

Rapport annuel 2025-2026 de Santé Ontario sur la protection de la vie privée et la sécurité

Mai 2026

Table des matières

Message du Directeur Général de la protection de la vie Privée et du Vice-Président, Cybersécurité et Services Fondamentaux.....	3
Introduction	4
Pleins feux sur la stratégie	6
Protection de la vie privée vs sécurité.....	9
Programme de cybersécurité.....	9
Programme de confidentialité	10
Loi sur la protection de la vie privée	12
Évolution du paysage réglementaire.....	13
Points clés en matière de confidentialité et de sécurité	13
Protection de la vie privée et sécurité en chiffres : Indicateurs clés	20
Points saillants des indicateurs clés de la protection de la vie privée	20
Points saillants des indicateurs de sécurité	24
Perspectives d'avenir	26
Annexe	30
Acronymes.....	30
Autorités de santé publiques de l'Ontario	32

Rapport 2025-2026 de Santé Ontario sur la protection de la vie privée et la sécurité

MESSAGE DU DIRECTEUR GÉNÉRAL DE LA PROTECTION DE LA VIE PRIVÉE ET DU VICE-PRÉSIDENT, CYBERSÉCURITÉ ET SERVICES FONDAMENTAUX

Depuis la création de Santé Ontario en 2019, nous nous sommes attachés à intégrer et à relier les différents maillons du système de santé afin d'améliorer les soins de santé prodigués aux Ontariens. Du point de vue de la confidentialité et de la sécurité, cela implique que d'énormes volumes de données doivent être collectés, partagés et conservés en toute sécurité.

Dans le même temps, le paysage numérique évolue plus rapidement que jamais, et à mesure que l'intelligence artificielle se généralise, l'omniprésence de cette technologie ainsi que les possibilités apparemment illimitées qu'elle offre en matière d'intégration dans les systèmes de santé exigent une vigilance accrue en matière de sécurité, ainsi qu'une réflexion approfondie sur les implications en termes de confidentialité et de sécurité.

Parallèlement, nous devons également faciliter l'accès aux données existantes et leur circulation afin de garantir une prestation efficace des soins de santé. À cette fin, nos équipes ont apporté une contribution importante à la conception des applications destinées aux cliniciens et aux patients, ainsi qu'aux initiatives Les patients avant la paperasse, afin de garantir que ces outils soient développés en accordant la priorité à la confidentialité et à la sécurité.

Il convient de noter que l'exercice financier 2025/2026 a marqué le début d'un nouveau cycle de révision triennale imposant la présentation de rapports détaillés au Commissaire à l'information et à la protection de la vie privée.

Les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité restent très actives et prévoient encore beaucoup d'activités au cours de l'exercice financier 2026/2027. Qu'il s'agisse d'apporter des innovations à notre système de santé, de faciliter l'accès à l'information ou de s'adapter pour répondre aux besoins numériques de demain, nos équipes ont à cœur de protéger la confidentialité et la sécurité de notre système de santé ainsi que des données personnelles qu'il contient.

Nadia Remtulla
Directeur, Protection de la vie privée et Directeur
général de la protection de la vie privée



Greg Moshonas
Vice-président, Cybersécurité et Services
fondamentaux



Introduction



Santé Ontario a été créée en vertu de la *Loi de 2019 sur la connexion des soins*, avec pour mission de connecter, de coordonner et de moderniser le système de santé de notre province. Santé Ontario supervise la prestation et la qualité des services cliniques, gère le financement et la responsabilisation de certaines parties du système de santé et mesure le rendement du système. Collectivement, ce travail permettra de garantir que les Ontariens reçoivent les meilleurs soins possibles, centrés sur le patient, au moment et à l'endroit où ils en ont besoin.

Notre travail est guidé par six priorités stratégiques à long terme :

- Réduire les inégalités en matière de santé
- Transformer les soins en plaçant la personne au cœur de l'approche
- Gestion opérationnelle du système de santé
- Améliorer les soins cliniques et l'excellence des services
- Maximiser la valeur du système en appliquant des preuves
- Renforcer la capacité de Santé Ontario à diriger

Pour remplir sa mission, Santé Ontario a besoin d'accéder aux données, y compris aux renseignements personnels sur la santé (RPS) et aux renseignements personnels (RP), des organisations et des particuliers de l'ensemble de l'Ontario. Lors du traitement de ces renseignements, Santé Ontario est assujettie à la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS), à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) et à la *Loi sur le don de vie* et s'engage à respecter les droits à la vie privée des personnes, à protéger leurs renseignements et à se conformer aux lois ontariennes sur la protection de la vie privée.

SI LES PATIENTS ESTIMENT QUE LES INFORMATIONS LES PLUS SENSIBLES LES CONCERNANT NE SONT PAS PROTÉGÉES, ILS PEUVENT LES DISSIMULER, CE QUI POURRAIT AVOIR DES REPERCUSSIONS SUR LEURS SOINS.

Santé Ontario doit continuellement démontrer sa capacité à protéger les milliards de données qu'il détient. Cela commence par instaurer la confiance dans les mesures de protection de la vie privée et de sécurité afin de garantir que les Ontariens puissent continuer à recevoir les meilleurs soins possibles.

Au cours de l'exercice 2025-2026, les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité de Santé Ontario, en collaboration avec d'autres partenaires commerciaux de Santé Ontario et de la province, ont continué de travailler ensemble pour permettre l'accès, répondre aux nouvelles dispositions de la LPRPS et faciliter la protection des données, la cybersécurité, l'interopérabilité et d'autres questions de conformité, tout en faisant évoluer et en faisant mûrir continuellement nos programmes de protection de la vie privée et de cybersécurité.

Ce rapport annuel sur la protection de la vie privée et la sécurité décrit les programmes de protection de la vie privée et de cybersécurité de Santé Ontario et présente un aperçu des principales

réalisations de l'exercice financier 2025/2026, qui visent à soutenir et à faire progresser Santé Ontario dans la réalisation de sa mission. Le rapport passe également en revue les indicateurs clés, dont certains sont communiqués au Commissaire à l'information et à la protection de la vie privée de l'Ontario (**CIPVP**), et présente les priorités en matière de protection de la vie privée et de sécurité pour l'exercice financier 2026/2027.

Pleins feux sur la stratégie

Projets en matière de confidentialité et de sécurité mettant en avant les priorités stratégiques

Réduire l'inégalité en matière de santé

Dépistage du cancer dans les communautés isolées

Dans le cadre du programme de dépistage du cancer colorectal ContrôleCancerColorectal Ontario, Santé Ontario offre l'option « Trousses à portée de main » aux Premières Nations vivant dans des communautés éloignées. Mises en place en partenariat avec ces communautés, les trousseaux sont fournies directement aux centres de santé et aux postes de soins infirmiers locaux. Désormais, les professionnels de la santé peuvent remettre des trousseaux aux patients admissibles lors de leurs consultations habituelles, ce qui élimine la nécessité d'attendre le courrier ou de se déplacer dans une autre communauté. Ce programme encourage des échanges constructifs entre les membres de la communauté et les professionnels de santé de confiance, et garantit que les RPS des patients ne sont utilisés que pour identifier les personnes admissibles et communiquer les résultats des tests



Transformer les soins en plaçant la personne au cœur de l'approche

Activation du visualiseur provincial des patients



Pour soutenir l'initiative d'accès intégré aux soins des patients (AIP) aux services de santé numériques du ministère de la Santé, Santé Ontario a développé le projet pilote d'application Visualiseur provincial des patients (VPP), qui permettra aux personnes d'accéder à leurs dossiers de santé dans le système provincial de dossier de santé électronique (DSE). Lors de sa première mise en service, les personnes pourront accéder à leurs dossiers du Système d'information des laboratoires de l'Ontario (SILO) et du Répertoire numérique des médicaments (RNM) et pourront également demander l'accès à leurs dossiers d'audit du DSE et à leurs dossiers d'identifiant numérique de santé (DHI). En consultation avec le Commissaire à l'information et à la protection de la vie privée de l'Ontario, le ministère de la Santé et les fournisseurs, Santé Ontario a mis en œuvre des contrôles techniques et administratifs pour protéger les RPS des patients tout en les rendant accessibles à chaque personne, comme l'exige la LPRPS.

Gestion opérationnelle du système de santé

Harmonisation du consentement

Santé Ontario a élaboré et mis en œuvre un modèle visant à harmoniser la gestion du consentement au sein du DSE, afin de remédier aux difficultés liées à la gestion fragmentée du consentement, qui résultaient des différences entre les technologies de stockage et les structures héritées. Ces modifications permettent d'harmoniser les modalités des directives de consentement, d'aligner les exigences de documentation pour les dérogations au consentement et de simplifier le processus pour les personnes qui en font la demande.

En donnant la priorité à ces changements, nos équipes aident les patients à mieux comprendre leurs droits en matière d'information et évitent ainsi les retards dans d'autres initiatives dépendant du nouveau modèle harmonisé.



Améliorer l'excellence des soins cliniques et des services

Transplantation d'organes : Intégrations de systèmes

Le soutien apporté à la phase 1 de l'intégration du Système d'allocation et de transplantation d'organes (SATO) avec le Système de données sur le don et la transplantation d'organes du Canada (CanODT) de l'Institut canadien d'information sur la santé (ICIS) a permis la soumission sécurisée et automatisée des données sur les receveurs de greffes et les donneurs vivants pour la production de rapports nationaux. Cette intégration améliore la qualité, la rapidité et l'efficacité des données tout en soutenant les activités vitales de don et de transplantation d'organes dans l'ensemble du système de santé. Nos équipes ont évalué l'intégration et formulé des recommandations afin de garantir que les RPS des patients ne soient accessibles qu'aux personnes requises à des fins de soins aux patients.



Maximiser la valeur du système en appliquant des preuves

Surveillance des capacités : Gestion des lits

En abandonnant la saisie manuelle et incohérente des données quotidiennes du recensement des lits au profit de l'utilisation des informations déjà envoyées au Répertoire des données cliniques sur les soins actifs et communautaires du DSE, Santé Ontario a amélioré la gestion et l'optimisation de la capacité des lits d'hôpitaux, permettant ainsi une surveillance plus rapide et plus complète tout en réduisant la charge de déclaration pour les hôpitaux.

En plus de garantir la confidentialité et la sécurité des données utilisées, ce projet s'alignait également sur une recommandation clé du rapport du Conseil ontarien des données sur la santé, qui stipulait : « Lorsque les données de santé sont utilisées à des fins positives, elles doivent être collectées une seule fois et utilisées à de nombreuses reprises à des fins appropriées et autorisées par la loi. »



Maximiser la valeur du système en appliquant des preuves

Utilisation des données et des services analytiques

Pour l'avenir, Santé Ontario continuera de collaborer avec le ministère de la Santé et le ministère des Soins de longue durée afin d'établir une autorité harmonisée en vertu de la Loi sur la protection des renseignements personnels sur la santé (LPRPS) pour Santé Ontario, ce qui améliorera la gouvernance des données et réduira les silos de données afin d'améliorer l'utilisation efficace et responsable des données dans l'ensemble du système de santé.



Protection de la vie privée vs sécurité

On peut avoir la sécurité sans avoir la protection de la vie privée, mais on ne peut pas avoir la protection de la vie privée sans avoir la sécurité.

Programme de cybersécurité



Le programme de cybersécurité de Santé Ontario est mis en œuvre grâce à un partenariat coordonné entre trois équipes spécialisées : le Centre de cybersécurité de Santé Ontario (OHCSC), le Bureau de la sécurité de l'information (ISO) et l'équipe de cybersécurité, de défense et de résilience (CSDR). Ensemble, ces équipes assurent la gouvernance, l'assurance et la capacité opérationnelle nécessaires pour protéger l'information et les actifs numériques au sein de Santé Ontario et soutenir la cyber-résilience dans l'ensemble du secteur provincial de la santé.

Gouvernance et partenariat en matière de cybersécurité



Le Centre de cybersécurité de Santé Ontario assure le leadership provincial, l'orientation stratégique et la gouvernance en matière de cybersécurité, soutenant une approche fondée sur les risques aux niveaux provincial, régional et des fournisseurs de services de santé.

Le Bureau de la sécurité de l'information établit la gouvernance de la sécurité de l'entreprise par le biais de l'architecture de sécurité, de la gestion des risques et de la conformité, de la gestion des risques liés à la sécurité des tiers, des évaluations des menaces et des risques et de la sensibilisation à la sécurité.

L'équipe Cybersécurité, Défense et Résilience assure les opérations de sécurité de première ligne, notamment la surveillance, la gestion des vulnérabilités, la gestion des identités et des accès, la réponse aux incidents, l'ingénierie des plateformes de sécurité et travaille au renforcement de la résilience numérique. Au cours de l'exercice financier, le périmètre de l'équipe a été élargi pour inclure une fonction de résilience numérique (continuité des activités et reprise après sinistre), favorisant un alignement plus étroit entre les opérations de sécurité et la planification de la reprise.

La sécurité est intégrée à tous les niveaux de Santé Ontario grâce à une approche de « sécurité dès la conception », qui consiste à intégrer des mesures de protection tout au long du cycle de vie du système afin de préserver la confidentialité, l'intégrité et la disponibilité des données et des services.

Programme de confidentialité



*La notion de **vie privée** désigne le droit fondamental des personnes à contrôler la circulation de leurs informations. Autrement dit, les personnes ont le droit de contrôler la manière dont leurs **informations** sont collectées, utilisées, divulguées, conservées et éliminées, dans la limite du raisonnable.*

Santé Ontario s'engage à respecter la vie privée et à protéger les RPS et les RP qu'elle détient ou contrôle. Pour appuyer cet engagement, Santé Ontario dispose d'un programme de protection de la vie privée robuste et adapté, conçu pour garantir qu'une culture de la protection de la vie privée soit non seulement établie, mais aussi ancrée dans l'ensemble de l'organisme, lui permettant ainsi de fonctionner conformément à ses obligations et responsabilités légales.

Santé Ontario estime que la loi constitue un minimum et non un maximum pour favoriser la conformité et le changement. C'est pourquoi elle s'appuie, comme fondement, sur les principes de « protection de la vie privée dès la conception » et les normes sectorielles qui contribuent à instaurer la confiance et à favoriser l'innovation. Santé Ontario doit constamment gagner et maintenir la confiance des Ontariens, du CIPVP, ainsi que de ses principaux intervenants et partenaires provinciaux afin de remplir sa mission.

Santé Ontario Vision, Mission, Valeurs



Notre vision

(Ce à quoi nous aspirons)

Ensemble, nous serons leaders pour la santé et le bien-être de tous.



Notre mission

(Notre raison d'être)

Créer des liens entre les systèmes de santé afin d'améliorer les résultats cliniques, les expériences et la valeur de manière équitable.



Nos valeurs

(Comment nous travaillerons ensemble)

- Intégrité
- Inspiration
- Ténacité
- Humilité
- Soins

Le Bureau de la protection de la vie privée est chargé de maintenir la confiance du public et de

protéger la vie privée des personnes tout en permettant l'utilisation des données conformément aux lois applicables en matière de protection de la vie privée afin de faire progresser la mission de Santé Ontario visant à optimiser les soins centrés sur le patient.



Par conséquent, le Bureau de la protection de la vie privée obtient l'approbation du CIPVP pour les politiques, les procédures et les pratiques de Santé Ontario tous les 3 ans, au moyen d'une révision triennale. Santé Ontario collabore actuellement avec le CIPVP dans le cadre du cycle de révision triennale de 2026. Cette révision démontre la diligence raisonnable et l'engagement continu de Santé Ontario à protéger la confidentialité,

l'intégrité et la disponibilité des renseignements des Ontariens grâce à des pratiques établies en matière de gouvernance, de gestion des risques, de protection de la vie privée et d'assurance de la sécurité.

Le programme de protection de la vie privée s'inscrit dans le portefeuille Stratégie, Planification, Protection de la vie privée, Analyse et Risques, où sont soutenus les efforts visant à éliminer les obstacles et à promouvoir les changements nécessaires à la transformation de l'écosystème des données de santé. Le programme de protection de la vie privée est dirigé par le Directeur général de la protection de la vie privée (DGPVP), qui relève directement du vice-président, Risques et protection de la vie privée et responsable des risques.

Une équipe de professionnels dévoués à la protection de la vie privée appuie le DGPVP dans le maintien de la confiance du public en gérant les opérations quotidiennes du Programme de protection de la vie privée de Santé Ontario, tout en atteignant un large éventail d'objectifs du Programme décrits ci-dessous.

En partenariat avec les équipes du programme de cybersécurité et d'autres partenaires commerciaux de tous les portefeuilles, le Bureau de la protection de la vie privée permet aux programmes et aux équipes d'atteindre les objectifs du plan d'activité annuel tout en minimisant les risques résiduels pour l'organisation en fournissant :

- des services opérationnels, de conseil et d'assurance
- des solutions de confidentialité pragmatiques, créatives et fondées sur les risques
- des exigences et des contrôles en matière de protection de la vie privée, qui seront intégrés dans les nouveaux projets, processus et programmes.

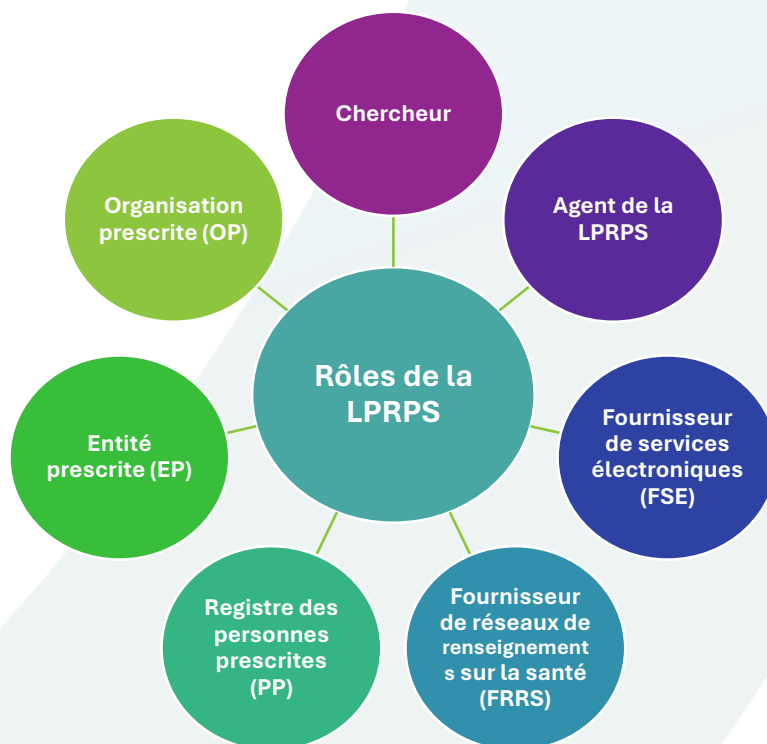
Loi sur la protection de la vie privée



Santé Ontario tire généralement son pouvoir de recueillir, d'utiliser et de divulguer des renseignements personnels sur la santé et des renseignements personnels des lois sur la protection de la vie privée, notamment la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), la *Loi de 1990 sur l'accès à l'information et la protection de la vie privée* (LAIPVP), la *Loi sur la connexion des soins*, la *Loi sur le don de vie* (GoLA), ainsi que des accords avec le ministère de la Santé.

Santé Ontario exerce ses activités dans le cadre de nombreux rôles et textes législatifs afin de remplir sa mission, notamment les suivants :

- organisation prescrite
- entité prescrite
- personne prescrite
- chercheur
- fournisseur de réseau d'information sur la santé
- agent de la LPRPS
- fournisseur de services électroniques
- institution relevant de la LAIPVP
- agence relevant de la GoLA



En vertu de ses pouvoirs légaux, Santé Ontario est en mesure de remplir sa mission et d'optimiser son utilisation autorisée des données à des fins positives.

Évolution du paysage réglementaire



Depuis 2019, le ministère de la Santé a pris des mesures importantes pour consulter les intervenants du secteur de la santé afin de « moderniser » la LPRPS. Parmi les facteurs

de changement, on peut citer l'accélération de la numérisation et de la virtualisation des soins et le soutien au droit des patients d'accéder numériquement à leurs dossiers médicaux. Ces changements ont une incidence directe sur Santé Ontario et sur les nombreux rôles importants qu'il joue pour aider à utiliser les données au profit de tous afin d'améliorer les soins aux patients.

Accès individuel au dossier de santé électronique (DSE) et aux identifiants numériques de santé (DHI)

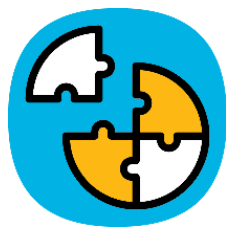
En janvier 2026, des modifications apportées à la LPRPS et au Règlement de l'Ontario n°329/04 sont entrées en vigueur. Elles autorisent et obligent Santé Ontario, en tant

qu'organisation prescrite, à permettre aux personnes d'accéder à certains dossiers contenant leurs RPS, notamment les dossiers cliniques conservés dans le DSE, les dossiers d'audit du DSE et les dossiers du DHI. Cela comprend la mise en place d'un nouveau canal d'accès numérique, qui s'appuie sur un nouveau service de vérification d'identité pour valider et vérifier l'identité d'une personne.

Rapport annuel individuel des atteintes au CIPVP

En vertu du projet de loi 194, la *Loi renforçant la cybersécurité et instaurant la confiance dans le secteur public*, à compter du 1er juillet 2025, Santé Ontario, en tant qu'établissement assujetti à la LAIPVP, est désormais tenu de soumettre un rapport annuel au CIPVP décrivant le nombre d'atteintes aux renseignements personnels (y compris les vols, les pertes ou les utilisations ou divulgations non autorisées) qui ont atteint le seuil de risque réel de préjudice grave (RRPG) ou d'autres circonstances prescrites et qui ont été signalées au CIPVP pour l'année civile précédente.

Points clés en matière de confidentialité et de sécurité



Les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité, en collaboration avec d'autres partenaires commerciaux, sont responsables de la protection de la vie privée, de la confidentialité, de la sécurité et de la disponibilité des données et permettent à Santé Ontario d'utiliser les données et autres ressources à l'appui de ses programmes et projets. Les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité

soutiennent les initiatives en remplissant, en examinant et/ou en approuvant :

- les évaluations des facteurs relatifs à la vie privée (y compris les évaluations des facteurs relatifs à la vie privée des fournisseurs)
- les accords juridiques
- les évaluations de sécurité et plans d'atténuation des risques

- les politiques et procédures
- les incidents de sécurité et pratiques de gestion des incidents
- la sensibilisation à la sécurité

Voici quelques points saillants de ce travail réalisé au cours de l'année 2025/2026.

Révision et approbation triennales par le Commissaire à l'information et à la protection de la vie privée

En tant que personne, entité et organisation prescrite, Santé Ontario est tenue de faire examiner et approuver ses pratiques en matière d'information par le CIPVP tous les trois ans.

En 2025, Santé Ontario a soumis au CIPVP les indicateurs organisationnels requis en matière de protection de la vie privée, de sécurité de l'information, de ressources humaines et autres. Cela comprenait des preuves exhaustives couvrant la période d'audit de trois ans, notamment des politiques, des normes et des procédures mises à jour en matière de confidentialité et de sécurité, des journaux d'outils de sécurité, des plans de traitement des risques pour les risques identifiés, des données sur les violations de données et des enregistrements des incidents de sécurité signalés.

Tout au long de 2026-2027, Santé Ontario répondra aux questions découlant des indicateurs signalés et fournira des renseignements et des documents supplémentaires à la demande du CIPVP.

Formation et sensibilisation à la protection de la vie privée – Journée annuelle de la protection de la vie privée

Durant la Semaine de la protection des données, Santé Ontario offre au personnel une

formation ciblée sur la protection de la vie privée afin de renforcer les connaissances fondamentales en matière de protection de la vie privée et de sécurité qu'il acquiert lors des séances d'orientation obligatoires et des formations annuelles sur la protection de la vie privée et la sécurité.

Modernisation du dossier de santé électronique : Visualiseur clinique provincial (VCP)

Santé Ontario a mis au point un programme de consolidation des visualiseurs afin de regrouper les trois visualiseurs cliniques existants en un seul visualiseur clinique provincial (VCP) standard permettant aux fournisseurs d'accéder aux RPS disponibles dans le DSE. Le VCP s'intégrera aux référentiels et registres de DSE existants et comprendra des contrôles pour garantir que l'accès aux RPS des patients ne soit disponible qu'aux fournisseurs à des fins de soins aux patients.

Systèmes d'information du RTDV

Le Système d'allocation et de transplantation d'organes (SATO) soutient les activités de don et de transplantation d'organes en Ontario. Afin d'améliorer la qualité des données, de réduire les risques et d'accroître l'efficacité, Santé Ontario a perfectionné les intégrations entre le SATO, les systèmes de dossiers médicaux électroniques des hôpitaux de transplantation et les systèmes de laboratoire d'antigènes leucocytaires humains, afin de permettre le transfert sécurisé et automatisé

des renseignements pertinents sur les patients dans le SATO.

De plus, Santé Ontario a participé à l'examen de l'Accord d'utilisation interprovincial du concentrateur d'interopérabilité d'iTransplant, qui permet une intégration technique partagée pour soutenir l'échange sécurisé, de système à système, de renseignements relatifs au don d'organes dans huit provinces canadiennes.

Accès Soins

Santé Ontario continue d'appuyer l'amélioration du programme Accès Soins du ministère de la Santé afin de faciliter l'accès des patients non affiliés à un médecin de famille et d'accroître le taux global d'affiliation en Ontario. Des RPS sont nécessaires pour évaluer l'état du programme. Santé Ontario a mis en place des contrôles administratifs et techniques pour s'assurer que la quantité minimale de RPS requise pour effectuer cette évaluation soit utilisée.

Échange de renseignements numériques sur la santé (ERNS)

Il est essentiel de permettre un partage sécurisé et respectueux de la vie privée des informations électroniques entre les dépositaires de renseignements sur la santé afin d'offrir aux Ontariens des soins de santé efficaces et intégrés.

Santé Ontario a mis au point des processus de certification et de conformité pour les spécifications d'interopérabilité approuvées afin de garantir que les fournisseurs, les dépositaires de renseignements sur la santé et les propriétaires d'actifs de santé numérique progressent vers une interopérabilité guidée par les normes provinciales.

Correspondance numérique

Santé Ontario continue de mener l'initiative visant à tirer parti des capacités numériques de

l'Ontario et à les développer afin de moderniser les communications relatives au dépistage du cancer et d'améliorer l'expérience de dépistage pour les Ontariens.

Cette initiative vise à aligner une solution de correspondance numérique sur la stratégie globale de Santé Ontario en matière de communication avec les Ontariens concernant leurs soins de santé. Cela permettra un accès plus facile et plus rapide aux dossiers de dépistage et pourrait potentiellement réduire le nombre d'incidents liés à l'envoi de courrier postal à une adresse postale obsolète ou incorrecte.

Programmes de dépistage améliorés et élargis

En 2025, Santé Ontario a lancé le Programme ontarien de dépistage de l'anévrisme de l'aorte abdominale (PODAAA). Le PODAAA est un programme de dépistage à l'échelle de la population qui détecte les anévrismes de l'aorte abdominale et réduit les ruptures et les décès évitables liés à ces anévrismes. Les RPS des patients sont utilisés pour identifier les participants admissibles et leur envoyer des lettres d'invitation au dépistage en fonction de leur âge. Des contrôles ont été mis en place pour surveiller l'accès aux RPS à ces fins.

Les patients avant la paperasse – Moderniser la communication avec les prestataires de soins

Dans le cadre de l'initiative « Les patients avant la paperasse », visant à réduire le fardeau administratif des soins primaires et à coordonner les flux de travail d'orientation afin de libérer du temps clinique, Santé Ontario a soutenu les initiatives suivantes :

- Admission centralisée
- Orientation électronique Ontario
- Formulaires électroniques

Santé Ontario a contribué à évaluer la capacité et la sécurité permettant aux dépositaires de renseignements sur la santé ne disposant pas de moyens numériques de soumettre des formulaires par l'intermédiaire de la solution des formulaires électroniques en utilisant le service Web One Health Launcher.

Ces initiatives visent à assurer une transition harmonieuse vers la soumission de formulaires numériques et à améliorer l'efficacité globale dans le contexte des soins primaires.

Préparation à la protection de la vie privée pour les soins intégrés

Santé Ontario promeut des modèles de soins intégrés qui reposent sur un partage rapide, sécurisé et approprié des renseignements sur la santé entre les équipes de santé de l'Ontario, leurs organisations membres et les réseaux de soins primaires.

Santé Ontario a entrepris une évaluation provinciale des besoins en matière de protection de la vie privée et de gestion de l'information afin d'éclairer une approche coordonnée en matière de protection de la vie privée, alignée sur la prestation de soins intégrés. Les besoins identifiés comprennent les suivants :

- Gouvernance intégrée de la protection de la vie privée
- Formation et sensibilisation à la protection de la vie privée
- Outils et ressources partagés
- Modèles simplifiés de partage de données

Intelligence artificielle

Santé Ontario a continué d'étendre l'utilisation des technologies d'intelligence artificielle (IA)

dans les contextes cliniques, analytiques et opérationnels.

Santé Ontario a joué un rôle actif de gouvernance et de conseil pour soutenir l'utilisation responsable de l'IA et veiller à ce que ces initiatives soient mises en œuvre d'une manière conforme à la LPRPS, à la LAIPVP et aux exigences provinciales en constante évolution en matière d'utilisation responsable de l'IA, y compris des contributions continues aux travaux du comité sur l'IA soutenant la mise en œuvre de la *Directive sur l'utilisation responsable de l'intelligence artificielle* de la province.

Au cours de l'exercice financier, les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité ont soutenu la mise en place des piliers fondamentaux nécessaires pour permettre un déploiement responsable de l'IA à Santé Ontario. Ce travail comprenait l'élaboration d'une politique en matière d'IA, la création et la mise à l'essai d'un cadre d'évaluation des risques et la mise en place d'un module de formation annuel sur l'IA pour soutenir la sensibilisation et la conformité. Des structures de gouvernance, des processus et des essais limités dans des domaines d'adoption ciblés ont également été mis en place au cours de l'année, jetant les bases d'une activation plus large de l'IA à l'avenir.

Grâce à ces fondements, Santé Ontario est en mesure de poursuivre une progression plus significative dans divers domaines stratégiques, notamment :

- Soutenir les entités de recherche externes en IA dans le domaine de la santé grâce au partage responsable des données de Santé Ontario
- Faire progresser la recherche interne en intelligence artificielle dans le domaine de la santé en tirant parti du positionnement

unique et des ressources en données de Santé Ontario

- Explorer les opportunités d'optimisation des opérations internes et d'entreprise grâce à l'IA.

À mesure que cette technologie transformatrice continue d'évoluer, la collaboration continue en matière de protection de la vie privée et de sécurité restera essentielle pour permettre ces évolutions de manière responsable et devrait se poursuivre dans un avenir prévisible.

Renforcement de l'architecture et des normes de sécurité

- **Architecture de réseau à confiance nulle :** Mise en place d'architectures de base couvrant les cinq piliers du modèle « confiance nulle » — identité, réseaux, terminaux, charges de travail et données —, soutenues par un cadre et des normes de « confiance nulle » d'entreprise afin de permettre une adoption cohérente et fondée sur les risques à l'échelle de l'organisation.
- **Norme d'architecture de sécurité dans le cloud AWS :** Nous avons élaboré une architecture de référence conforme aux meilleures pratiques du secteur afin de guider le déploiement et l'exploitation sécurisés des produits et services au sein de l'environnement AWS de Santé Ontario.
- **Évaluation de la sécurité des sauvegardes dans le cloud :** Nous avons mené une évaluation complète des services de sauvegarde dans le cloud sur Azure et AWS, où résident les systèmes critiques et les données sensibles, ce qui a permis de formuler des recommandations concrètes pour renforcer la protection et soutenir l'amélioration continue.

Amélioration de la gestion et de l'assurance des risques d'entreprise

- **Gestion des risques de sécurité liés aux tiers- (TPSRM) :** Mise en œuvre d'un cadre de TPSRM à l'échelle de l'entreprise pour évaluer et gérer les risques liés à la sécurité des fournisseurs à l'aide d'attestations standardisées, de certifications sectorielles et de contrôles contractuels renforcés, favorisant la souveraineté des données et une évaluation cohérente des risques.
- **Évaluation de la maturité de la cybersécurité (CSF NIST 2.0) :** Nous avons réalisé la première évaluation de la maturité en cybersécurité de l'entreprise à l'aide de la plateforme Axio360, établissant ainsi une base de référence pour toutes les fonctions du CSF NIST (Gouverner, Identifier, Protéger, Détecter, Répondre, Récupérer). Les résultats ont permis d'orienter les priorités au niveau de la direction et d'établir la feuille de route en matière de cybersécurité pour l'exercice financier 2026/2027.
- **Évaluation de la préparation à l'audit du COS 2 de type II :** Lancement des activités de préparation à l'audit du COS 2 Type II pour certains services cloud hébergés dans Azure et AWS, identification des priorités de correction et mise en place d'un programme d'assurance indépendant pluriannuel aligné sur la LPRPS et les exigences provinciales.

Amélioration de la visibilité des risques et de l'efficacité des contrôles

- **Transformation de l'évaluation des menaces et des risques (EMR) :** Nous avons consolidé plusieurs modèles d'évaluation dans un cadre d'EMR unifié et hiérarchisé, avec des modèles, des notations et des correspondances de

contrôle standardisés, améliorant ainsi la qualité, l'évolutivité et les rapports au niveau de l'entreprise.

- **Modernisation du registre des risques d'entreprise** : Mise en place d'une plateforme centralisée de gouvernance, de risque et de conformité (GRC), abandonnant l'ancien registre des risques de sécurité et améliorant la transparence, la préparation aux audits et le reporting des risques dans les domaines de la protection de la vie privée, de la sécurité et de la réglementation.
- **Tests de pénétration et validation des contrôles** : Améliorer la maturité des tests de sécurité en organisant un exercice de « purple team » axé sur les environnements Azure et AWS, y compris les machines virtuelles et les plateformes de conteneurs OpenShift, afin d'évaluer l'efficacité des mécanismes de détection et de réaction en conditions réelles.

Renforcement de la gouvernance et de la cohérence en matière de sécurité

- **Échange de connaissances en matière de sécurité de l'information (ISKE)** : ISKE a continué à se développer en tant que forum inter-fonctionnel pour la sécurité, la confidentialité, la conformité, l'architecture et les opérations. L'adoption d'une cadence trimestrielle début 2026 a permis d'améliorer l'alignement avec la planification stratégique, de mieux cerner les risques prioritaires et de soutenir des pratiques de gestion des risques cohérentes.

Amélioration de la détection, de la surveillance et de la réponse aux menaces

- **Centre d'opérations de sécurité hybride (COS) fonctionnant 24h/24 et 7j/7** :

Maintien de capacités de surveillance, de détection et de réponse continues grâce à un modèle de COS hybride. Les principales actions entreprises ont consisté en des prolongations de contrats afin d'assurer une couverture ininterrompue, des progrès vers un système d'acquisition d'un COS de nouvelle génération et des améliorations de l'efficacité grâce à une intégration plus étroite avec les opérations technologiques.

- **Gestion des interventions en cas d'incidents de cybersécurité** : Renforcement de la préparation et de la réponse aux incidents grâce à la mise à jour des politiques, des manuels d'intervention et à une supervision coordonnée des incidents majeurs. Dans le cadre du modèle opérationnel provincial de cybersécurité, Santé Ontario a continué d'apporter son soutien aux partenaires du secteur de la santé lors d'incidents cybernétiques importants.

Sécurisation des terminaux, des identités et des accès

- **Détection et réponse des terminaux (DRT)** : Nous avons finalisé un audit complet de la couverture des terminaux, en intégrant les appareils précédemment non gérés et en validant l'état des terminaux, la télémétrie et l'application des politiques afin d'améliorer la visibilité et de réduire les risques résiduels.
- **Protection et surveillance renforcées de l'identité** : Couverture étendue de la détection et de la réponse aux services d'annuaire d'entreprise, améliorant la visibilité des attaques basées sur l'identité et renforçant la capacité de l'organisation à détecter et à répondre aux menaces basées sur les identifiants.
- **Services organisationnels de gestion des identités et de l'accès (SOGIA)** : Un niveau

de modernisation avancé des SOGIA, avec une orientation vers la gouvernance, l'évolutivité et la réduction des risques. Parmi les réalisations, citons la mise en œuvre d'un modèle de modernisation des SOGIA, l'intégration de la gouvernance et de l'administration des identités dans les opérations, et la formalisation de la gouvernance et des feuilles de route pluriannuelles alignées sur les exigences du NIST et de la LPRPS.

- **Secure Access Service Edge (SASE) :** Poursuite de la modernisation de l'accès sécurisé à distance et d'entreprise, en faisant évoluer les cas d'utilisation des VPN traditionnels vers un modèle SASE basé sur des politiques, qui s'inscrit dans la stratégie « Confiance nulle » plus large de Santé Ontario.

Protection des données et des applications

- **Gouvernance des données d'entreprise et protection de l'information :** Extension des outils de sécurité et de gouvernance des données à l'ensemble de l'environnement de productivité de l'entreprise, permettant une classification cohérente des informations, la prévention des pertes de données (PPD) et la conformité aux normes de traitement de l'information.
- **Test dynamique de sécurité des applications (DAST) :** Opérationnalisation de DAST au sein des flux de travail de développement, élargissement de l'intégration des applications et soutien aux équipes produit dans l'identification et la correction des vulnérabilités plus tôt dans le cycle de vie, conformément aux pratiques du DSO.
- **Gestion -des vulnérabilités axée sur les produits :** Amélioration de la gestion des vulnérabilités dans les environnements de

centres de données grâce à une extension au-delà de l'infrastructure pour inclure les risques liés aux applications et à la configuration, permettant une appropriation, une priorisation et une remédiation éclairées par les risques plus claires.

- **Gestion -automatisée des certificats et des clés :** Gestion avancée des certificats et des clés cryptographiques pour une gestion du cycle de vie axée sur l'automatisation et les politiques, y compris les certificats publics en libre-service et les capacités fondamentales pour prendre en charge les futures opérations sans intervention humaine.

Renforcer les capacités cybernétiques à l'échelle du secteur : Centre de cybersécurité de Santé Ontario

Au cours de l'exercice financier 2025/2026, le Centre de cybersécurité de Santé Ontario a concentré ses efforts sur la mise en œuvre et la stratégie du Modèle opérationnel provincial de cybersécurité (MOPC). Ces étapes comprenaient :

- **La planification avancée de l'expansion du MOPC** pour les soins primaires, les unités de santé publique et les soins à domicile et communautaires, définissant les options d'intégration initiales et les approches stratégiques pour l'intégration dans la prochaine itération du MOPC.
- **Nous avons élaboré une première version préliminaire d'une trousse d'outils provinciale en matière de cybersécurité** afin de fournir des directives claires et concrètes aux petits fournisseurs de services de santé, aux équipes cliniques et opérationnelles et aux partenaires de mise en œuvre pour soutenir, améliorer et s'aligner sur les orientations provinciales en matière de cybersécurité.

- **La préparation et la capacité de réponse aux incidents validées** grâce à la participation à deux exercices de simulation multipartites avec des intervenants du ministère et du secteur.
- **Le développement avancé du Critical Controls Tracker** pour permettre une mesure cohérente des progrès et de la maturité par rapport aux contrôles de cybersécurité prioritaires chez les fournisseurs de services de santé de soins aigus.
- **En partenariat avec le Centre d'excellence en cybersécurité du MSPEA**, nous avons mis en œuvre un processus de notification des incidents à l'échelle du secteur, aligné sur la réglementation en matière de cybersécurité de la *loi EDSTA (Loi sur l'amélioration de la sécurité numérique et de la confiance)*, en vigueur à compter du 1er juillet.

Protection de la vie privée et sécurité en chiffres : Indicateurs clés



Les indicateurs clés de la protection de la vie privée et de la sécurité suivants mettent en lumière une partie du travail accompli par les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité en 2025/2026 et fournissent une mesure de la conformité de Santé Ontario aux exigences législatives et réglementaires ainsi qu'aux pratiques respectives en matière d'information.

Points saillants des indicateurs clés de la protection de la vie privée

Gestion des atteintes à la vie privée de Santé Ontario

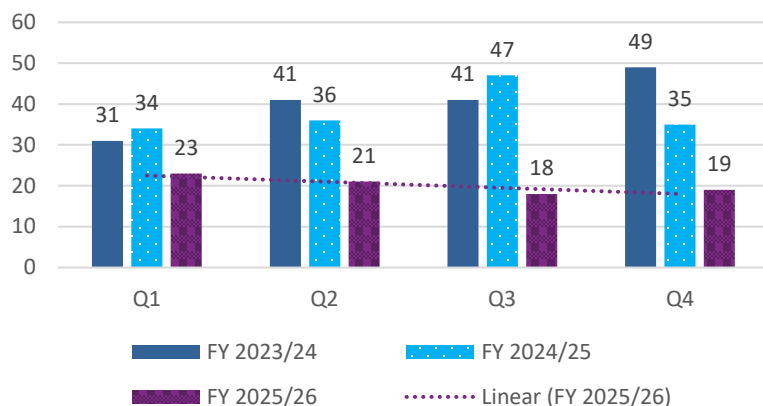
Santé Ontario gère, ou a la garde ou le contrôle, d'un grand volume de dossiers et d'ensembles de données, et ces référentiels et registres contiennent des données relatives aux interactions individuelles avec le système de santé de l'Ontario et contiennent des RPS. Les indicateurs ci-dessous incluent les violations des politiques de protection de la vie privée et les violations où des RPS ont été perdues, volées ou traitées de manière non autorisée.

Pour mémoire...

À elle seule, la partie des données relatives aux DSE contient plus de 15,5 milliards d'enregistrements correspondant à environ 28,8 millions de personnes distinctes et contenant des RPS.

Un exemple d'atteinte à la vie privée est celui d'un employé qui accède à des RPS alors que cela n'est pas nécessaire à l'exercice de ses fonctions, ou celui d'un organisme externe qui envoie des RPS à Santé Ontario alors que ce dernier n'a ni demandé ni besoin de ces renseignements.

Atteintes à la vie privée



Toutes les atteintes à la vie privée, suspectées ou confirmées, font l'objet d'une enquête menée par le Bureau de la protection de la vie privée en collaboration avec les parties prenantes concernées, et des stratégies et recommandations d'atténuation sont mises en œuvre pour prévenir de futures atteintes.

Santé Ontario a constaté une diminution du nombre d'atteintes signalées au cours de l'exercice 2025-2026¹. Les sources de violations

comprennent les violations passives par courriel, telles que les courriels contenant des RPS envoyés à Santé Ontario par les dépositaires de renseignements sur la santé.

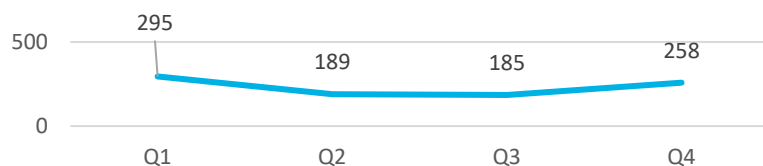
Programme de dépistage du cancer de l'Ontario – Correspondance mal acheminée

Au cours de l'exercice financier 2025/2026, Santé Ontario a envoyé par la poste environ 9,9 millions de correspondances à des personnes dans le cadre du Programme de dépistage du cancer de Santé Ontario, y compris par exemple des rappels pour se faire dépister et les résultats des tests de dépistage. Ces lettres constituent un élément essentiel du programme de dépistage du cancer, qui aide les personnes à détecter le cancer plus tôt, lorsqu'il y a de meilleures chances de le traiter avec succès, ce qui conduit à de meilleurs résultats de santé.

Dans certains cas, en raison d'adresses obsolètes ou incorrectes provenant des sources de données, ce courrier est mal acheminé. Il y a eu notamment une augmentation du nombre de correspondances cette année en raison des changements apportés aux critères d'admissibilité du Programme ontarien de dépistage du cancer du sein et de la mise en œuvre du nouveau Programme de dépistage AAA. En conséquence, le nombre de courriers retournés à Santé Ontario est passé de 738 en 2024/2025 à 927 en 2025/26. Cependant, le courrier mal acheminé, mal distribué ou ouvert ne représente que 0,009%

du volume total du courrier soumis au filtrage, un chiffre similaire aux 0,01% enregistrés en 2024/2025.

Atteintes à la vie privée dans la correspondance relative aux soins contre le cancer



Chaque courrier renvoyé est examiné par le Centre de contact pour le dépistage du cancer de Santé Ontario, qui invalide l'adresse erronée et tente de mettre à jour le dossier du destinataire prévu avec l'adresse

correcte. Santé Ontario envoie également une lettre de notification de violation au destinataire prévu

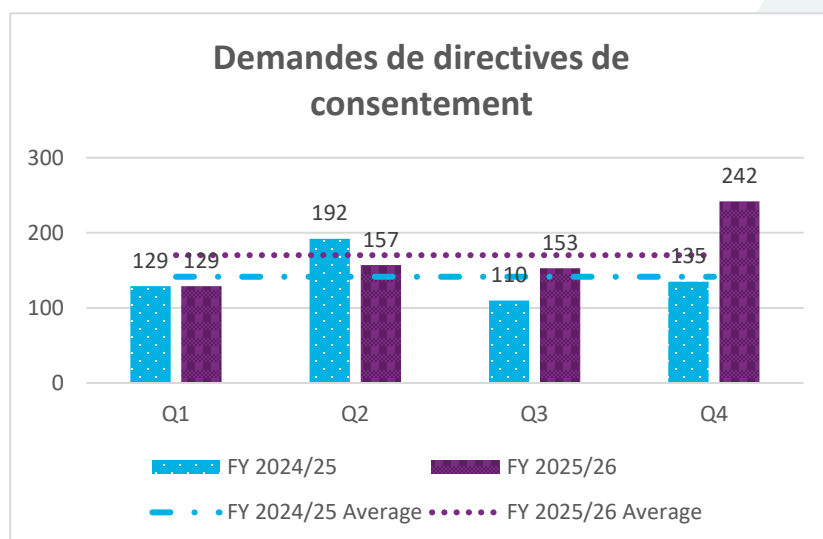
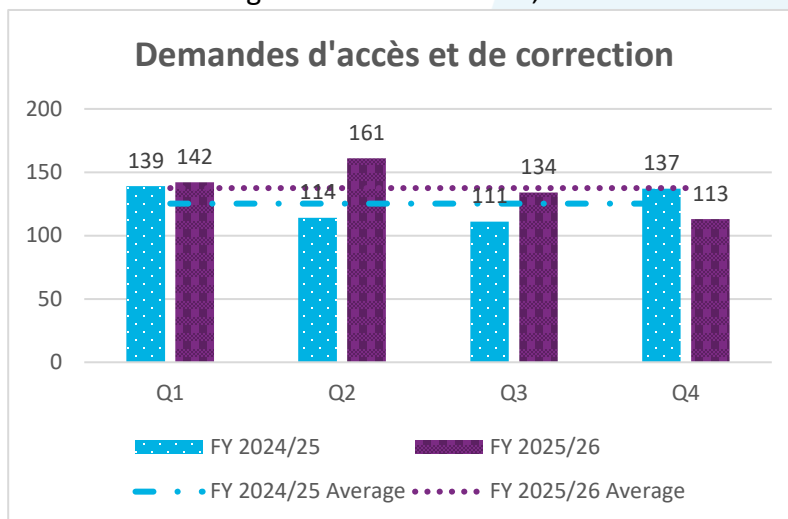
¹ Les incidents liés au Programme de dépistage des centres de contact sont consignés dans le document intitulé « Programme de dépistage du cancer de l'Ontario – Correspondance mal acheminée ».

si le courrier a été mal acheminé et ouvert par une personne autre que le destinataire prévu, à condition que Santé Ontario soit en mesure de confirmer l'adresse correcte.

Demandes d'accès et de correction des DSE et demandes de directives de consentement

Le traitement des demandes relatives à la confidentialité des DSE concernant l'accès, la correction et les directives de consentement aide les patients à exercer leurs droits à la vie privée tels que prévus par la loi. Dans le cadre de son rôle d'organisation prescrite par la province en ce qui concerne le DSE provincial et en sa qualité d'agent des dépositaires de renseignements sur la santé, Santé Ontario :

- Reçoit et met en œuvre les demandes des patients visant à ajouter, modifier ou révoquer une directive de consentement concernant leurs RPS figurant dans le DSE
- Facilite et aide les dépositaires de renseignements sur la santé participants dans les démarches administratives liées aux demandes d'accès individuelles aux dossiers contenant des RPS dans le DSE, et apporte son soutien au processus de correction le cas échéant.

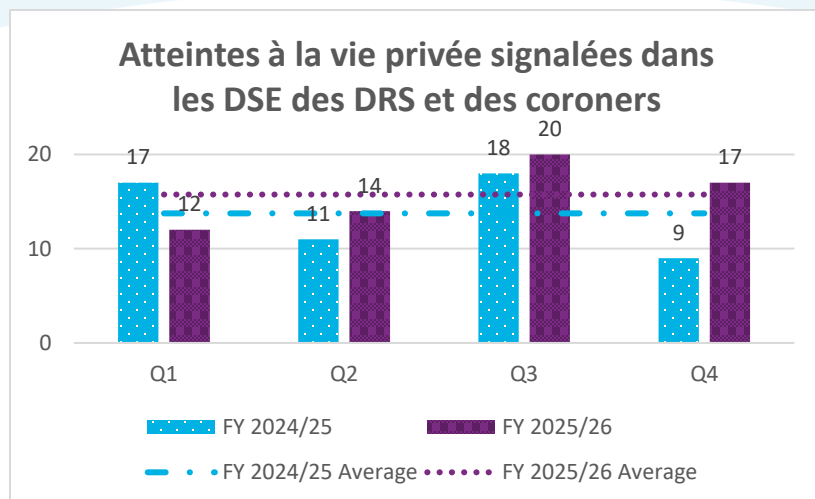


Au cours de l'exercice financier 2025/2026, le volume des demandes d'accès a augmenté de 10% et celui des demandes de directives de consentement de 20%. Il convient de noter que la forte augmentation des demandes de directives de consentement au T4 est attribuable à la campagne harmonisée de notification du consentement, au cours de laquelle nous avons informé les patients de la mise à jour du cadre de consentement et les avons invités à confirmer ou à

mettre à jour leurs demandes de directives dans leur dossier. Cette hausse devrait se stabiliser.

Gestion des incidents liés à la confidentialité des DSE – Dépositaires de renseignements sur la santé et coroners

Les dépositaires de renseignements sur la santé et les coroners sont tenus de mettre en œuvre et de respecter leurs propres politiques internes de gestion des incidents de confidentialité pour la gestion des incidents de confidentialité concernant les RPS accessibles à travers le DSE. De plus, les



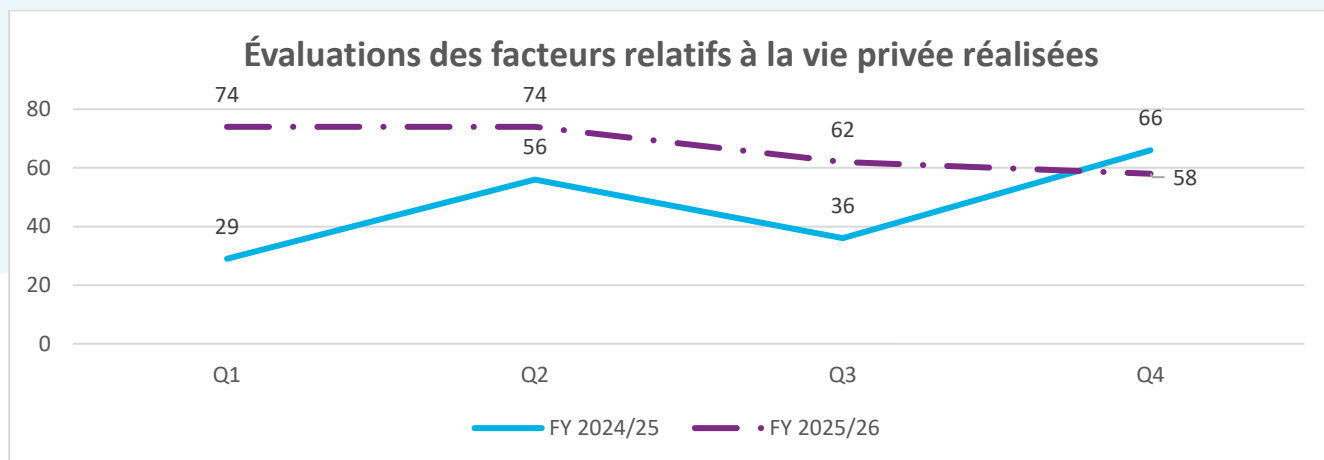
dépositaires de renseignements sur la santé et les coroners qui accèdent au DSE ou y contribuent doivent aviser Santé Ontario dès que possible lorsqu'ils constatent ou prennent connaissance d'une atteinte à la vie privée liée aux RPS accessibles à travers le DSE. Dès réception de cette notification, Santé Ontario signale l'atteinte à la vie privée à tout autre dépositaire de renseignements sur la santé ou coroner concerné qui a causé l'atteinte ou ayant contribué à

l'intégration des RPS dans le DSE. Afin de soutenir davantage le processus de gestion des incidents, Santé Ontario fournit aux dépositaires de renseignements sur la santé des rapports d'audit des DSE qui leur permettent de vérifier et de contrôler leur conformité à la LPRPS.

Évaluations des facteurs relatifs à la vie privée

L'une des principales obligations et fonctions du Bureau de la protection de la vie privée consiste à réaliser des évaluations des facteurs relatifs à la vie privée (EFVP) qui servent à évaluer les nouveaux programmes, services, processus, systèmes d'information ou mises à jour de la loi ou de la réglementation afin d'identifier les risques pour la vie privée et de recommander des stratégies d'atténuation. Les EFVP offrent un niveau de garantie que les problèmes et les risques liés à la protection de la vie privée sont identifiés et résolus. Elles peuvent également contribuer à faire comprendre comment Santé Ontario gère les RPS ou les RP et démontrer comment Santé Ontario respecte ses obligations législatives et réglementaires ainsi que son engagement en matière de protection de la vie privée envers le grand public.

Au cours du dernier exercice financier, Santé Ontario a réalisé ou supervisé 268 EFVP, comparativement à 187 l'année précédente, ce qui représente en moyenne une augmentation de 43,3% du volume. Cette augmentation est attribuée en partie au volume important d'initiatives et de projets hautement prioritaires entrepris par Santé Ontario, tels que « Les patients avant la paperasse », le dépistage des anévrismes de l'aorte abdominale (AAA) en Ontario et l'accès intégré aux soins des patients, ainsi qu'à la complexité croissante des évaluations requises.



Points saillants des indicateurs de sécurité

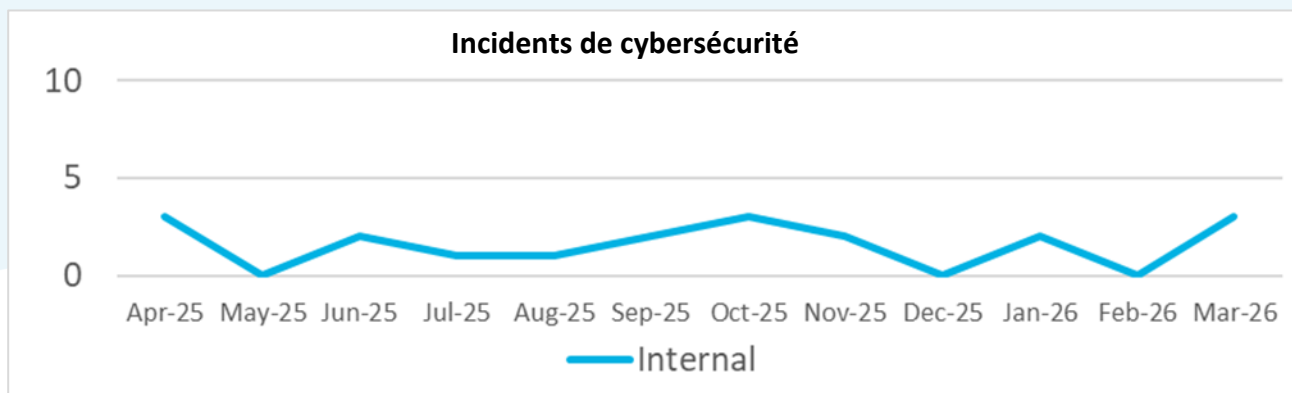


Incidents de cybersécurité (internes et externes)

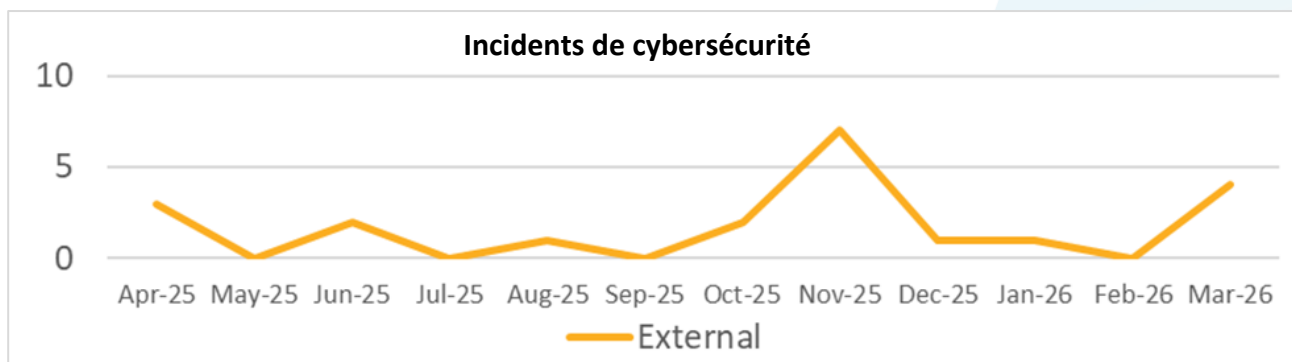
Au cours de l'exercice financier 2025/2026, la plupart des incidents détectés en interne étaient de faible gravité et ont été identifiés et atténués rapidement grâce à une surveillance et à des contrôles automatisés, sans impact significatif sur les systèmes ou les données. Ces événements impliquaient principalement des tentatives d'accès non autorisé ou des interactions avec du contenu malveillant.

Les incidents signalés à l'extérieur dans l'ensemble du secteur de la santé sont restés stables et n'ont pas affecté le système de santé de l'Ontario, ce qui témoigne d'une sensibilisation, d'une orientation et d'une coordination efficaces en matière de cybersécurité avec les partenaires. Depuis la mise en œuvre du MPOC, le secteur des soins aigus a enregistré une baisse du nombre de incidents cybernétiques de grande gravité, avec moins d'événements évoluant vers un « Code Gris » ou entraînant des perturbations généralisées dans la prise en charge des patients. Cela témoigne d'une amélioration de la détection, du confinement et du rétablissement, appuyée par une réponse coordonnée du secteur. Toutefois, l'activité liée aux incidents cybernétiques en dehors du secteur des soins aigus est restée stable ou a augmenté, et le paysage des menaces continue de gagner en sophistication. Pris dans leur ensemble, ces éléments confirment la nécessité d'élargir l'approche du MOPC et de continuer à renforcer les capacités cybernétiques dans l'ensemble du système de santé afin de garantir une résilience cohérente à l'échelle du système.

Ensemble, ces tendances témoignent de capacités de surveillance éprouvées et d'une gestion efficace des risques de cybersécurité dans un environnement de menaces dynamique.



Incidents de cybersécurité internes : Événements survenant dans les systèmes appartenant à ou gérés par Santé Ontario, où Santé Ontario mène l'enquête, le confinement et la correction.



Incidents de cybersécurité externes : Événements survenant dans des systèmes détenus et exploités par des organisations externes (par exemple, hôpitaux, fournisseurs de services, fournisseurs), pour lesquels Santé Ontario fournit un soutien consultatif, de coordination ou de supervision.

Évaluation des menaces et des risques

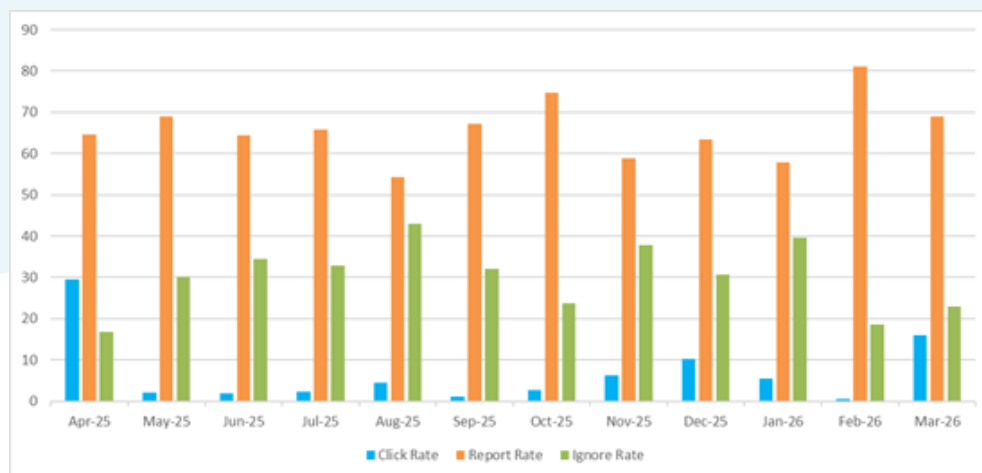
Au cours de l'exercice financier 2025/2026, Santé Ontario a continué de faire progresser son programme de gestion des risques de sécurité grâce à des activités d'évaluation et d'assurance soutenues. Le Bureau de la sécurité de l'information a réalisé 109 évaluations de sécurité dans le cadre de 56 projets, comprenant des évaluations des risques liés aux menaces internes et externes, des évaluations de sécurité (architecture) et des tests de pénétration, afin d'identifier et d'atténuer les risques de cybersécurité dans les systèmes et plateformes de l'entreprise.

Activités clés en matière de cybersécurité : 2024-2025 (GESTION DES RISQUES)

	EMR interne	EMR externe	Autres évaluations de sécurité	Test de pénétration
Nombre d'évaluations réalisées par type	21	19	50	19

Campagnes de simulation d'hameçonnage

Santé Ontario a mené régulièrement des simulations d'hameçonnage -à l'échelle de l'organisation afin d'évaluer la réaction des employés face à des menaces par courriel- de plus en plus sophistiquées.



Au cours de l'exercice financier 2025/2026, les résultats sont restés globalement stables, avec une certaine variabilité due à des scénarios plus réalistes et plus avancés. Les périodes de forte activité de clics ont été suivies d'une

amélioration des comportements de signalement, avec des performances encore plus solides observées plus tard dans l'année, reflétant une meilleure reconnaissance des tentatives d'hameçonnage et un respect accru des procédures de signalement.

Perspectives d'avenir



Pour continuer à remplir sa mission principale d'intégration du système de santé et de soutien à des soins de qualité supérieure axés sur le patient, Santé Ontario a besoin de données, notamment de RPS et de RP. Au cours de la dernière année, les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité ont travaillé avec diligence pour optimiser l'utilisation des données dans le cadre des soins aux patients, tout en veillant à ce que les données de santé soient gérées conformément aux obligations légales des agences et à leur engagement en matière de protection de la vie privée et de confidentialité. De par ses rôles prescrits, Santé Ontario dispose d'une grande latitude pour utiliser les données qui lui sont confiées et assume d'importantes responsabilités. Par conséquent, le travail se poursuit.

Vous trouverez ci-dessous un exemple de priorités clés supplémentaires pour 2026/2027 (en plus des travaux en cours décrits ci-dessus) pour les équipes du Bureau de la protection de la vie privée et du Programme de cybersécurité.

Intelligence artificielle

- Poursuivre le développement du cadre de gouvernance de l'IA de Santé Ontario afin de mettre l'accent sur l'implication précoce, l'évaluation -fondée sur les risques, la documentation et une responsabilité clairement définie, afin de garantir que les initiatives reposant sur l'IA -restent transparentes, conformes à la loi et en adéquation avec les attentes du secteur public en matière d'utilisation fiable des données. Cela comprend le soutien d'une approche coordonnée pour l'expansion responsable de l'IA dans divers cas d'utilisation internes et externes qui améliorent la qualité des soins reçus par les Ontariens et soutiennent des opérations plus efficaces tirant parti des données de Santé Ontario.

- Parallèlement, alors que les menaces liées à l'IA- ne cessent de gagner en rapidité et en ampleur, Santé Ontario va accélérer la mise en œuvre de mesures d'amélioration, fondées sur l'évaluation des risques-, visant à renforcer ses pratiques en matière de cybersécurité et de gouvernance. Les principaux axes de travail sont les suivants :
 - Accélérer l'identification et la correction des vulnérabilités grâce à une automatisation accrue afin de réduire les périodes d'exposition.
 - Mettre en œuvre une gestion continue de l'exposition aux menaces afin d'identifier et de combler les failles de sécurité à la vitesse de la machine.
 - Réduire la surface d'attaque externe en renforçant les contrôles sur les systèmes- et services exposés à Internet.
 - Faire progresser la maturité du modèle Confiance nulle en matière de contrôle des identités, des appareils, des réseaux et des données afin de limiter les déplacements latéraux.
 - Mettre en place un cadre d'évaluation des menaces et des risques spécifiques à l'IA-, couvrant les risques liés à la sécurité, à la protection de la vie privée, à l'éthique et aux aspects opérationnels tout au long du cycle de vie de l'IA.
 - Améliorer la capacité de réaction aux incidents et de reprise après sinistre informatique afin de permettre une maîtrise et une restauration rapides à la suite -d'événements liés à l'IA.

Placer les patients avant la paperasse : orientation électronique et admission centralisée

- Dans le cadre du programme « Les patients avant la paperasse », diriger la mise en œuvre et l'amélioration continue d'outils numériques tels que l'orientation électronique et l'admission centralisée afin de rationaliser les flux de travail des prestataires, d'améliorer l'accès sécurisé des patients et de mettre en place des améliorations garantissant des processus d'orientation et d'accueil efficaces et respectueux de la vie privée, permettant ainsi une coordination fluide entre les différents lieux de soins, réduisant la charge administrative et favorisant des soins coordonnés et dispensés en temps opportun.

Services de santé supplémentaires pour l'accès des patients

- Permettre aux Ontariens d'accéder à leurs renseignements sur la santé au-delà des données de laboratoire et des médicaments grâce à Mon dossier de santé et favoriser l'adoption de ces services en intégrant de nouveaux services de santé à travers le compte Mon Ontario pour la santé.

Accès Soins

- Moderniser le programme Accès Soins en optimisant le processus d'inscription et en améliorant l'expérience des patients et des prestataires de soins.

Soins de santé primaires

- Soutenir le développement d'un système provincial de dossiers médicaux électroniques qui garantisse des services numériques connectés et de haute qualité aux cliniciens et aux patients de toute la province.

Renforcer l'assurance, la gouvernance et la gestion des données

- **COS 2 Type II – Phase 2 (Remédiation)** : Santé Ontario fera progresser la phase 2 de son programme de COS 2 Type II en remédiant aux lacunes de contrôle relevées lors de l'évaluation de l'état de préparation. Ce travail permettra de renforcer l'environnement de contrôle au regard des critères des services de confiance, d'améliorer la préparation aux audits et de faire évoluer les pratiques d'assurance relatives aux -services numériques basés sur le cloud.
- **Souveraineté des données** : L'organisation continuera de faire progresser son approche de la souveraineté des données en réponse à l'évolution des attentes réglementaires et à la complexité croissante des services numériques mondiaux. S'appuyant sur les pratiques existantes en matière de protection de la vie privée, de sécurité et de gouvernance des données, Santé Ontario continuera d'évaluer et d'affiner son approche visant à soutenir un contrôle, une gouvernance et une autorité juridique appropriés et cohérents sur ses données et actifs numériques, tant à l'interne que dans l'ensemble du secteur provincial de la santé.

Amélioration de la préparation aux menaces et de la résilience opérationnelle

- **Simulations de menaces cybernétiques** : Santé Ontario mettra en œuvre un programme continu de simulation des menaces cybernétiques, comprenant des tests de pénétration, des évaluations des menaces et des risques, et des exercices sur table. Ces activités permettront d'améliorer la préparation, de renforcer la coordination et d'apporter une réponse rapide et efficace aux incidents cybernétiques.
- **Secure Access Service Edge (SASE)** : Les travaux se poursuivront afin de moderniser l'accès sécurisé à l'entreprise et l'accès à distance, en poursuivant la transition des cas d'utilisation des VPN traditionnels vers un modèle SASE- basé sur des politiques. Les priorités pour l'exercice financier 2026/2027 comprennent la réduction de la dette technique, la normalisation de l'expérience utilisateur et le renforcement du soutien opérationnel, tout en maintenant des contrôles de sécurité rigoureux conformes à la stratégie « Confiance nulle » de Santé Ontario.

Réduire les risques liés à l'identité, au courriel -et aux données

- **Services organisationnels de gestion des identités et de l'accès** : Santé Ontario poursuivra la phase 2 du Programme de modernisation des SOGIA en mettant l'accent sur la réduction des risques liés à l'identité- grâce à la généralisation d'une authentification multifactorielle résistante à l'hameçonnage-, au renforcement des contrôles -d'accès conditionnel, à l'amélioration de la gouvernance de l'accès aux services et aux fournisseurs, ainsi qu'à la poursuite du déploiement et de -l'optimisation de la Gouvernance et administration des identités (GAI) et de la gestion des accès privilégiés (GAP) dans le cloud.

- **Sécurité renforcée du courriel** : L'organisation va se doter d'une technologie de pointe en matière de sécurité des courriels et la mettre en œuvre afin d'améliorer la détection et la prévention de l'hameçonnage, des attaques par compromission des courriels professionnels -et d'autres menaces sophistiquées véhiculées par courriel.
- **Amélioration de la prévention des pertes de données** : Santé Ontario va perfectionner davantage son programme de PPD en étendant sa couverture aux types de données prioritaires et aux canaux de collaboration au sein des environnements cloud. Les efforts porteront sur l'amélioration de la cohérence des politiques, l'ajustement des contrôles aux processus opérationnels et le renforcement des rapports et de la surveillance afin de mieux protéger les RPS, les RP et autres informations sensibles.

Annexe

Acronymes

Acronyme	Définition
AAA	Anévrisme de l'aorte abdominale
IA	Intelligence artificielle
AWS	Amazon Web Services
CHRIS	Système d'information sur la santé des clients
DGPVP	Directeur général de la protection de la vie privée
CSDR	Cybersécurité, défense et résilience
CSF	Cadre de cybersécurité
MOPC	Modèle opérationnel (provincial) de cybersécurité
DAST	Test dynamique de sécurité des applications
RNM	Répertoire numérique des médicaments
DHI	Identifiant numérique de santé
ERNS	Échange de renseignements numériques sur la santé
PPD	Prévention des pertes de données
DRT	Détection et réponse des terminaux
EDSTA	Loi sur l'amélioration de la sécurité numérique et de la confiance
DSE	Dossier de santé électronique
SOGIA	Services organisationnels de gestion des identités et de l'accès
FSE	Fournisseur de services électroniques
LAIPVP	Loi sur l'accès à l'information et la protection de la vie privée
EF	Exercice financier
GoLA	Loi sur le don de vie
GRC	Gouvernance, risques et conformité
DRS	Dépositaire(s) de renseignements sur la santé
DÉI	Dossier d'évaluation intégrée
GAI	Gouvernance et administration des identités
AIP	Accès intégré aux soins des patients
CIPVP	Commissaire à l'information et à la protection de la vie privée (de l'Ontario)
ISO	Bureau de la sécurité de l'information
ISKE	Échange de connaissances en matière de sécurité de l'information
MSPEA	Ministère des Services au public et aux entreprises et de l'Approvisionnement
NIST	Institut national des normes et de la technologie
PODAAA	Programme ontarien de dépistage de l'anévrisme de l'aorte abdominale
SATO	Système d'allocation et de transplantation d'organes

OHSC	Centre de cybersécurité de Santé Ontario
SILO	Système d'information de laboratoire de l'Ontario
GAP	Gestion des accès privilégiés
VCP	Visualiseur clinique provincial
VPP	Visualiseur provincial des patients
RPS	Renseignements personnels sur la santé
LPRPS	Loi sur la protection des renseignements personnels sur la santé
RP	Renseignements personnels
EFVP	Évaluation(s) des facteurs relatifs à la vie privée
EP	Entité prescrite
PP	Personne prescrite
OP	Organisation prescrite
RRPG	Risque réel de préjudice grave
SASE	Secure Access Service Edge
COS	Centre d'opérations de sécurité
COS 2	Contrôle des organisations de services 2
TPSRM	Gestion des risques de sécurité liés aux tiers
EMR	Évaluation des menaces et des risques
RTDV	Réseau Trillium pour le don de vie
RPV	Réseau privé virtuel

Autorités de santé publiques de l'Ontario

Entité prescrite (EP)

Santé Ontario est désignée comme une « entité prescrite » aux fins du paragraphe 45(1) de la LPRPS. Le paragraphe 45(1) de la LPRPS autorise les dépositaires de renseignements sur la santé (tels que les hôpitaux, les laboratoires et les médecins) à divulguer des RPS sans consentement à Santé Ontario en tant qu'entité prescrite aux fins d'analyse ou de compilation de renseignements statistiques concernant la gestion, l'évaluation ou le suivi de l'affectation des ressources ou de la planification de tout ou partie du système de santé, y compris la prestation de services (planification et gestion du système de santé). Par exemple, la collecte et l'utilisation des RPS en tant qu'entité prescrite permettent au Réseau rénal de l'Ontario (RRO) de Santé Ontario de réaliser une analyse de planification des capacités pour les services rénaux offerts par les programmes rénaux régionaux de l'Ontario.

Personne prescrite (PP)

Santé Ontario est également désignée comme « personne prescrite » aux fins du paragraphe 39(1)(c) de la LPRPS en ce qui concerne son rôle dans la compilation et la tenue de trois registres désignés en vertu du paragraphe 13(1) du Règlement de l'Ontario 329/04 : i) le Registre ontarien de dépistage du cancer (RODC), ii) le registre des services cardiaques et vasculaires (géré par l'ancienne CorHealth) et iii) le registre des maladies chroniques. Cette désignation autorise Santé Ontario à recueillir, utiliser et divulguer des RPS dans ces registres afin de faciliter ou d'améliorer la prestation de soins de santé.

Organisation prescrite (OP)

Santé Ontario est une organisation prescrite en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS). En tant qu'organisation prescrite, Santé Ontario a le pouvoir et le devoir de développer et de maintenir le dossier de santé électronique (DSE) provincial, de mener des activités liées à l'identifiant numérique de santé (DHI), de fournir aux personnes l'accès à leurs DSE et DHI, et d'accomplir d'autres tâches prescrites.

Le DSE contient un enregistrement numérique sécurisé des renseignements personnels sur la santé des personnes, fournis par des dépositaires autorisés de renseignements sur la santé, et offre un moyen électronique permettant aux professionnels de la santé et à d'autres entités autorisées d'accéder à ces renseignements personnels sur la santé pour la prestation de soins ou à d'autres fins autorisées. Pour une description du DSE et un résumé des types de renseignements personnels sur la santé reçus par Santé Ontario pour développer et tenir à jour le DSE, veuillez consulter le site Web de Santé Ontario [Description et liste des référentiels du dossier de santé électronique \(DSE\)](#).

Les activités liées à l'identifiant numérique de santé (DHI) menées par Santé Ontario comprennent la fourniture de services visant à valider et à vérifier l'identité d'une personne, à authentifier son identité chaque fois qu'elle utilise son DHI pour accéder à un outil de santé numérique, ainsi qu'à gérer les comptes. Pour une description des activités liées à l'identifiant numérique de santé (DHI) menées par Santé Ontario, consultez [la description des activités liées à l'identifiant numérique de santé \(DHI\)](#) de Santé Ontario.

Agent de la LPRPS

La définition d'agent dans la LPRPS inclut toute personne (y compris les organisations, comme Santé Ontario) qui est autorisée par un dépositaire de renseignements sur la santé à effectuer des services ou des activités concernant les RPS au nom et aux fins du dépositaire. Par exemple, en tant qu'agent de la LPRPS, Santé Ontario est autorisée à gérer certains éléments du programme Health811 au nom du ministère de la Santé, qui est le dépositaire des renseignements sur la santé.

Chercheur

Santé Ontario gère un programme de recherche visant à développer de nouvelles connaissances grâce à la recherche épidémiologique, interventionnelle, sur les services de santé, la surveillance et les politiques, ainsi qu'à la synthèse et à la diffusion des connaissances. Santé Ontario peut utiliser les RPS qu'elle a recueillis en tant qu'entité ou personne prescrite à des fins de recherche, sous réserve des restrictions et conditions énoncées dans la LPRPS.

Fournisseur de services électroniques (FSE) et Fournisseur de réseaux de renseignements sur la santé (FRRS)

Santé Ontario fournit des services d'information électronique aux dépositaires de renseignements sur la santé afin de leur permettre de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer les RPS, et/ou d'échanger des RPS entre eux. En fournissant de tels services, Santé Ontario agit à titre de FSE et/ou de FRRS, conformément au Règlement de l'Ontario 329/04, art. 6 (1) et 6 (2) de la LPRPS. Ces rôles limitent strictement l'utilisation des RPS par Santé Ontario à ce qui est nécessaire pour soutenir les services électroniques offerts aux dépositaires. Santé Ontario fournit de nombreux services d'application en tant que FRRS, notamment le Système d'information sur la santé des clients (**CHRIS**), ainsi que la technologie de consultation électronique qui permet aux fournisseurs et aux organismes de soins de santé de partager des RPS à des fins de soins de santé.

Institution LAIPVP

Santé Ontario est une institution au sens de la LAIPVP et est assujettie à ses dispositions. La LAIPVP régit la collecte, l'utilisation, la divulgation et la conservation des RP. La collecte de RP par Santé Ontario directement auprès d'un patient, par exemple dans le cadre du Réseau des conseillers des patients et des familles, est soumise aux restrictions énoncées dans la LAIPVP. La LAIPVP accorde également au public un droit d'accès (par exemple, par le biais de demandes d'accès à l'information ou « DAI ») aux documents détenus ou contrôlés par une institution.

Loi sur le don de vie

Le Réseau Trillium pour le don de vie (RTDV), qui fait partie de Santé Ontario, recueille, utilise et divulgue des RP, y compris des RPS, aux fins de la planification, de la coordination, du soutien, de la recherche et de la production de rapports sur tous les aspects du don et de la transplantation d'organes et de tissus. Ce traitement des RP est autorisé par la *Loi sur le don de vie*, qui permet au RTDV de recueillir, directement ou indirectement, des informations sur les personnes à des fins de don et de transplantation d'organes et de tissus. De plus, la loi autorise l'agence à utiliser et à divulguer des RP à certaines personnes, à des installations spécifiquement désignées ou à conclure des accords de partage de données avec d'autres organisations, à condition que des mécanismes de confidentialité appropriés soient en place.

Vous souhaitez obtenir ces informations dans un format accessible? 1-877-280-8538, ATS 1-800-855-0511, info@ontariohealth.ca