Santé Ontario

Norme sur les fournisseurs d’identités de la fédération d’identité

Version : 1.7

Identificateur du document : 3525

Contrôle des documents

Date de la prochaine révision : Tous les deux ans ou autrement établi par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEUR(S)	DATE D'APPROBATION
V.-p. des Services numériques SO & CISO, planification technologique et sécurité de l'information	7 novembre 2017
Comité ConnexionSécurité	2018-03-26
V.-p. des Services numériques SO & CISO, planification technologique et sécurité de l'information	23 avril 2020
Comité ConnexionSécurité	18 mars 2021

Historique des révisions

Nº DE VERSION	DATE DE LA VERSION	CHANGEMENTS	CHANGÉ PAR
1.1	5 août 2014	Version finale (v.1.1) avec changements apportés par le Bureau de la protection de la vie privée et l'équipe de sécurité	Clara Wong
1.2	30 janvier 2015	Section mise à jour par rapport aux journaux système et à la partie II modifiée pour inclure les politiques de sécurité des DSE	Alan Douthwaite
1.3	22 juin 2015	Définition consolidée et mise à jour de « session d'accès à distance » dans le glossaire.	Clara Wong
1.3	26 juin 2015	Incorporation des commentaires de l'équipe de sécurité.	Clara Wong
1.31	10 novembre 2016	Mise à jour de la fréquence de réinitialisation des mots de passe pour permettre un maximum d'un an comme fréquence de réinitialisation des mots de passe et pour ajuster les registres d'authentification des exigences en matière d'authentification.	Clara Wong
1.40	28 mars 2017	Mise à jour de la norme afin de l'harmoniser avec les politiques de sécurité relatives aux DSE. Fusion de contenu provenant de la politique et des pratiques des autorités locales d'enregistrement et inclusion d'exigences relatives à des audits périodiques des comptes.	Raviteja Addepalli
1.41	7 novembre 2017	Mise à jour pour inclure les exigences d'authentification provinciale à deux facteurs	Marianne White
1.5	16 mars 2018	Mise à jour de la norme afin d'inclure l'accès du patient au DSE et les recommandations du NIST relatives aux mots de passe (NIST 800-63B)	Geovanny Diaz / Ola Edidi
1.6	31 mars 2020	Mettre à jour la norme dans un nouveau modèle et apporter des révisions mineures pour plus de clarté.	John Limarzi

Nº DE VERSION DES CHANGEMENTS	DATE DE LA VERSION CHANGÉ PAR	RÉSUMÉ
1.7	21 janvier 2021	Examen du document avec des modifications mineures, des références mises à jour et le cycle d'examen tous les deux ans.	Ana Fukushima

Norme sur les fournisseurs d'identités de la fédération d'identité

Objet

La présente norme établit les exigences obligatoires minimales applicables aux fournisseurs d'identités (les « FI ») qui seront accrédités pour fournir des services d'identité et d'authentification (« services d'IA ») à la fédération d'identité de Santé Ontario (« fédération »).

Spécifiquement, la présente norme gouverne l'inscription et l'authentification par le FI de l'accès des utilisateurs finaux aux services de santé électroniques, aux applications, aux renseignements et aux ressources (collectivement, les « services fédérés ») qui sont accessibles par l'entremise du système fédéré de Santé Ontario – une infrastructure technologique composée d'applications, de systèmes, de registres, de bases de données, de fichiers, d'applications de portail et d'outils.

Pour en savoir plus sur ce document, veuillez envoyer un courriel à ConnexionSécurité de Santé Ontario à oh- ds_connecting.security@ontariohealth.ca.

Portée

Le présent document s'applique à tous les FI accrédités par Santé Ontario pour fournir des services d'IA à la fédération et à ses représentants

La fédération est un réseau dont les membres fournissent des services fédérés ou y accèdent par l'entremise du système fédéré de Santé Ontario.

Le programme ONE® ID de Santé Ontario est l'opérateur de fédération de la fédération, à savoir un « courtier » qui transmet les demandes d'accès des utilisateurs finaux aux services fédérés, avec les validations d'identité provenant de leurs FI, afin de permettre aux fournisseurs d'applications de prendre des décisions éclairées en matière d'autorisation.

La présente norme et toute convention qui y est associée seront interprétées de manière à être en vigueur et valide en vertu des lois et de la réglementation applicables, y compris :

- La *Loi sur les sociétés de développement* et le *Règlement de l'Ontario 43/02* comme modifié;
- La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) et le *Règlement de l'Ontario 329/04*, comme modifié;
- La *Loi sur l'accès à l'information et la protection de la vie privée* et ses règlements (LAIPVP).

En cas de divergence ou d'écart entre la présente norme et les lois et la réglementation applicables, les lois et la réglementation auront préséance.

Définitions

Politique d'utilisation acceptable : les exigences de Santé Ontario concernant l'utilisation acceptable du système fédéré ou des services fédérés, modifiées de temps à autre.

Fournisseur d'application : un organisme qui fournit une ou plusieurs applications de santé électronique qui peuvent être consommées en tant que services fédérés par l'entremise du système fédéré de Santé Ontario.

Authentifier ou authentification : tout processus permettant de valider l'identité électronique d'un utilisateur final comparativement à son identité dans le monde réel.

Partie faisant autorité : une tierce personne, un organisme ou un processus par l'entremise duquel l'identité réelle d'un utilisateur final peut être corroborée ou qui est acceptée par un FI accrédité pour la corroboration de l'identité réelle d'un utilisateur final (p. ex., un employeur pourrait être une partie faisant autorité pour ses employés).

Autoriser ou autorisation : tout processus permettant de déterminer si l'accès aux services fédérés est accordé ou refusé, en se fondant sur des règles d'affaires précises définies par les fournisseurs d'applications. Services.

Questions de sécurité : questions qu'un utilisateur final doit sélectionner parmi un menu déroulant et auxquelles il doit répondre pendant l'enregistrement, et qui sont utilisées par la suite pour authentifier cet utilisateur final.

Renseignements de base sur l'identité : renseignements minimaux sur l'enregistrement que le FI est tenu de recueillir pour fournir les services d'IA, comme définis de façon plus précise dans la présente norme.

Authentifiants : renseignements qui sont délivrés et associés à un utilisateur final par l'entremise d'un processus d'enregistrement pour faciliter l'authentification. L'authentifiant comprend, notamment, un ID d'utilisateur (ID d'ouverture de session), un mot de passe, un jeton, un certificat de clé publique (certificat PKI), ou toute combinaison de ceux-ci.

Fédération d'identité de Santé Ontario (« fédération ») : réseau informatique dont les membres fournissent des services fédérés ou y accèdent par l'entremise du système fédéré de Santé Ontario.

Utilisateur final : une personne qui est autorisée à accéder à un ou plusieurs services fédérés, généralement en tant que représentant d'un organisme parrainant.

Renseignements sur les utilisateurs finaux : tous les renseignements utilisés pour l'enregistrement de l'utilisateur final, y compris l'ID d'utilisateur et les renseignements de base sur l'identité. Renseignements sur les utilisateurs finaux peuvent comprendre des renseignements personnels.

Inscrire ou inscription : processus consistant à donner à un utilisateur final un accès à certains services fédérés.

Opérateur de la fédération : dans le contexte de la fédération, fait référence à Santé Ontario.

Service fédéré : services de santé électroniques, ressources et renseignements qui sont accessibles par l'entremise du système fédéré.

Système fédéré : l'infrastructure technologique de la fédération, qui comprend des applications, des systèmes, des registres, des bases de données, des fichiers, des applications de portail et des outils.

Dépositaire de renseignements sur la santé : au même sens que dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* [paragraphe 3(1)].

Système d'accès et de gestion de l'identité (IAMS) : le système informatique et les applications du FI, ainsi que les pratiques, les politiques et les procédures connexes pour la création, le maintien, la protection, la validation, les vérifications de l'assertion et la gestion des identités électroniques.

Services d'identité et d'authentification (services d'IA) : les services électroniques fournis par un FI qui comprennent la validation de l'identité de l'utilisateur final, la délivrance d'authentifiants et l'envoi de renseignements sur l'authentification.

Fournisseur d'identités (FI) : une organisation qui fournit des services d'IA au sein de la fédération.

Lois et réglementation : la *Loi de 2004 sur la protection des renseignements personnels sur la santé* et la totalité des statuts, des règlements, des codes, des ordonnances, des décrets, des règles, des règlements municipaux ou des jugements, ordonnances, décisions ou sentences judiciaires, arbitrales, administratifs, ministériels, départementaux ou réglementaires, adoptés ou promulgués par tout organisme de réglementation conformément à toute autorité prescrite par la loi ou toute exigence, et dans tous les cas, applicable et contraignante au Canada ou en Ontario.

Niveau d'assurance : le niveau de confiance qui peut être établi à l'enregistrement ou à l'authentification de l'identité électronique d'un utilisateur final, ou qui est exigé de ceux-ci.

Portails et applications pour les patients : applications (affiliées ou non à un dépositaire de renseignements sur la santé) qui facilitent l'accès du patient au DSE. Ces applications peuvent être :

- Commandées par le fournisseur (le fournisseur facilite la communication avec le patient);
- Fournies directement au patient (le patient a un accès direct au DSE);
- Commandées par le patient (le patient délègue l'accès à un mandataire spécial ou à d'autres délégués, p. ex., un membre de la famille ou un médecin).

Renseignements personnels sur la santé (RPS) : au même sens que dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* [paragraphe 4(1)].2004-87741

Renseignements personnels (RP) : au même sens que dans la *Loi sur l'accès à l'information et la protection de la vie privée* [paragraphe 2(1)].

Violation touchant la protection de la vie privée : une violation touchant la protection de la vie privée comprend :

- Une violation de la LPRPS et de ses règlements, y compris :
    - La collecte, l'utilisation ou la divulgation de RPS de façon non conforme à la LPRPS et à ses règlements;
    - La conservation, le transfert ou l'élimination de RPS de façon non conforme à la LPRPS et à ses règlements;
    - Toute circonstance dans laquelle des RPS sont volés, perdus, utilisés ou divulgués sans autorisation ou consultés par des personnes non autorisées;
    - Toute circonstance dans laquelle des dossiers de RPS font l'objet d'une copie, d'une modification ou d'une élimination non autorisée.
- Une violation de la LAIPVP, y compris :
    - La collecte, l'utilisation ou la divulgation de RP de façon non conforme à la LAIPVP et à ses règlements;
    - La conservation, le transfert ou l'élimination de RP de façon non conforme à la LAIPVP et à ses règlements;

- Toute circonstance dans laquelle des RP sont volés, perdus, utilisés ou divulgués sans autorisation ou consultés par des personnes non autorisées;
- Toute circonstance dans laquelle des dossiers de RP font l'objet d'une copie, d'une modification ou d'une élimination non autorisée;

- Une violation des politiques, des procédures ou des pratiques de protection de la vie privée mises en œuvre par Santé Ontario;
- Une violation des dispositions en matière de protection de la vie privée figurant dans des accords conclus par Santé Ontario avec des intervenants externes et des fournisseurs tiers de services, y compris les dispositions en matière de protection de la vie privée dans les accords avec les mandataires de la LPRPS, les accords relatifs au partage de données, les accords de confidentialité et de non-divulgation et les accords avec les fournisseurs tiers de services retenus par Santé Ontario.

Les violations touchant la protection de la vie privée peuvent être intentionnelles ou accidentelles.

Évaluation de l'impact sur la protection de la vie privée (ÉIPVP) : une évaluation détaillée entreprise afin d'évaluer les répercussions d'un service nouveau ou modifié de façon importante dans le but de déterminer son impact réel et potentiel sur la protection des renseignements personnels et les RPS inclus dans le service. Cette évaluation mesure la conformité à la *Loi sur la protection des renseignements personnels* qui s'applique et les répercussions plus vastes à ce chapitre. L'évaluation aborde tous les éléments techniques, les processus administratifs, le cheminement des renseignements personnels, les contrôles de gestion de l'information et les processus des ressources humaines liés à un service et elle établit des façons dont les risques d'entrave à la vie privée qui y sont liés peuvent être atténués.

Privilège : attribué aux comptes afin de conférer des droits accrus au sein d'un système ou d'une application. Les droits typiques comprennent la capacité de déroger aux contrôles du système ou de l'application, de gérer les comptes des utilisateurs finaux, de modifier ou de gérer le contenu, d'écrire dans les fichiers de système, ou d'effectuer la maintenance.

Enregistrer ou enregistrement : le processus par lequel une identité électronique unique est établie pour un utilisateur final, qui est associé à un niveau d'assurance.

Représentant : dans le cas de Santé Ontario ou d'un participant, les administrateurs, dirigeants, employés, agents, conseillers, sous-traitants ou fournisseurs de services de Santé Ontario ou du participant, ainsi que les administrateurs, dirigeants, employés, agents, sous-traitants ou fournisseurs de services d'une de ces parties.

Authentification fondée sur le risque (AFR) : un système d'authentification qui tient compte du profil de l'utilisateur qui demande l'accès à un système, ainsi que le système auquel cet utilisateur tente d'accéder, qui détermine le profil de risque pour cette tentative d'accès. Le profil de risque est alors utilisé pour déterminer la nature du procédé d'authentification. L'authentification fondée sur le risque permet à l'application de demander des authentifiants supplémentaires à l'utilisateur, mais seulement lorsque le niveau de risque est approprié.

Atteinte à la sécurité : une atteinte à la sécurité comprend :

- Une violation des politiques, des procédures ou des pratiques de sécurité mises en œuvre par Santé Ontario;
- Une violation des dispositions en matière de sécurité figurant dans des accords qui ont été conclus par Santé Ontario avec des intervenants externes et des fournisseurs tiers de services, y compris les dispositions en matière de sécurité dans les accords avec les mandataires de la LPRPS, les accords relatifs au partage de données, les accords de confidentialité et de non-divulgation et les accords avec les fournisseurs tiers de services retenus par Santé Ontario.

Les atteintes à la sécurité peuvent être intentionnelles ou accidentelles.

Renseignements sensibles : renseignements qui causeraient des torts, de l'embarras ou un avantage économique injuste s'ils étaient divulgués sans autorisation, p. ex., violation du devoir de confidentialité ou du devoir de protéger la vie privée des personnes en ce qui concerne leurs RPS ou leurs RP.
Organisme parrainant Un organisme (généralement un dépositaire de renseignements sur la santé) qui a le droit d'accéder à un ou plusieurs services fédérés dans le but de prodiguer des soins de santé ou d'aider à la prestation de soins de santé en Ontario.

Évaluation des menaces et des risques (EMR) : un processus conçu pour identifier et analyser les menaces et les risques pour les processus, les programmes, l'infrastructure et les applications d'ITI, menant à des recommandations concernant des mesures appropriées pour protéger les actifs et l'information contre la perte, le vol, la destruction, la modification ou la corruption.

ID d'utilisateur : renseignements électroniques composés d'une chaîne de caractères qui identifie de façon unique un utilisateur final dans un système d'information.

Devra/Doit : utilisés pour les besoins absolus, c.-à-d. qu'ils ne sont pas facultatifs.

Devrait : utilisé lorsque des raisons valables existent dans certaines circonstances pour ne pas mettre en œuvre l'exigence. Cependant, le responsable de la mise en œuvre doit comprendre les implications avant de choisir une solution différente et doit envisager de mettre en œuvre des contrôles compensatoires.

Peut : l'exigence n'est qu'une recommandation qui est fournie à titre d'exemple de la mise en œuvre et n'est pas destinée à être exhaustive.

Exigences normales

1. Accréditation

1.1. Exigences en matière d'accréditation

Pendant le processus d'accréditation, Santé Ontario examinera le Système d'accès et de gestion de l'identité (SAGI) du FI.

Le FI doit :

- Attester qu'il possède l'autorité, le personnel et les ressources techniques nécessaires pour fournir des services d'IA;
- Aider à l'examen de Santé Ontario en fournissant la documentation ou les autres renseignements requis;
- Informer Santé Ontario de tout changement à son SAGI et à ses politiques, ses pratiques ou ses technologies en matière d'enregistrement ou d'authentification;
- Convenir de respecter la totalité des lois et de la réglementation applicables, comme la LPRPS et, et aider Santé Ontario à les respecter;
- Convenir de respecter la totalité des accords applicables;
- Répondre à toute recommandation faite par Santé Ontario ou ses partenaires de prestation en matière de mesures correctives afin d'aborder toute lacune décelée par ses examens;
- Désigner un ou plusieurs représentants pour assurer la liaison avec Santé Ontario.

1.2. Exemptions

Dans des cas exceptionnels, un FI peut demander à être exempté d'une ou de plusieurs exigences de la présente norme en présentant une demande écrite à Santé Ontario, laquelle doit indiquer les raisons de la demande. Toutes les demandes devront être remises à Santé Ontario avant que le FI fournisse ou continue à fournir des services d'IA. Toutes les demandes devront être examinées et doivent être approuvées par les intervenants appropriés. Santé Ontario devra travailler avec le FI et il peut apporter des recommandations visant à assurer la conformité de celui-ci. De telles recommandations peuvent être assujetties à des conditions, par exemple l'exigence que la conformité soit atteinte à l'intérieur d'une certaine période déterminée par Santé Ontario, conformément à l'accord entre celui-ci et le FI.

Si le FI ne met pas en œuvre les changements recommandés ou ne le fait pas conformément aux conditions énoncées, le cas échéant, voici ce que devra faire Santé Ontario :

- Ne pas accréditer le FI;
- Prendre toute autre mesure conformément à l'accord conclue entre Santé Ontario et le FI.

1.3. Renseignements supplémentaires

Santé Ontario peut recueillir, consigner, utiliser ou divulguer des renseignements à des fins d'enregistrement ou d'inscription à tout service fédéré, par exemple afin de refléter les besoins commerciaux changeants ou de respecter les lois et la réglementation applicables.

1.4. Changements à un SAGI accrédité

Le FI doit informer Santé Ontario de tout changement ultérieur à un SAGI que Santé Ontario avait accrédité, ainsi que de tout changement à ses politiques, pratiques, processus ou technologies d'enregistrement ou d'authentification, conformément aux modalités des accords avec Santé Ontario ou le plus tôt possible, et avant la mise en œuvre de ces changements, si l'approbation de Santé Ontario est requise.

1.5. Reprises d'examens

Santé Ontario peut répéter une partie ou la totalité de l'examen d'accréditation, selon les besoins, pour des raisons qui peuvent inclure leur modification ou une vérification de la conformité avec toute politique ou norme de la fédération.

Santé Ontario devra effectuer ou répéter un examen si, à un moment quelconque, il est informé, il soupçonne ou il détecte de toute autre façon que des changements importants ont été apportés à un SAGI ou aux politiques, pratiques, processus ou technologies d'enregistrement ou d'authentification d'un FI.

1.6. Résiliation

L'utilisation d'un SAGI peut être résiliée par Santé Ontario ou un FI sur remise d'un préavis raisonnable, conformément aux modalités des accords entre ces parties.

2. Suspension et révocation

2.1. Suspension

2.1.1. Règles générales relatives à la suspension

Le FI peut suspendre un compte si :

- Des renseignements sont découverts ou révélés indiquant qu'il est raisonnablement probable que les renseignements, la documentation ou toute autre chose fournie ou faite pour établir l'enregistrement étaient trompeurs, faux ou frauduleux;
- Un utilisateur final n'a pas respecté une politique, une norme ni un accord de la fédération, ou encore les modalités de tout service fédéré;
- La suspension est demandée par un FI ou un utilisateur final pour une raison quelconque (p. ex., congé autorisé).

Veuillez également consulter les exigences relatives à la suspension de comptes lorsque les mots de passe ne sont pas utilisés pendant les périodes indiquées dans la section 4.3.4.

2.1.2. Urgence

Santé Ontario se réserve le droit de suspendre immédiatement l'accès d'un utilisateur final aux services fédérés s'il estime qu'il existe une urgence ou une autre situation qui justifierait une telle mesure, notamment une atteinte aux services fédérés ou à l'intégrité des données qu'ils contiennent.

2.1.3. Réactivation

Un compte qui a été suspendu par le FI en raison de la possibilité de renseignements trompeurs, faux ou frauduleux ne doit pas être utilisé ni réactivé, sauf s'il a été confirmé que les renseignements, la documentation ou les autres faits matériels pertinents sont vrais, exacts et complets.

2.1.4. Documentation

Le FI doit documenter et conserver dans un dossier les raisons des situations suivantes :

- Une suspension;
- Les mesures ayant été prises à ce sujet;
- Les détails concernant toute enquête.

2.2. Révocation

2.2.1. Règles générales relatives à la révocation

Le FI doit révoquer le compte d'un utilisateur final si :

- La personne n'a plus besoin du compte (p. ex., elle est décédée, elle a démissionné ou elle a pris sa retraite);
- Il a été déterminé que le compte en question est un duplicata;
- Il est déterminé que les renseignements, la documentation ou toute autre chose fournie ou faite pour établir l'enregistrement étaient trompeurs, faux ou frauduleux;
- L'identité a été compromise de toute autre façon (p. ex., vol d'identité).

Le FI peut révoquer le compte d'un utilisateur final à la demande de celui-ci pour n'importe quelle raison.

2.2.2. Documentation

Le FI doit documenter et conserver dans un dossier les raisons des situations suivantes :

- Une révocation;
- Les mesures ayant été prises à ce sujet;
- Les détails concernant toute enquête.

3. Enregistrement et droit

3.1. Établissement et maintien des autorités locales d'enregistrement

Chaque DRS doit veiller à ce qu'une personne légalement responsable (PLR) ou son remplaçant identifie au moins une personne pouvant agir comme autorité locale d'enregistrement (ALE) afin de gérer l'inscription de ses agents et des fournisseurs de services électroniques qui ont besoin d'accéder aux services de la fédération.

La PLR doit veiller à ce qu'une nouvelle ALE :

- Dispose du temps et des ressources requises pour s'acquitter des tâches;
- Occupe son poste actuel de façon stable (ne devrait pas être

réaffecté);

- Satisfait aux qualifications relatives au niveau d'assurance 2 (voir la section 3.4) conformément à la Norme sur les fournisseurs d'identités de la fédération d'identité;
- Comprend l'importance du respect des politiques, particulièrement celles sur la protection de la vie privée et la sécurité de l'information.

3.1.1. Modifications

Les modifications au statut d'une ALE approuvée peuvent être fondées sur une demande de la part de la PLR, ou à la discrétion de l'autorité d'enregistrement (AE) si l'on découvre ou soupçonne que l'ALE ne respecte pas les politiques, les procédures ni les accords pertinents. Si le statut d'une ALE est révoqué ou suspendu, la PLR doit soumettre une demande de levée de la suspension avant que le statut puisse être rétabli.

3.1.2. Documentation

Santé Ontario ou son remplaçant, agissant en tant qu'AE, doit conserver une copie de toutes les demandes d'approbation, de suspension ou de révocation du statut d'ALE d'une personne.

3.2. Règles générales relatives à l'enregistrement

Le FI doit valider l'identité des utilisateurs finaux ou de leurs propres représentants pendant l'enregistrement et avant la délivrance d'authentifiants.

Le FI peut déterminer ses propres exigences en matière d'enregistrement pour les utilisateurs finaux. Toutefois, au minimum, le FI doit :

- Valider les renseignements de base sur l'identité, énoncés dans la section 3.2.1;
- S'assurer que les méthodes utilisées permettent d'atteindre le niveau d'assurance requis;
- S'assurer que chaque personne enregistrée :
  - Est âgée d'au moins 16 ans;
  - Présente suffisamment de renseignements pour valider son identité et l'authentifier de façon positive lors de demandes d'accès ultérieures aux services fédérés.

Les utilisateurs finaux doivent présenter deux pièces d'identité, au moins une pièce d'identité avec photo qui représente véritablement l'utilisateur final (voir la section 13 pour obtenir une liste des documents primaires et des documents secondaires qui sont actuellement acceptés pour l'inscription).

Toutefois, cela ne serait pas requis si une interaction directe ou personnelle a déjà eu lieu entre le FI et la personne inscrite pour valider l'identité de cette dernière et si le FI dispose des dossiers nécessaires pour le prouver. De plus, le FI ne doit pas accepter un numéro de carte Santé d'une province quelconque, y compris l'Ontario, ni un numéro d'assurance sociale, pour confirmer l'identité d'une personne pour les produits et les services de Santé Ontario, y compris les services fédérés.

De plus, les exigences en matière d'enregistrement du FI doivent être au moins aussi strictes que celles de ONE®ID. Pour obtenir de plus amples renseignements, veuillez consulter la politique sur ONE® ID de Santé Ontario et les normes associées.

Exigences spéciales pour l'accès des patients aux portails et aux applications qui leur sont dédiés

Validation d'identité

1. Les patients doivent s'inscrire en personne pour obtenir l'accès. Lorsque cela est nécessaire, l'inscription en ligne est permise, mais ne doit être effectuée que par l'entremise d'une application vidéo sécurisée (p. ex., Skype ou WebEx).

2. Dans des circonstances spéciales (p. ex., le patient est à l'extérieur du pays, maladie très grave, distance de déplacement excessive), l'inscription par téléphone est possible. Les utilisateurs doivent répondre correctement au moins aux 6 questions suivantes :

    - Date de naissance;
    - Adresse et code postal;
    - Numéro de la carte Santé;
    - Nom du médecin de famille;
    - Nom de la personne-ressource en cas d'urgence;
    - Nom du plus proche parent.

3. Pour avoir le droit de s'inscrire pour obtenir un compte leur permettant d'accéder à leurs propres dossiers médicaux, les patients doivent être âgés de 14 ans ou plus.

4. Une carte Santé avec photo est une pièce d'identité primaire acceptable pour qu'un patient puisse s'inscrire afin d'avoir accès à un portail ou à une application pour les patients.

Phase de l'inscription à effectuer soi-même

5. Après la validation réussie de l'identité, le patient peut recevoir un NIP à des fins d'auto-inscription. Le NIP :

    - Doit être unique, aléatoire et contenir au moins 6 caractères;
    - Ne nécessiter aucune complexité;
    - N'est valide que pendant 30 jours, après quoi il doit être généré de nouveau.

6. Le portail ou l'application pour les patients doit demander aux patients de fournir au moins les renseignements suivants lors de l'auto-inscription :

    - NIP;
    - Date de naissance;
    - Numéro du dossier médical du patient.

Accès au dossier du patient par un mandataire spécial

7. Lorsqu'un mandataire spécial demande l'accès au dossier d'un patient, la documentation suivante doit être fournie en personne :

    - Un formulaire de délégation dûment rempli et signé fourni par l'équipe de [la solution de DSE];
    - Un document d'identité contenant une photo qui représente véritablement le mandataire spécial (voir la section 13 pour obtenir une liste des documents primaires et des documents secondaires actuellement acceptés pour l'inscription);
    - Une pièce justificative comme un certificat de naissance détaillé, une procuration, un testament et un certificat de décès, ou d'autres documents acceptables remis par un tribunal.

Remarque : Aux fins de vérification, l'application doit permettre de saisir et de stocker les données sur la confirmation de la vérification de l'identité, le fournisseur qui a effectué la vérification et toute pièce justificative.

3.2.1. Renseignements de base sur l'identité

Voici les renseignements de base sur l'identité que le FI doit recueillir afin d'enregistrer un utilisateur final :

- Nom légal (le prénom et le nom de famille de l'utilisateur final sont des champs obligatoires. Le FI peut saisir une valeur nulle comme deuxième prénom de l'utilisateur final);
- Le cas échéant, tous les titres professionnels et les numéros de permis de la personne.

Lorsque l'organisation tire parti du service provincial d'authentification à deux facteurs de ONE ID, le numéro de téléphone de l'utilisateur final doit être consigné et conservé en lieu sûr.

3.3. Renseignements attribués

Pendant l'enregistrement, le FI doit attribuer les renseignements suivants à chaque utilisateur final :

- Un ID unique d'utilisateur (voir ci-dessous);
- Les renseignements requis pour définir et conserver les authentifiants (voir la section 4.2);
- Un niveau d'assurance (c.-à-d. AL1, AL2, AL3) pendant l'enregistrement de chaque utilisateur final correspondant à la rigueur du processus d'enregistrement et à la solidité des preuves fournies pour appuyer l'identité.

Le FI doit s'assurer que les utilisateurs finaux se voient attribuer un ID d'utilisateur qui permette d'identifier de manière unique l'utilisateur final au sein du système fédéré.

Les ID d'utilisateurs doivent avoir un format approuvé par le FI.

REMARQUE : Le format normal des ID d'utilisateurs de ONE®ID pour les particuliers est le suivant :

- [prénom préféré].[nom de famille préféré]@[ONEID.on.ca], p. ex., , John.Doe@ONEID.on.ca

3.4. Niveaux d'assurance

3.4.1. Définitions

Un niveau d'assurance fait référence au niveau de confiance qui peut être donné à une identité prétendue. Le niveau d'assurance requis pour l'accès à un service fédéré est déterminé par Santé Ontario en se fondant, notamment, sur les exigences commerciales des fournisseurs d'applications et sur l'applicabilité et le caractère approprié des exigences en matière d'identité correspondant aux différentes classes d'information, comme indiqué ci-dessous :

Niveau de assurance	Classe d'information	Description du niveau d'assurance
AL1	AL1 convient à des renseignements dont le niveau de sensibilité est « non classifié », et est normalement utilisé pour les renseignements publics et les communications internes, comme les documents internes et les communications non classifiés, qui sont normalement destinés à la communication entre les membres du personnel. Si ces renseignements sont compromis, on peut raisonnablement prévoir qu'ils ne causeront aucun tort ni aucune perte importante aux parties concernées et que la correction ne nécessiterait que des mesures administratives. AL1 est insuffisant lors de l'accès aux renseignements	Une identité non vérifiée : Une personne fournit tous les renseignements relatifs à l'identification, qui sont acceptés tels quels. Aucune assurance n'est requise quant à la véracité de l'identité prétendue.
AL2	AL2 convient à des renseignements dont le niveau de sensibilité est élevé au sein de Santé Ontario et du secteur de la santé, et qui ne sont destinés qu'à des personnes particulières et autorisées. Si ces renseignements sont compromis, on peut raisonnablement prévoir qu'ils causeront des torts ou des pertes financières graves à une ou plusieurs des parties concernées et que la correction nécessiterait des mesures	Une identité vérifiée : La personne est identifiée de façon unique par l'entremise d'un processus d'enregistrement géré et l'identité prétendue est vérifiée au moyen de preuves documentaires auxquelles peuvent s'ajouter des preuves contextuelles dans des
AL3	AL3 convient à des renseignements extrêmement sensibles et de la plus grande valeur au sein de Santé Ontario et du secteur de la santé. Ces renseignements ne sont destinés qu'à des personnes nommées et autorisées. Pour décider si un AL3 est requis, Santé Ontario et les fournisseurs d'applications devront se demander : • Si une situation ou le contexte entourant l'accès à l'information ou l'utilisation de celle-ci nécessite une confirmation de l'identité supérieure au niveau AL2.	Une identité corroborée : La personne est identifiée de façon unique par l'entremise d'un processus d'enregistrement géré et l'identité prétendue est vérifiée et corroborée par des sources faisant autorité (p. ex., l'émetteur des preuves documentaires présentées).

Pour obtenir des exigences supplémentaires relatives aux niveaux d'assurance, le FI devrait consulter la Norme sur le niveau d'assurance en matière d'identité de ONE® ID.

3.4.2. Niveau minimal d'assurance

Santé Ontario exige typiquement que les identités électroniques de tous les utilisateurs finaux atteignent un niveau d'assurance minimal AL2 pour accéder aux services fédérés avec les RP ou les RPS. Par conséquent, le FI doit pouvoir enregistrer et authentifier les utilisateurs finaux à un niveau minimal de AL2.

Lorsqu'un niveau AL3 est requis, le FI doit mettre en œuvre des mesures plus strictes d'enregistrement ou d'authentification, par exemple :

- La définition d'exigences plus strictes relatives aux authentifiants des utilisateurs finaux;
- L'exigence d'un nombre plus important de facteurs d'authentification.

L'accès à certains services fédérés peut exiger que les utilisateurs finaux aient accès à d'autres services fédérés. Lorsque de multiples inscriptions sont requises, le niveau d'assurance de l'utilisateur final doit être égal ou supérieur au niveau d'assurance le plus élevé requis par les services fédérés.

3.5. Exigences relatives au processus pour AL3

Lorsqu'un niveau AL3 est requis, l'identité doit être corroborée. La corroboration de l'identité peut être effectuée par l'un des moyens suivants :

- Une vérification directe par une partie faisant autorité (p. ex., Bureau de l'état civil, Revenu Canada);
- Un professionnel tiers digne de confiance (p. ex., avocat, médecin, membre du clergé).

Elle peut également nécessiter l'échange ou la confirmation de secrets partagés, à savoir des renseignements connus par le corroborateur au sujet d'une personne inscrite potentielle. Par exemple, comme pour les passeports, il peut être demandé à un tiers de confirmer la durée pendant laquelle une personne inscrite potentielle a résidé au Canada de façon ininterrompue.

Parties faisant autorité

Quelques exemples de parties faisant autorité acceptées par Santé Ontario figurent ci-dessous, selon la catégorie d'utilisateurs finaux :

- Pour les employés (p. ex., l'employeur ou une vérification du Centre IPC pendant le processus d'embauche);
- Pour les sociétés (p. ex., un registre d'entreprise);
- Pour les médecins (p. ex., l'Ordre des médecins et chirurgiens);
- Pour les citoyens (p. ex., le Bureau de l'état civil, Citoyenneté et Immigration, Revenu Canada ou Revenu Québec).

En cas de doute, on conseille au FI de consulter Santé Ontario pour déterminer si un tiers serait accepté comme partie faisant autorité aux fins de la corroboration de l'identité.

3.6. Exigences relatives à la documentation

Pour s'enregistrer au niveau AL2 :

- Tous les documents d'identité doivent contenir une photo de l'utilisateur final;
- Les titres professionnels et les numéros de permis (le cas échéant).

Pour s'enregistrer au niveau AL3 :

- Tous les documents d'identité doivent contenir une photo de l'utilisateur final;
- Une copie du document d'identité doit être prise et conservée dans les dossiers;
- Les titres professionnels et les numéros de permis (le cas échéant);
- Les utilisateurs finaux doivent signer leur demande d'enregistrement à la main.

3.7. Création et gestion de comptes

3.7.1. Liste des comptes

Le FI doit conserver une liste des comptes attribués utilisés par chaque utilisateur pour la consommation de services fédérés, y compris le nom de la personne ayant donné l'autorisation. De tels renseignements doivent être mis à la disposition de Santé Ontario sur demande ou pendant une vérification.

3.7.2. Résolution des duplications

Une duplication apparente signifie une correspondance totale de tous les renseignements de base sur l'identité (voir la section 3.2.1). Le FI doit avoir mis en place des processus permettant d'identifier et de résoudre les duplications apparentes, par exemple :

- Renvoyer la question au dépositaire de renseignements sur la santé sous la délégation ou l'autorité duquel l'utilisateur final accède aux services fédérés ou les utilise;
- Confirmer ou demander des renseignements ou des preuves supplémentaires à l'utilisateur final.

3.8. Gestion des droits

3.8.1. Affectation d'un parrain

La personne légalement responsable (PLR) doit identifier une ou plusieurs personnes nommées, un ou plusieurs groupes ou un ou plusieurs rôles ayant l'autorité nécessaire pour agir comme parrain.

3.8.2. Critères en matière de droits

L'accès aux applications et aux services varie selon les critères en matière de droits des propriétaires des données et de l'application.

Certaines applications et données permettent un accès pour la recherche, tandis que d'autres interdisent un tel accès. L'utilisation de certaines applications est réservée exclusivement aux administrateurs techniques. Veuillez consulter le Guide des procédures relatives à la gestion des droits de Santé Ontario pour obtenir les exigences nécessaires pour inscrire les utilisateurs finaux à des applications et des services.

- Si un agent ou un fournisseur de services électroniques a plusieurs rôles, p. ex., il est à la fois un clinicien et un gestionnaire de risques, le parrain peut attribuer à cette personne un accès à [la solution de DSE] afin de recueillir des RPS pour prodiguer ou aider à prodiguer des soins de santé, il doit veiller à ce que l'utilisateur final comprenne ses permissions et ses obligations;
- Une fois l'accès à [la solution de DSE] révoqué, les agents ou les fournisseurs de services électroniques doivent se réinscrire officiellement pour que cet accès soit rétabli.

Exigences relatives à la documentation

- Nom de la personne fournissant l'autorisation qui est le parrain du droit.

3.8.3. Examen des comptes

- Un examen de tous les comptes actifs et des inscriptions aux services fédérés doit être effectué au moins une fois par an;
- L'examen devrait être coordonné avec le parrain autorisé afin de s'assurer que tous les accès par les comptes sont appropriés et à jour;
- Lorsque des écarts sont découverts, des mesures doivent être prises pour corriger les privilèges d'accès;
- Les comptes qui n'ont pas été utilisés depuis 180 jours ou plus doivent être suspendus;
- Pour les portails et les applications pour les patients seulement, le patient doit être informé que son compte a été inactif pendant 365 jours ou plus et que les mesures appropriées seront prises; si le patient ne répond pas, son compte sera suspendu.

3.9. Conservation des renseignements sur l'utilisateur final et changements ultérieurs

Le FI doit conserver dans ses dossiers les renseignements sur l'utilisateur final ainsi que tout changement ultérieur apporté à ces renseignements. Le FI doit conserver de façon permanente ses dossiers de renseignements sur les utilisateurs finaux et doit transférer ces renseignements à Santé Ontario, conformément à l'accord conclue entre le FI et Santé Ontario. La conservation permanente est requise parce qu'il est impossible de déterminer d'avance le moment de la présentation d'une demande d'accès ou d'une enquête sur une brèche. Les renseignements sur les utilisateurs finaux seraient requis dans les deux cas pour associer les comptes aux identités des utilisateurs finaux dans le monde réel.

Ce qui est consigné	**Détails dans le dossier (minimum)**	**Période de conservatio**
Renseignements sur les utilisateurs finaux	• À condition que l'ID d'utilisateur soit un attribut d'ancre (invariable et unique) qui ne change pas avec le temps. S'il ne s'agit pas d'un attribut d'ancre, un autre attribut d'ancre doit également être conservé dans les dossiers. Autrement dit, le dossier doit soit indiquer l'association entre l'identité de l'utilisateur final dans le monde réel et son identité électronique unique et immuable à un moment donné, soit il doit indiquer tous les changements, le cas échéant, à l'identité électronique de l'utilisateur final. • Prénom légal; • Nom de famille légal; • Titres professionnels et numéros de permis; • Niveau d'assurance attribué par le FI (section 3.4); • Numéro de téléphone, lorsque le service provincial d'authentification à deux facteurs est utilisé;	Permanent

Voir également la section 9.2 pour obtenir les exigences de conservation des journaux d'audit.

4. Authentification

4.1. Facteurs d'authentification

L'authentification à un facteur peut être utilisée lors de l'accès au système fédéré à partir d'un environnement sécurisé (p. ex., en utilisant le Réseau privé géré des fournisseurs de services de santé). L'authentification à un facteur ne serait pas appropriée dans toutes les situations, par exemple lorsqu'un niveau AL3 est requis (voir la section 3.4).

Au sein de la fédération, l'authentification doit nécessiter deux facteurs ou plus lors d'un accès aux services fédérés à partir :

- D'Internet ou d'environnements ou endroits non protégés;
- D'une application au point de service, comme un système d'information hospitalier (SIH), si l'utilisateur est éloigné (ailleurs que sur le site);
- Lors d'un accès à une fonction privilégiée, p. ex., administrateur de système.

L'authentification forte nécessite généralement l'utilisation d'un mot de passe fort (voir la section 4.3.2) combiné avec un deuxième facteur. Parmi les technologies utilisées pour le deuxième facteur, on peut citer les suivantes : jetons de sécurité matérielle, rappels, messages SMS, authentification fondée sur le risque, mots de passe à utilisation unique, certificats de machines, biométrie et certificats personnels.

Toutefois, certains services fédérés peuvent nécessiter l'utilisation de types spécifiques de deuxièmes facteurs, p. ex., jetons de sécurité matériels. Dans de tels cas, les types requis de deuxièmes facteurs doivent être mis en œuvre afin d'accéder aux services fédérés en question.

Les principes susmentionnés concernant l'authentification à deux facteurs s'appliquent lors d'un accès aux services fédérés à partir de navigateurs situés sur des appareils électroniques portatifs (p. ex., téléphones intelligents, tablettes).

Exigences spéciales pour les portails et les applications pour les patients

Les exigences en matière d'authentification à plusieurs facteurs continuent à s'appliquer par défaut aux portails et aux applications pour les patients. Pour accommoder les utilisateurs, le patient a la possibilité de désactiver l'authentification à plusieurs facteurs pendant ou après l'inscription.

4.2. Questions de sécurité

Lorsque le FI choisit d'utiliser des questions de sécurité pour l'authentification des utilisateurs finaux, il doit mettre en place des processus et des politiques, par exemple :

- Des exigences concernant la nature ou le nombre de questions permises ou requises;
- Le stockage et la transmission des réponses aux questions de sécurité;
- Les droits ou les obligations des utilisateurs finaux en matière de définition ou de changement de leurs questions de sécurité.

De plus, le SAGI du FI doit veiller à ce que :

- Il soit interdit aux utilisateurs finaux de définir leurs propres questions de sécurité (c.-à-d., ils doivent plutôt les choisir dans une liste prédéfinie);
- Les questions de sécurité soient liées ou affiliées au dossier d'enregistrement de chaque final;
- Interdire aux personnes non autorisées de voir ou de modifier les questions de sécurité des utilisateurs finaux.

À des fins d'authentification pendant une ouverture de session, l'utilisation de questions de sécurité n'est permise que lorsqu'elles sont utilisées conjointement avec :

- Des mécanismes d'authentification fondés sur le risque (p. ex., reconnaissance d'appareils);
- Des tests heuristiques (p. ex., vérifications de l'adresse IP ou de l'identité du navigateur).

Cliquez sur le lient pour obtenir de plus amples renseignements sur la Norme de ONE ID concernant les questions de sécurité

4.3. Gestion des authentifiants

Les authentifiants comprennent les mots de passe, les questions de sécurité et, lorsque le service provincial d'authentification à deux facteurs est utilisé, le numéro de téléphone de l'utilisateur final est considéré comme un authentifiant et doit être géré de façon sécuritaire.

4.3.1. Exigences générales

Le FI est chargé de la mise en œuvre de mesures appropriées en matière de distribution, de maintien et de protection des authentifiants. Le FI doit avoir mis en place une procédure exhaustive de gestion des authentifiants visant à assurer l'utilisation de mots de passe d'une force et d'une complexité suffisantes.

4.3.2. Création de mots de passe

Les exigences suivantes s'appliquent aux mots de passe qui peuvent être utilisés pour authentifier les utilisateurs qui accèdent aux services fédérés.

- Le FI doit rendre obligatoires les mots de passe forts,
  qui doivent :
  - Compter au moins 8 caractères avec un maximum de 64 caractères;
  - Inclure des caractères ou des chiffres provenant d'au moins trois des catégories de complexité suivantes :
    - Au moins une lettre majuscule (de A à Z);
    - Au moins une lettre minuscule (de A à Z);
    - Au moins un chiffre (de 0 à 9);
    - Au moins un caractère non alphanumérique (~!@#$%^&*_-+=‘ |\(){}[]:;"‘<>,.?/).

Pour permettre l'absence de complexité, la vérification en direct des nouveaux mots de passe doit être effectuée et présentée aux utilisateurs pendant la création des mots de passe. La vérification en direct doit effectuer une comparaison avec une liste de mots de passe couramment utilisés : liste noire, dictionnaire, noms d'utilisateurs, noms de services, chaînes séquentielles et mots de passe utilisés lors de brèches précédentes.

- L'historique des mots de passe devrait empêcher la réutilisation des 5 derniers mots de passe;
- Lorsque la technologie le permet, des phrases passe doivent être utilisées (p. ex., 24SussexDrive) au lieu d'un mot de passe qui est généralement plus court;
- Lorsque la technologie le permet, un logiciel qui interdit l'utilisation des schémas reconnaissables doit être utilisé;
- Les mots de passe ne doivent pas inclure la totalité ni une partie du prénom ou du nom de famille de l'utilisateur final, ni tout renseignement personnel facile à obtenir (p. ex., noms des membres de la famille ou des animaux de compagnie, dates de naissance, dates d'anniversaire, la totalité ou une partie d'un ID d'utilisateur ou d'un surnom bien connu);
- Les mots de passe initiaux ou temporaires doivent être uniques, impossibles à deviner et doivent respecter la présente norme concernant la force des mots de passe.

4.3.3. Diffusion des mots de passe

- Un mot de passe initial devrait être généré par un service automatisé et envoyé directement et de façon sécuritaire à l'utilisateur final (p. ex., en personne, par la poste, par téléphone ou par courriel chiffré);
- Le FI doit veiller à ce que les mots de passe soient envoyés aux utilisateurs finaux auxquels ils sont destinés (p. ex., ils doivent être envoyés à une adresse postale ou de courriel confirmée ou à un numéro de téléphone terrestre figurant dans les dossiers);
- Le processus de diffusion des mots de passe doit pouvoir faire l'objet d'un audit;
- Les mots de passe du système ne doivent pas être remis à des employés ni à des entrepreneurs qui n'ont pas signé d'accord de non-divulgation ou qui ne sont pas autorisés à recevoir de tels renseignements.

4.3.4. Administration des authentifiants

- Le FI doit valider l'identité de l'utilisateur final avant de lui remettre des authentifiants lui permettant d'accéder;
- Le FI peut choisir ses méthodes d'authentification, à condition qu'elles soient documentées convenablement, c.-à-d. en prenant contact avec les service de dépannage du FI, qui, après avoir validé l'identité d'un utilisateur final en lui demandant des renseignements que lui seul devrait connaître (p. ex., questions de sécurité), remettront un mot de passe temporaire à l'utilisateur final;
- Les fonctions du service d'assistance qui aident à contrôler l'accès, particulièrement la réinitialisation des authentifiants, ne doivent pas permettre au personnel de voir, d'entendre ni d'apprendre les mots de passe temporaires des utilisateurs finaux;
- Les administrateurs de système qui ont des droits globaux ne doivent pas créer et maintenir les authentifiants des utilisateurs finaux;
- D'anciens authentifiants ne doivent pas être transmis aux utilisateurs finaux;
- L'explication la plus brève possible doit accompagner un refus d'accès lorsqu'un mot de passe ne respecte pas les règles de création ou de modification d'un mot de passe. Le message devrait fournir les coordonnées pour le service de soutien aux utilisateurs finaux. (p. ex., « accès refusé – veuillez prendre contact avec votre administrateur de système »).
- L'accès doit être refusé après cinq tentatives incorrectes consécutives de saisie du mot de passe, pendant au moins 30 minutes. Le FI devra consigner les refus d'accès attribuables à la saisie à cinq reprises consécutives de mots de passe incorrects dans un journal d'audit ou de système, qui doit être examiné et, lorsque la situation le justifie, faire l'objet d'une enquête conformément aux procédures de surveillance et de renvoi au niveau supérieur établies ou approuvées par le FI ou conformément aux modalités des accords entre le FI et Santé Ontario.

4.3.5. Affichage des mots de passe

- Un SAGI ne doit pas afficher ni répéter les caractères d'un mot de passe sur des appareils de sortie ou pendant la saisie, mais ceux-ci peuvent être représentés à l'écran par des caractères spéciaux, comme des astérisques (la visibilité temporaire des mots de passe est permise, selon les limites de la technologie).

4.3.6. Expiration des mots de passe

- Les mots de passe permanents utilisés pour l'accès aux services fédérés doivent expirer 90 jours après leur délivrance ou leur modification. Un maximum d'un an est permis, lorsque le FI respecte les autres contrôles sur les mots de passe décrits dans les politiques de sécurité relatives aux DSE et la norme relative aux FI.

- Après l'expiration d'un mot de passe, l'accès aux services fédérés doit être suspendu jusqu'à la création d'un nouveau mot de passe.

4.3.7. Changement apporté aux authentifiants

- Un FI doit fournir un mécanisme sécuritaire permettant aux utilisateurs finaux de changer, de récupérer ou de réinitialiser leurs authentifiants (p. ex., lorsque l'accès d'un utilisateur final est verrouillé ou celui-ci a oublié son mot de passe).
- Le FI devra exiger que les utilisateurs finaux changent leurs mots de passe initiaux lors de la première utilisation (s'ils n'ont pas été définis par l'utilisateur final).
- Le processus de réinitialisation des authentifiants doit inclure une authentification positive forte du demandeur, afin qu'il puisse être effectué pour tout utilisateur final qui ne peut pas être identifié visuellement (p. ex., demandes par téléphone).

4.3.8. Stockage des mots de passe

- Lorsque des gestionnaires de mot de passe de type Password Locker ou des logiciels de stockage sont mis en œuvre, ces produits doivent exiger des mots de passe forts ainsi qu'une authentification et une transmission sécurisées.
- Le cas échéant, l'ouverture de session automatisée par Password Locker doit être authentifiée par un mot de passe fort (ou la biométrie, si possible).
- Les méthodes non sécurisées d'ouverture de session, comme les macros, les scripts, le « grattage-écran » et les touches de fonction, ne sont pas permises.
- Les navigateurs ne doivent pas être utilisés pour stocker les mots de passe, les remplir automatiquement ni les mettre en mémoire cache, ni encore pour remplir des formulaires.

4.3.9. Authentification téléphonique

- Une authentification provinciale à deux facteurs est offerte dans le cadre de la méthode d'interdiction d'authentification basée sur le risque et, à ce titre, l'authentification téléphonique peut être contournée (si un appareil est reconnu) ou l'utilisateur peut se voir refuser l'accès (s'il s'agit d'une adresse IP ou d'un appareil à risque) en fonction de règles du service.
- Les fournisseurs d'identité sont chargés de déterminer quand un utilisateur a besoin d'une authentification avant d'autoriser l'accès aux DSE. Par exemple, pour les utilisateurs distants plutôt que pour les utilisateurs physiquement dans les murs de l'organisme. Les fournisseurs d'identité doivent utiliser le service d'authentification uniquement lorsque cela est nécessaire pour accéder aux actifs des DES.

4.3.9.1. Gestion de numéros de téléphone

- Les fournisseurs d'identité doivent saisir et conserver en toute sécurité les numéros de téléphone transmis au courtier de la fédération dans le but d'authentifier leurs utilisateurs.
- Les fournisseurs d'identité doivent fournir des numéros de téléphone non partagés ou passer par un standard. Il faut noter qu'au moins dans un premier temps, les extensions, les IVR et les ATS ne seront pas pris en charge
- Les fournisseurs d'identité doivent s'assurer qu'ils sont autorisés à fournir les numéros de téléphone des utilisateurs à des fins d'authentification;

- Les fournisseurs d'identité doivent disposer de mécanismes pour gérer l'exactitude des numéros de téléphone transmis au courtier de la fédération et les mettre à jour.

4.3.9.2. Liste de numéros à ne pas appeler

- Santé Ontario tient à jour une liste de numéros de téléphone « À ne pas appeler » et peut rejeter un numéro de téléphone envoyé par le fournisseur d'identité s'il apparaît sur cette liste.
  - Par exemple, elle peut contenir des numéros de téléphone tels que les numéros 1 900

5. Assertions relatives à l'identité et attributs

Le FI doit veiller à l'exactitude de toutes les assertions et respecter les exigences des spécifications. Le FI assume la responsabilité de toute inexactitude dans les assertions relatives à l'identité qu'il soumet à Santé Ontario ou à d'autres membres de la fédération.

Les ID d'utilisateurs délivrés aux utilisateurs finaux par le FI doivent être envoyés en tant qu'assertions dans le format acceptable (voir les spécifications) à Santé Ontario ou aux autres membres de la fédération, afin d'être saisis dans un dépôt qui sera hébergé et géré par Santé Ontario.

Si le FI est informé d'une assertion d'attributs inexacts, il doit :

- Informer Santé Ontario immédiatement en appelant le service de dépannage de Santé Ontario au 1 866 250-1554, car cela pourrait sous-entendre une atteinte à la vie privée ou à la sécurité;
- Prendre toutes les mesures nécessaires pour corriger l'inexactitude;
- Suivre les recommandations et les instructions de Santé Ontario, si celui-ci en fournit;
- Fournir les avis requis conformément aux modalités des accords applicables.

Lorsque le FI fait des assertions répétées d'attributs inexacts, Santé Ontario peut suspendre l'utilisation du SAGI du FI ou révoquer l'accréditation du FI, si celui-ci ne corrige pas ces déficiences dans la période de correction précisée par Santé Ontario. Santé Ontario devra fournir une aide raisonnable au FI pour corriger ces déficiences.

6. Avis d'acceptation aux utilisateurs finaux

Le FI doit mettre en œuvre des systèmes ou des procédures de contrôle de l'accès qui :

- Fournissent aux utilisateurs finaux une déclaration écrite de leurs droits et responsabilités relatifs à l'accès (p. ex., en présentant des règles relatives aux types de données, de fichiers ou de renseignements auxquels seuls des employés particuliers peuvent accéder);
- Exigent que les utilisateurs finaux indiquent leur acceptation des droits et responsabilités divulgués en matière d'accès.

7. Authentifiants suspendus, expirés ou révoqués

Le FI doit refuser l'authentification des utilisateurs finaux dont les authentifiants sont suspendus, expirés ou révoqués.

8. Transmission d'authentifiants

Le FI doit créer une clé de session afin d'authentifier les transmissions ultérieures de données pendant la même session.

9. Consignation des transactions

9.1. Contenu minimal des journaux d'audit

Le FI doit conserver des journaux d'audit qui contiennent, au minimum, les renseignements suivants :

- Authentification (le journal d'audit doit pouvoir associer l'action effectuée à la personne qui a effectué l'action).
- À condition que l'ID d'utilisateur soit un attribut d'ancre (invariable et unique) qui ne change pas avec le temps. S'il ne s'agit pas d'un attribut d'ancre, un autre attribut d'ancre doit également être conservé dans les dossiers. Autrement dit, le dossier doit soit indiquer l'association entre l'identité de l'utilisateur final dans le monde réel et son identité électronique unique et immuable à un moment donné, soit il doit indiquer tous les changements apportés, le cas échéant, à l'identité électronique de l'utilisateur final.
- Le résultat de l'authentification (réussite/échec);
- Les données relatives à l'authentification (c.-à-d. le type de procédé d'identification utilisé et les détails relatifs à l'authentification);
- La date et l'heure de l'événement.

Lorsqu'il agit comme fournisseur d'un réseau d'information sur la santé (FRIS), Santé Ontario est tenu par la loi de prendre des mesures qui sont raisonnables dans les circonstances pour conserver un dossier électronique de tous les accès à la totalité ou une partie des renseignements personnels sur la santé conservés dans le dossier de santé électronique, et de s'assurer que le dossier permet d'identifier la ou les personnes qui ont accédé aux renseignements et la date, l'heure et l'emplacement de l'accès. Le cas échéant, le FI devra aider Santé Ontario à satisfaire à cette exigence de la réglementation.

9.2. Conservation des journaux d'audit

Le FI doit conserver des journaux d'audit concernant :

- Les événements d'authentification pendant 60 jours en ligne et un minimum de 24 mois dans des archives;
- Les renseignements sur les authentifiants des utilisateurs finaux de façon permanente;
- Des événements relatifs à son SAGI pendant 60 jours en ligne et un total de 24 mois dans des archives. Pour obtenir de plus amples renseignements, veuillez consulter la norme sur la journalisation de sécurité et la surveillance des DSE [le lien doit être mis à jour].

Le FI doit conserver ses journaux d'audit pendant les périodes indiquées dans cette section et doit transférer ces renseignements à Santé Ontario, conformément à l'accord conclue entre le FI et Santé Ontario. Des journaux d'audit seraient requis dans les deux cas pour associer les comptes aux identités des utilisateurs finaux dans le monde réel. Les exigences relatives aux journaux d'audit sont résumées ci-dessous :

Ce qui est consigné	Détails dans le dossier (minimum)	Période de conservation
Authentification Événements	˅ ID d'utilisateur; ˅ Résultat de l'authentification (réussite/échec); ˅ Données relatives à l'authentification; Type d'authentification utilisé, p. ex., authentification fondée sur la connaissance, authentification téléphonique, jeton RSA; ○ Détails de l'authentification, p. ex., l'utilisateur final a réussi l'authentification à la deuxième tentative; ˅ La date et l'heure de l'événement.	60 jours en ligne total de 24 mois dans les archives
Renseignements sur les utilisateurs finaux et les authentifiants	˅ ID d'utilisateur; ˅ Authentifiants des utilisateurs finaux (p. ex., numéros de série des jetons attribués aux utilisateurs finaux); ˅ Prénom légal; ˅ Nom de famille légal; ˅ Titres professionnels et numéros de permis; ˅ Nom de la personne autorisée (c.-à-d. parrain); ˅ Niveau d'assurance attribué par le FI (section 3.4); ˅ Modifications apportées aux champs susmentionnés (y compris les valeurs précédentes et les valeurs actuelles, qui a effectué les changements et à quel moment); ˅ Modifications apportées aux authentifiants (p. ex., réinitialisation des mots de passe, changements aux questions de sécurité ou aux réponses, réinitialisation des NIP des jetons); ○ Mises à jour de l'authentification, y compris la date de mise à jour, qui a mis à jour le numéro de téléphone, les valeurs précédentes et les valeurs actuelles.	Permanent
Événements du SAGI	Tous les événements qui ont lieu dans le SAGI du FI dans le cadre d'un événement d'authentification avec le système fédéré, par exemple :	60 jours en ligne total de 24 mois dans les archives

Ce qui est consigné	Détails dans le dossier (minimum)	Période de conservation
	⌄ Qui a effectué l'accès et à quel moment (p. ex., administrateurs de système, opérateurs et fonctions semblables); ⌄ Ce que cette personne a fait pendant l'accès; ⌄ Les alarmes de surveillance qui ont été déclenchées et à quel moment. Les événements de cette catégorie excluent les éléments qui se trouvent sous « Événements d'authentification » et « Renseignements sur les authentifiants ». Voir : les archives de la politique sur la journalisation de sécurité	et la surveillance des DSE
Assertions relatives à l'identité (réponses SAML envoyées par le FI à l'opérateur de la fédération)	Non requis	Sans objet

9.3. Journalisation ininterrompue

Le FI doit veiller à ce que les journaux d'audit soient opérationnels en tout temps. L'enregistrement, la modification des renseignements sur l'enregistrement et l'authentification ne doivent pas avoir lieu si les journaux d'audit ne fonctionnent pas.

9.4. Sécurisation de l'accès aux journaux d'audit

Le FI doit protéger l'accès aux dossiers et aux journaux d'audit, ainsi qu'aux outils d'audit du système, pour éviter le mauvais usage et la compromission.

Le FI doit mettre en œuvre des mesures de sécurité appropriées pour protéger les dossiers et les journaux d'audit contre l'altération, par exemple :

- Mettre en œuvre des segments de réseau distincts avec des contrôles de l'accès appropriés;
- Envoyer les journaux d'audit à un système de gestion d'information et d'événements de sécurité (GIES).

10. Soutien à la clientèle

10.1. Heures d'ouverture

Les Services aux FI doivent être accessibles 24 heures sur 24, 7 jours sur 7.

Pour les FI utilisant le service provincial d'authentification à deux facteurs, les service de dépannage doivent être équipés pour traiter les appels des utilisateurs concernés et permettre de corriger les problèmes 24 heures sur 24, 7 jours sur 7, par exemple, modifier le numéro de téléphone rapidement et en toute sécurité. Cela peut inclure la mise en œuvre d'un processus de gestion des erreurs approprié pour les erreurs qui se produisent pendant l'authentification, par exemple, un utilisateur ne peut pas terminer l'authentification, car son téléphone ne peut pas obtenir de signal.

Lorsque les FI utilisent la méthode d'appel direct de l'authentification provinciale à deux facteurs, ils doivent être en mesure de surveiller les authentifications OOBA qui ont échoué et de prendre les mesures appropriées si nécessaire.

10.2. Représentants du service à la clientèle

Le FI doit enregistrer et inscrire les employés chargés d'effectuer l'enregistrement et l'authentification des utilisateurs finaux et d'aider les utilisateurs finaux ayant des problèmes liés à ses services d'IA, dans les limites de l'autorité déléguée par le FI.

Au besoin, le FI doit également transférer les appels au service de dépannage de Santé Ontario ou à celui d'autres membres de la fédération, et recevoir des appels en provenant.

10.3. Niveau d'assurance

Les représentants du FI doivent être enregistrés au niveau AL2 ou à un niveau supérieur. Les agents d'enregistrement du FI ne peuvent pas enregistrer les utilisateurs finaux à un niveau d'assurance supérieur à leur propre niveau d'assurance, quel que soit le nombre de documents d'identité présentés par l'utilisateur final ou le type de validation d'identité effectuée.

10.4. Accès aux renseignements

Le FI doit uniquement fournir à ses représentants un accès aux renseignements dont ils ont besoin pour s'acquitter des tâches qui leur sont confiées.

10.5. Authentification des utilisateurs finaux

Le FI doit authentifier les personnes qui prennent contact avec leurs représentants par l'entremise de processus bien définis. Au minimum, le FI doit exiger que les personnes présentent une preuve d'identité équivalente à celle requise pendant l'enregistrement initial ou des renseignements que seul l'utilisateur final devrait connaître, p. ex., des questions de sécurité.

Références

Loi sur les sociétés de développement, L.R.O. 1990, chapitre D.10, Règlement de l'Ontario 43/02, comme modifié en Règlement de l'Ontario 54/05

- *Loi sur l'accès à l'information et la protection de la vie privée*
- NTI-GO 25.13 Exigences en matière de sécurité pour les applications Web (version 1.2), 26 mars 2009
- NTI-GO 25.0 Exigences générales en matière de sécurité
- Politique ministérielle sur l'identification, l'authentification et l'autorisation (IAA) électroniques : ministère des Services gouvernementaux (juillet 2012)
- ONE® ID Challenge Questions Standard
- ONE®ID Identification Information and User Name Standard
- ONE® ID Identity Assurance Standard
- ONE® ID Password Standard
- ONE®ID Policy
- *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS)
- *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chapitre 5 (LPRPDE)

Documents des politiques de sécurité sur les DSE de Santé Ontario

- Politique de sécurité de l'information
- Norme d'utilisation acceptable des données et des technologies de l'information
- Norme sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Procédures de l'autorité locale d'enregistrement
- Norme sur la fédération d'identité
- Norme sur la continuité des activités
- Norme sur la cryptographie
- Norme sur les fournisseurs de services électroniques
- Norme sur la gestion de sécurité de l'information
- Norme sur la gestion de l'information et des éléments d'actif
- Norme sur les réseaux et les opérations
- Norme sur la journalisation de sécurité et la surveillance
- Norme sur le cycle de vie de développement des systèmes
- Norme sur la sécurité matérielle
- Norme sur la gestion des menaces et des risques

Annexe A : Documents d'identité acceptés

Documents d'identité primaires et secondaires pour ONE®ID

Cette section fournit une liste des documents actuellement acceptés par ONE®ID comme documents primaires ou secondaires. Les documents primaires fournissent une preuve plus rigoureuse de l'identité; les documents secondaires sont délivrés par une institution qui a été approuvée par Santé Ontario.

Documents primaires

	Documents d'identité primaires acceptés
1	Certificat de naissance délivré par une province ou un territoire du Canada
2	Certificat canadien de naissance à l'étranger
3	Certificat canadien de statut d'Indien ou de Métis
4	Carte de résident permanent du Canada
5	Certificat de citoyenneté canadienne (document papier ou carte plastifiée, à l'exception des certificats commémoratifs)
6	Certificat de naturalisation (document papier ou carte plastifiée, à l'exception des certificats commémoratifs)
7	Carte de citoyenneté délivrée par un pays étranger où elles existent (p. ex., Mexique, Europe)
8	Confirmation de résidence permanente (IMM 5292)
9	CANPASS (un permis de passage à la frontière dans les régions éloignées qui permet au porteur d'entrer au Canada dans certaines régions éloignées sans se présenter à un point d'entrée, tant que les marchandises importées sont déclarées.)
10	Nexus (un laissez-passer express à la frontière accessible aux personnes à faible risque qui ont réussi une vérification rigoureuse de sécurité au Canada et aux États-Unis, y compris la prise d'empreintes digitales biométriques, une photo et une entrevue personnelle avec des agents d'immigration. Pour conserver ce laissez-passer, une nouvelle demande doit être présentée tous les deux ans).
11	Permis d'enregistrement d'arme à feu
12	Carte de résident permanent (p. ex., carte Maple Leaf)
13	Permis de conduire (y compris un permis de conduire progressif)
14	Passeport canadien (actuellement valide)
15	Passeport valide délivré par un pays étranger
16	Déclaration de naissance vivante d'une province canadienne (copie certifiée)
17	Immigration Canada – Document d'identification des demandeurs d'asile
18	Carte avec photo de l'Ontario
19	Carte Santé de l'Ontario avec photo (seulement pour l'inscription d'un patient à un portail ou à une application pour les patients)

Documents secondaires

Documents d'identité secondaires acceptés	
1	Tout document figurant dans la liste des documents d'identité primaires acceptés, sauf celui inscrit comme document d'identité primaire.
2	Carte de sécurité de la vieillesse
3	Certificat délivré par un ministère ou un organisme gouvernemental (p. ex., mariage, divorce, adoption)
4	Lettre de la section du statut de réfugié
5	Autorisation de travailler au Canada
6	Permis d'un ministre canadien
7	Carte de visa d'immigrant au Canada
8	Autorisation d'étudier au Canada
9	Fiche d'établissement (IMM 1000)
10	Document indiquant l'enregistrement d'un changement légal de nom, accompagné par une preuve de l'utilisation du nom précédent pendant les 12 mois précédents.
11	Document d'enregistrement à jour de l'ordre d'une profession de la santé couverte par la *Loi de 1991 sur les professions de la santé réglementées*. (audiologie et orthophonie, podologie, chiropratique, hygiène dentaire, technologie dentaire, arts dentaires, denturologie, diététique, massothérapie, technologie de laboratoires médicaux, technologie en radiation médicale, médecine, profession de sage-femme, soins infirmiers, ergothérapie, optique, optométrie, pharmacie, physiothérapie, psychologie et thérapie respiratoire)
12	Permis ou carte de membre d'une association professionnelle (pour toute profession de la santé réglementée, y compris les suivantes : Association des sages-femmes de l'Ontario, Denturist Association of Ontario, Nurse Practitioner Association of Ontario, Ontario Association of Medical Radiation Technologists, Ontario Association of Naturopathic Doctors, Ontario Association of Orthodontists, Ontario Association of Speech Language Pathologists and Audiologists, Association chiropratique de l'Ontario, Ontario Dental Association, Ontario Medical Association, Association des infirmières et infirmiers de l'Ontario, Ontario Opticians Association, Ontario Pharmacists' Association, Ontario Physiotherapy Association, Ontario Podiatric Medical Association, Ontario Society of Chiropodists, Ontario Society of Medical Technologists, Association des infirmières et infirmiers autorisés de l'Ontario, Registered Practical Nurses Association of Ontario, ou Respiratory Therapy Society of Ontario)
13	Carte d'employé fédéral, provincial ou municipal
14	Carte actuelle d'employé d'une organisation commanditaire
15	Carte de syndicat
16	Autre carte d'identité fédérale, y compris militaire
17	Carte Plein air du ministère des Richesses naturelles de l'Ontario
18	Carte d'identité d'étudiant
19	Carte BYID (autrefois carte de l'âge de la majorité)
20	Carte avec photo de l'INCA
21	Carte d'identité délivrée en vertu de la *Loi sur les droits des aveugles*
22	Tout document figurant dans la liste des documents d'identité primaires acceptés, sauf celui inscrit comme document d'identité primaire.
23	Carte de sécurité de la vieillesse

Documents non acceptés

Les deux documents suivants ne peuvent pas être utilisés pour la vérification de l'identité pendant le processus d'enregistrement, en raison de règlements juridiques ou statutaires.

Documents d'identité secondaires non acceptés	
1	La carte Santé de l'Ontario avec photo est autorisée pour l'inscription d'un patient aux portails et aux applications pour les patients.
2	Cartes d'assurance sociale