eHealth Ontario
It's working for you

Politique relative aux fournisseurs de services d'authentification

Services d'identité et d'authentification

Ontario
eHealth Ontario

Table des matières

1 Contexte

1.1 Fédération d'identité de cyberSanté Ontario

1.1.1 La fédération d'identité de cyberSanté Ontario (**la « fédération »**), administrée par cyberSanté Ontario (**l'« organisme »**), est un réseau qui permet à ses membres d'offrir des services de santé électroniques **(« services fédérés »**) ou d'y accéder au moyen du **système fédéré** de l'organisme – une infrastructure technologique composée d'applications, de systèmes, de registres, de bases de données, de documents, de portails et d'outils.

1.1.2 Le programme ONE^{MD} ID de l'organisme est l'opérateur de la fédération – un « courtier » qui transmet les demandes d'accès des utilisateurs finaux aux services fédérés, avec la validation de leur identité par les fournisseurs de services d'authentification (**« FSA »**), afin de permettre aux fournisseurs d'application de prendre des décisions éclairées en matière d'autorisations.

1.2 But

1.2.1 La présente politique définit :

a) les exigences d'accréditation pour les FSA;

b) les normes minimales pour les services d'identité et d'authentification (**« services d'IA »**) fournis par les FSA accrédités aux utilisateurs finaux;

c) les politiques opérationnelles liées à l'accès aux services fédérés et à leur utilisation, notamment :

- les responsabilités de l'utilisateur final;
- les dispositions en matière de surveillance et de conformité;
- les exigences en matière de protection de la vie privée et de sécurité.

1.3 Objectifs

1.3.1 La présente politique contribue aux objectifs suivants :

a) Définir les obligations et les responsabilités liées à l'enregistrement et à l'authentification des utilisateurs finaux pour leur permettre d'accéder aux services fédérés.

b) S'assurer que les services d'IA respectent les normes définies, afin que les utilisateurs finaux puissent s'enregistrer et s'authentifier :

- à l'aide de processus cohérents, bien définis, fiables et sécuritaires;
- avec le niveau d'assurance requis pour accéder aux services fédérés.

c) Établir des exigences en matière de protection de la vie privée et de sécurité afin de protéger les renseignements personnels ou les renseignements personnels sur la santé accessibles par les services fédérés.

1.4 Portée et application

1.4.1 Le présent document s'applique à tous les FSA accrédités et à leurs préposés.

1.4.2 La présente politique définit des exigences minimales pour les FSA accrédités et les services d'IA qu'ils offrent à l'intérieur de la fédération.

1.5 Exceptions à la politique

1.5.1 Le directeur principal de l'identification, de l'accès et de la protection de la vie privée est responsable de veiller au respect de la présente politique.

1.5.2 Dans des cas exceptionnels, un FSA peut demander d'être exempté d'une ou de plusieurs exigences de la présente politique en écrivant à l'organisme un message décrivant la ou les raisons de la demande. Toutes les demandes doivent être examinées et approuvées par les gestionnaires des services d'identité ONE ID et des services de sécurité.

1.6 Violations

1.6.1 Toute violation de la présente politique par un FSA ou un de ses préposés est sujette aux pénalités décrites dans l'entente contractuelle conclue entre le FSA et l'organisme. De plus, l'organisme peut aussi employer un autre recours disponible en vertu d'une loi ou d'un règlement applicable.

1.7 Terminologie

1.7.1 Le présente politique suit certaines conventions de rédaction, avec des exigences et des obligations précises :

Doit : Cette exigence est obligatoire.

Devrait : Le responsable de la mise en œuvre doit prendre cette mesure, à moins que les exigences opérationnelles soient différentes. Les exceptions doivent être approuvées par les gestionnaires en tant que modifications à la pratique normalisée.

Peut : Le responsable de la mise en œuvre doit choisir au moins une option parmi celles proposées, selon ce qu'exige le contexte.

1.7.2 Les pronoms et leur variations englobent le féminin et le masculin et tous les termes utilisés au singulier englobent le pluriel, et vice-versa, en fonction du contexte.

1.7.3 Le verbe « comprendre » et le mot « notamment » n'introduisent pas des énumérations exhaustives et signifient, respectivement « comprendre, sans s'y limiter » et « notamment, sans s'y limiter ».

1.7.4 Les mots et les termes de la présente politique dont la signification diffère de la définition généralement acceptée sont définis dans le glossaire.

2 Politique relative aux fournisseurs de services d'authentification

2.1 Accréditation

2.1.1 Pour être accrédité, un FSA doit :

a) être en mesure de valider l'identité des utilisateurs finaux à un niveau d'assurance de 2 ou plus;

b) conclure toutes les ententes applicables avec l'organisme;

c) avoir un système d'accès et de gestion de l'identité (« SAGI ») et fournir des services d'IA qui, selon l'examen de l'organisme, respectent les exigences des normes relatives aux fournisseurs de services d'authentification de la fédération d'identité de cyberSanté Ontario (les « normes ») et, le cas échéant, les spécifications sur les attributs de la fédération et les spécifications sur les services fédérés (ensemble, les « spécifications ») de la fédération d'identité de cyberSanté Ontario.

2.1.2 Si le SAGI ou les services d'IA offerts par un FSA ne respectent pas toutes les exigences, l'organisme peut recommander des changements afin de remédier à la situation. Si le FSA n'applique pas les changements recommandés ou ne les applique pas d'une manière qui satisfait l'organisme, ce dernier n'accréditera pas le FSA.

2.1.3 L'organisme doit tenir une liste des FSA accrédités et la fournir sur demande aux membres de la fédération et aux utilisateurs finaux.

2.2 Rôles et responsabilités

2.2.1 Les responsabilités d'un FSA accrédité comprennent :

a) la validation de l'identité (p. ex., valider la véritable identité des utilisateurs finaux et leur assigner un identifiant unique);

b) la gestion des authentifiants (p. ex., donner les authentifiants appropriés selon le niveau d'assurance requis pour un service fédéré);

c) la gestion du SAGI (p. ex., entretenir ou mettre à niveau le SAGI);

d) les politiques et les normes (p. ex., établir et appliquer des politiques liées aux services d'IA et les normes relatives aux FSA qui concordent avec celles de l'organisme);

e) la conformité (p. ex., respecter toutes les politiques, les normes et les lignes directrices sur la protection de la vie privée et la sécurité de la fédération, ainsi que les ententes juridiques, les lois et les règlements;

f) le soutien aux clients (p. ex., fournir des services de dépannage aux utilisateurs finaux).

2.3 Enregistrement

2.3.1 Lors de l'enregistrement, le FSA doit assigner à chaque utilisateur final les renseignements suivants, conformément aux exigences décrites dans les normes relatives aux fournisseurs de services d'authentification :

a) Un identifiant unique;
b) Un niveau d'assurance;
c) Les renseignements nécessaires pour créer et conserver un mot de passe.

2.3.2 Généralement, les utilisateurs finaux doivent atteindre un niveau d'assurance de 2 ou plus pour être autorisés à accéder aux services fédérés, surtout si des renseignements de nature délicate, notamment des renseignements personnels (RP) ou des renseignements personnels sur la santé (RPS), sont accessibles à partir des services en question.

Les exigences liées au niveau d'assurance sont exposées avec plus de précision les normes.

2.3.3 Le FSA doit veiller à ce que le respect de la Politique d'utilisation acceptable de l'organisme par les utilisateurs finaux qui accèdent aux services fédérés fasse partie des conditions d'enregistrement.

2.4 Authentification

2.4.1 Aucune interaction entre le système fédéré et l'utilisateur final ne doit être autorisée avant que l'organisme n'ait reçu une authentification acceptable.

2.4.2 Le FSA doit établir des processus d'authentification pour valider l'association entre les authentifiants et l'identité réelle, conformément aux exigences des normes.

2.4.3 Les renseignements minimaux obligatoires pour authentifier les utilisateurs finaux sont décrits dans les normes relatives fournisseurs de services d'authentification.

2.4.4 Une méthode d'authentification qui comprend des questions d'identification doit respecter les exigences des normes relatives aux fournisseurs de services d'authentification.

2.4.5 L'organisme peut, à son exclusive discrétion, revoir ses exigences pour accepter une authentification après avoir donné un avis écrit au FSA, conformément aux termes des ententes applicables.

2.4.6 Pour faciliter l'accès mobile aux services fédérés, le FSA devrait être capable d'authentifier sur différents types d'appareils électroniques mobiles (p. ex., téléphone intelligent, tablette), selon les exigences des normes relatives aux fournisseurs de services d'authentification.

2.4.7 Le FSA doit s'assurer de l'exactitude des identités et attributs électroniques soumis à l'organisme.

2.5 Soutien à la clientèle

2.5.1 Le FSA doit avoir des préposés aux services à la clientèle enregistrés et inscrits qui effectuent les tâches d'enregistrement, d'authentification et de soutien des utilisateurs finaux clients, dans les limites des pouvoirs délégués par le FSA.

2.5.2 Les préposés aux services à la clientèle du FSA doivent être enregistrés à un niveau d'assurance de 2 ou plus.

2.5.3 Les préposés aux services à la clientèle du FSA doivent seulement avoir accès aux renseignements nécessaires pour accomplir les tâches qui leur sont assignées.

2.5.4 Les personnes qui communiquent avec un préposé aux services à la clientèle du FID doivent s'authentifier selon un processus défini par le FSA, conformément aux exigences définies dans les sections pertinentes des normes relatives aux fournisseurs de services d'authentification.

2.6 Protection des renseignements personnels

2.6.1 Le FID ne doit recueillir, utiliser, conserver et communiquer des renseignements, notamment les RPS et les RP, qu'à des fins d'enregistrement ou d'authentification, et seulement dans la mesure nécessaire aux fins auxquelles ils ont été recueillis.

2.6.2 Le FSA doit séparer les renseignements recueillis aux fins d'enregistrement et d'authentification des autres renseignements et veiller à ce qu'ils soient traités conformément aux ententes, lois et règlements applicables.

2.6.3 Le FSA doit fournir une copie physique de l'Évaluation de l'impact sur la protection de la vie privée à l'organisme pour faciliter la réalisation de toute Évaluation de l'impact sur la protection de la vie privée obligatoire par l'organisme.

2.6.4 Le FSA doit respecter les exigences de la politique sur l'Évaluation de l'impact sur la protection de la vie privée de l'organisme.

2.6.5 Le FSA doit se conformer à tout plan de traitement des risques exigé par l'organisme en lien avec la prestation de services d'identité et d'authentification. Si le FSA n'applique pas les changements recommandés ou ne les applique pas d'une manière satisfaisante pour l'organisme, ce dernier peut enclencher un recours défini dans son entente avec le FSA.

2.7 Vérification de la conformité en matière de protection de la vie privée

2.7.1 L'organisme peut effectuer un examen portant sur la protection de la vie privée et des données par le FSA selon la fréquence et le programme proposés par le directeur général de la protection de la vie privée et l'agent de conformité.

2.7.2 Le cas échéant, l'organisme doit fournir un préavis conformément à l'entente conclue avec le FSA.

2.8 Mesures de sécurité

2.8.1 Le FSA doit veiller à ce que son SAGI et les services d'IA qu'il offre respectent les exigences et les normes relatives au fournisseur de services d'authentification.

2.9 Normes de la fédération

2.9.1 Le FSA doit respecter les normes relatives au fournisseur de services d'authentification.

2.10 Utilisateurs finaux

2.10.1 Pour avoir le droit d'accéder à des services fédérés, un utilisateur final doit :

a) être enregistré et authentifié par un FSA accrédité;
b) avoir reçu du FSA un avis décrivant le fondement légal et les raisons de la collecte, de l'enregistrement, de l'utilisation et de la communication de tout renseignement sur l'utilisateur final, notamment les RP et les RPS;
c) consentir à la collecte, à l'enregistrement, à l'utilisation et à la communication des renseignements d'enregistrement;
d) accepter de se plier à la *Politique d'utilisation acceptable* de l'organisme.

2.11 Sélection du FSA

2.11.1 Un utilisateur final peut choisir One[MD] ID, géré par l'organisme, comme FSA pour accéder aux services fédérés.

2.11.2 Un service client peut fournir des services d'IA à ses préposés internes s'il a été accrédité en tant que FSA de la fédération. Par exemple, un hôpital accrédité comme FSA pour la fédération peut offrir des services d'IA à son personnel lorsqu'il utilise les services fédérés.

2.11.3 Un utilisateur final peut aussi choisir son FSA dans la liste de ceux accrédités par l'organisme. Par exemple, un médecin qui veut utiliser les services fédérés peut passer par un FSA accrédité qui fournira des preuves de son identité à l'organisme en son nom et confirmera qu'il a été authentifié.

2.12 Autorisation

2.12.1 Les fournisseurs d'application sont responsables des autorisations : ce sont eux qui décident de donner l'accès à un utilisateur final aux services fédérés qu'ils offrent et qui déterminent les limites de ce droit.

2.12.2 Conformément aux normes relatives au fournisseur de services d'authentification, les fournisseurs d'application peuvent également définir des règles pour déterminer quels utilisateurs finaux peuvent avoir accès aux services fédérés qu'ils offrent, notamment en fonction du rôle, par exemple en donnant aux utilisateurs finaux un niveau d'accès correspondant au niveau de confidentialité et de séparation des privilèges approprié pour chaque rôle.

2.12.3 L'organisme doit appliquer toutes les règles d'autorisation établies par les fournisseurs d'application.

2.13 Entente légale

2.13.1 Le FSA doit signer toutes les ententes applicables avec l'organisme avant de fournir des services d'IA. Les dispositions applicables de la présente politique doivent se refléter dans ces ententes.

2.14 Suspension, résiliation et révocation

2.14.1 L'organisme peut suspendre, résilier ou révoquer les droits d'un FSA (notamment son accréditation) ou d'un de ses préposés ayant enfreint la présente politique, conformément aux ententes applicables.

2.14.2 L'organisme doit donner un avis de toute suspension, résiliation ou révocation conformément aux conditions des ententes applicables conclues entre l'organisme et le FSA.

2.15 Conformité

2.15.1 Le FSA doit offrir des services d'IA en conformité avec la présente politique et les lois et règlements applicables.

2.15.2 Le FSA doit établir, consigner et appliquer ses propres politiques, normes, processus et procédures nécessaires au respect des normes relatives au fournisseur de services d'authentification.

2.16 Vérification

2.16.1 L'organisme peut mettre en œuvre des processus pour vérifier la conformité à la présente politique.

2.17 Vérification

2.17.1 L'organisme peut vérifier régulièrement la conformité d'un FSA.

2.17.2 L'organisme peut exercer ses droits en vertu de la présente section à différents fins, notamment pour vérifier que le FSA respecte une politique, une norme ou une entente applicable.

2.17.3 Le FSA doit fournir les renseignements, l'accès et l'aide raisonnablement demandés par l'organisme aux fins de vérification. Plus précisément, le FSA doit autoriser l'organisme et ses représentants à entrer dans ses locaux ou à les inspecter, ainsi qu'à consulter tout renseignement, dossier ou document en sa possession ou sous son contrôle, conformément aux ententes applicables conclues entre le FSA et l'organisme.

3 Approbation et administration

3.1 Approbation

3.1.1 La présente politique est publiée sous l'autorité du directeur général.

3.1.2 La présente politique entre en vigueur à la date de son approbation définitive.

3.1.3 L'application de la présente politique commence à la date de son approbation définitive.

3.2 Administration

3.2.1 Le directeur de programme principal, Identification, accès et protection de la vie privée est responsable de l'administration de la présente politique.

3.3 Publication et avis

3.3.1 Une copie de la présente politique et des documents liés doit être consultable en format électronique sur le site Web de l'organisme.

3.3.2 Les changements importants apportés à la présente politique doivent être notifiés aux FSA.

3.4 Interprétation

3.4.1 L'interprétation de la présente politique relève du directeur de programme principal, Identification, accès et protection de la vie privée, de même que la résolution de tout différend à son sujet.

3.4.2 L'interprétation des éléments de la présente politique liés à la sécurité relève du directeur général de la sécurité de l'information et VP des services de sécurité.

3.4.3 L'interprétation des éléments de la présente politique liés à la vie privée relève du directeur général de la protection de la vie privée.

3.4.4 La présente politique doit être interprétée conformément aux autres politiques de cyberSanté Ontario, notamment la *Politique sur la protection de la vie privée et des données*, la *Politique sur la protection des renseignements personnels sur la santé*, la *Politique sur la protection de la vie privée*, *Politique d'utilisation acceptable* et la *Politique de sécurité de l'information*.

3.4.5 Chaque disposition de la présente politique et de toute entente s'y rattachant doit être interprétée conformément aux lois et règlements applicables, notamment :

g) Le Règlement de l'Ontario 43/02, modifié par le Règl. de l'Ont. 339/08, pris en application de la *Loi sur les sociétés en développement;*

h) La *Loi de 2004 sur la protection des renseignements personnels sur la santé* et le Règlement de l'Ontario 329/04, avec ses modifications successives;

i) La *Loi sur l'accès à l'information et la protection de la vie privée.*

3.5 Désignation d'organisations

3.5.1 Lorsque la présente politique fait référence à une entité organisationnelle (division, comité, etc.) ou à un poste, la désignation vise aussi l'entité ou le poste qui lui a succédé le cas échéant.

3.6 Modification

3.6.1 La présente politique peut être revue annuellement et révisée au besoin. Le FSA devrait régulièrement consulter le site Web de l'organisme pour vérifier s'il y a des avis de modification à la présente politique.

3.7 Coordonnées

3.7.1 Il est possible d'obtenir des renseignements sur la présente politique à l'adresse suivante :

ONE[MD] ID Business Solutions

cyberSanté Ontario

415, rue Yonge, Toronto (Ontario)

M5B 2E7

Glossaire

Terme	Définition
Politique d'utilisation acceptable	Politique décrivant les exigences de l'organisme concernant l'utilisation acceptable du système fédéré et des services fédérés, avec ses modifications successives, accessible sur http://www.ehealthontario.on.ca/fr/.
Fournisseur d'application	Organisation fournissant une ou plusieurs applications de santé électroniques offertes en tant que services fédérés au moyen du système fédéré de l'organisme.
Authentification (authentifier)	Processus validant l'identité électronique d'un utilisateur final au regard de son identité réelle.
Autorisation (autoriser)	Processus déterminant si l'accès aux services fédérés est accordé ou refusé en fonction de règles opérationnelles précises établies par les fournisseurs d'application.
Questions d'identification	Questions qu'un utilisateur final doit choisir dans une liste déroulante et auxquelles il doit répondre pendant l'enregistrement, et qui servent ensuite à l'authentifier.
Utilisateur final	Personne autorisée à accéder à un ou plusieurs services fédérés, généralement en tant que représentant d'un service client.
Inscrire ou Inscription	Processus donnant à un utilisateur final accès à un service fédéré en particulier.
Service fédéré	Service de santé, ressource ou renseignement électronique accessible par le système fédéré.
Dépositaire de renseignements sur la santé	S'entend au sens du paragraphe 3(1) de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*.
Système d'accès et de gestion de l'identité (SIGA)	Système informatique, applications et pratiques, politiques et procédures liées au FSA permettant la création, le maintien à jour, la protection, la validation, l'évaluation et la gestion des identités électroniques.
Services d'identité et d'authentification (services d'IA)	Services électroniques fournis par un FSA comprenant la validation de l'identité d'un utilisateur final, la création d'authentifiants et l'envoi de renseignements sur l'authentification.

Terme	Définition
Fournisseur de services d'authentification (FSA)	Personne physique ou morale fournissant des services d'IA au sein de la fédération.
Lois et règlements	*Loi de 2004 sur la protection des renseignements personnels sur la santé* et lois, règlements, codes, ordonnances, décrets, règles, règlements municipaux, jugements d'un tribunal, d'un arbitre, d'une administration, d'un ministère, d'un service ou d'une autorité de réglementation, ou décisions adoptés, promulgués ou rendus par un organisme de réglementation conformément à une autorité ou exigence légale quelconque et, dans tous les cas, applicables, obligatoires et exécutables au Canada ou en Ontario.
Niveau d'assurance	Niveau de confiance nécessaire à l'enregistrement et à l'authentification de l'identité électronique d'un utilisateur final, ou pouvant lui être accordé.
Renseignements personnels sur la santé (RPS)	S'entend au sens du paragraphe 4(1) de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*.
Renseignements personnels (RP)	S'entend au sens du paragraphe 2(1) de la *Loi sur l'accès à l'information et la protection de la vie privée*.
Évaluation de l'impact sur la protection de la vie privée	Évaluation détaillée visant à mesurer les effets d'un nouveau service ou d'un service qui a subi des changements majeurs et à déterminer son impact actuel et potentiel sur la protection des RP et des RPS compris dans le service. L'évaluation mesure la conformité aux lois sur la protection de la vie privée et les répercussions plus larges sur la protection de la vie privée. Elle porte sur les éléments technologiques, les processus opérationnels, la circulation des renseignements personnels, les contrôles de gestion de l'information et les processus de ressources humaines associés à un service pour trouver des moyens de réduire les risques liés à la vie privée relativement à ce service.
Enregistrement (enregistrer)	Processus par lequel une identité électronique unique est établie pour un utilisateur final et est associée à un niveau d'assurance.
Renseignement de nature délicate	Renseignement qui, communiqué sans autorisation, pourrait causer un tort ou entraîner une situation délicate ou un avantage économique injuste, p. ex., une violation de l'obligation de garder le secret ou de l'obligation de protéger la vie privée des personnes en ce qui a trait à leurs RPS ou leurs RP.

Terme	Définition
Service client	Organisation (généralement un dépositaire de renseignements sur la santé) ayant le droit d'accéder à un ou plusieurs services fédérés pour offrir des soins de santé ou aider à la prestation de soins de santé en Ontario.
Évaluation des menaces et des risques (EMR)	Processus conçu pour reconnaître et analyser les menaces et les risques des processus, des programmes, de l'infrastructure et des applications d'ITI, en vue de faire des recommandations sur les protections appropriées contre la perte, la destruction, la modification ou la corruption des biens et des renseignements.
Identifiant	Renseignement électronique composé d'une chaîne de caractères qui identifie précisément un utilisateur final dans un système d'information.

Références et documents connexes

Document	Emplacement
Corporate Policy on Electronic Identification, Authentication and Authorization (IAA) du ministère des Services gouvernementaux de l'Ontario (juillet 2012)	Sur demande
Politique de protection de la vie privée reliée aux responsabilités des tiers fournisseurs de services	Sur demande.
Politique de sécurité de l'information de cyberSanté Ontario	https://www.ehealthontario.on.ca/images/uploads/pages/documents/Information_Security_Policy_Final_FR.pdf
Politique d'utilisation acceptable de cyberSanté Ontario	https://www.ehealthontario.on.ca/images/uploads/pages/documents/Politique.dutilisation.acceptable.pdf
Politique sur la protection de la vie privée de cyberSanté Ontario	https://www.ehealthontario.on.ca/images/uploads/pages/documents/PI_PrivacyPolicy_FR.pdf
Politique sur la protection de la vie privée et des données de cyberSanté Ontario	http://www.ehealthontario.on.ca/images/uploads/pages/documents/Privacy_and_Data_Protection_Policy_FR.pdf

Document	Emplacement
Politique sur la protection des renseignements personnels sur la santé de cyberSanté Ontario	https://www.ehealthontario.on.ca/images/uploads/pages/documents/PHI_PrivacyPolicy_FR.pdf
Politique sur l'Évaluation de l'impact sur la protection de la vie privée	Sur demande.

Les documents suivants, connexes à la politique, peuvent servir à son interprétation.

Document	Emplacement
Règlement de l'Ontario 43/02 modifié par le Règl. de l'Ont. 339/08, pris en application de la *Loi sur les sociétés en développement*	https://www.ontario.ca/fr/lois/loi/90d10
Loi sur l'accès à l'information et la protection de la vie privée	https://www.ontario.ca/fr/lois/loi/90f31
Loi de 2004 sur la protection des renseignements personnels sur la santé	https://www.ontario.ca/fr/lois/loi/04p03