacunes repérées.
- Santé Canada doit encourager l'exécution d'évaluations de l'incidence sur la protection des renseignements personnels au sein des projets qui n'ont toujours pas procédé à une telle évaluation. Il est possible de se procurer des lignes directrices sur la façon de réaliser des évaluations de l'incidence auprès de certaines administrations : lignes directrices du Secrétariat du Conseil de gestion de l'Ontario sur la protection de la vie privée, British Columbia Ministry of Management Services Corporate Privacy Impact Assessment Guidelines et Government of Alberta Privacy Impact Assessment Guidelines. En l'absence de lignes directrices sur la protection des renseignements personnels, les projets peuvent utiliser les *Politiques et les lignes directrices sur la protection des renseignements personnels du Secrétariat du Conseil du Trésor*.

Facilitation de l'apprentissage partagé

- Il faut cerner les projets qui ont des pratiques exemplaires en matière de protection des renseignements personnels (dans n'importe quel secteur opérationnel) et réunir leurs processus relatifs aux meilleures pratiques en un dossier collectif sur les leçons tirées. L'information doit être ensuite diffusée auprès des projets afin de favoriser l'établissement d'un milieu d'apprentissage partagé, ce qui améliorera les pratiques en matière de protection des renseignements personnels au sein des projets et renforcera les pratiques louables.

Aide relative à la protection des renseignements personnels

- Santé Canada doit fournir une orientation en matière de protection des renseignements personnels à tous les projets, en les informant de toutes les politiques à ce sujet et en répondant à toutes les demandes éventuelles de renseignements sur la procédure. Il faut transmettre aux sites l'information sur les personnes-ressources pertinentes afin que les employés des projets sachent à qui poser des questions liées à la protection des renseignements personnels.