# Rapport annuel sur la protection de la vie privée et la sécurité de Santé Ontario 2024-2025

Mai 2025

Santé Ontario

# Table des matières

# Introduction

Santé Ontario est un organisme intégré du ministère de la Santé qui a pour mandat de transformer, de relier et de coordonner le système de soins de santé de notre province afin de veiller à ce que les Ontariens reçoivent les meilleurs soins possibles. Cela comprend la fourniture de renseignements, d'outils numériques et de services au ministère de la Santé, aux fournisseurs de soins de santé et aux organismes du secteur de la santé en Ontario, nécessaires pour prioriser les personnes et les patients, en améliorant leur expérience de soins de santé et leurs résultats de santé plus près de chez eux.

Pour remplir son mandat, Santé Ontario nécessite l'accès à des données, y compris des renseignements personnels sur la santé (**RPS**) et des renseignements personnels (**RP**), provenant d'organismes et de personnes de partout en Ontario. Dans le traitement de ces renseignements, Santé Ontario est soumise 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**), ainsi qu'à la *Loi sur le don de la vie,* et s'engage à respecter les droits des particuliers en matière de protection de la vie privée, à protéger leurs renseignements et à respecter les lois sur la protection des renseignements personnels de l'Ontario.

La coordination et l'expansion de solutions de santé numériques et connectées, habilitées par la protection de la vie privée, l'utilisation responsable des données et la protection des données chez Santé Ontario sont complexes, passionnantes et en évolution rapide. Ensemble avec la modernisation des lois sur la protection des renseignements personnels, ils peuvent avoir une incidence positive sur les Ontariens, y compris sur les résultats de santé. Que ce soit des stratégies pour donner aux Ontariens un meilleur accès à leurs données de santé ou pour garantir que les droits à la vie privée soient respectés, établir un cadre de confidentialité et d'éthique pour l'utilisation de l'apprentissage automatique et de l'intelligence artificielle dans la recherche, examiner les pratiques de gestion de l'information des fournisseurs, appuyer la modernisation de la LPRPS ou ancrer la gouvernance et la gestion des données, le travail des équipes du Bureau de la protection de la vie privée et du Bureau de la sécurité de l'information de Santé Ontario a une incidence significative et tangible. Cela crée de la confiance, favorise l'innovation et permet à Santé Ontario de réaliser ses principales priorités stratégiques.

Un médecin sage a dit un jour : « Si les patients croient qu'ils reçoivent de bons soins, ils reçoivent de bons soins. » « Si les patients croient qu'ils reçoivent de mauvais soins, ils reçoivent de mauvais soins. »

De même, si les patients croient que les renseignements les plus sensibles les concernant ne sont pas protégés, ils peuvent retenir ces renseignements, ce qui pourrait en retour avoir une incidence sur leurs soins. Si les fournisseurs de soins de santé ont des préoccupations concernant la capacité de Santé Ontario à protéger les milliards d'actifs de données qu'elle détient, cela pourrait également avoir une incidence sur les soins des Ontariens. L'approche de Santé Ontario en matière de confidentialité et de sécurité favorise la confiance et permet de garantir que les Ontariens reçoivent les meilleurs soins possibles.

En 2024-2025, les équipes de protection de la vie privée et de sécurité de l'information de Santé Ontario, en collaboration avec d'autres partenaires opérationnels de l'organisme et de la province, ont continué à travailler ensemble pour éliminer les obstacles et aborder les nouvelles autorisations en vertu de la LPRPS, la protection des données, la cybersécurité, l'interopérabilité et d'autres questions de conformité, tout en faisant évoluer et mûrir de façon continue ses programmes de protection de la vie privée et de sécurité de l'information. La présent Rapport annuel sur la protection de la vie privée et la sécurité décrit les programmes de protection des renseignements personnels et de sécurité de Santé Ontario, et met en évidence les jalons atteints au cours de l'exercice 2024-2025 qui appuient et font progresser Santé Ontario dans l'accomplissement de son mandat. Le rapport examine également les mesures clés, dont certaines sont déclarées au Bureau du Commissaire à l'information et à la protection de la vie privée de l'Ontario (**CIPVP**), et se projette vers les priorités en matière de protection de la vie privée et de sécurité pour 2025-2026.

# Contexte

## Programme de cybersécurité de Santé Ontario

Le programme de cybersécurité de Santé Ontario est un partenariat collaboratif composé de trois équipes spécialisées : le Centre de cybersécurité de Santé Ontario, le Bureau de la sécurité de l'information et la Défense en matière de cybersécurité. Ensemble, ces équipes facilitent, renforcent et appuient la position de sécurité de l'information et de cybersécurité de Santé Ontario et du secteur de la santé provincial. Le programme vise à protéger les renseignements et les actifs du système, en veillant à l'harmonisation avec les objectifs opérationnels et les normes de l'industrie, tout en renforçant l'accès aux soins pour les patients et les fournisseurs.

**Gouvernance et partenariat en cybersécurité**

Le **Centre de cybersécurité de Santé Ontario (CCSO)** assure la direction, le leadership et la gouvernance en matière de cybersécurité pour le système de soins de santé de la province. Le Centre appuie une vision pour la gestion des risques en matière de cybersécurité dans l'ensemble du secteur provincial de la santé, et repose sur le soutien à la mise en œuvre des capacités de cybersécurité aux niveaux provincial, régional et des fournisseurs de services de santé. Le centre travaille en étroite collaboration avec le Bureau de la sécurité de l'information de Santé Ontario et l'équipe de Défense en matière de cybersécurité de Santé Ontario afin de mettre en œuvre une approche collective visant à protéger les actifs numériques de Santé Ontario.

Grâce à la création d'un programme de sécurité fondé sur les risques dans le portefeuille de l'Excellence numérique en santé, le **Bureau de la sécurité de l'information de Santé Ontario** (**BSI**) a conçu des mesures de protection physiques, techniques et administratives pour garantir un environnement sûr et sécurisé pour la prestation de solutions de santé numériques. Ces mesures de protection sont mises en œuvre conformément aux exigences législatives, aux normes internationales et aux décisions prioritaires fondées sur les risques afin d'assurer la confidentialité, l'intégrité et la disponibilité des données et des services.

Le Bureau de la sécurité de l'information est responsable de l'architecture de la sécurité, de la gouvernance de la sécurité, de la gestion des risques et de la conformité, de la gestion des risques de sécurité des tiers, des évaluations des menaces et des risques, et de la sensibilisation et de la formation en matière de sécurité. L'équipe fournit des services pour l'identification, l'évaluation et l'atténuation des risques de sécurité; des services de conseil en sécurité interne; et appuie la réponse aux incidents et aux violations en collaboration avec l'équipe de **Défense en matière de cybersécurité** (**DCS**).

L'équipe de DCS est responsable de la défense de première ligne et de la gestion des composants techniques de la sécurité chez Santé Ontario. Ce groupe comprend le Centre des opérations de sécurité (**COS**), la gestion des vulnérabilités, la gestion des identités et des accès (**GIA**), l'intervention en cas d'incident, et l'ingénierie des plateformes de sécurité. La DCS gère et priorise diverses initiatives en cours en fonction du risque interne du point et du contexte des menaces externes en constante évolution.

Chez Santé Ontario, en conformité avec son Programme de confidentialité, la sécurité est un principe de conception fondamental intégré dans tous les systèmes et opérations numériques. Grâce à une approche de « sécurité par conception », nous intégrons les considérations de sécurité tout au long du cycle de développement et des opérations, en déterminant et en atténuant les risques de façon proactive pour protéger les renseignements sensibles et se défendre contre les cybermenaces.

# Programme de confidentialité

Santé Ontario s'engage à respecter la vie privée des personnes et à protéger les RPS et les RP qu'elle détient ou contrôle. Pour appuyer cet engagement, Santé Ontario dispose d'un Programme de confidentialité solide et adapté, conçu pour garantir qu'une culture de protection de la vie privée soit non seulement établie, mais également ancrée dans l'organisme, lui permettant d'agir conformément à ses obligations et responsabilités légales. Santé Ontario croit que la législation est la base et non la limite pour favoriser la conformité et le changement. Par conséquent, elle maintient comme fondement les principes de « Protection de la vie privée dès la conception » et les normes de l'industrie, qui permettent d'établir la confiance et de favoriser l'innovation. Santé Ontario doit continuellement gagner et maintenir la confiance des Ontariens, du CIPVP ainsi que de ses principaux intervenants et partenaires provinciaux afin de remplir son mandat.

Le Bureau de la protection de la vie privée, avec ses partenaires en sécurité de l'information et d'autres partenaires opérationnels, est chargé des suivants :

- maintenir la confiance du public et protéger la vie privée des particuliers ainsi que la confidentialité, la sécurité et la disponibilité de milliards d'actifs de données;
- permettre à nos partenaires commerciaux de recevoir, de recueillir et d'utiliser ces actifs de données conformément aux lois sur la protection de la vie privée applicables et à l'appui du mandat de Santé Ontario d'optimiser les soins axés sur le patient;
- obtenir l'approbation du CIPVP des politiques et procédures de Santé Ontario tous les trois ans afin de continuer à respecter le mandat de Santé Ontario;
- éliminer les obstacles et plaider en faveur des changements nécessaires pour transformer l'écosystème des données de santé.

La gouvernance de la vie privée et la structure de responsabilité de Santé Ontario garantissent que la gestion de son Programme de confidentialité est surveillée et harmonisée avec ses objectifs et son cadre juridique. Le Programme fait partie du portefeuille Stratégie, Planification, Protection de la vie privée, Analyse et Risque dont la mission est de s'efforcer de répondre aux besoins de Santé Ontario et de les dépasser tout en améliorant les outils, les méthodes et les processus. Le Programme de confidentialité est dirigé par le directeur de la protection de la vie privée (**DPVP**), lequel relève directement du directeur général, Stratégie, Planification, Protection de la vie privée, analyse et risque de Santé Ontario. Une équipe de professionnels de la vie privée dévoués, de gestionnaires et d'un directeur appuie le DPVP dans le maintien de la confiance du public en gérant les opérations quotidiennes du Programme de confidentialité de Santé Ontario, notamment :

- collaborer avec le ministère de la Santé, le CIPVP et d'autres intervenants provinciaux sur l'établissement de nouvelles autorisations qui permettront à Santé Ontario d'offrir de nouveaux services et programmes aux Ontariens;
- déteminer des occasions de simplifier les autorisations et pratiques existantes, atténuer les risques pour Santé Ontario en concevant des exigences opérationnelles en matière de protection de la vie privée axées sur l'utilisateur pour de nouveaux programmes, services et technologies;
- évaluer les propositions des fournisseurs et aider à la gestion des fournisseurs;

- appuyer de nouvelles acquisitions et utilisations de données, diriger des initiatives d'élaboration de politiques;
- superviser l'élaboration et le déploiement de la formation obligatoire et opportune sur la protection de la vie privée;
- gérer l'ensemble des obligations opérationnelles en matière de protection de la vie privée, y compris l'application des directives en matière de consentement individuel, l'enquête et la gestion des violations de la vie privée, et collaborer avec les fournisseurs de soins de santé partout en Ontario pour répondre aux demandes d'accès et de correction.

En partenariat avec l'équipe de la Sécurité de l'information et d'autres partenaires opérationnels dans tous les portefeuilles, le Bureau de la protection de la vie privée offre non seulement des services opérationnels, de conseil et d'assurance, mais également des solutions de protection de la vie privée pragmatiques, créatives et fondées sur les risques qui permettent aux portefeuilles et aux programmes d'atteindre les objectifs annuels du plan opérationnel tout en réduisant au minimum le risque résiduel pour l'organisme. En raison de ces partenariats étroits, les exigences et les contrôles en matière de protection de la vie privée sont intégrés dans les nouveaux projets, processus et programmes de manière à faciliter la capacité de Santé Ontario à remplir son mandat tout en protégeant les droits à la vie privée des Ontariens.

# Législation sur la vie privée

Santé Ontario tire son mandat et son autorité de collecter, d'utiliser, de divulguer et de gérer autrement les RPS et les RP de ses désignations en vertu de la LPRPS, de la LAIPVP, de la *Loi sur le don de la vie* et de la *Loi pour des soins interconnectés*. La liste suivante décrit les diverses autorisations légales en matière de protection de la vie privée sur lesquelles Santé Ontario s'appuie pour remplir son mandat, pour ses opérations, et pour optimiser son utilisation autorisée des données à des fins bénéfiques.

## Entité prescrite (EP)

Santé Ontario est désignée comme une « entité prescrite » aux fins du paragraphe 45(1) de la LPRPS. Ce paragraphe permet aux dépositaires de renseignements sur la santé (comme les hôpitaux, les laboratoires et les médecins) de divulguer des RPS sans consentement à Santé Ontario en tant qu'entité prescrite aux fins de l'analyse ou du rassemblement de renseignements statistiques concernant la gestion, l'évaluation ou la surveillance de la répartition des ressources au système de santé, en tout ou en partie, 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 offerts par les programmes rénaux régionaux de l'Ontario.

## Personne prescrite (PP)

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

## Organisation prescrite (OP)

Santé Ontario est désignée comme une « organisation prescrite » aux fins de la partie V.1 de la LPRPS. Cette désignation accorde à Santé Ontario l'autorité d'élaborer et de tenir à jour le dossier de santé électronique (**DSE**), en s'appuyant sur le cadre opérationnel et de protection de la vie privée qui a été initialement mis en place en vertu de l'article 6.2 du Règlement de l'Ontario (**Règl. de l'Ont.**) 329/04 en décembre 2011.

Le DSE est composé des registres provinciaux des clients et des fournisseurs, des laboratoires, des médicaments sur ordonnance, des services d'imagerie diagnostique (services communs) et des référentiels de documents cliniques, où les dossiers sont reçus des dépositaires de renseignements sur la santé comme les hôpitaux et les équipes de santé familiale. En tant qu'organisation prescrite, Santé Ontario permet l'accès aux RPS détenus dans le DSE pour les fournisseurs de soins de santé autorisés dans le cadre de la prestation de soins de santé, grâce à l'application ConnexionOntario. Santé Ontario est également autorisée à permettre l'accès aux RPS aux coroners et aux médecins hygiénistes pour d'autres utilisations autorisées.

Dans un avenir proche, Santé Ontario sera autorisée à fournir aux Ontariens un moyen numérique d'accéder à leurs RPS détenus dans le DSE.

## Agent de la LPRPS

La définition d'agent en vertu de la LPRPS comprend toute personne (y compris des organisations, comme Santé Ontario) qui est autorisée par un dépositaire de renseignements sur la santé à fournir des services ou à mener des activités à l'égard de RPS au nom du dépositaire et à ses fins. Par exemple, en tant qu'agent de la LPRPS, Santé Ontario est autorisée à gérer des composantes du programme Santé811 (**H811**) au nom du ministère de la Santé, qui en est le dépositaire.

## 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 à titre d'entité prescrite ou de personne prescrite aux fins de la recherche, sous réserve des restrictions et des conditions énoncées dans la LPRPS.

## Fournisseur de services électroniques (FSE) et fournisseur de réseau d'information sur la santé (FRIS)

Santé Ontario fournit des services de renseignements électroniques aux dépositaires de renseignements sur la santé pour leur permettre de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer des RPS, ou d'échanger des RPS entre eux. En fournissant ces services, Santé Ontario agit à titre de FSE ou de FRIS, conformément au Règl. de l'Ont. 329/04, articles 6(1) et 6(2) de la LPRPS. Ces rôles limitent strictement l'utilisation des RPS par Santé Ontario à ceux qui appuient les services électroniques aux dépositaires. Santé Ontario offre de nombreux services d'application en tant que FRIS, y compris le Client Health and Related Information System (**CHRIS**), ainsi que la technologie eConsultation qui permet aux fournisseurs de soins de santé et aux organisations d'échanger des RPS aux fins de soins de santé.

## Institution FIPPA

Santé Ontario est une « institution » au sens de la LAIPVP et est assujettie à ses exigences. La LPRPS régit la collecte, l'utilisation, la communication 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 représentants des patients et 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 de « **DAI** ») aux documents en la possession ou sous le contrôle d'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 des rapports sur tous les aspects des services de don et de transplantation d'organes et de tissus. Cette gestion des renseignements personnels est autorisée par la *Loi sur le don de vie*, qui permet au RTDV de recueillir, directement ou indirectement, des renseignements sur des personnes aux fins des services de don et de transplantation d'organes et de tissus. De plus, la Loi confère à l'Agence le pouvoir d'utiliser et de divulguer des RP à certains particuliers, à des établissements désignés ou de conclure des ententes d'échange de données avec d'autres organisations, à condition que des mécanismes appropriés de protection de la vie privée soient en place.

# Paysage réglementaire en changement

Depuis 2019, le ministère de la Santé a pris des mesures significatives pour consulter les intervenants du secteur de la santé afin de « moderniser » la LPRPS. Certains des moteurs du changement ont été l'accélération des soins numériques et virtuels ainsi que le soutien aux droits des patients d'accéder à leurs dossiers par voie numérique. Ces changements ont une incidence directe sur Santé Ontario et les nombreux rôles importants qu'elle joue pour appuyer l'utilisation des données au profit de tous dans l'amélioration des soins aux patients.

## Accès individuel au dossier de santé électronique (DSE) (nouveau)

En juillet et décembre 2024, des modifications au Règlement de l'Ontario 329/04 et à la LPRPS ont été proposées pour permettre à Santé Ontario, en tant qu'organisation prescrite, de fournir aux particuliers un accès numérique à leurs dossiers de RPS détenus dans le DSE, en commençant par les services de laboratoire, de médicaments et de pharmacie. Cet accès numérique reposera sur le service de vérification d'identité décrit ci-dessous. Santé Ontario continue de collaborer avec le ministère de la Santé concernant ces changements proposés, qui ne sont pas encore en vigueur.

## Identifiant de santé numérique (ISN) (nouveau)

En juillet et décembre 2024, des modifications au Règlement de l'Ontario 329/04 et à la LPRPS ont été proposées pour permettre à Santé Ontario, sous une nouvelle autorisation de la LPRPS, de fournir aux particuliers un moyen numérique de valider et de vérifier leur identité, afin de se connecter aux outils de santé numériques offerts par Santé Ontario et d'autres organisations de soins de santé partout dans la province. Ce service de vérification d'identité appuiera l'accès individuel au DSE tel que décrit ci-dessus.

Santé Ontario continue de collaborer avec le ministère de la Santé concernant ces changements proposés, qui ne sont pas encore en vigueur.

## Contribution obligatoire au DSE (nouveau)

Le 1er janvier 2025, des modifications au Règlement de l'Ontario 329/04 en vertu de la LPRPS sont entrées en vigueur; ce qui impose une contribution au DSE de certains secteurs prioritaires afin d'assurer des dossiers patients plus complets. Plus précisément, en plus de l'exigence existante pour les exploitants d'hôpitaux publics, les exploitants de pharmacies communautaires accréditées et les centres de services de santé communautaire intégrés sont désormais également tenus de contribuer certains RPS au DSE comme demandé par Santé Ontario et conformément aux spécifications d'interopérabilité de Santé Ontario.

## Projet de loi 194 : Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public (nouvelle)

Le projet de loi 194 a été présenté en mai 2024 avec deux annexes. L'annexe 1 a introduit une nouvelle législation, la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* (**LRSCN**), visant à renforcer la

cybersécurité dans le secteur public. L'annexe 2 modifie la *Loi sur l'accès à l'information et la protection de la vie privée* (**LAIPVP**) pour améliorer et moderniser les mesures de protection de la vie privée. La LRSCN s'applique à l'ensemble des secteurs publics provinciaux et municipaux, et donne au gouvernement la capacité d'édicter des règlements qui exigent aux entités du secteur public les suivants :

- avoir des programmes de cybersécurité qui comprennent des aspects liés à l'attribution de responsabilités internes, à la sensibilisation à l'éducation, à la réponse aux incidents et à la supervision des programmes; et
- soumettre des rapports d'incidents de cybersécurité et établir des exigences pour de tels rapports.

La LRSCN donne également au ministre des Services au public et aux entreprises la capacité d'établir des normes techniques et de publier des directives en matière de cybersécurité.

La LRSCN introduit des obligations en matière d'intelligence artificielle (IA) pour les organisations du secteur public, comme Santé Ontario, y compris :

- diffuser des renseignements sur leur utilisation;
- élaborer et mettre en œuvre un cadre de responsabilisation;
- gérer les risques associés à l'utilisation d'un système d'IA;
- nommer une personne pour superviser l'utilisation des systèmes d'IA et répondre à d'autres obligations stipulées.

Enfin, la LRSCN donne au gouvernement le pouvoir d'édicter des règlements régissant le traitement des renseignements des mineurs par les sociétés d'aide à l'enfance et aux conseils scolaires.

**Modifications à la LAIPVP**

Au sens de la LAIPVP, Santé Ontario est une « institution » en ce qui concerne sa gestion des renseignements personnels. Le projet de loi 194 introduit de nouvelles exigences en matière de déclaration des atteintes à la vie privée et d'évaluation des facteurs relatifs à la vie privée pour les institutions régies par la LAIPVP. Il élargit également les pouvoirs du CIPVP pour enquêter sur la conformité en matière de protection de la vie privée, accordant au CIPVP de nouveaux pouvoirs de rendre des ordonnances.

Les changements dans la déclaration des atteintes à la vie privée pour les atteintes liées aux RP et la notification comprennent les suivants :

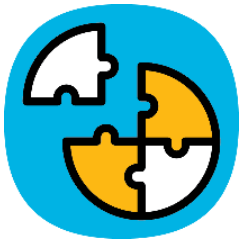
- Le projet de loi 194 utilise le seuil de « risque réel de préjudice grave » (RRPG) pour le signalement des atteintes et l'avis connexe. Santé Ontario sera tenu de rendre compte au CIPVP et d'informer les particuliers concernés s'il y a des raisons de croire qu'il y a un RRPG associé à une atteinte aux RP.
- Santé Ontario sera tenue de conserver un dossier de chaque vol, perte et utilisation ou divulgation non autorisée de RP qu'elle signale au CIPVP.
- Santé Ontario devra soumettre un rapport annuel au CIPVP qui résume le nombre de vols, de pertes et d'utilisations ou de divulgations non autorisées de RP.
- Santé Ontario sera tenue de réaliser des évaluations des facteurs relatifs à la vie privée (**EFVP**) avec des exigences de contenu précises avant de recueillir des renseignements personnels et de mettre à jour les EFVP lorsqu'un

changement dans le traitement des RP est prévu.

- Santé Ontario, lorsqu'elle agit en tant qu'« institution » en vertu de la LAIPVP, est tenue de mettre en œuvre des mesures de protection raisonnables pour protéger les RP contre le vol, la perte et l'utilisation ou la divulgation non autorisée, et pour se protéger contre la copie, la modification ou l'élimination non autorisées.
- Le projet de loi 194 élargira les pouvoirs d'enquête en matière de conformité à la vie privée du CIPVP, lui donnant le pouvoir de mener des examens fondés sur des plaintes et proactifs des pratiques en matière de traitement de l'information.
- Enfin, le projet de loi 194 permettra de soumettre des rapports confidentiels de « lanceurs d'alerte » directement au CIPVP, interdisant au CIPVP de révéler l'identité de la personne ayant fait le rapport.

À partir du 1er juillet 2025, la LRSCN ainsi que toutes les modifications à la LAIPVP introduites dans le projet de loi 194 seront entrées en vigueur.

# Principaux jalons et réalisations en matière de protection de la vie privée et de sécurité



En 2024-2025, les équipes de protection de la vie privée et de sécurité se sont concentrées sur l'atteinte des objectifs suivants.

## Conseil ontarien des données sur la santé (CODS) (mis à jour)

En 2024-2025, le Bureau de la protection de la vie privée, en collaboration avec l'Excellence numérique en santé et l'équipe de CorHealth, a soumis la première demande au Groupe de travail consultatif sur le DSE et par la suite au Conseil ontarien des données sur la santé (**CODS**), afin que le ministre ordonne à Santé Ontario en tant qu'organisation prescrite de divulguer les RPS détenus dans le DSE, à Santé Ontario en tant que personne prescrite, de faciliter ou d'améliorer la prestation des soins cardiaques par le biais du Système d'information sur la collecte de données (**SICD**). Cette demande a été approuvée en janvier 2025.

Le SICD est un service d'analyse moderne en soutien à l'efficacité des procédures chirurgicales des centres cardiaques CorHealth.

Le SICD recueille des données sur les temps d'attente pour les procédures chirurgicales auprès des 20 centres cardiaques participant au réseau CorHealth des services cardiaques et vasculaires. Les données limitées du DSE, lorsqu'elles sont interrogées, garantiront que les dossiers cardiaques sont aussi précis que possible.

Créé en 2021, le CODS offre au ministre de la Santé des conseils sur la gestion stratégique des données de santé de l'Ontario en vue de favoriser un système de santé axé sur la personne et l'apprentissage. Le directeur général, Stratégie, Planification, Protection de la vie privée et analyse de l'Ontario participe en tant que membre du

CODS et offre des conseils sur la gestion de l'intégration des données de santé des Ontariens afin de générer des analyses, des aperçus et des innovations nécessaires au secteur de la santé et aux décideurs gouvernementaux. Le CODS agit également en tant que Comité consultatif sur les dossiers de santé électroniques pour remplir le mandat législatif indiqué à l'article 55.11 (1) de la LPRPS.

Le site Web du Ministère contient la description suivante du rapport du CODS sur l'utilisation des données pour les soins intégrés :

« En novembre 2022, le CODS a partagé son rapport avec le ministère de la Santé sur la façon dont l'Ontario peut utiliser les données pour créer un système de santé plus intégré pour les patients. Les recommandations du rapport du CODS aideront la province à continuer d'exploiter les données pour

appuyer des soins plus connectés et pratiques en Ontario. Le Conseil a formulé les recommandations stratégiques clés suivantes pour orienter la transformation de l'écosystème de données sur la santé de l'Ontario :

- Intégrer et utiliser les données sur la santé pour faire progresser les résultats en matière de santé et d'équité pour les gens, les collectivités et les populations.
- Promouvoir l'équité en matière de santé au moyen de la collecte, de l'analyse et de l'utilisation appropriées des données.
- Établir une gouvernance et des politiques dignes de confiance à l'échelle du système pour les données sur la santé en tant que bien public.
- Respecter et appuyer la souveraineté des données des peuples inuits, métis et des Premières Nations.
- Renforcer la capacité d'intendance de données et permettre l'échange par défaut. » [1]

## Groupe de travail consultatif sur le DSE (mis à jour)

Le Groupe de travail consultatif sur le DSE (le Groupe de travail) est un organe consultatif permanent qui appuie le CODS et lui rend compte dans le cadre de son Comité consultatif sur le DSE. Le Groupe de travail est composé d'un membre du Conseil à titre de président du Groupe de travail, ainsi que de représentants du secteur de la santé élargi de l'Ontario ayant des intérêts dans le DSE et la protection de la vie privée des RPS. Cela comprend les dépositaires des renseignements sur la santé, le CIPVP, et le public ainsi que les représentants de Santé Ontario dans leur capacité d'organisation prescrite et en tant que responsables de la gestion et de l'exploitation du DSE. Les représentants de Santé Ontario comprennent le DPVP, le directeur de la Gestion des produits et de la livraison (Laboratoire, Médicaments et Gestion des données du DSE) et le gestionnaire de la Protection de la vie privée chargé des services d'assurance pour Santé Ontario en tant qu'organisation prescrite.

Le mandat du Groupe de travail consultatif sur le DSE définit les objectifs du groupe de travail, et comprend[2] :

« Le Groupe de travail élaborera et formulera des recommandations au Conseil au sujet des aspects suivants de l'article 55.11 de la LPRPS :

a) des pratiques et procédures que l'organisation prescrite, Santé Ontario, doit mettre en place pour protéger la vie privée des particuliers dont elle reçoit les RPS et pour maintenir la confidentialité des renseignements;
b) les pratiques et procédures que l'organisation prescrite, Santé Ontario, doit avoir en place pour répondre ou faciliter une réponse à une demande faite par un particulier en vertu de la Partie V pour un dossier de RPS concernant le particulier qui est accessible au moyen du DSE;
c) les mesures de protection administratives, techniques et physiques que l'organisation prescrite, Santé Ontario, devrait mettre en place pour protéger la vie privée des particuliers dont elle reçoit les RPS et pour maintenir la confidentialité des renseignements;
d) le rôle de l'organisation prescrite, Santé Ontario, dans l'assistance à un dépositaire de renseignements sur la santé pour s'acquitter de ses obligations d'informer les particuliers en vertu des paragraphes 12 (2) et 55.5 (7) dans le cas où des RPS

[1] https://www.ontario.ca/fr/page/rapport-du-conseil-des-donnees-sur-la-sante-de-lontario-une-vision-pour-lecosysteme-des-donnees-sur-la-sante-de-lontario

[2] Mandat du Groupe de travail consultatif sur le DSE du Conseil ontarien des données sur la santé, ébauche 4.0

accessibles au moyen du DSE sont volés ou perdus, ou sont recueillis, utilisés ou divulgués sans autorisation;

e) la fourniture d'un avis au cas où des RPS accessibles au moyen du DSE sont volés ou perdus, ou sont recueillis, utilisés ou divulgués sans autorisation;
f) tout ce qui est mentionné dans la partie V.1 de la LPRPS ou dans les règlements comme pouvant faire l'objet d'une recommandation du comité consultatif;
g) des réponses aux propositions pour un accès secondaire aux données dans le DSE tel que décrit à l'article 55.10 de la LPRPS;
h) toute autre question renvoyée par le ministre au Groupe de travail par l'entremise du Conseil. »

## Formation et sensibilisation à la vie privée – Journée de la protection de la vie privée (mis à jour)

La Semaine de la protection des données se passait du 27 au 31 janvier 2025, et était une prolongation de la Journée de la protection des données (28 janvier). Cette semaine est célébrée au niveau international; elle constitue un moyen de sensibiliser le public à l'importance de la protection de la vie privée et de la protection des données tout en soulignant l'incidence de la technologie sur notre vie au quotidien. Le 28 janvier, le CIPVP a organisé un événement pour la Journée de la protection des données : Les enjeux clés abordés comprenaient les derniers développements en matière de technologies d'amélioration de la confidentialité et comment elles permettent aux organisations d'utiliser des données sans compromettre la vie privée.

Pour accroître davantage la sensibilisation à la vie privée parmi les employés de Santé Ontario, l'équipe de confidentialité a déployé une campagne d'un mois visant à fournir des messages clés sur la protection de la vie privée sur les écrans de verrouillage des ordinateurs afin d'aider à renforcer l'apprentissage, a publié une série de bulletins hebdomadaires tout au long du mois de janvier sur divers thèmes, et a introduit un tout nouvel article de blogue mettant en vedette la directrice générale de la protection de la vie privée de Santé Ontario. Voici des exemples de thèmes du bulletin hebdomadaire :

- Votre résolution 2025 : Augmenter votre connaissance en matière de protection des données
- La protection de la vie privée au travail et au-delà
- Modèles de conception trompeurs et votre vie privée
- Littératie numérique et vie privée : Autonomiser les aînés et les jeunes de l'Ontario à l'ère numérique
- Adopter l'IA en gardant la vie privée à l'esprit
- Blogue Vantage Point : « Sharing Versus Over-Sharing » (Partager ou trop partager)

## Examen et approbation de Santé Ontario par le Commissaire à l'information et à la protection de la vie privée (CIPVP) (mis à jour)

À titre de personne prescrite, d'entité prescrite et d'organisation prescrite, Santé Ontario est tenue de faire examiner et approuver ses pratiques en matière d'information par le CIPVP de manière régulière.

L'approbation du CIPVP permet à Santé Ontario de continuer à remplir son mandat, qui comprend la planification du système de santé, le dépistage du cancer, la recherche, la gestion de l'information sur les temps d'attente, et l'élaboration et la tenue à jour du DSE provincial.

Tout au long de 2024-2025, Santé Ontario a travaillé avec diligence à la préparation de l'examen triennal de 2026 par le CIPVP. Le 1er août 2025, Santé Ontario soumettra des indicateurs de protection de la vie privée, de

sécurité de l'information, de ressources humaines et organisationnels au CIPVP.

Le CIPVP examinera les indicateurs soumis, demandera des documents et des renseignements supplémentaires, au besoin, et déterminera les politiques, procédures et pratiques qui seront au centre de cet examen triennal du CIPVP.

Les politiques, procédures et pratiques seront évaluées pour s'assurer qu'elles protègent les RPS reçus par Santé Ontario dans le cadre de ses statuts prescrits, et pour savoir si Santé Ontario respecte ces politiques, procédures et pratiques.

## Faciliter l'utilisation des données à Santé Ontario – Stratégie provinciale sur les données de santé et le numérique (SPDSN) (mise à jour)

Santé Ontario détient des actifs de données clés du système de santé qui ont été transférés des anciennes agences de santé de l'Ontario conformément à la *Loi de pour des soins interconnectés*. Santé Ontario continue d'acquérir de nouveaux actifs de données pour la planification et la gestion du système, et à la demande du ministère de la Santé à des fins autorisées. Même si ces actifs de données continuent d'être gérés conformément aux autorisations et pratiques existantes, l'équipe de protection de la vie privée, de sécurité de l'information et d'acquisition et de services de données travaille en étroite collaboration avec des collègues du ministère de la Santé pour étudier, par le biais de modifications réglementaires supplémentaires et de décisions stratégiques, des occasions d'élargir ou de simplifier les pouvoirs de Santé Ontario afin d'optimiser l'utilisation de ses actifs de données.

En attendant, l'utilisation élargie de ces actifs de données dans l'organisation exige la mise en œuvre de pratiques et de procédures en matière de protection de la vie privée, de sécurité et de gestion de l'information qui répondent, au minimum, aux exigences du CIPVP concernant le rôle de Santé Ontario en tant qu'entité prescrite et personne prescrite. Au cours de l'année à venir, les équipes de protection de la vie privée, de sécurité de l'information et d'acquisition de données continueront d'appuyer ce travail, qui progressera en parallèle avec l'élaboration de la Stratégie de données et d'analyse de Santé Ontario et les efforts du ministère de la Santé concernant la modernisation de la LPRPS.

Des discussions bilatérales sont en cours entre le ministère de la Santé et Santé Ontario pour établir les priorités à court terme pour l'élaboration et la mise en œuvre des Services provinciaux de données de santé et numériques (**SPDSN**), y compris :

- Recommander des orientations stratégiques
  pour appuyer une approche « Recueillir une seule fois, utiliser plusieurs fois » pour l'utilisation des données et simplifier les pouvoirs de Santé Ontario en matière de protection de la vie privée.
- Déterminer les exigences pour appuyer les recommandations stratégiques et évaluer l'incidence des changements stratégiques proposés.
- Travailler avec le ministère de la Santé pour modifier la LPRPS afin d'élargir les registres de Santé Ontario en un Registre des maladies chroniques qui permettra la création du Programme ontarien de dépistage de l'anévrisme de l'aorte abdominale et la planification de l'amélioration de la qualité.

Conformément aux recommandations énoncées par le CODS, le projet stratégique actuel de la SPDSN est axé sur l'étude d'options qui permettront à Santé Ontario de « Recueillir les données une fois, et de les utiliser plusieurs fois », appuyée par l'unification et l'avancement des pratiques de gouvernance des données grâce à

l'établissement d'un cadre de gouvernance et de gestion des données, l'harmonisation des normes, et la modernisation de l'infrastructure existante de données et numérique.

## Faire mûrir le Processus de gestion des incidents de la vie privée (nouveau)

Au cours de 2024-2025, le Bureau de la protection de la vie privée a continué à faire évoluer le processus de gestion des incidents de la vie privée de Santé Ontario comme suit :

- Diriger la révision de la *Politique et procédures de gestion des incidents de confidentialité* et de la *Politique et procédures de gestion des incidents de confidentialité du DSE* afin de préciser les processus que les agents de Santé Ontario doivent suivre lors de la gestion des incidents de confidentialité.
- Fournir des séances de formation sur la gestion des incidents de confidentialité aux employés de Santé Ontario.

Organiser le premier exercice sur table sur l'enquête d'incidents précis de confidentialité. Les exercices sur table offrent un aperçu du processus d'intervention aux incidents de confidentialité, précisent les rôles et les responsabilités, et cernent les lacunes, en vue d'améliorer la sensibilisation au processus de gestion des incidents de confidentialité. Cet exercice a réussi avec la participation du personnel de Santé Ontario provenant du Bureau de la protection de la vie privée, des Communications, de la Défense de la cybersécurité, des Ressources humaines et des Services juridiques.

## Projet d'optimisation de la confidentialité (nouveau)

L'équipe de confidentialité a trouvé des occasions pour pour simplifier un certain nombre d'activités du programme de confidentialité, y compris optimiser des processus d'admission, examiner l'utilisation d'outils et de technologies, établir des processus de priorisation des projets avec ses nombreux partenaires opérationnels et jeter les bases d'un cadre amélioré de gestion des risques et des contrôles en matière de protection de la vie privée grâce à un modèle de « Trois lignes de défense » (**3 LD**). La mise en œuvre de ces améliorations créera des occasions pour augmenter l'efficacité opérationnelle, réduire la charge de travail manuelle et permettre aux unités opérationnelles de jouer un rôle plus proactif dans la gestion quotidienne, y compris l'atténuation des risques opérationnels. Ce travail se poursuivra jusqu'à la fin de l'exercice 2025-2026.

## Faire avancer les capacités cybernétiques à l'échelle du secteur : Centre de cybersécurité de Santé Ontario (mis à jour)

En 2024/25, le Centre de cybersécurité de Santé Ontario (**CCSO**) a concentré ses efforts sur la mise en œuvre et la stratégie du *Modèle opérationnel provincial de cybersécurité* (**MOC**).

Ces étapes comprenaient :

- Améliorer les pratiques exemplaires en passant au Cadre de cybersécurité 2.0 de l'Institute of Standards and Technology (**NIST**);
- Élaborer et mettre en œuvre un suivi initial des contrôles critiques pour mesurer les progrès et la maturité des contrôles critiques prioritaires par les fournisseurs de services de santé (**FSS**) critiques;
- Améliorer le renseignement sur les menaces et la surveillance en lançant une plateforme d'Échange de renseignement sur les cybermenaces (**CTIX**);
- Tester la préparation et les processus d'intervention en cas d'incident établis au moyen de la participation à deux exercices

sur table avec le Ministère et les partenaires du secteur;
- Déterminer et prioriser la protection des actifs précieux en élaborant un référentiel d'actifs des joyaux de la couronne;
- Mobiliser les FSS au-delà du cadre des entités de soins aigus pour mieux comprendre et élaborer des stratégies sur la manière dont ces fournisseurs peuvent être intégrés dans la prochaine version du MOPC; et
- Faire progresser des capacités, du contenu et des ressources sur le portail de cybersanté dédié pour le secteur.

Le MOPC démontre constamment son efficacité à améliorer la disponibilité et la résilience des soins aux patients, posant ainsi les bases de son élaboration et de son amélioration continues. Les patients et les communautés de la province continueront de profiter d'un système de santé qui protège les services et les données des patients; ce qui entraîne de meilleurs résultats en matière de santé. La prochaine phase du MOPC favorise une approche plus coopérative en matière de cybersécurité, stimulant des avancées à l'échelle du secteur pour protéger les soins et les renseignements des patients tout en renforçant les défenses contre les nouvelles cybermenaces.

## Harmoniser les Normes de cybersécurité (nouveau)

Pendant l'exercice financier 2024-2025, en collaboration avec les équipes du Programme d'architecture, des Services de réseau et des Opérations infonuagiques, les normes suivantes en matière d'architecture de sécurité ont été mises en œuvre :

- **Norme d'architecture à vérification systématique** : Cette approche fournit une architecture de référence pour une stratégie de cybersécurité fondée sur les risques. La communication entre les utilisateurs, les systèmes et les appareils est continuellement authentifiée, autorisée et validée. Une architecture à vérification systématique applique des stratégies d'accès en fonction du contexte, comme le rôle de l'utilisateur, l'heure de la journée, la géolocalisation, l'appareil et les données qu'elle demande. Le niveau d'accès accordé est ajusté de façon dynamique en fonction du niveau de confiance établi avec le sujet. En bref, plus un système d'information peut développer de la confiance envers un sujet, plus l'accès à ce sujet peut être accordé.
- **Norme de zone de sécurité de réseau** : Le zonage de sécurité est un élément clé de la stratégie de défense en profondeur pour protéger les réseaux de Santé Ontario et appuyer la prestation de services électroniques, l'interconnectivité et l'interopérabilité. La norme définit le zonage de sécurité et les flux de communication de haut niveau qui sont autorisés entre les zones afin que les services et les équipes de Santé Ontario puissent améliorer leur position de sécurité. Les directives de cette norme s'appliquent aux environnements sur place et dans le nuage.
- **Norme d'architecture de sécurité infonuagique Amazon AWS :** Cette norme définit une architecture de référence pour garantir une mise en œuvre et un déploiement sécurisés des produits et services chez le locataire AWS de Santé Ontario.
- **Norme DevSecOps :** Cette norme fournit le cadre directeur pour intégrer la sécurité dans le processus DevOps, en veillant à ce que les considérations de sécurité soient intégrées tout au long du cycle de vie du développement logiciel.
- **Analyseur de sécurité des applications dynamiques (DAST)** : Ce mécanisme de test de sécurité a été introduit dans les abonnements de produits Azure pour intégrer les tests de sécurité dès le début

du cycle de développement du produit. DAST est également fourni pour les environnements sur place de Santé Ontario (**CODS**) et devrait commencer les tests de sécurité.

## Risque des tiers : Renforcer la résilience au-delà des murs de Santé Ontario (nouveau)

Les auteurs malveillants ciblent de plus en plus les fournisseurs de technologie et de services, car compromettre un fournisseur tiers de confiance peut être un moyen efficace d'accéder à de nombreuses organisations et à des fournisseurs en aval. Par conséquent, les politiques et pratiques existantes de Santé Ontario pour gérer les risques de sécurité liés aux tiers évoluent pour faire face à l'augmentation et à la complexité de ses relations avec les fournisseurs et des partenariats dans le secteur de la santé.

Le Bureau de la sécurité de l'information (**BSI**) de Santé Ontario a entrepris des améliorations du programme de Gestion des risques de sécurité des tiers (**GRST**) conformément aux recommandations de l'industrie pour faire évoluer les capacités de GRST. L'intégration améliorée des fonctions de GRST dans les unités opérationnelles garantit une meilleure intégration des processus avec des fonctions clés d'entreprise comme l'approvisionnement, la gouvernance de projet, l'exécution des opérations et la gestion des risques d'entreprise. Une surveillance solide des risques de sécurité des tiers et des rapports de tableau de bord tout au long de la relation avec les tiers offrent une visibilité continue sur les risques de sécurité des tiers et facilitent la mobilisation efficace de la haute direction et les décisions en matière de risque. L'exploitation de manière constructive des certifications industrielles (par exemple, ISO/IEC 27001, HITRUST r2), des attestations de contrôle (par exemple, SOC 2) et des audits de tiers comme prévus permet de faciliter et de normaliser l'évaluation des risques de sécurité des tiers, et d'optimiser les ressources de sécurité. Avec la consultation des intervenants, le BSI a établi et officialisé la *Norme de gestion des risques de sécurité des tiers* et le *Cadre de gestion des risques de sécurité des tiers* au cours de l'exercice financier 2024-2025, et le *Cadre* sera mis en œuvre au cours de l'exercice financier 2025-2026.

## La maturité est importante : Comprendre notre préparation en matière de sécurité (nouveau)

Dans le cadre de l'engagement continu de Santé Ontario à renforcer sa résilience en matière de cybersécurité, les équipes de cybersécurité de Santé Ontario ont lancé une initiative interne d'Évaluation de la maturité en cybersécurité. Cette évaluation s'appuie sur la plateforme Axio360, harmonisée avec le NIST Cybersecurity Framework (**CSF**) 2.0 nouvellement mis à jour, et adaptée au Centre de cybersécurité de Santé Ontario.

L'objectif de cette initiative est d'évaluer systématiquement la position de cybersécurité actuelle de Santé Ontario, de déterminer les points forts, de trouver des occasions d'amélioration et de prioriser les améliorations ciblées. Cette évaluation proactive appuie l'harmonisation avec les normes provinciales de cybersécurité et renforce le rôle de notre organisation dans un modèle de sécurité intégré du système de santé plus vaste.

Cette initiative a commencé au quatrième trimestre de l'exercice 2024-2025, en collaboration avec des partenaires internes de plusieurs unités opérationnelles, et devrait fournir des renseignements stratégiques qui éclaireront directement directement la planification, le financement et la définition des objectifs en matière de cybersécurité pour l'exercice 2025-2026. L'évaluation servira

également de première étape vers l'amélioration continue, permettant de garantir que Santé Ontario est bien positionnée pour gérer les menaces en évolution, protéger les données sensibles qui lui sont confiées, et maintenir la confiance du public.

## Renforcer la collaboration en matière de sécurité de l'information à Santé Ontario (mis à jour)

Les équipes de cybersécurité de Santé Ontario continuent de renforcer leur approche collaborative grâce à l'évolution de l'Échange de connaissances en sécurité de l'information **(ECSI)**. Lancé comme une amélioration stratégique du précédent Comité directeur de la sécurité de l'information (**CDSI**), l'ECSI a été élaborée pour mieux répondre aux besoins évolutifs des équipes interfonctionnelles en favorisant une approche plus proactive et intégrée de la sécurité de l'information dans l'organisation.

Les réunions de l'ECSI, tenues tous les deux mois, rassemblent des partenaires des domaines de la cybersécurité, de la protection de la vie privée, des produits, de la conformité, de l'architecture et des opérations. Les séances comprennent des présentations en vedette, des mises à jour clés et, à l'avenir, des conférenciers invités externes qui fournissent des renseignements sur les tendances, les risques et les pratiques exemplaires. Les sujets comprenaient les menaces de cybersécurité, la conformité réglementaire, la protection des données, la sécurité infonuagique et du réseau, ainsi que les stratégies d'intervention en cas d'incident.

Chaque séance est conçue pour aller au-delà des mises à jour régulières, en utilisant des présentations en vedette pour mettre en lumière des sujets opportuns et pertinents comme les tendances en matière de cybersécurité, les rapports du CIPVP et la conformité réglementaire, la protection des données, les stratégies d'intervention en cas d'incident, la sécurité infonuagique et du réseau, et la gestion des accès. Les réunions comprennent des formats divers, allant des présentations, des discussions en groupe aux études de cas et aux séances de questions-réponses, afin d'optimiser la mobilisation et d'encourager un dialogue ouvert entre les disciplines.

L'ECSI promeut l'échange ouvert de connaissances, appuie l'harmonisation entre les équipes techniques et opérationnelles, et favoriser une solide culture de sensibilisation à la cybersécurité, de responsabilité et de résilience face à l'évolution des cyberrisques.

## Amplifier la formation et la sensibilisation à la sécurité (mis à jour)

Santé Ontario a acheté la plateforme de sensibilisation et de formation en cybersécurité de l'Autorité canadienne pour les enregistrements Internet (**ACEI**) pour appuyer la formation et la sensibilisation régulières et annuelles à la cybersécurité fondées sur les rôles, les simulations d'hameçonnage adaptatives, et éclairer les plans visant à améliorer le profil de cyberrisque de Santé Ontario. Santé Ontario a adopté la solution de l'ACEI pour améliorer son infrastructure de cybersécurité et protéger ses actifs et opérations numériques. Cette solution permet à Santé Ontario de renforcer la résilience de son personnel pour protéger les renseignements sensibles et atténuer les cybermenaces.

Au cours de l'exercice financier 2024-2025, Santé Ontario a réussi à achever plusieurs initiatives critiques dans le cadre de la solution de l'ACEI :

- **Déploiement de protocoles de sécurité avancés :** Santé Ontario a intégré des protocoles de sécurité de pointe, y compris une protection contre les menaces fondée sur le DNS et des mécanismes

automatiques d'intervention en cas d'incidents; ce qui a considérablement réduit le risque de cyberattaques.

- **Programmes de formation et de sensibilisation :** Des séances de formation exhaustives ont été organisées pour sensibiliser le personnel sur les pratiques exemplaire en matière de cybersécurité et sur l'utilisation de l'outil de l'ACEI, renforçant ainsi la position de sécurité globale de l'organisation.
- **Audits de sécurité réguliers :** Des audits de sécurité réguliers ont été effectués pour trouver les vulnérabilités et garantir la conformité aux normes de cybersécurité nationales et internationales.
- **Collaboration avec l'ACEI :** La collaboration continue avec les experts de l'ACEI a facilité le déploiement rapide des mises à jour et l'optimisation des mesures de sécurité adaptées aux besoins précis de Santé Ontario.
- **Campagnes de hameçonnage :** Santé Ontario réalise des campagnes mensuelles de simulation de hameçonnage pour évaluer la sensibilisation du personnel. Au cours de la dernière année, nous avons réduit les incidents de hameçonnage grâce à des programmes de formation et à des mesures de sécurité renforcées, y compris des systèmes de détection des menaces avancés.

## De la sensibilisation à l'action : Augmenter la sensibilisation et la littératie en matière de sécurité

Pour suivre le rythme et mieux se défendre contre divers incidents et cyberattaques, il fallait un nouveau moyen amélioré de sensibiliser les membres de l'équipe de Santé Ontario.

Le Bureau de la sécurité de l'information (**BSI**) avec le soutien des équipes du Centre de cybersécurité et de la Défense en matière de cybersécurité a mis en œuvre les programmes suivants pour mettre en place un environnement de culture de sécurité plus solide :

**Communication interne :**

- Publication d'articles de sécurité régulière et opportune sur Pulse de Santé Ontario (par exemple, page intranet interne) pour renforcer les messages clés.
- Organisation de séances régulières de dîner-causerie avec les membres de l'équipe de Santé Ontario sur des sujets pertinents et des événements en temps réel pour stimuler les connaissances.

**Boucle de rétroaction dynamique :**

- Surveillance de nouvelles techniques d'attaque en collaborant avec un fournisseur de services de sécurité gérés (**FSSG**) et en les intégrant directement dans des campagnes de sensibilisation dans les jours suivant leur observation.
- Des tactiques et techniques supplémentaires utilisées par les cyberattaquants sont facilitées par le cycle de formation pour accroître les connaissances des membres de l'équipe.

**Améliorer la formation et la sensibilisation annuelles à la sécurité**

- Revitalisation du module de formation annuel pour intégrer de nouveaux domaines, technologies, et sujets

pertinents afin d'offrir un apprentissage amélioré.
- Réalisation d'un déploiement de ludification et d'une compétition de défi de sécurité dans le cadre d'une campagne de sensibilisation à la cybersécurité plus vaste.
- Tenue d'une discussion informelle avec des dirigeants en sécurité et des séances sur les parcours en cybersécurité pour sensibiliser les membres de l'équipe sur les parcours professionnels en cybersécurité.

**Participer à l'apprentissage et au perfectionnement**

- Réaliser une analyse fondée sur les besoins en partenariat avec l'équipe d'apprentissage et de perfectionnement de Santé Ontario pour déterminer les domaines du programme actuel de sensibilisation à la cybersécurité qui pourraient être améliorés et renforcés.

**Mois de la sensibilisation à la cybersécurité**

Au cours du mois d'octobre, des séances interactives et des articles intéressants sur l'intranet ont joué un rôle central dans la promotion de la mobilisation dans l'ensemble de la communauté. Le mois a également été enrichi par des stratégies de mobilisation créatives, comme les messages d'écran de verrouillage thématiques et des arrière-plans de réunion Microsoft Teams conçus pour garder la cybersécurité dans l'esprit de nos membres d'équipe. Grâce à ces approches éducatives et expérientielles variées, le programme a pris des mesures pour favoriser une culture organisationnelle proactive et bien éclairée, capable de gérer les défis continus en matière de cybersécurité.

## Moderniser les identités numériques, améliorer la gouvernance des données et renforcer la gestion des menaces et de la réponse connexe (nouveau)

**Surveillance et intervention du Centre des opérations de sécurité hybride**

Au cours de l'exercice financier 2024-2025, le Centre des opérations de sécurité (**COS**) hybride 24 heures sur 24, 7 jours sur 7, de Santé Ontario a mené d'importantes activités de surveillance et d'intervention. Cette fonction critique a permis d'assurer la détection et l'atténuation des menaces en temps réel, maintenant l'intégrité et la sécurité de nos systèmes dans toute l'organisation. Ces efforts ont été essentiels pour renforcer nos mécanismes de cyberdéfense et réduire l'incidence des cybermenaces possibles. Cette initiative tient compte de notre engagement à nous adapter à l'évolution rapide du paysage des cybermenaces et à maintenir un niveau élevé de sécurité et de conformité.

**Gestion des vulnérabilités axée sur le produit**

En réponse à l'évolution du paysage des menaces, Santé Ontario a mis en œuvre une nouvelle stratégie axée sur les produits visant à mieux prioriser et atténuer les vulnérabilités. Cette approche élargit la portée de la gestion des vulnérabilités pour inclure les vulnérabilités des applications et des configurations, améliorant ainsi la responsabilité, la visibilité et les efforts d'atténuation pour chaque groupe de produits. Cette stratégie a permis une gestion des vulnérabilités plus ciblée et efficace, garantissant que des contrôles compensatoires sont mis en œuvre, renforçant ainsi la position de sécurité globale de nos produits et appuyant les objectifs de l'organisation.

**Protection pour les systèmes d'exploitation (SE) inadmissibles à la PEPT**

Au cours de l'exercice financier 2024-2025, le COS a relevé le défi de protéger les systèmes

d'exploitation (**SE**) qui sont inadmissibles pour les solutions avant-gardistes de protection évolutive des points de terminaison (**PEPT**). En effectuant des recherches approfondies, une étude de validation (**EV**) et des achats, Santé Ontario a trouvé une solution qui offre une protection de sécurité comparable à celle de la PEPT pour ces systèmes. Le projet a commencé avec la mise en œuvre en cours d'un ensemble ciblé de systèmes, garantissant que ces systèmes sont protégés contre les menaces possibles à la sécurité. Cette approche proactive atténue les risques associés à ces systèmes et renforce la protection de nos actifs numériques, en tenant compte de notre approche novatrice en matière de cybersécurité.

**Programme de gestion des identités et des accès d'entreprise**

Le Programme de gestion des identités et des accès d'entreprise (**GIAE**) est une initiative stratégique conçue pour moderniser et sécuriser la gestion des identités numériques et des accès de Santé Ontario. Au cœur de la GIAE se trouve un cadre d'identité centralisé et évolutif qui garantit que les particuliers reçoivent le bon accès aux bonnes ressources et au bon moment – et pour les bonnes raisons. Le programme tire parti de technologies avancées, y compris l'authentification multifacteur (**AMF**), l'authentification unique, et le contrôle d'accès basé sur les rôles (**RBAC**), pour appliquer des contrôles de sécurité solides. Ces capacités protègent les données sensibles, réduisent l'exposition aux menaces internes, et appuient la conformité aux normes réglementaires.

En 2024-2025, le programme a atteint plusieurs jalons importants :

- Achat et mise en œuvre réussis de la plateforme Saviynt, intégrant les capacités de Gouvernance et d'Administration des Identités (**IGA**) et de Gestion des accès privilégiés dans le nuage (**GAPN**)
- Configurations fondamentales achevées, y compris les intégrations avec Cloud AD, Entra ID et Workday de Santé Ontario
- Rapprochement des processus opérationnels entre les anciens répertoires et ceux fondés sur le nuage, et migration de la solution CyberArk PAM sur place vers la plateforme infonuagique de logiciel-service (**SaaS**) privilégiée CyberArk, marquant un changement majeur vers des services d'identité modernes, évolutifs et alimentés par l'IA.

À la suite de ces changements, le programme a apporté une importante valeur opérationnelle. En particulier, le programme a considérablement réduit l'utilisation sur place, éliminé les temps d'arrêt perturbateurs pour les cycles de mise à jour, et réduit les heures supplémentaires. Le passage au nuage a également permis d'optimiser l'affectation des ressources, de réduire le coût total de possession, et a permis à l'organisation de mettre hors service les anciens outils.

**Programme de gestion des certificats et des clés « Zero Touch »**

Le programme de gestion des certificats et des clés « Zero Touch » (**PGCCZT**) est une approche modernisée de la gestion des certificats numériques et des clés de chiffrement avec un minimum d'intervention humaine. Ce programme vise à améliorer la sécurité et l'efficacité des opérations cryptographiques dans l'organisation. Le PGCCZT cherche à automatiser la gestion du cycle de vie des certificats et des clés, de l'émission et du renouvellement à la révocation et au stockage, en tirant parti des technologies modernes comme la chaîne de blocs et l'intelligence artificielle.

En 2024-2025, le PGCCZT a abordé la méfiance mondiale envers les certificats racines d'Entrust en utilisant un processus semi-automatisé pour remplacer les anciens certificats par de nouveaux certificats achetés. Dans le cadre de cet effort de modernisation,

l'équipe a élaboré et lancé un appel d'offres pour l'initiative du PGCCZT plus vaste, jetant les bases d'une plateforme de gestion du cycle de vie des certificats entièrement automatisée et alimentée par l'IA. En parallèle, l'équipe de l'infrastructure à clé publique (**ICP**) a réussi à émettre ou à renouveler plus de 5 000 certificats (publics et privés), renforçant la confiance numérique et la résilience opérationnelle dans toute l'entreprise.

**Programme de gestion des interventions en cas d'incidents de cybersécurité**

Le Programme de gestion des interventions en cas d'incident de cybersécurité (**PGICIC**) est consacré à la préparation, à l'intervention et à la reprise à la suite des incidents de cybersécurité. Ce programme joue un rôle crucial dans le maintien de la résilience et de l'intégrité des opérations numériques de l'organisation.

Dans une époque où les cybermenaces sont de plus en plus sophistiquées et omniprésentes, la capacité à gérer rapidement et efficacement les incidents est primordiale. Le PGICIC englobe un ensemble complet de procédures et d'outils conçus pour détecter, analyser et atténuer les répercussions des incidents de cybersécurité. Cela comprend l'établissement d'une équipe d'intervention en cas d'incident, le déploiement de systèmes de surveillance avancés, et la création de plans détaillés d'intervention en cas d'incident.

Le PGICIC a considérablement amélioré la capacité de l'organisation à répondre aux incidents cybernétiques et à s'en remettre, réduisant ainsi au minimum les temps d'arrêt et atténuant les dommages. Le programme a favorisé une culture de vigilance et de préparation, garantissant que les employés sont bien équipés pour reconnaître et signaler les menaces possibles. Grâce à des formations régulières et à des simulations, l'organisation a développé une capacité solide d'intervention en cas d'incident qui peut rapidement contrer et contenir les menaces.

**Tester Microsoft Purview**

L'outil Microsoft Purview est une solution complète conçue pour améliorer la gouvernance des données et la protection de l'information chez Santé Ontario. Cet outil a été introduit pour répondre au besoin croissant de mesures solides de sécurité des données à l'ère de l'intelligence artificielle (**IA**). Microsoft Purview offre une couverture intégrée pour gérer et protéger les données sensibles tout au long de leur cycle de vie, où qu'elles se trouvent. L'outil comprend des fonctionnalités comme la prévention de la perte de données, la gestion de la position de sécurité des données, les barrières d'information, la protection de l'information, la gestion des risques internes, et la gestion des accès privilégiés.

La mise en œuvre de Microsoft Purview est conforme aux Normes de classification et de gestion de l'information de Santé Ontario, garantissant que les données sont correctement étiquetées et protégées. Le déploiement de Microsoft Purview a commencé par une validation de principe impliquant environ 70 personnes. Cette phase initiale a introduit des étiquettes de données qui respectent les normes de Santé Ontario, et a démontré l'efficacité de l'outil pour protéger les renseignements sensibles. Le projet est dirigé par l'équipe d'ingénierie de la plateforme de sécurité.

Les avantages de Microsoft Purview comprennent une visibilité améliorée sur les données dans toute l'organisation, une sécurité des données renforcée, et une conformité aux exigences réglementaires.

## Sécuriser l’accès à distance au moyen de Netskope (nouveau)

La solution Netskope est un outil d’accès à distance conçu pour améliorer l’accès sécurisé à Internet et privé pour Santé Ontario. Il a été sélectionné comme l’outil principal d’entreprise de Secure Service Edge (**SSE**) pour remplacer Zscaler, qui avait été utilisé dans une validation de principe avec environ 3 000 utilisateurs, car il offrait une solution plus rentable et intégrée avec des fonctionnalités de sécurité complètes. Netskope offre un accès Internet sécurisé et privé, s’intègre parfaitement aux outils de sécurité existants, et constitue une étape importante dans le parcours de l’organisation vers un modèle de sécurité à vérification systématique.

Le déploiement progressif de Netskope a commencé à la mi-février et a été achevé le 31 mars 2025. Ce déploiement consistait en une installation à distance sur les appareils des utilisateurs; ce qui garantit une perturbation minimale de leur flux de travail.

# Initiatives clés de programmes et de projets

Le Bureau de la protection de la vie privée, en collaboration avec le Bureau de la sécurité de l'information et d'autres partenaires opérationnels, est chargé de protéger la vie privée des particuliers ainsi que la confidentialité, la sécurité et la disponibilité des actifs de données, et de permettre à l'Agence d'utiliser les données et d'autres actifs pour appuyer ses programmes et projets. Un exemple de ces programmes et initiatives est énuméré ci-dessous.

## Visualiseur provincial pour les patients – Permettre aux particuliers d'accéder à leurs dossiers de RPS conservés dans le DSE (mis à jour)

Dans le passé, les particuliers ont pu accéder directement à certains de leurs dossiers de santé au moyen des portails pour patients (par exemple, MyChart, myUHN) qui ne sont ni développés ni tenus à jour par Santé Ontario.

Le DSE provincial est développé et tenu à jour par Santé Ontario à titre d'organisation prescrite. Pour favoriser de meilleurs soins, il est essentiel de fournir aux particuliers un accès numérique à leurs RPS détenus dans le DSE provincial. Santé Ontario développe un Visualiseur provincial pour les patients qui permettrait à Santé Ontario de fournir aux particuliers un accès direct et numérique à leurs dossiers conservés dans le DSE. Même si les modifications législatives et réglementaires qui permettraient à Santé Ontario de mettre le visualiseur à disposition ne soient pas encore en vigueur, on s'attend à ce que Santé Ontario, en tant qu'organisation prescrite, agisse comme si elle avait la garde ou le contrôle des dossiers afin de permettre à un particulier d'accéder aux dossiers du Système d'information des laboratoires de l'Ontario (**SILO**) et du Répertoire numérique des médicaments (**RNM**) dans un premier temps, puis aux dossiers du Service commun d'imagerie diagnostique (**SCID**) et au Répertoire des données cliniques sur les soins actifs et communautaires (**RDCsac**).

Santé Ontario continue de travailler avec le ministère de la Santé pour s'assurer que ce programme appuiera au mieux les particuliers dans l'accès numérique à leurs dossiers détenus dans le DSE, tout en protégeant simultanément ces dossiers très sensibles de RPS. Au cours de la dernière année, le ministère de la Santé et Santé Ontario ont continué à collaborer sur un cadre qui peut appuyer Santé Ontario dans son parcours pour répondre aux exigences en matière de confidentialité, de sécurité, de technologie, de procédures et de programmes afin de permettre le lancement de ce programme. Ce programme est également harmonisé avec le pilier « Accès numérique pour les patients » de la stratégie Priorité au numérique pour la santé du Ministère.

## Identité numérique de santé – Permettre aux particuliers de valider et de vérifier leur identité pour se connecter aux outils de santé numériques (mis à jour)

Lorsque des particuliers cherchent à accéder à des RPS, ils doivent vérifier leur identité afin de s'assurer que ces renseignements très sensibles ne sont partagés que lorsque cela est approprié.

Santé Ontario met en œuvre un programme provincial d'identité numérique de santé (Accès des patients), tirant parti des composants d'une solution existante, intégrée aux services d'entreprise

gouvernementaux communs du ministère des Services gouvernementaux et des Services aux consommateurs (**MSGSC**), en vue de fournir aux Ontariens une identité numérique fiable et sécurisée pouvant servir à accéder aux services et renseignements numériques de santé.

Voici les principaux objectifs :

- Mettre en place d'une solution de gestion de l'identité et de l'accès des patients sécurisée, fiable et provinciale.
- Intégrer cette solution avec le Visualiseur provincial pour les patients comme un service de santé numérique prioritaire.
- Fournir un moyen sécurisé, fondé sur des normes et efficace pour intégrer des services de santé numériques supplémentaires à l'avenir, par exemple, Santé811, Correspondance numérique.

Les membres de l'équipe de protection de la vie privée et des services juridiques de Santé Ontario ont fourni des recommandations détaillées au Ministère pour éclairer un cadre juridique qui donnerait à Santé Ontario un nouveau rôle et un nouveau pouvoir légal en vertu de la LPRPS pour superviser ce programme d'identité numérique pour la province.

Les organismes de réglementation de la vie privée fédéraux, provinciaux et territoriaux du Canada (y compris l'Ontario) ont émis une résolution conjointe appelant les gouvernements et les intervenants à veiller à ce que les droits à la vie privée et à la transparence soient pleinement respectés tout au long de la conception, de l'exploitation et de l'évolution d'un écosystème d'identité numérique au Canada. Les membres de l'équipe juridique et de protection de la vie privée de Santé Ontario travaillent avec les partenaires opérationnels de Santé Ontario, le Ministère et le MSGSC pour s'assurer que le programme est conforme à cette résolution, et consulteront le CIPVP à cet égard.

## Accroître l'accès des fournisseurs aux dossiers médicaux des patients : Visualiseur clinique provincial (VCP) et Bases de données cliniques du DSE (mis à jour)

Santé Ontario finance et appuie trois visualiseurs cliniques en Ontario qui offrent des fonctionnalités chevauchantes aux cliniciens, mais qui desservent diverses régions et continuent de subir des mises à jour de manière autonome, principalement orientées par les feuilles de route des produits et la rétroaction des utilisateurs finaux. Santé Ontario participe à un programme pour regrouper ces trois visualiseurs cliniques en un visualiseur clinique provincial normalisé qui permet aux fournisseurs d'accéder aux renseignements de santé disponibles dans le DSE. Ce programme consiste non seulement à établir le visualiseur unique, VCP, à intégrer les référentiels et registres de DSE existants, à préparer le lancement technique, mais aussi à des activités de gestion du changement, y compris la planification et l'élaboration de stratégies pour l'intégration, la formation, la communication et la préparation des projets pilotes. De plus, et en lien avec « Accès individuel au DSE » ci-dessus, pour tenir compte des exigences d'accès individuel, la portée de la Stratégie de consolidation des visualiseurs a été élargie pour inclure également un visualiseur provincial pour les patients (**VPP**) en vue de fournir aux particuliers un moyen numérique d'accéder à leurs renseignements du DSE.

Les équipes de confidentialité et de sécurité de l'information ont achevé les travaux préliminaires sur les exigences opérationnelles pour le VCP.

En même temps, le Répertoire des données cliniques sur les soins actifs et communautaires (**RDCsac**) utilise une technologie vieillissante et approche de la fin de sa vie utile. Cela a entraîné des lacunes en matière de fonctionnalité, de technologie et de données pour les cliniciens. Santé Ontario remplacera le RDCsac existant par un nouveau Répertoire des données cliniques (**RDC**) sur la nouvelle plateforme

commune des Bases de données cliniques (**BDC**), y compris la configuration du répertoire, la configuration de la terminologie, la migration des données, la configuration des entrées et sorties de données, et la migration des données du RDCsac vers un nouveau RDC. D'autres actifs de données cliniques de Santé Ontario, y compris ceux qui font partie du DSE, tireront également parti du RDC, et ce projet sera réalisé sur plusieurs phases et années.

Le Bureau de la protection de la vie privée fournit des exigences en matière de protection de la vie privée, des garanties, des conseils, des évaluations des risques et des travaux influents pour favoriser tous les aspects de cette initiative complexe de remplacement, de développement et de migration.

Le Bureau de la sécurité de l'information a été mobilisé et appuie l'initiative, de la planification à l'exécution. Des examens des architectures de sécurité, des évaluations des menaces et des risques ainsi que des tests de pénétration ont été recommandés et seront réalisés pour cerner les menaces possibles et les risques, et proposer des mesures d'atténuation.

## Collaboration pour mettre en œuvre des programmes de dépistage du cancer améliorés et élargis (nouveau)

En octobre 2024, Santé Ontario a lancé une expansion du Programme de dépistage du cancer du sein de l'Ontario qui a réduit l'âge de début de 50 à 40 ans. Les travaux d'expansion ont exigé la collaboration entre le Bureau de la protection de la vie privée de Santé Ontario, le Portefeuille des soins primaires et communautaires, et l'Excellence numérique en santé. Une évaluation des facteurs relatifs à la vie privée a été réalisée pour permettre des changements dans les systèmes de collecte de données, mettre à jour les produits de rapport d'analyse, et lancer des améliorations au site Web de déclaration des temps d'attente de l'Ontario, permettant aux personnes en Ontario qui sont admissibles pour le dépistage de trouver les sites de dépistage qui répondent le mieux à leurs besoins (comme les exigences linguistiques ou d'accessibilité) et fournissant des renseignements sur les temps d'attente aux sites de dépistage.

En mars 2025, Santé Ontario a lancé le dépistage du virus du papillome humain (VPH) comme le nouveau test amélioré pour le Programme ontarien de dépistage du cancer du col de l'utérus, qui remplace le test Pap comme test de dépistage principal du cancer du col de l'utérus en Ontario. Le dépistage du VPH est plus sensible et exige des tests moins fréquents. Cette transition exigeait un soutien en matière de confidentialité pour intégrer des partenaires de laboratoire, lancer de nouveaux systèmes de collecte de données et parcours de données, et favoriser une nouvelle logique opérationnelle pour les campagnes de correspondance. Des évaluations des facteurs relatifs à la vie privée ont été réalisées pour appuyer cette initiative multidimensionnelle, ainsi que des modifications réglementaires avec le ministère de la Santé. Un soutien complexe en matière de protection de la vie privée était également nécessaire pour appuyer les nouveaux accords, annuler les anciens accords et étudier les autorités législatives de Santé Ontario pour favoriser la production de rapports analytiques sur les nouveaux tests.

## Intelligence artificielle et protection de la vie privée (nouveau)

Au mois d'avril, l'équipe d'apprentissage et de perfectionnement de Santé Ontario, en collaboration avec les équipes de cybersécurité, de sécurité de l'information, de protection de la vie privée, des services juridiques et des produits d'entreprise, a organisé la séance *Démystifier l'IA : Présentation de l'IA et de son utilisation chez Santé Ontario* en avril.

Un aperçu de l'intelligence artificielle (**IA**) a été présenté, tout en introduisant les Lignes directrices sur l'intelligence artificielle générative de Santé Ontario. La séance visait à mettre en exergue des

sujets clés comme le nouveau paysage réglementaire, les risques juridiques et les cadres juridiques, tout en soulignant l'utilisation responsable de l'IA et les principes de confidentialité qui se chevauchent pour des technologies d'IA générative responsables, fiables et respectueuses de la vie privée.

L'équipe de confidentialité participe activement au Comité interne sur l'IA de Santé Ontario, qui a pour mandat de mettre en œuvre la Directive sur l'utilisation responsable de l'intelligence artificielle. Cette directive provinciale s'applique à tous les ministères et agences de l'Ontario, et s'applique à tous les systèmes qui utilisent l'IA (non définie) dans le cadre du développement, de la prestation ou de la prise de décision concernant une politique, un programme ou un service; et exige la divulgation de l'utilisation de l'IA et l'établissement d'un cadre de gestion des risques.

## Expansion de l'ensemble de données provinciales sur la santé mentale et les dépendances (nouveau)

Le Centre d'excellence pour la santé mentale et la lutte contre les dépendances (**CESMLD**) de Santé Ontario appuie le développement d'un système complet et connecté de santé mentale et de lutte contre les dépendances dans toute la province. Au cours de la dernière année, l'équipe de confidentialité a appuyé le CESMLD dans l'expansion de la collecte de données pour réaliser les trois piliers, auprès de 71 nouveaux fournisseurs de services de santé contribuant à l'Ensemble de données provincial (**EDP**).

L'équipe de confidentialité a réalisé des évaluations des facteurs relatifs à la vie privée liées à de nouveaux ensembles de données propres à des programmes cliniques pour des programmes prioritaires, y compris la dépression et les troubles liés à l'anxiété, la schizophrénie et la psychose, les troubles alimentaires et les troubles liés à l'utilisation de substances. En coordination avec l'équipe de projet, l'équipe de sécurité a établi des normes pour l'évaluation de la sécurité avant l'intégration de nouveaux sites pour la soumission de données sur la SMD.

## Expansion de l'application eRéclamations (nouveau)

Une version multilocataire a été déployée avec succès dans l'application eRéclamations et est maintenant en production. Les équipes de la confidentialité et de la sécurité étaient des acteurs clés, fournissant à l'équipe de projet des consultations continues en matière de protection de la vie privée et de sécurité. Les évaluations nécessaires en matière de protection de la vie privée et de sécurité ont été effectuées en temps opportun, garantissant une livraison sans heurts. La version 4.0 de l'application eRéclamations établit les bases pour en faire une plateforme qui prendra en charge plusieurs programmes (appelés locataires dans l'application), ce qui constitue l'objet du projet d'expansion de l'application eRéclamations.
L'exploitation de cette plateforme pour d'autres programmes de Santé Ontario (locataires), où la détermination et le remboursement sont fondamentaux, permettra d'intégrer de nouveaux programmes dans cette plateforme architecturale mise à jour. En résumé, cette version comprend des mises à jour comme les nouveaux écrans d'interface utilisateur, un contrôle d'accès amélioré, des mises à jour de diverses tables et fonctions, ainsi qu'un délai d'expiration de session mis à jour.

## Santé 811 (mis à jour)

Santé 811 agit comme une « porte d'entrée numérique » unique vers le système de santé de l'Ontario, offrant un emplacement où tous les Ontariens peuvent accéder à des renseignements sur la santé, des conseils et un tri initial pour se connecter aux services de santé financés par l'État partout dans la province et recevoir des conseils tout au long de leur parcours de soins de santé. Le Ministère a attribué le contrat à Santé Ontario, qui supervise maintenant la mise en œuvre, la gestion continue et les opérations ou le rendement de ce service. À titre de mandataire de la LPRPS du ministère de la Santé, Santé Ontario, par l'intermédiaire de ses équipes de confidentialité et de sécurité de l'information, a été responsable de l'examen et de l'approbation des évaluations des facteurs relatifs à la vie privée et des évaluations des risques et des menaces du fournisseur Santé811, des plans d'atténuation des risques, des politiques et procédures, ainsi que des pratiques de gestion des incidents afin de garantir que Santé811 dispose de contrôles de protection de la vie privée et de sécurité conformes aux exigences du ministère, de Santé Ontario, et à l'accord-cadre.

Le travail se poursuit sur un cadre incitatif fondé sur la valeur et visant à réduire les coûts, et à démontrer la valeur créée et les résultats générés par Santé811. Les membres des équipes de confidentialité, des services juridiques et autres affaires de Santé811 et de Santé Ontario travaillent avec le ministère de la Santé sur des processus et des évaluations des risques qui permettraient la collecte, l'utilisation et la divulgation des actifs de données existants et nouveaux, ainsi qu'un ensemble solide d'accords.

De plus, dans le cadre de l'exploitation du service et de la gestion continue, les équipes de confidentialité et de sécurité de Santé Ontario ont informé et appuyé plusieurs examens de documents sur les exigences opérationnelles préalables et sur les exigences opérationnelles, y compris des améliorations d'accès épisodique aux soins, la prise de rendez-vous en ligne, la recherche unique et l'optimisation de la recherche, ainsi que le Programme ontarien de dépistage du cancer du sein pour ne citer que quelques exemples.

## Principaux projets (mis à jour)

L'équipe de la confidentialité a été un partenaire clé dans la planification et le travail réalisés avec les sept Principaux projets (**PP**) qui ont été lancés au cours de l'exercice financier 2024-2025. Santé Ontario, en tant que fournisseur de réseau d'information sur la santé (**FRIS**), devait apporter des modifications et des améliorations au système CHRIS pour permettre au système de faciliter l'exécution du programme des PP, et devait réaliser sept évaluations des facteurs relatifs à la vie privée (**EFVP**). Les EFVP étaient axées sur les Partenaires principaux du système de santé (**PPSS**), qui ont été désignés comme étant le locataire CHRIS du Projet principal individuel. Les EFVP se sont concentrées sur les PPSS et leur interaction avec le système CHRIS dans le cadre des Principaux projets. Santé Ontario a travaillé en étroite collaboration avec les Équipes de Santé Ontario (**ESO**) participantes (et leurs PPSS), de Santé à domicile Ontario et diverses équipes de Santé Ontario pour réaliser ces sept EFVP complètes. Les résultats des EFVP étaient essentiels à l'établissement de politiques, de processus et d'accords pour appuyer la mise en œuvre des Principaux projets, y compris l'intégration des PPSS dans le système CHRIS. Santé Ontario a communiqué les résultats de ces EFVP aux PP participants et à Santé à domicile Ontario. Santé Ontario a atténué tous ses risques en matière de protection de la vie privée. Les PP participants travaillent encore à mettre au point certaines des stratégies d'atténuation des risques qui ont été indiquées dans les EFVP. Les PP ont été lancés en 2024-2025 sans le système CHRIS, avec des plans pour l'intégrer au début du deuxième trimestre de 2025-2026. L'équipe de la confidentialité continuera de travailler avec les partenaires et programmes

de soutien pour appuyer l'intégration du système CHRIS conformément aux constatations et recommandations des EFVP.

L'équipe de sécurité a achevé l'évaluation des risques pour les Principaux projets ainsi que pour 20 sites de partenaires afin de s'assurer que les sites disposent d'une mise en œuvre suffisante des contrôles de sécurité avant l'intégration.

## Services CHRIS et l'avenir des soins à domicile (mis à jour)

Le Bureau de la protection de la vie privée a travaillé en étroite collaboration avec l'équipe opérationnelle du produit CHRIS pour se préparer aux futurs modèles de prestation de soins à domicile grâce au développement d'un centre régional, s'éloignant du modèle actuel d'établissement de locataires CHRIS. Une EFVP a été réalisée pour évaluer l'incidence de l'utilisation du système CHRIS par les ESO, où elles sont composées de plusieurs dépositaires de renseignements sur la santé. Les constatations et recommandations des EFVP ont servi à éclairer le travail sur les Principaux projets et l'élaboration d'un nouvel accord-cadre avec les FRIS pour le système CHRIS et les systèmes et lignes directrices connexes, ainsi que les lignes directrices sur la protection de la vie privée pour les locataires de CHRIS. Le déploiement d'un modèle régional de CHRIS conformément aux recommandations de l'EFVP garantit que le système CHRIS est en mesure d'appuyer les efforts provinciaux en vue de la modernisation des soins à domicile.

## Fournitures d'équipement médical (FEM) (mis à jour)

Le ministère de la Santé de l'Ontario (**MSO**) a désigné le système CHRIS dans son Manuel de la santé numérique comme un actif numérique. Même si Santé Ontario ne fournit pas directement de soins aux patients de l'Ontario, l'organisation propose des programmes et des outils numériques qui permettent aux organisations de soins de santé de coordonner la prestation des soins aux patients dans plusieurs régions de l'Ontario. Par conséquent, afin de moderniser la chaîne d'approvisionnement du secteur public, Santé à domicile Ontario a conclu un certain nombre de contrats avec des fournisseurs pour des fournitures d'équipement médical (**FEM**) qui exigeaient une intégration avec le système CHRIS pour la prestation de services.

Santé Ontario a réalisé 12 EFVP pour appuyer ce travail – une EFVP évaluant les améliorations globales apportées au système CHRIS pour appuyer ce travail, et 11 EFVP pour examiner diverses intégrations de fournisseurs au système CHRIS. L'intégration du projet auprès des fournisseurs a abouti à un transfert automatisé des bons de commande liés aux FEM vers les fournisseurs sous contrat et à une notification des fournisseurs à Santé à domicile Ontario concernant l'exécution des bons de commande. Santé Ontario a réussi à achever ces 12 EFVP pour respecter les délais du projet, et a collaboré avec divers groupes en interne ainsi qu'avec Santé à domicile Ontario et des fournisseurs pour atténuer les risques trouvés au cours du processus.

L'équipe de sécurité du BSI a participé au processus d'approvisionnement en indiquant les exigences de sécurité et en évaluant les réponses. Après la sélection, certains des partenaires de FEM ont fourni des rapports SOC2 de type II et d'autres ont effectué une auto-évaluation de sécurité fondée sur le NIST. L'équipe de sécurité du BSI a examiné les documents et s'est assurée que les contrôles de sécurité applicables requis sont mis en œuvre dans leur environnement.

## Système d'attribution et de greffe d'organes (SAGO), Intégrations (mis à jour)

Le Système d'attribution et de greffes d'organes (**SAGO**) a été lancé en 2022 par Santé Ontario. Le SAGO a remplacé l'ancien système « TOTAL », qui était utilisé par le Réseau Trillium pour le don de vie pour gérer l'attribution et la greffe d'organes en Ontario.

Les utilisateurs externes du SAGO, comme le personnel des hôpitaux de greffe et les laboratoires d'antigène leucocytaire humain (**ALH**), copient manuellement les données des patients de leurs systèmes (c'est-à-dire les DME et les LIS) dans le SAGO. Pour améliorer la qualité des soins aux patients dans le parcours de greffe, Santé Ontario a collaboré avec le fournisseur du SAGO et les laboratoires d'ALH pour intégrer le SAGO avec les systèmes de DME des hôpitaux de greffe de l'Ontario, qui comprennent sept sites, et les systèmes de laboratoire d'ALH, qui comprennent cinq sites. L'intégration facilitera un transfert unidirectionnel des données pertinentes des patients des hôpitaux de greffes et des laboratoires d'ALH vers les champs de données du SAGO existants. L'intégration vise à remplacer la saisie manuelle actuelle des données par le personnel des hôpitaux de greffe et des laboratoires d'ALH dans le SAGO, améliorant ainsi la qualité et l'intégrité de la solution.

Voici les résultats escomptés de l'intégration :

- Réduction du risque clinique en éliminant ou en réduisant la documentation en double et la transcription des documents.
- Amélioration de la rapidité d'accès aux données des patients entre les systèmes.
- Des flux de travail plus efficaces dans la réduction de la saisie de données en double et la réduction des redondances au minimum.
- Amélioration des résultats des patients grâce à la collecte de renseignements précis sur les patients.

Pour appuyer ce changement, le Bureau de la protection de la vie privée a dirigé l'élaboration d'une EFVP afin d'évaluer les risques pour la vie privée et de proposer des recommandations pour atténuer ces risques. L'EFVP et le travail connexe ont été essentiels au lancement de la première intégration en tant que test. Le Bureau de la protection de la vie privée a travaillé en étroite collaboration avec le service juridique pour élaborer un accord-cadre et a fourni une expertise en matière de protection de la vie privée aux programmes participants alors qu'ils prévoient de s'intégrer au SAGO. Le Bureau de la sécurité de l'information a réalisé une évaluation des menaces et des risques, élaboré un plan de traitement des risques, et participé à l'atténuation des risques trouvés.

En 2025-2026, le RTDV entreprendra l'expansion de l'intégration pour un système et des processus plus sûrs afin d'appuyer la greffe conformément aux pratiques de confidentialité qui ont été mises en action par l'EFVP.

## Échange de renseignements numériques sur la santé (ERNS) (mis à jour)

Il est essentiel de permettre l'échange de renseignements électroniques entre les dépositaires de renseignements sur la santé en vue d'offrir aux Ontariens des soins de santé efficaces et intégrés. La LPRPS a été modifiée le 1er janvier 2021 pour faciliter l'interopérabilité entre les actifs de santé numériques. Dans le cadre de ces modifications sur l'ERNS, Santé Ontario est chargé de définir les exigences d'interopérabilité (y compris la confidentialité et la sécurité de l'information) pour les systèmes électroniques, de déterminer les spécifications, et de travailler activement avec les fournisseurs et les dépositaires des renseignements sur la santé par le biais d'un programme pour surveiller et garantir la conformité. Santé Ontario a élaboré des processus de certification et de conformité pour les spécifications d'interopérabilité approuvées afin de garantir que les fournisseurs, les dépositaires des renseignements sur la santé et les propriétaires d'actifs numériques en santé avancent vers une interopérabilité orientée par des normes au niveau provincial. Des évaluations de la vie privée et de la sécurité ont été réalisées sur un outil acquis pour appuyer et automatiser les processus de certification et de conformité afin de déterminer les risques et de proposer des mesures d'atténuation. En 2024-2025, Santé Ontario a tenu des consultations avec le CIPVP concernant le Répertoire numérique des médicaments (**RNM**), les Systèmes d'information des laboratoires de l'Ontario (**SILO**) et les spécifications d'interopérabilité du Système d'information et de signalement d'efficience des soins chirurgicaux (**SERIS**). Santé Ontario a également reçu l'approbation d'une modification à la spécification d'interopérabilité du Répertoire des données cliniques sur les soins actifs et communautaires (**RDCsac**) précédemment approuvée par le ministère de la Santé.

## Correspondance numérique (mise à jour)

Santé Ontario a lancé une initiative en 2023 pour tirer parti des capacités numériques de l'Ontario et les élargir afin de moderniser les communications sur le dépistage du cancer et d'améliorer l'expérience de dépistage pour les Ontariens. L'initiative vise à harmoniser une solution de correspondance numérique avec la stratégie plus vaste de Santé Ontario pour communiquer avec les Ontariens au sujet de leur santé. Le Bureau de la protection de la vie privée et le Bureau de la sécurité de l'information ont été mobilisés pour fournir un soutien tout au long du cycle de vie du projet afin de garantir que les principes de la protection de la vie privée et de la sécurité dès la conception sont tenus en compte dans la conception et la prestation de la solution, et pour s'assurer que les risques sont déterminés et atténués grâce à la collaboration avec les partenaires opérationnels, et à une évaluation officielle des risques en matière de vie privée et une évaluation des risques et des menaces.

Les Ontariens pourront choisir de recevoir des correspondances de dépistage au moyen d'un portail en ligne sécurisé, avec authentification par le biais de Compte Mon Ontario pour la santé. Pour le produit minimal viable de départ, seule la correspondance de dépistage du cancer colorectal sera disponible, et la correspondance papier se poursuivra en parallèle.

En 2024, on a obtenu la rétroaction des utilisateurs finaux au moyen de plusieurs séances de mobilisation, avec une courte évaluation des facteurs relatifs à la vie privée (**EFVP**) réalisée pour garantir des pratiques exemplaires. Tout au long de 2024 et jusqu'en 2025, le contenu destiné aux utilisateurs finaux pour le futur portail en ligne a été créé, y compris le contenu relatif à la vie privée comme l'Avis de collecte et les Conditions d'utilisation. Une EFVP conceptuelle a été réalisée à la mi-2024 pour analyser les décisions de conception du projet jusqu'à présent, avec une EFVP complète prévue au mi 2025. En mai 2025, un fournisseur externe a été intégré pour achever la création du portail en ligne et des API connexes, le Bureau de la protection de la vie privée étant fortement

impliqué dans la demande de propositions (DP), la sélection du fournisseur et les processus d'énoncé des travaux (ET). Une mise en service provisoire du portail en ligne est prévue pour le deuxième trimestre de 2026-2027.

## Les patients avant la paperasse – Moderniser la communication avec les fournisseurs (mis à jour)

Santé Ontario travaille en partenariat avec le ministère de la Santé pour élaborer et mettre en œuvre un plan stratégique complet de cinq ans pour les Patients avant la paperasse (**PB4P**). Ce plan vise à alléger le fardeau administratif des médecins en Ontario tout en améliorant l'accès aux services de santé pour les Ontariens. Dans le cadre de cette initiative, Santé Ontario a déterminé cinq cas d'utilisation principaux, à savoir les aiguillages et l'admission centrale, les ordonnances, les demandes et résultats de laboratoire, les notes médicales, et les processus administratifs, qui serviront de base à la réduction des tâches administratives et à l'amélioration de l'efficacité globale de la prestation des soins de santé dans la province.

Dans le cadre de l'initiative PB4P, Santé Ontario vise à élaborer un processus clinique intégré qui incorpore des outils de communication numérique pour diverses tâches de soins de santé. Cela comprend l'échange d'aiguillages, la réalisation de consultations, la commande de résultats de laboratoire et d'examens d'imagerie diagnostique, ainsi que la gestion des processus d'admission centrale. L'objectif est de mettre en œuvre entièrement cette approche intégrée et des solutions numériques sans faille au cours des cinq prochaines années.

L'équipe de la confidentialité a joué un rôle actif dans le renforcement des capacités dans des initiatives provinciales à grande échelle de PB4P, notamment grâce à sa participation substantielle dans la formation d'un comité de représentants des patients et familles (**RPF**). Ce comité est essentiel pour intégrer la perspective des patients dans les 13 volets de travail de l'initiative PB4P, garantissant que ces efforts demeurent axés sur le patient et ont une incidence.

Pour faire progresser l'état futur du réseau d'aiguillage électronique, Santé Ontario a réussi à établir des fournisseurs officiels (**FO**) au moyen d'un processus d'approvisionnement ouvert et concurrentiel lancé en novembre 2023. L'équipe de la confidentialité et de la sécurité est actuellement mobilisée pour appuyer les intégrations complexes de ces FO avec la Passerelle provinciale de coordination des soins (**PPCS**) et le Répertoire provincial des services de santé (**RPSS**) en préparation du prochain lancement technique. Ces intégrations exigent des évaluations complexes, et l'équipe a réalisé cinq de ces évaluations pour appuyer ce travail. De plus, les équipes ont évalué l'outil eForms Designer dans le cadre du flux de travail de l'Admission centrale en vue de faciliter la numérisation de 17 formulaires d'aiguillage, permettant l'utilisation de formulaires numériques et du nouveau réseau d'aiguillage pour le lancement au premier trimestre de 2025-2026. De plus, l'équipe a achevé les évaluations d'approvisionnement pour les fournisseurs d'admission centrale afin d'améliorer davantage l'état futur de l'aiguillage électronique.

Le flux de travail des formulaires électroniques se concentre sur la réduction de la charge administrative dans le [flux] principal, en particulier le temps consacré à remplir divers formulaires. Le groupe de travail sur les formulaires de l'Association médicale de l'Ontario et du ministère de la Santé a déterminé 12 formulaires prioritaires à mettre en œuvre, en commençant par le Formulaire d'évaluation de la santé (**FES**) des soins de longue durée numérisé pour remplacer l'envoi actuel par télécopieur ou courriel des soins primaires à Santé à domicile Ontario. En février 2024, le flux de travail de lancement de production limitée (**LPL**) des formulaires électroniques a été lancé dans le cadre de l'initiative PB4P. Pour appuyer cette initiative, l'équipe de confidentialité a réalisé deux EFVP en vue de faciliter l'intégration de la solution de formulaires électroniques directement avec les dossiers médicaux électroniques (**DME**). De plus, l'équipe de confidentialité et de sécurité a aidé à évaluer la capacité de permettre aux dépositaires de renseignements sur la santé, qui n'ont pas de moyens numériques, de soumettre des formulaires au moyen de la solution de formulaires électroniques à l'aide du service en ligne, One Health Launcher. Ce soutien vise à garantir une transition sans heurts vers des soumissions de formulaires numériques et à améliorer l'efficacité globale dans le cadre des soins primaires. Tout au long de l'exercice financier, les équipes de confidentialité et de sécurité de l'information ont été activement impliquées dans le soutien aux lancements des aiguillages, de l'admission centrale et des processus administratifs. Le travail sur ces initiatives se poursuit, alors que le Bureau de la protection de la vie privée et le Bureau de la sécurité de l'information restent activement mobilisés dans des efforts continus pour appuyer la transformation de la manière dont les Ontariens accèdent aux soins de santé.

# Confidentialité et sécurité en quelques chiffres : Mesures clés

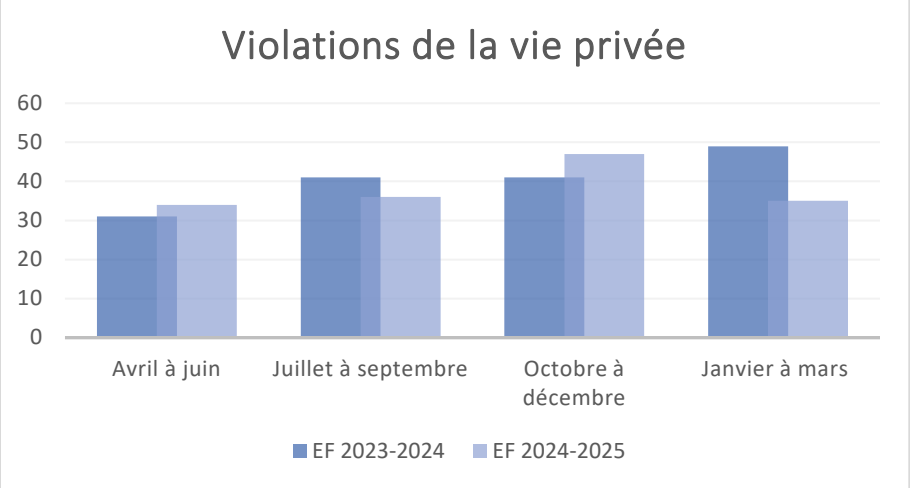
Les indicateurs clés de confidentialité et de sécurité suivants mettent en évidence certains des travaux réalisés par les équipes de confidentialité et de sécurité de l'information en 2024-2025 et fournissent une mesure de la conformité de Santé Ontario aux exigences législatives et réglementaires ainsi qu'aux pratiques d'information respectives.

## Points saillants des indicateurs de confidentialité

### 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. Santé Ontario gère des référentiels et des registres qui contiennent des données liées aux rencontres individuelles avec le système de santé de l'Ontario et contiennent des RPS sur la santé, tandis que la partie des DSE des actifs de données à elle seule compte plus de 11 milliards de dossiers, représentant environ 27,3 millions de particuliers uniques impliquant des RPS. Les indicateurs ci-dessous comprennent les violations des politiques de protection de la vie privée et les atteintes où des RPS ont été perdus, volés ou traités de manière non autorisée. Un exemple d'atteinte à la vie privée est lorsqu'un employé accède à des RPS alors que cela n'est pas nécessaire pour l'exercice de ses fonctions. Un autre exemple est lorsque qu'une organisation externe envoie des RPS à Santé Ontario alors que Santé Ontario n'a pas demandé ni n'a besoin de ces renseignements.

Le volume des atteintes est assez faible par rapport au volume des dossiers, des transactions et du potentiel d'erreur humaine dans l'ensemble du système de santé et de Santé Ontario. Le Bureau de la protection de la vie privée enquête sur toutes les atteintes à la vie privée soupçonnées et confirmées, en collaboration avec les intervenants concernés, avec des stratégies d'atténuation et des recommandations étant mises en œuvre pour prévenir de futures atteintes.



Dans l'ensemble, Santé Ontario a constaté une légère diminution du nombre d'atteintes signalées au cours de 2024-2025[3].

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

Au cours de l'exercice 2024-2025, Santé Ontario a envoyé environ sept millions de correspondances aux particuliers dans le cadre du Programme de dépistage du cancer de Santé Ontario, y compris, par exemple, des rappels pour se faire dépister, et des résultats de tests de dépistage. Ces lettres constituent un élément essentiel du Programme de dépistage du cancer, qui aide les particuliers à détecter le cancer plus tôt, lorsque les chances de le traiter avec succès sont meilleures; ce qui entraîne de meilleurs résultats de santé.

Dans certains cas, en raison d'adresses obsolètes ou inexactes provenant de sources de données, ce courrier est mal acheminé. Il y a eu une légère augmentation du nombre de correspondances qui ont été livrées à une adresse obsolète ou inexacte et retournées à Santé Ontario, atteignant 519 en 2023-2024, comparativement à 738 en 2024-2025. La correspondance mal acheminée, mal livrée ou ouverte ne représente que 0,01 % du volume total de la correspondance de dépistage.

Chaque instance de courrier retourné est examinée par le Centre de contact de dépistage du cancer de Santé Ontario, qui infirme l'adresse inexacte et tente de mettre à jour le dossier du destinataire prévu avec la bonne adresse. Santé Ontario envoie également une lettre de notification de l'atteinte au destinataire prévu si le courrier a été mal acheminé et ouvert par un destinataire non prévu, et si Santé Ontario est en mesure de mettre à jour l'adresse.

## Demandes d'accès et de correction des DSE et demandes de directive de consentement

Le traitement des demandes de protection de la vie privée des DSE liées à l'accès, à la correction et aux directives de consentement, appuie les patients dans l'exercice de leurs droits à la vie privée en vertu de la loi. Dans le cadre du rôle de Santé Ontario en tant qu'organisation prescrite en ce qui concerne le DSE provincial et en tant que dépositaire des renseignements sur la santé, Santé Ontario :

- Reçoit et met en œuvre les demandes des patients pour ajouter, modifier ou révoquer une directive de consentement dans leurs dossiers de RPS dans le DSE;
- Aide les dépositaires contributeurs de renseignements sur la santé avec le processus administratif lié aux demandes d'accès individuelles pour les dossiers de RPS dans le DSE, ainsi que pour appuyer le processus de correction, le cas échéant.

| **Demandes d'accès et de correction** | | | | |
|---|---|---|---|---|
| | Avril à juin | Juillet à septembre | Octobre à décembre | Janvier à mars |
| EF 2023-2024 | 129 | 121 | 108 | 154 |
| EF 2024-2025 | 139 | 114 | 111 | 137 |

[3] Veuillez noter que les incidents du Programme de dépistage des centres de contact ne sont pas inclus dans le tableau, et sont signalés séparément dans la section « Programme de dépistage du cancer de l'Ontario – Correspondance mal acheminée ».

| Demandes de directive en matière de consentement | | | | |
|---|---|---|---|---|
| | Avril à juin | Juillet à septembre | Octobre à décembre | Janvier à mars |
| EF 2023-2024 | 143 | 101 | 138 | 109 |
| EF 2024-2025 | 129 | 192 | 110 | 566 |

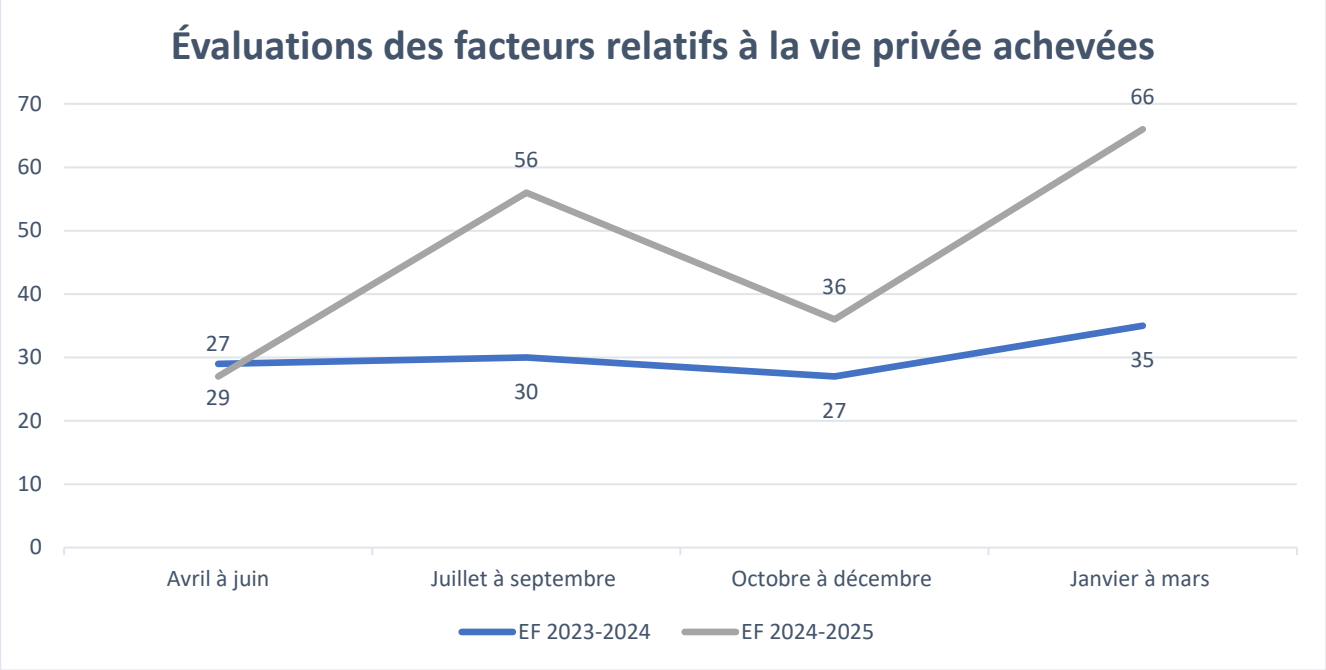
## Gestion des incidents de confidentialité des DSE – Dépositaires des renseignements sur la santé et coroners

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 liés aux RPS accessibles par le biais du DSE. De plus, les dépositaires de renseignements sur la santé (**DRS**) et les coroners qui accèdent ou contribuent aux dossiers du DSE doivent informer Santé Ontario dès la première occasion raisonnable après avoir déterminé ou pris connaissance d'une atteinte à la vie privée liée aux RPS accessibles par le biais du DSE. À la réception de cet avis, Santé Ontario signale l'atteinte à la vie privée à tout autre dépositaire de renseignements sur la santé pertinent ou au(x) coroner(s) qui a causé l'atteinte ou qui a contribué au dossier de RPS dans le DSE. Pour appuyer davantage le processus de gestion des incidents, Santé Ontario fournit des rapports d'audit des DSE aux dépositaires de renseignements sur la santé qui leur permettent d'auditer et de surveiller leur conformité à la LPRPS.

| Atteintes à la vie privée du DSE signalées par le DRS et le coroner | | | | |
|---|---|---|---|---|
| | Avril à juin | Juillet à septembre | Octobre à décembre | Janvier à mars |
| EF 2023-2024 | 19 | 12 | 11 | 14 |
| EF 2024-2025 | 17 | 11 | 18 | 9 |

## Évaluations des facteurs relatifs à la vie privée

Au cours du dernier exercice financier, Santé Ontario a réalisé ou supervisé la réalisation de 185 EFVP par rapport à 121 l'année précédente. Une obligation clé et une fonction exercée par le Bureau de la protection de la vie privée est l'achèvement des EFVP qui servent à évaluer les nouveaux éléments ou les mises à jour de la législation ou de la réglementation, des programmes, des services, des processus ou des risques de protection de la vie privée des systèmes d'information, et à recommander des stratégies d'atténuation. Les EFVP fournissent un niveau d'assurance que les problèmes et les risques liés à la vie privée sont identifiés et résolus. Elles peuvent également promouvoir une compréhension de la manière dont Santé Ontario gère les RPS ou les RP, et démontrer les façons dont Santé Ontario respecte ses obligations législatives et réglementaires ainsi que son engagement en matière de protection de la vie privée envers le grand public.




L'augmentation significative des EFVP depuis l'exercice précédent est attribuée en partie au grand volume d'initiatives de haute priorité liées au (i) déploiement de l'ESO (Principaux projets – 7 EFVP) et à la (ii) modernisation de la chaîne d'approvisionnement du secteur public au moyen d'intégrations de systèmes (Équipement et fournitures médicaux – 11 EFVP). Ces EFVP en particulier seront fondamentales et appuieront tout déploiement ultérieur de l'ESO sur le système CHRIS et les intégrations des systèmes de fournisseurs CHRIS liés aux équipements et fournitures médicaux.

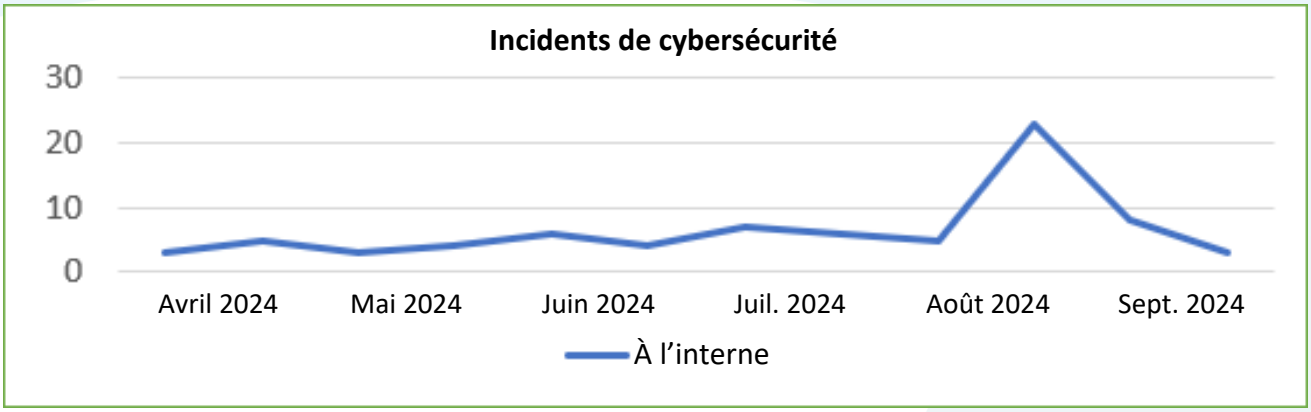
# La sécurité en quelques chiffres : Mesures clés

## Incidents de cybersécurité

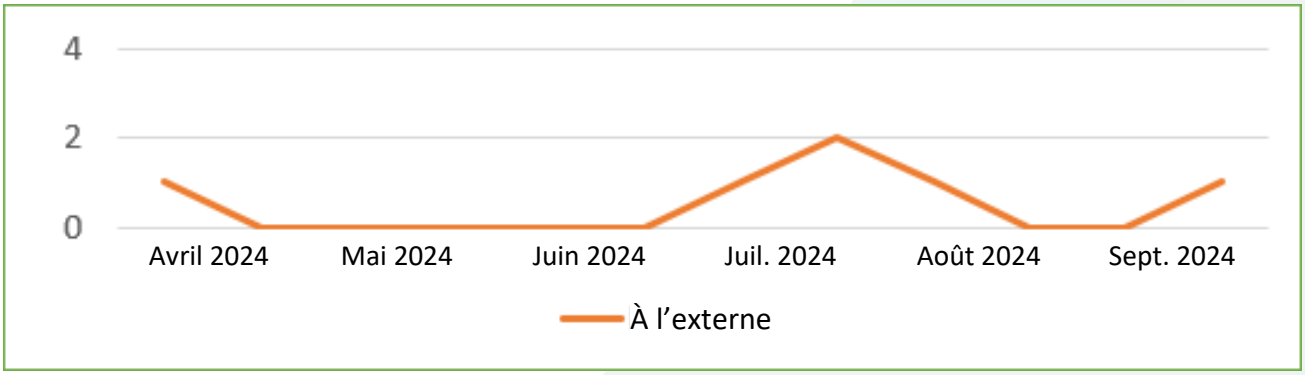
Au cours de la période d'avril 2024 à mars 2025, les incidents internes, caractérisés principalement par une faible gravité, ont principalement entraîné d'activités d'utilisateurs non autorisés, comme des tentatives de connexion à des adresses URL malveillantes ou des tentatives d'authentification échouées depuis des emplacements inconnus. Ces incidents sont efficacement détectés et bloqués tôt par des outils cybernétiques automatisés, garantissant une incidence minimale sur les actifs de Santé Ontario. Malgré la faible gravité, tous les incidents internes sont suivis méticuleusement dans tous les niveaux de gravité, confirmant la solidité des mécanismes de surveillance internes de Santé Ontario.

Sur le plan externe, la tendance des incidents signalés a montré une baisse globale. La majorité de ces incidents, qui ont été signalés par le secteur et classés avec une gravité plus élevée, n'ont pas touché

les actifs de Santé Ontario. Cette baisse indique le succès de la sensibilisation et des conseils fournis par Santé Ontario, qui ont considérablement renforcé la sensibilisation à la cybersécurité parmi les entités externes, menant à une amélioration de la réponse aux mesures de confinement et d'éradication. La hausse notable au quatrième trimestre n'a pas eu d'incidence sur la tendance générale à la baisse des incidents.




**Incidents de cybersécurité à l'interne :** Les incidents internes de cybersécurité sont classés comme de vraies attaques positives, impliquant des activités malveillantes visant à compromettre les systèmes de Santé Ontario. La plupart de ces incidents varient de faible à moyenne gravité, grâce à l'efficacité des défenses de cybersécurité automatisées pour détecter et bloquer rapidement de telles activités.a




**Incidents de cybersécurité externes :** Les incidents externes sont généralement de haute gravité et sont signalés à Santé Ontario lorsque des attaques malveillantes exigent des arrêts de système. Même si ces incidents présentent un risque pour les systèmes de Santé Ontario, ce risque est atténué grâce à des défenses de cybersécurité solides et à une collaboration active avec les organisations externes concernées.

## Évaluations des menaces et des risques

Les mesures de sécurité ci-dessous fournissent des renseignements sur le nombre d'évaluations des risques et des menaces (**ERM**) internes et externes effectuées, ainsi que sur les évaluations de sécurité et les tests de pénétration réalisés sur de nouveaux systèmes ou des changements opérationnels. De plus, afin de se conformer aux pratiques exemplaires et normes de l'industrie, les chiffres ci-dessous détaillent le nombre d'analyses des vulnérabilités complètes effectuées sur diverses infrastructures réseau à Santé Ontario.

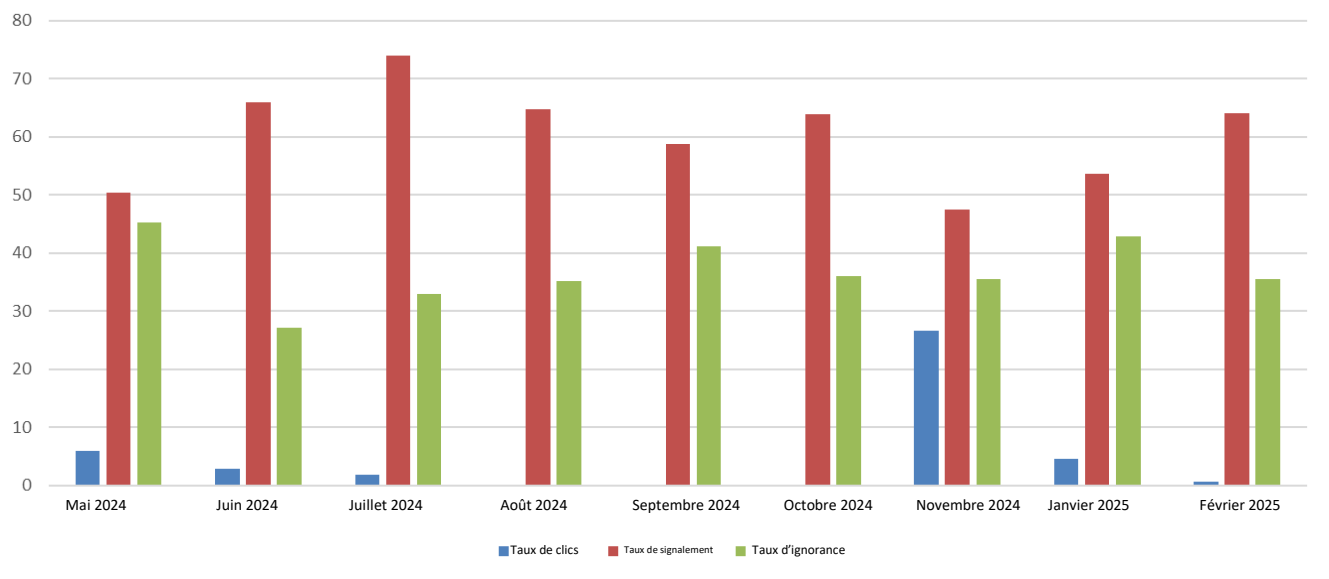
Au cours de l'exercice financier 2024-2025, le BSI a réalisé (exécuté et examiné) plus de 150 évaluations de sécurité pour plus de 50 projets.

| Principales activités de cybersécurité – 2024-2025 (GESTION DES RISQUES) | | | | |
|---|---|---|---|---|
| | **EMR à l'interne** | **EMR à l'externe** | **Évaluations de la sécurité** | **Test de pénétration** |
| **Nombre d'évaluations achevées par type** | 5 | 10 | 20 | 8 |

| Principales activités de cybersécurité – 2024-2025 (GESTION DES RISQUES) | | | | |
|---|---|---|---|---|
| **Évaluations précises du DSE** | **NIST (Auto-évaluations)** | **EMR** Examen | **Test de pénétration** Examen | **Examen de l'analyse des vulnérabilités (AV)** |
| **Nombre d'évaluations achevées par type** | 50 | 20 | 15 | 30 |

## Résultats de la campagne de simulations d'hameçonnage de Santé Ontario

Au cours de l'exercice financier 2024-2025, les campagnes de sensibilisation à l'hameçonnage de Santé Ontario continuent de montrer une amélioration mesurable de la vigilance et de la réactivité des utilisateurs. Les campagnes ont suivi quatre mesures de rendement clés : taux de clics, taux de signalement, taux d'ignorance et taux de correction – pour évaluer la mobilisation et éclairer les futures stratégies de sensibilisation. Les taux de clics ont régulièrement diminué, passant de 5,9 % en mai à des niveaux proches de zéro en février, illustrant une susceptibilité réduite aux tentatives de hameçonnage. Même si une augmentation notable à 26,7 % a eu lieu en novembre, attribuée à une simulation de hameçonnage délibérément difficile qui a servi de test de stress précieux pour la sensibilisation des utilisateurs. En même temps, les taux de signalement sont restés élevés, atteignant des sommets de 74 % en juillet et de 64,5 % en février; ce qui indique une confiance accrue des utilisateurs dans l'identification et le signalement des courriels suspects.



Le taux d'ignorance a fluctué entre 27 % et 43 %, suggérant une occasion de mobiliser davantage un segment d'utilisateurs prudents, mais passifs au moyen d'efforts de sensibilisation ciblés. Fait encourageant, les taux de correction après clic sont restés constamment élevés, avec un taux d'achèvement de la formation de 100 % sur plusieurs mois, renforçant la capacité de Santé Ontario à répondre efficacement aux lacunes de sensibilisation et à les combler. Dans l'ensemble, ces tendances tiennent compte d'une culture de sécurité en maturation – une culture qui privilégie la sensibilisation, le signalement en temps opportun et l'amélioration continue pour se protéger contre les menaces par courriel.

Les résultats des campagnes d'hameçonnage sont liés aux campagnes d'hameçonnage mensuelles où des courriels malveillants simulés sont envoyés aux employés. Un taux de signalement élevé et un faible taux de clics sont les résultats souhaités. Même si le taux d'ignorance ne pose pas de risque de sécurité direct, ce n'est pas non plus la mesure optimale. Un taux de signalement élevé indique que le personnel est conscient de la sécurité. Un faible taux de clics est attribué à des initiatives de sensibilisation et de formation efficaces. À mesure que la complexité augmente, ces résultats peuvent être touchés. Les campagnes sont appliquées de manière uniforme à Santé Ontario avec une complexité variable.

# Perspectives d'avenir

Pour continuer à remplir son mandat principal d'intégration du système de santé et de soutien à des soins axés sur le patient de qualité supérieure, Santé Ontario a besoin de données – RPS et RP. Le Bureau de la protection de la vie privée, le Bureau de la sécurité de l'information et les équipes de cybersécurité ont travaillé avec diligence au cours de la dernière année pour optimiser l'utilisation des données et 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 à protéger la vie privée et la confidentialité. Grâce à ses rôles prescrits, Santé Ontario a une grande latitude pour utiliser les données qui lui sont confiées et des responsabilités importantes. Par conséquent, le travail se poursuit.

Voici un échantillon de priorités clés supplémentaires pour 2025-2026 (en plus du travail en cours décrit ci-dessus) pour les équipes de protection de la vie privée et de cybersécurité.

## Systèmes d'information du RTDV (mis à jour)

Un travail considérable a été entrepris pour appuyer la mise au point du contrat du fournisseur du Système de gestion des donateurs (**SGD**) à la fin de 2024-2025. Avec le nouveau contrat en place, le Bureau de la protection de la vie privée est en mesure d'entreprendre une EFVP complète du Système de gestion des donateurs de bout en bout. De plus, à mesure que les intégrations du SAGO avancent, des travaux sont déjà en cours pour appuyer les prochaines phases du développement du SAGO. Le Bureau de la protection de la vie privée sera essentiel pour garantir la conformité en matière de vie privée et l'intégration des principes de protection de la vie privée dès la conception dans le développement ultérieur du SAGO. Cela impliquera de mettre à jour les EFVP existantes.

## Accès Soins (nouveau)

Le programme Accès Soins (**AS**) a été établi en 2009 par le ministère de la Santé pour connecter les patients non rattachés à des praticiens de soins primaires et augmenter le taux de rattachement

global en Ontario.  Le programme permet aux personnes sans fournisseur de soins de santé familial régulier de s'inscrire pour obtenir de l'aide afin de trouver des médecins et des infirmiers praticiens qui acceptent de nouveaux patients dans leur communauté.
En soutien au mandat de l'Équipe d'action pour les soins primaires (**EASP**) et en préparation des améliorations futures au programme d'AS, le Ministère a demandé aux ressources de confidentialité de Santé Ontario de réaliser un examen des contrôles de confidentialité existants en place pour le programme d'AS de bout en bout, de trouver les lacunes possibles et de recommander des activités pour combler ces lacunes. Le Ministère a également demandé à Santé Ontario de réaliser une évaluation des facteurs relatifs à la vie privée, qui est en cours.

## Améliorer la résilience cybernétique et opérationnelle : Intégrer les capacités partagées, les stratégies de défense et la formation pour une culture de sécurité (nouveau)

Au cours de l'exercice financier 2025-2026, le Programme de cybersécurité de Santé Ontario mettra l'accent sur un certain nombre d'initiatives clés en matière de défense en cybersécurité et de sécurité de l'information visant à améliorer la sécurité et la résilience opérationnelle dans l'organisation :

- **Le Programme de gestion des certificats et des clés « Zero Touch » (PGCCZT) se concentre sur l'automatisation et la cryptographie :** Approfondir l'automatisation, améliorer la souplesse cryptographique et élargir la préparation pour la technologie post-quantique. Les initiatives clés comprennent l'extension de la rotation des certificats TLS et l'automatisation de la gestion du cycle de vie des clés.
- **Mesures proactives du chargé de la mise en œuvre :** Élargir son champ d'application pour inclure la chasse aux menaces et l'analytique avancée. Le programme affinera les plans d'intervention en cas d'incidents et améliorera la collaboration avec des partenaires externes pour faire face aux cybermenaces en évolution.
- **Améliorations de l'intégration et de la sécurité de la GIAE :** Intégrer un cadre de gestion des identités, élargir la couverture de l'authentification multifacteur et du système d'authentification unique, et réaliser des audits pour trouver les vulnérabilités.
- **Solution Netskope :** Élargir l'intégration avec d'autres outils de sécurité comme Microsoft Defender et Saviynt pour renforcer davantage la position de sécurité de l'organisation.
- **Microsoft Purview :** Élargir le déploiement de Microsoft Purview pour couvrir des domaines supplémentaires comme les partages de fichiers dans le nuage, Teams, SharePoint, les fichiers PDF et Power BI. L'accent sera mis sur le balisage des actifs de données pour la classification et l'élaboration de politiques de prévention des pertes de données pour appuyer la gouvernance des données.
- **Élever la position de sécurité :** Affiner les stratégies adaptatives de Santé Ontario face aux nouvelles menaces et travailler à garantir que nos systèmes sont résilients contre les cyberattaques. Les domaines clés d'intervention comprendront l'expansion de notre gestion des vulnérabilités axée sur les produits, l'amélioration de nos capacités du COS et l'optimisation supplémentaire de nos cadres de protection de l'identité. Grâce à ces efforts,

nous visons à rester en avance sur la courbe en matière de cybersécurité, en protégeant les actifs numériques de notre organisation et en appuyant ses objectifs à long terme.

- **Élargir les tests de sécurité des applications :** Élargir les mises en œuvre du DAST dans divers aspects de nos opérations. Les tests de sécurité commenceront dans les environnements sur place de Santé Ontario, visant les applications nouvelles et existantes pour garantir des évaluations de vulnérabilité approfondies et des protocoles de correction. De plus, nous prévoyons de peaufiner et d'optimiser les processus de DAST dans nos abonnements Azure dans le nuage. Cela consiste à améliorer les mécanismes d'intégration, à augmenter la fréquence des analyses de sécurité et à exploiter des outils analytiques avancés pour tirer des renseignements exploitables des résultats des analyses.

- **Simulation des cybermenaces et résilience :** Actuellement, Santé Ontario réalise des exercices sur table ponctuels et des tests de pénétration. Toutefois, au cours de l'exercice 2025-2026, nous prévoyons d'acheter des outils qui permettront à Santé Ontario d'effectuer ces exercices plus fréquemment, avec une souplesse accrue d'envergure et une planification régulière, améliorant ainsi la préparation et la résilience.
    - La fonction d'exercice sur table permettra aux dirigeants et aux principaux intervenants de simuler des incidents cybernétiques à fort impact et de les étudier dans un format structuré et fondé sur la discussion. Ces exercices permettront de façonner la prise de décision stratégique, à préciser les rôles et les responsabilités, et à améliorer la préparation de l'organisation face aux événements imprévus.

    - La capacité de test d'intrusion (équipe rouge/équipe violette) fournira des évaluations ciblées des systèmes d'information, déterminera les vulnérabilités possiblement exploitables, permettra de prioriser la correction de ces vulnérabilités et évaluera ou améliorera l'efficacité des contrôles de sécurité existants.

- **Faire progresser les campagnes d'hameçonnage :** Introduire de nouvelles stratégies pour renforcer les défenses contre les attaques d'hameçonnage. Les plans comprennent un module de formation des employés mis à jour sur les nouvelles tactiques, une collaboration avec des experts en cybersécurité externes et une surveillance continue avec des protocoles de sécurité adaptatifs. Notre objectif est de favoriser une culture de la sécurité et de maintenir la vigilance à tous les niveaux.

Le renforcement de la la résilience cybernétique grâce à des capacités et des contrôles partagés reste essentiel pour Santé Ontario et son travail visant à mettre en œuvre davantage le Modèle opérationnel de cybersécurité provincial dans l'ensemble du secteur de la santé. Dans l'avenir, Santé Ontario concentrera ses efforts sur l'amélioration de la résilience du secteur de la santé grâce aux initiatives suivantes :

**Faire progresser le Modèle opérationnel de cybersécurité provincial au-delà des hôpitaux de soins aigus**

- Élaboration continue de la stratégie du modèle dans les soins primaires, les soins de longue durée et la santé publique.

**Améliorer le Suivi des contrôles critiques**

- Appuyer les fournisseurs de services de santé dans l'élaboration et l'exécution de feuilles de route pour l'état cible de maturité de la mise en œuvre des contrôles critiques.

**Optimisation continue des plateformes provinciales du MOC**

- Augmenter la participation des partenaires et des fournisseurs de services dans la plateforme d'Échange de renseignement sur les cybermenaces (**CTIX**).
- Mettre en œuvre les mises à jour de la plateforme provinciale de maturité en cybersécurité, y compris l'amélioration de la fonctionnalité d'utilisateur avancée, l'interface, et les capacités de signalement.

**Mettre en œuvre le durcissement proactif et la réduction de la surface d'attaque (DPRSA)**

- Déterminer les occasions de collaboration et de partenariat avec le Centre d'excellence en cybersécurité du ministère des Services gouvernementaux et des Services aux consommateurs sur l'avenir de l'adoption par le secteur de la santé de la solution provinciale de réduction des attaques.

Santé Ontario s'engage à élargir son infrastructure de sécurité en mettant en œuvre des systèmes avancés de renseignement sur les menaces et en élargissant la protection aux nouvelles plateformes numériques. L'organisation investit dans des outils de surveillance améliorés pour favoriser la détection et l'intervention en temps réel aux cybermenaces, en garantissant des mécanismes de défense proactifs. De plus, Santé Ontario continuera de renforcer les partenariats avec des organisations et des experts en cybersécurité pour anticiper les menaces évolutives et tirer parti des technologies de pointe. Des programmes d'amélioration continue seront lancés pour affiner les protocoles et stratégies de sécurité en fonction des dernières tendances de l'industrie et des paysages de menaces.

# Acronymes

| Acronyme | Signification |
|---|---|
| **3 LD** | Trois lignes de défense |
| **AI** | Accès à l'information |
| **ALH** | Antigène leucocytaire humain |
| **AMF** | Authentification multifacteur |
| **AS** | Accès Soins |
| **BDC** | Bases de données cliniques |
| **BSI** | Bureau de la sécurité de l'information |
| **CABR** | Contrôle d'accès basé sur les rôles |
| **CCS** | Cadre de cybersécurité |
| **CCSO** | Centre de cybersécurité de Santé Ontario |
| **CDSI** | Comité directeur de la sécurité de l'information |
| **CHRIS** | Système d'information sur la santé des clients |
| **CIPVP** | Bureau du Commissaire à l'information et à la protection de la vie privée de l'Ontario |
| **CODS** | Conseil ontarien des données sur la santé |
| **COS** | Centre des opérations de sécurité |
| **CTIX** | Échange de renseignement sur les cybermenaces |
| **DAST** | Analyseur de sécurité des applications dynamiques |
| **DCS** | Défense en cybersécurité |
| **DME** | Dossier médical électronique |
| **DPVP** | Directeur de la protection de la vie privée |
| **DRS** | Dépositaire de renseignements sur la santé |
| **DSE** | Dossier de santé électronique |
| **EASP** | Équipe d'action en soins primaires |
| **ECSI** | Échange de connaissances en sécurité de l'information |
| **EFVP** | Évaluation des facteurs relatifs à la vie privée |
| **EMR** | Évaluation des menaces et des risques |
| **EP** | Entité prescrite |
| **ERNS** | Échange de renseignements numériques sur la santé |
| **ESO** | Équipe de Santé Ontario |
| **EV** | Étude de validation |
| **FEM** | Fournitures d'équipement médical |
| **FES** | Formulaire d'évaluation de la santé |
| **FO** | Fournisseur officiel |
| **FRIS** | Fournisseur de réseau d'information sur la santé |
| **FSE** | Fournisseur de services électroniques |
| **FSS** | Fournisseurs de services de santé |
| **FSSG** | Fournisseur de services de sécurité gérés |
| **GAI** | Gouvernance et administration des identités |
| **GAPN** | Gestion des accès privilégiés dans le nuage |

| | |
|---|---|
| **GIA** | Gestion des identités et des accès |
| **GIAE** | Gestion des identités et des accès d'entreprise |
| **GRC** | Gouvernance, Risque et Conformité |
| **IA** | Intelligence artificielle |
| **INS** | Identité numérique de santé |
| **LAIPVP** | *Loi sur l'accès à l'information et la protection de la vie privée* |
| **LPL** | Lancement en production limité |
| **LPRPS** | *Loi sur la protection des renseignements personnels sur la santé* |
| **LRSCN** | Loi visant à renforcer la sécurité et la confiance en matière de numérique |
| **MOC** | Modèle opérationnel de cybersécurité |
| **MS** | Ministère de la Santé |
| **MSGSC** | Ministère des Services gouvernementaux et des Services aux consommateurs |
| **NIST** | National Institute of Standards and Technology |
| **OP** | Organisation prescrite |
| **PB4P** | Les patients avant la paperasse |
| **PEPT** | Protection évolutive des points de terminaison |
| **PGCCZT** | Programme de gestion des certificats et des clés « Zero Touch » |
| **PGICIC** | Programme de gestion des interventions en cas d'incidents de cybersécurité |
| **PP** | Principaux projets |
| **PP** | Personne prescrite |
| **PPCS** | Passerelle provinciale de coordination des soins |
| **PPSS** | Partenaire principal du système de santé |
| **RDC** | Référentiel de données cliniques |
| **RDCsac** | Répertoire des données cliniques sur les soins actifs et communautaires |
| **Règl. de l'Ont.** | Règlement de l'Ontario |
| **RNM** | Répertoire numérique des médicaments |
| **RODC** | Registre ontarien de dépistage du cancer |
| **RP** | Renseignements personnels |
| **RPF** | Représentant des patients et familles |
| **RPS** | Renseignements personnels sur la santé |
| **RPSS** | Répertoire provincial des services de santé |
| **RRO** | Réseau rénal de l'Ontario |
| **RRPG** | Risque réel de préjudice grave |
| **RTDV** | Réseau Trillium pour le don de vie |
| **S811** | Santé 811 |
| **SaaS** | Logiciel-service |
| **SAGO** | Système d'attribution et de greffe d'organes |
| **SCID** | Service commun d'imagerie diagnostique |
| **SE** | Système d'exploitation |
| **SERIS** | Système d'information et de signalement d'efficience des soins chirurgicaux |

| | |
|---|---|
| **SGD** | Système de gestion des donneurs |
| **SICD** | Système d'information sur la collecte de données |
| **SILO** | Système d'information de laboratoire de l'Ontario |
| **SLD** | Soins de longue durée |
| **SPDSN** | Services provinciaux de données de santé et numériques |
| **SSO** | Authentification unique |
| **SSRS** | Système de santé, rendement et soutien |
| **TTX** | Exercice sur table |
| **VCP** | Visualiseur clinique provincial |
| **VPP** | Visualiseur provincial pour les patients |

Avez-vous besoin de ces renseignements dans un format accessible? 1-877-280-8538, ATS 1-800-855-0511, info@ontariohealth.ca.
Document available in English, please contact info@ontariohealth.ca