eHealth Ontario
It's working for you.

WEBINAIRE SUR LES DOSSIERS DE SANTÉ ÉLECTRONIQUES (DSE) – UTILISATION SÉCURITAIRE

Ontario
eHealth Ontario

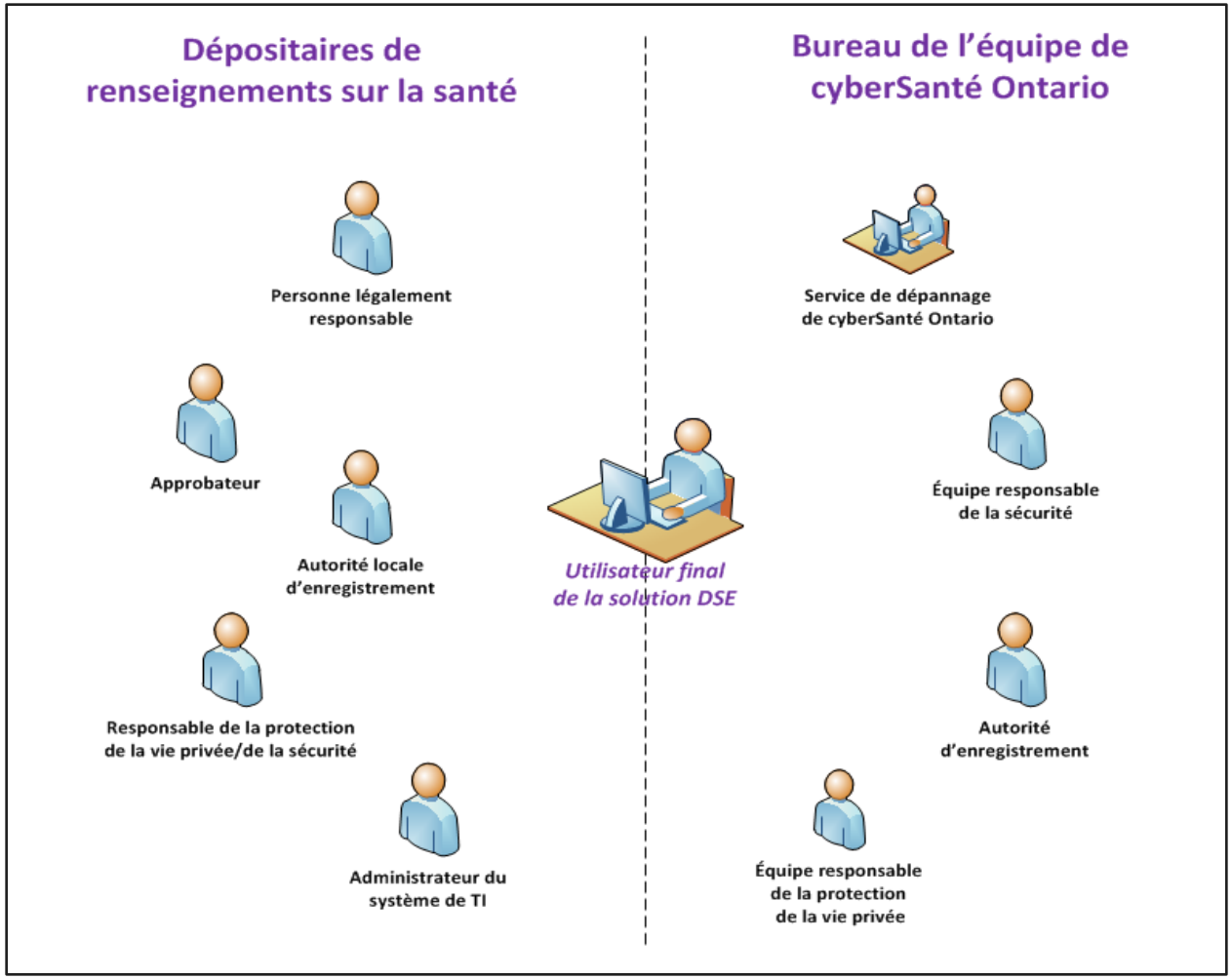
Programme

- Quelles sont les conditions de sécurité à respecter avant d'utiliser la solution DSE?
- Qui sont les principaux intervenants?
- À quoi ressemblera la solution?
- En quoi consiste la structure de gouvernance de la protection de la vie privée et de la sécurité?
- Politiques sur la sécurité des DSE et préparation en vue de leur application
- En quoi consiste l'évaluation de la sécurité?
- Coordonnées
- Annexes

Quelles sont les conditions de sécurité à respecter avant d'utiliser la solution DSE?

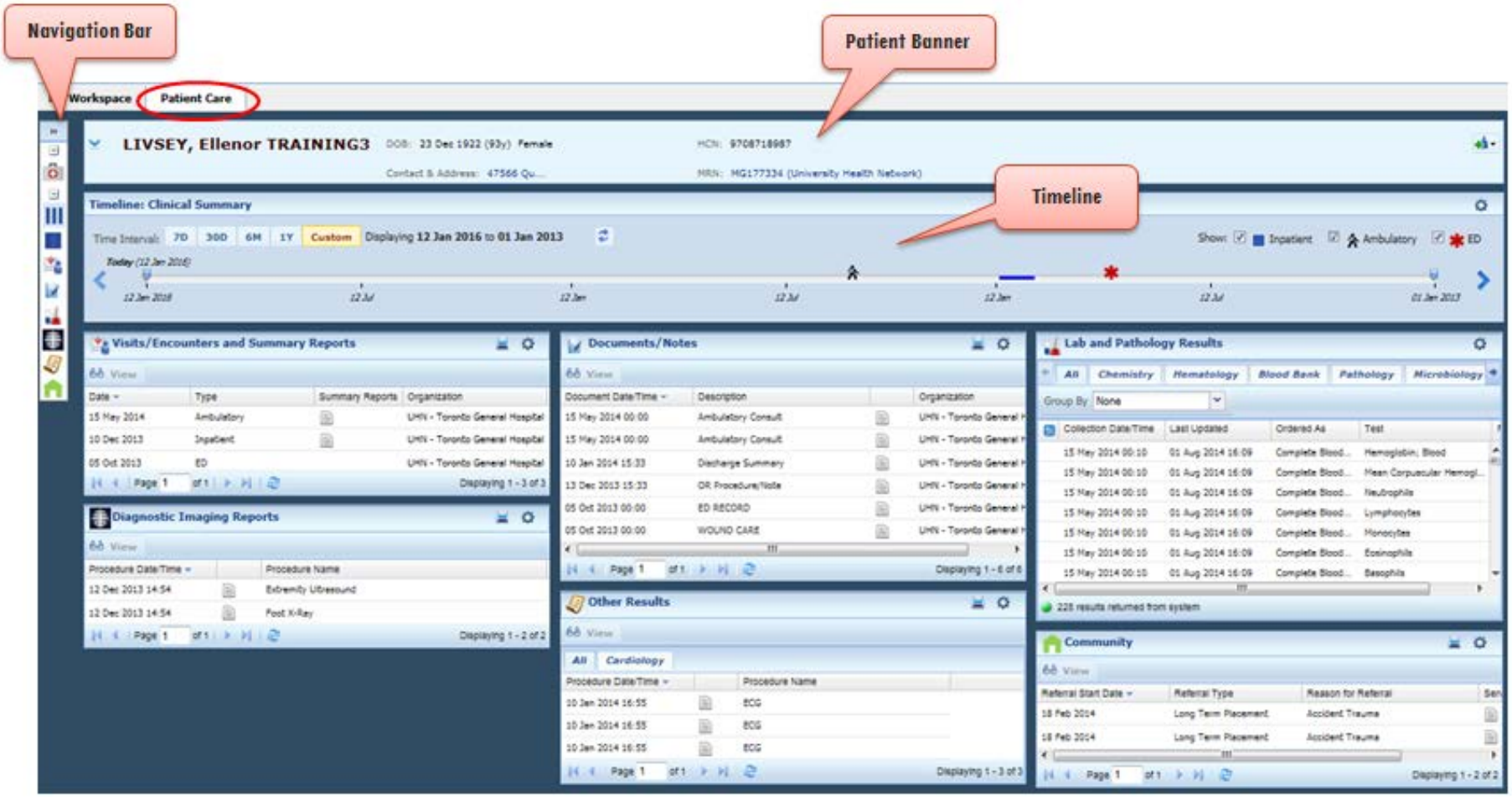
- Visionner ce webinaire.
- Suivre la formation sur la sécurité et la protection de la vie privée.
- Remplir l'évaluation de la sécurité :
  - Examiner le formulaire rempli avec cyberSanté Ontario.
  - Combler les lacunes.
  - Une fois connecté, on vous demandera de remplir une attestation annuelle de conformité (conformément à la politique d'Assurance de DSE.
- Utiliser [la solution DSE]!

Qui sont les principaux intervenants?



Comment peut-on accéder à la solution DSE?

À quoi ressemble la solution?[replace pic]



L'interface de ConnexionOntario est présentée ci-dessus à titre d'exemple.

En quoi consiste la structure de gouvernance de la protection de la vie privée et de la sécurité?

eHealth Ontario
It's working for you.

POLITIQUES SUR LA SÉCURITÉ DES DSE ET PRÉPARATION EN VUE DE LEUR APPLICATION

Ontario
eHealth Ontario

Politiques sur la sécurité des DSE

1. Politique de sécurité de l'information
2. Politique d'utilisation acceptable des données et des technologies de l'information
3. Politique sur les pratiques de l'autorité locale d'enregistrement*
4. Politique sur la cryptographie
5. Politique sur les fournisseurs de services électroniques
6. Politique sur la gestion de l'information et des éléments d'actif
7. Politique sur la gestion des incidents de sécurité de l'information
8. Politique sur les réseaux et les opérations
9. Politique sur la gestion des menaces et des risques

Il faut se conformer aux exigences (« obligatoire » ou « doit/doivent ») avant d'utiliser la solution

Les établissements sont tenus de respecter les politiques sur la sécurité des DSE en vertu des ententes conclues avec cyberSanté Ontario

1. Politique de sécurité de l'information

- **Principes :** Principes généraux de la politique qui dirigent le lecteur vers les différentes sous-politiques.
- **Dérogations aux exigences en matière de sécurité de l'information :** Description du processus de dérogation applicable lorsqu'un organisme ne peut pas se conformer à une exigence.
- **Rôles et responsabilités :** Description du rôle et des responsabilités :
  - du Comité ConnexionSécurité;
  - du Comité stratégique de cyberSanté Ontario;
  - de l'Équipe des opérations en matière de protection de la vie privée et de sécurité des DSE;
  - des dépositaires de renseignements sur la santé.

Objectif : Établir le cadre de gestion de la sécurité de l'information :

- en définissant les principes en matière de sécurité de l'information qui régissent les renseignements personnels sur la santé, la solution DSE et les systèmes d'information ou les technologies de l'information liés à la solution DSE;
- en décrivant les rôles et les responsabilités visant à assurer l'application des principes énoncés dans la politique.

1. Politique de sécurité de l'information

Vos responsabilités

- Élaborer, mettre en œuvre et tenir à jour une politique de sécurité de l'information qui appuie les exigences des politiques de sécurité visant les DSE.
  - Un modèle de politique de sécurité visant les DSE est mis à la disposition des organismes qui n'ont pas encore adopté de politique.
- Désigner un responsable de la sécurité de l'information.
- Veiller à ce que les mandataires et les fournisseurs de services électroniques :
  - connaissent leurs responsabilités en matière de sécurité de l'information;
  - signent un contrat d'utilisateur final avant d'avoir accès à la solution DSE;
  - soient tenus responsables de leurs actions (et subissent des mesures disciplinaires en cas de non-conformité).

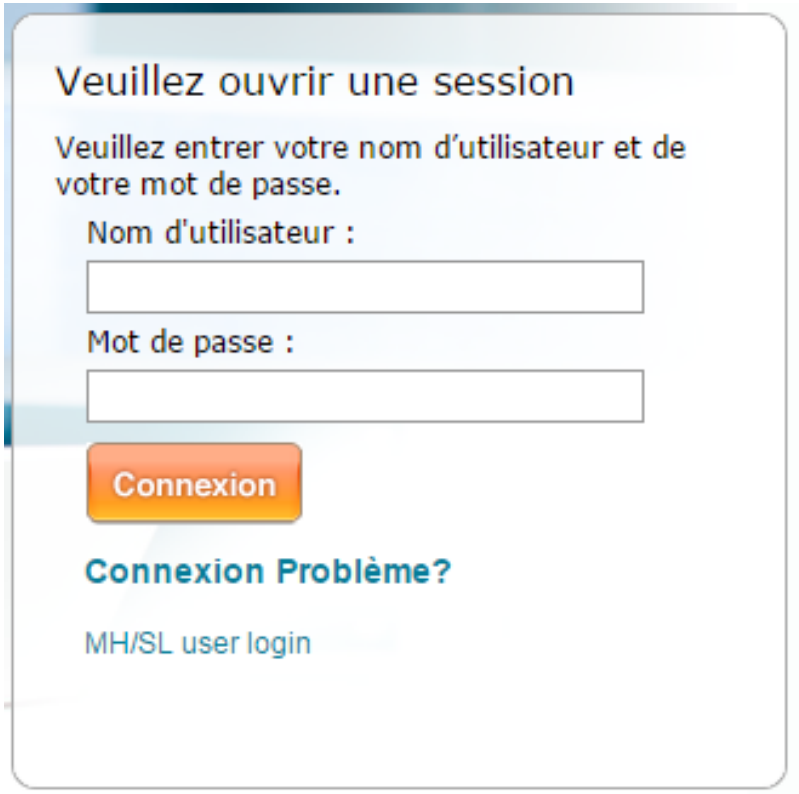
2. Politique d'utilisation acceptable des données et des technologies de l'information

- **Dispositions générales**
  - Utiliser seulement les identifiants assignés.
  - Utiliser seulement les outils approuvés du dépositaire de renseignements sur la santé.
  - Ne jamais prendre les données en photo.
  - Lorsqu'une session est ouverte, verrouiller les postes de travail laissés sans surveillance.
- **Envoi de renseignements personnels sur la santé par courriel**
  - Éviter d'utiliser des comptes de courriel externes pour envoyer des renseignements personnels sur la santé à l'équipe des opérations en matière de protection de la vie privée et de sécurité des DSE ou à cyberSanté Ontario, ou pour les recevoir.
  - Chiffrer les courriels qui comprennent des renseignements personnels sur la santé, et utiliser une solution de transfert de fichiers ou un système de courriel sécuritaires (p. ex., ONE Mail).

Objectif : Définir les exigences en matière d'utilisation visant les personnes qui ont accès à la solution DSE

2. Politique d'utilisation acceptable des données et des technologies de l'information

- **Création et protection des mots de passe**
  - Créer un mot de passe fort.
  - Garder son mot de passe secret et éviter de le noter, ou le ranger dans un endroit sécuritaire.
  - Suivre les directives lorsqu'on soupçonne que le mot de passe a été compromis.



2. Politique d'utilisation acceptable des données et des technologies de l'information

- **Travail à distance**
  - Utiliser une solution d'accès à distance approuvée.
  - Ne jamais utiliser la solution dans un lieu où des personnes non autorisées peuvent voir les renseignements (p. ex., cafés Internet, transport en commun et autres lieux publics).
  - Ne jamais laisser un appareil informatique mobile pouvant se connecter à la solution DSE sans surveillance dans un lieu public.
  - Obliger les utilisateurs à ranger les appareils informatiques mobiles dans le coffre ou à le placer hors de vue lorsqu'ils doivent les laisser dans un véhicule.
  - Veiller à ce que l'emplacement où sont enregistrés les renseignements personnels sur la santé d'un appareil mobile soit doté d'un système de chiffrement.
- **Signalement des incidents liés à la sécurité de l'information**
  - Demander aux utilisateurs de signaler immédiatement les incidents présumés ou confirmés liés à la sécurité de l'information de la solution DSE.

2. Politique d'utilisation acceptable des données et des technologies de l'information

Préparation

- ✓ Examiner la politique interne, le niveau de sensibilisation et d'éducation et les programmes de formation de votre établissement.
- ✓ Cerner les lacunes (p. ex., messages manquants dans vos programmes internes).
- ✓ Envisager d'utiliser les modules de formation sur la protection de la vie privée et la sécurité des DSE pour combler les lacunes sur le plan de la formation.
- ✓ Envisager d'utiliser le modèle de politique sur la sécurité de l'information des DSE pour combler les lacunes de votre politique.

3. Politique sur les pratiques de l'autorité locale d'enregistrement

- **La personne légalement responsable doit désigner :**
  - une ou plusieurs personnes, groupes ou intervenants qui pourront agir à titre d'approbateur (personne qui approuve l'accès);
  - une ou plusieurs personnes qui agiront à titre d'autorité locale d'enregistrement pour gérer l'inscription des mandataires et des fournisseurs de services électroniques.
- Les autorités locales d'enregistrement doivent vérifier l'identité des personnes de votre établissement qui ont besoin d'un accès à la solution DSE, et veiller à ce qu'elles obtiennent les autorisations nécessaires pour utiliser le système.
- Votre établissement pourrait déjà avoir des autorités locales d'enregistrement affectées aux services d'ONE ID ou de ClinicalConnect qui peuvent s'acquitter de ces responsabilités.
- Dans certains organismes, une même personne ou un même groupe peut assumer les rôles d'autorité locale d'enregistrement et d'approbateur.

Objectif : Définir les procédures de désignation des autorités locales d'enregistrement, des mandataires et des fournisseurs de services électroniques en vue de l'utilisation de la solution DSE

N.B. – Les éléments liés à l'enregistrement et à l'inscription énoncés dans les politiques et normes de cyberSanté Ontario au sujet des prestataires qui assurent la gestion fédérée de l'identité que les établissements doivent respecter sont compris dans l'évaluation de sécurité.

3. Politique sur les pratiques de l'autorité locale d'enregistrement

- Il y a deux grands types de portail :
  - les portails des fournisseurs, que les fournisseurs de soins de santé utilisent dans le cadre de la prestation de soins aux patients;
  - les portails d'administration des sites, qui offrent des fonctions dorsales comme la production de rapports sur la protection de la vie privée ou l'administration des comptes des utilisateurs.

Conditions d'accès :

Portails des fournisseurs : Donner l'accès seulement aux personnes qui recueillent des renseignements personnels sur la santé dans le cadre de la prestation de soins de santé, p. ex. :

- Membre d'une profession de la santé réglementée
- Résidents qui donnent des soins aux patients.
- Personnel administratif
- Commis de salle commune

Portails d'administration des sites : Donner l'accès seulement aux personnes qui appuient les fonctions définies et permises, p. ex. :

- Gestion des directives sur le consentement (à venir)
- Production de rapports
- Administration des comptes des utilisateurs sur le portail d'administration

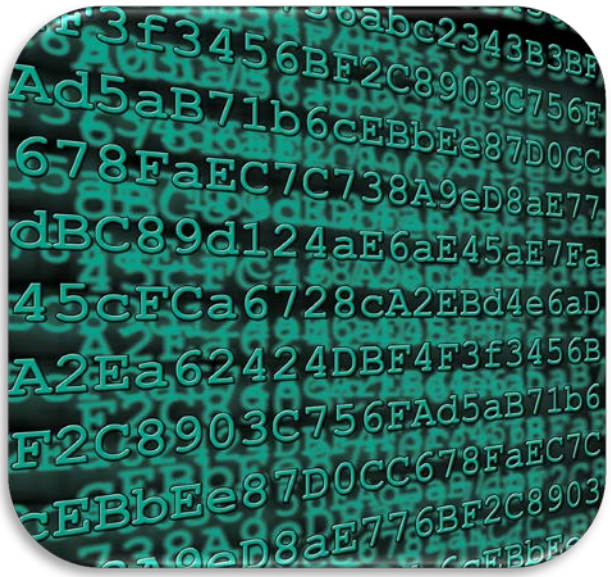
3. Politique sur les pratiques de l'autorité locale d'enregistrement

Préparation

- ✓ Penser aux personnes de votre établissement qui pourraient agir à titre d'approbateur ou d'autorité locale d'enregistrement.
- ✓ Examiner les conditions d'accès et identifier les groupes ou intervenants qui pourraient avoir besoin d'un accès au portail des fournisseurs ou au portail d'administration du site.
- ✓ Examiner les exigences en matière de vérification de l'identité et déterminer si votre établissement les respecte.

4. Politique sur la cryptographie

Cryptographie : Opération par laquelle un texte ordinaire est rendu inintelligible pour quiconque ne possède pas de clé (p. ex., un mot de passe).



- ✓ Utiliser des algorithmes cryptographiques approuvés par le bureau de l'équipe de la solution DSE.
- ✓ Désigner les principaux dépositaires.

Préparation

- ✓ Dresser la liste des solutions de cryptographie utilisées par votre établissement (cryptographie des appareils utilisés pour accéder à la solution DSE).
- ✓ Vérifier si elles sont conformes aux normes.

Objectif : Définir les mesures de contrôle de la sécurité de l'information nécessaires pour implémenter les solutions de chiffrement et les gérer

5. Politique sur les fournisseurs de services électroniques

- Avant de signer un contrat avec de nouveaux fournisseurs de services électroniques qui vous aideront à utiliser [la solution DSE], ceux-ci doivent subir une évaluation pour cerner les risques potentiels liés à la protection de la vie privée et à la sécurité.
- Lors de la création ou du renouvellement d'une entente de service avec un fournisseur de services électroniques, consigner et décrire les systèmes et les services d'information offerts.
- Les fournisseurs de services électroniques doivent appliquer les mesures de contrôle de la sécurité de l'information et de la protection de la vie privée appropriées lorsqu'ils vous offrent des services vous permettant d'utiliser la solution DSE.

Préparation

- ✓ Revoir les ententes de fournisseurs de services électroniques à renouveler, et veiller à ce qu'elles comprennent les exigences de la politique de sécurité des DSE.
- ✓ Les ententes actuelles avec les fournisseurs doivent comprendre les politiques de sécurité des DSE. Lorsque les mesures de la politique de sécurité des DSE sont appliquées par un fournisseur de services électroniques, les organismes doivent l'attester.

Objectif : Définir les exigences en matière de gestion des fournisseurs de services électroniques

6. Politique sur la gestion de l'information et des éléments d'actif

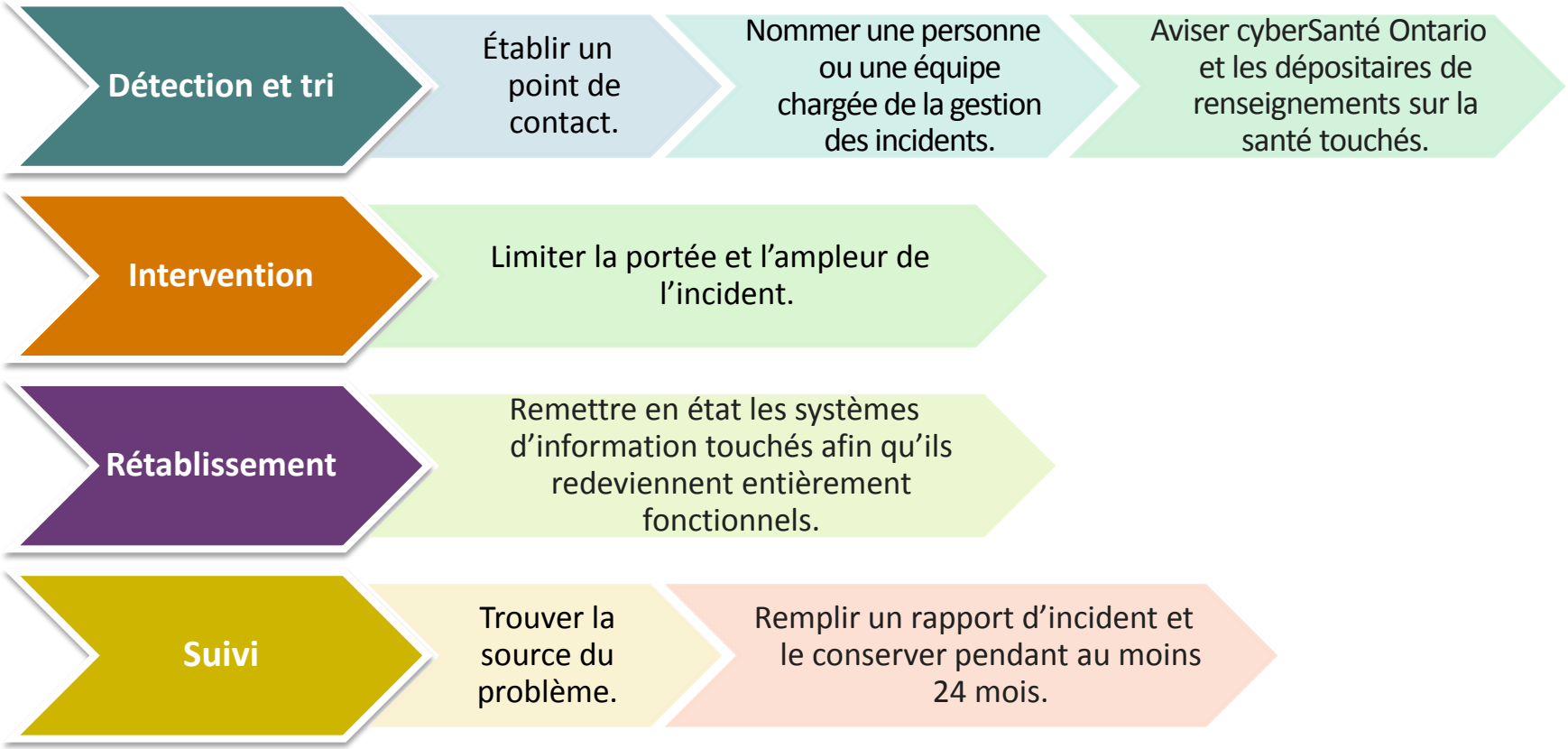
- Les organismes doivent transmettre les renseignements personnels sur la santé de manière sécuritaire (p. ex., à cyberSanté Ontario, au bureau de l'équipe de la solution DSE ou à la solution DSE).
- Appliquer au moyen de courriels sécuritaires, de la cryptographie ou d'un tunnel de réseau privé virtuel.

Préparation

✓Déterminer si votre établissement utilise des méthodes sécuritaires de transmission des renseignements personnels sur la santé.

Objectif : Définir les mesures de contrôle de sécurité de l'information nécessaires pour protéger l'information tout au long de son cycle de vie

7. Politique sur la gestion des incidents de sécurité de l'information



Objectif : Définir les exigences en matière de création d'un processus de gestion des incidents en lien avec la sécurité (« incidents »)

7. Intervenants dans le cadre de la gestion des incidents en lien avec la sécurité

- **Auteur du signalement de l'incident au dépositaire de renseignements sur la santé –** L'auteur constate le problème et le signale au point de contact du dépositaire (responsable de la sécurité ou de la protection de la vie privée).
- **Point de contact du dépositaire –** Les chefs de bureau ou les responsables de la sécurité ou de la protection de la vie privée agissent souvent à titre de point de contact. Le point de contact affecte une équipe d'intervention et de rétablissement en cas d'incident (au besoin) et peut aussi se charger de signaler le problème au service de dépannage de cyberSanté Ontario.
- **Équipe d'intervention et de rétablissement en cas d'incident –** L'équipe est responsable de la détection et du tri, de l'intervention, du rétablissement et du suivi après l'incident. Le responsable de la sécurité ou le fournisseur de services de TI peut occuper ce rôle.

N.B. : Un modèle de gestion des incidents en lien avec la sécurité est mis à la disposition de votre organisme, qui pourra y consigner les incidents et l'utiliser comme rapport final.

7. Processus de gestion des incidents en lien avec la sécurité

Préparation

- ✓ Examiner le processus de gestion des incidents en lien avec la sécurité de votre établissement.
- ✓ Déterminer s'il est possible de l'utiliser pour gérer les incidents liés à la solution DSE.
- ✓ Comprendre qu'il faut signaler les incidents d'ici la fin du prochain jour ouvrable.
- ✓ Utiliser le modèle de signalement des incidents pour consigner les renseignements nécessaires et produire le rapport final.
- ✓ Lorsqu'un incident touche plusieurs dépositaires de renseignements sur la santé, cyberSanté Ontario peut vous aider à le signaler. Il faut l'indiquer lors de l'appel au service de dépannage de cyberSanté Ontario.

8. Politique sur les réseaux et les opérations

- Créer un réseau pour invités (créer un profil différent pour les personnes qui n'utilisent pas la solution DSE).
- Contrôler le trafic du réseau (protéger les données du réseau « interne » des menaces de l'Internet « externe »).
- Examiner la configuration de la passerelle de sécurité au moins une fois par année.
- Installer un logiciel de détection des virus (détection des maliciels et réparation) sur les ordinateurs, les ordinateurs portables, les appareils portatifs, etc.
- Garder les logiciels de détection des maliciels et de réparation à jour.

Préparation

- ✓ Examiner les pratiques actuelles liées au réseau.
- ✓ Déterminer si votre établissement utilise des logiciels de détection des maliciels et de prévention appropriés.

Voir le document Exigences en matière de configuration du système pour plus de renseignements.

Objectif : Définir les exigences liées à l'installation et à l'entretien de réseaux et de systèmes d'information sécuritaires liés à la solution DSE et de ceux des dépositaires qui consultent ou consignent des renseignements sur la santé dans la solution DSE

9. Politique sur la gestion des menaces et des risques

- Fournir des directives sur l'évaluation de la menace et des risques (EMR).
- Donner aux établissements l'autorisation de demander des résumés (résultats) des EMR de la solution DSE.
- Demander aux établissements de restreindre l'accès aux EMR et de les utiliser de manière sécuritaire.

Préparation

✓ Après une demande d'obtention d'une EMR, appliquer des mesures de sécurité et réserver l'accès aux personnes autorisées.

Objectif : Définir les exigences visant les évaluations de la menace et des risques

eHealth Ontario
It's working for you.

EN QUOI CONSISTE L'ÉVALUATION DE LA SÉCURITÉ?

Ontario
eHealth Ontario

Comment dois-je remplir l'évaluation de la sécurité?

Étape 1

Suivre les instructions pour remplir le formulaire d'évaluation de sécurité des DSE.

Étape 2

Soumettre l'évaluation remplie :

- Protéger le document à l'aide d'un mot de passe ***fort,*** et l'***envoyer par courriel*** à l'équipe responsable de la sécurité de ConnexionOntario à l'adresse connecting.security@ehealthontario.on.ca. (Voir les annexes ***Chiffrement d'un document Word 2010*** et ***Création et communication d'un mot de passe fort.***)

Étape 3

Examiner l'évaluation avec l'équipe responsable de la sécurité de ConnexionOntario :

- Examiner les résultats de l'évaluation et préparer ensemble des plans pour résoudre tout problème de conformité.

Exemple de l'outil d'évaluation de la sécurité

Évaluation de sécurité des dossiers de santé électroniques – À l'intention des organismes ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect^MC

Coordonnées

Dénomination sociale* (*p. ex., Équipe de santé familiale de Maville*) :

Formulaire déposé par :	Adresse courriel professionnelle :	Numéro de téléphone :

Instructions

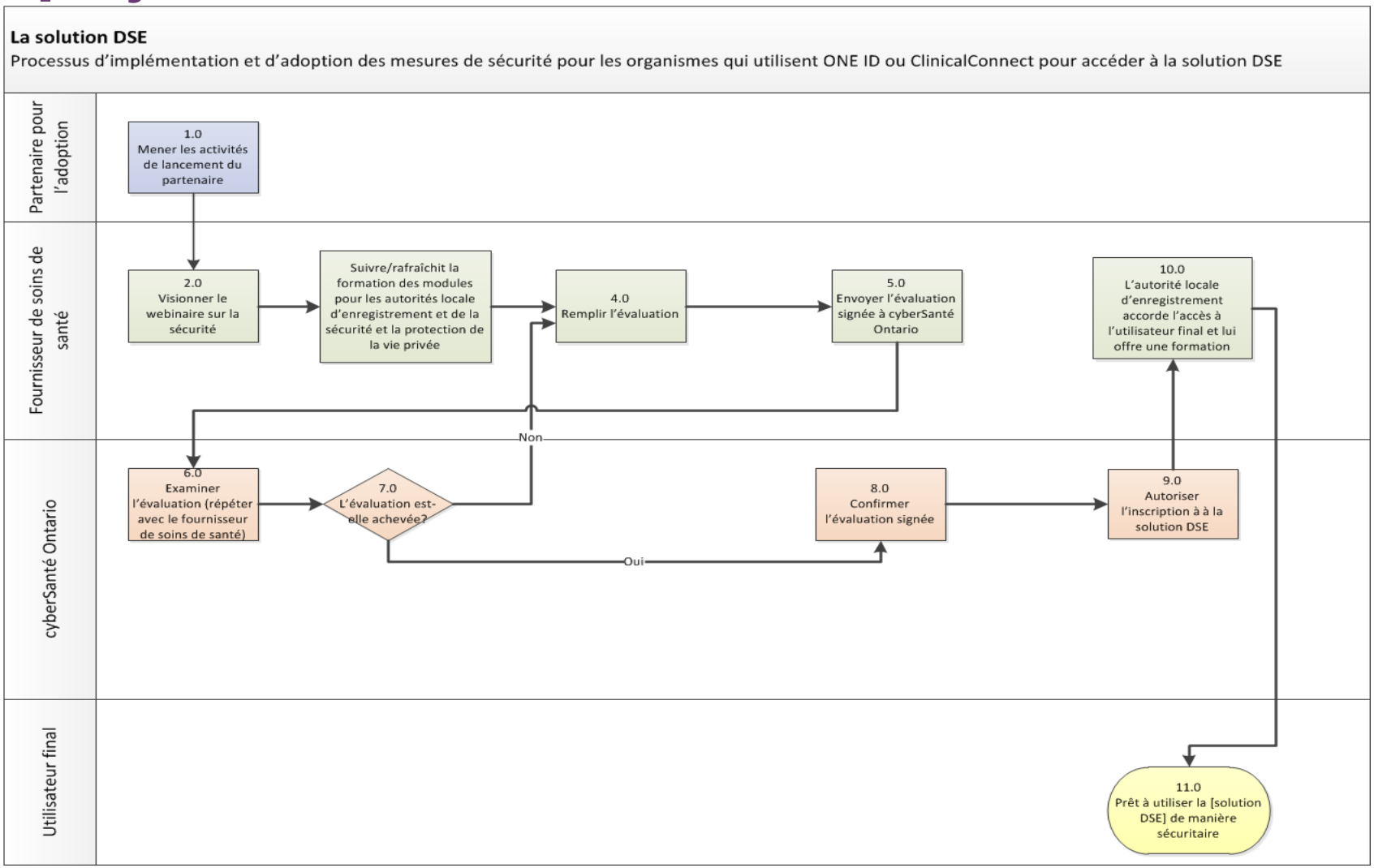
Avant de commencer l'évaluation de sécurité, vous devriez passer en revue le *Webinaire sur les dossiers de santé électroniques (DSE) – Utilisation sécuritaire* à l'intention des organismes ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect. Nous vous conseillons fortement de vous familiariser avec les pratiques de l'autorité locale d'enregistrement et de l'approbateur de votre fournisseur d'identité. Vous voudrez peut-être aussi suivre les formations pertinentes offertes.

1. L'évaluation suivante établit **12** importantes mesures de contrôle qu'un dépositaire de renseignements sur la santé doit respecter. Pour en savoir plus sur chaque exigence, consultez l'*Annexe : Orientation pour la mise en œuvre et portée* ou le *Guide de sécurité des DSE à l'intention des organismes ayant seulement des droits de visualisation qui ont un compte ONE ID ou ClinicalConnect.*
2. Passez en revue les obligations en matière de sécurité de l'ensemble des politiques et analysez attentivement chacune des exigences de la colonne ***Exigences de haut niveau des politiques*** avant d'indiquer si votre organisme y est conforme ou non.

...

1	Mesures de contrôle générales en matière d'utilisation	Passez en revue les mesures de contrôle suivantes et indiquez si vous y êtes conformes ou non. **Les utilisateurs :** a. sont responsables des actions exécutées sur la [solution DSE] à l'aide de leur nom d'utilisateur; {1.2} b. doivent signaler immédiatement les incidents présumés ou constatés relativement à la sécurité de l'information de la [solution DSE] au premier point de contact responsable (p. ex., service de dépannage, responsable de la protection de la vie privée, gestionnaire ou superviseur); {1.31}	Mesures non respectées : Plan(s) de conformité : Échéancier prévu :

Aperçu de l'évaluation de la sécurité des établissements



Comment mon évaluation de sécurité sera-t-elle protégée?

Qui aura accès à mon évaluation?

- L'équipe responsable de la sécurité de ConnexionOntario de cyberSanté Ontario, y compris les analystes et les responsables de la sécurité.
- Les partenaires pour l'adoption peuvent obtenir des renseignements sur la progression de l'évaluation en lien avec l'état de préparation de votre établissement à utiliser la solution.

Comment sera-t-elle communiquée?

- Elle sera chiffrée, protégée par un mot de passe et communiquée seulement aux personnes autorisées.

Sera-t-elle conservée? Si oui, combien de temps?

- Oui, elle sera protégée par des contrôles d'accès et conservée par cyberSanté Ontario pendant 10 ans.

Coordonnées

Ressource	Coordonnées	Demandes
Équipe responsable de la sécurité de ConnexionOntario	connecting.security@ehealthontario.on.ca	Adresse de courriel générale de l'équipe responsable de la sécurité de ConnexionOntario. Utilisez cette adresse pour envoyer votre évaluation remplie ou pour demander de l'aide.
Bureau de la protection de la vie privée de cyberSanté Ontario (généralités)	privacy@ehealthontario.on.ca 1 416 946-4767	Questions générales sur la protection de la vie privée en lien avec les DSE de l'Ontario, les directives de consentement de ConnexionOntario ou du Service commun d'imagerie diagnostique pour les particuliers, demandes d'accès ou de correction, demandes de renseignements, plaintes
Bureau de la protection de la vie privée de cyberSanté Ontario	privacyoperations@ehealthontario.on.ca 1 416 946-4767	Directives de consentement de ConnexionOntario ou du Service commun d'imagerie diagnostique remplies par les responsables de la protection de la vie privée, demandes d'accès ou de correction, demandes de renseignements, plaintes, rapports de vérification, rapports de vérification du Système d'information de laboratoire de l'Ontario, résumé d'un rapport de violation de la vie privée.
Service de dépannage de cyberSanté Ontario	1 866 250-1554 servicedesk@ehealthontario.on.ca	Signalement de toute violation réelle ou présumée de la vie privée et de tout incident en lien avec la sécurité relatifs à ConnexionOntario, le Système d'information de laboratoire de l'Ontario ou le Service commun d'imagerie diagnostique.
Service de dépannage de ConnexionOntario	1 888 802-1967 support@connectinggta.ca	Soutien de premier niveau pour les problèmes techniques liés à l'utilisation de ConnexionOntario.

N'envoyez pas de renseignements personnels sur la santé (p. ex., captures d'écran, objet de la demande) à cyberSanté Ontario par courriel.
Envoyez vos coordonnées, et cyberSanté Ontario communiquera avec vous.

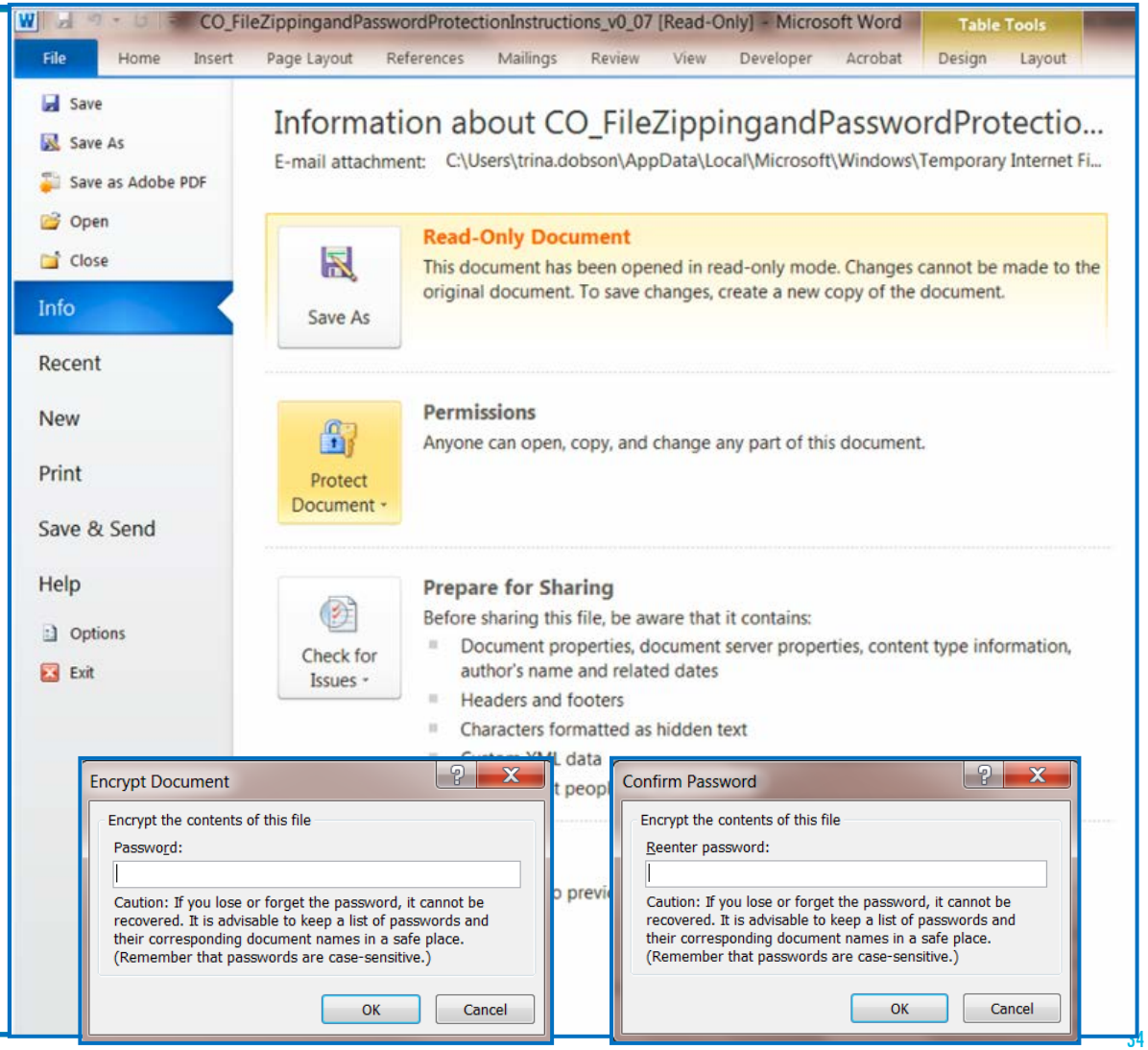
eHealth Ontario
It's working for you.

ANNEXES

Ontario
eHealth Ontario

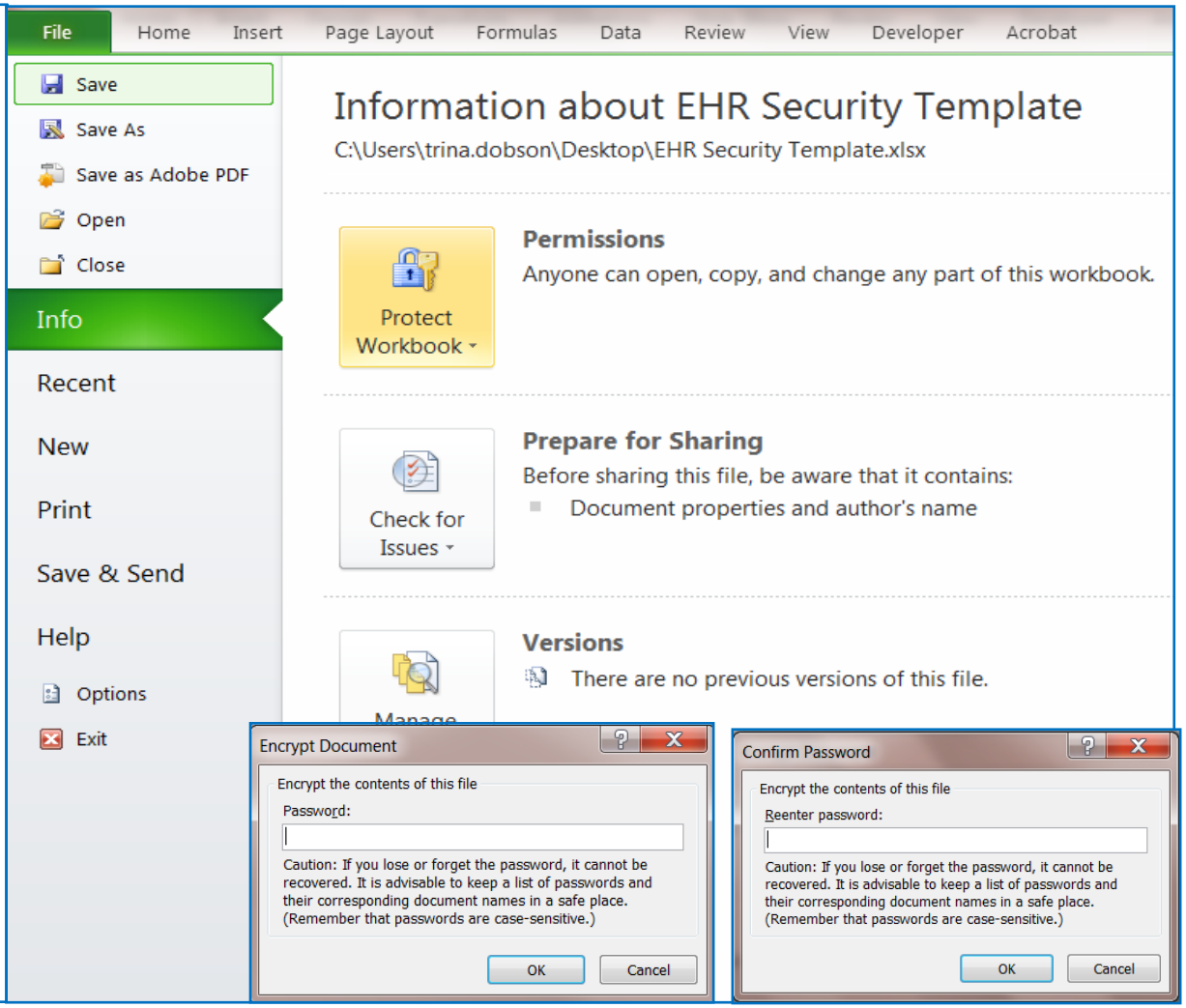
Chiffrement d'un document Microsoft Word 2010

1. Ouvrir le document.
2. Sous l'onglet **Fichier,** cliquer sur **Informations.**
3. Ouvrir le menu déroulant **Protéger le document,** puis cliquer sur **Chiffrer avec mot de passe.**
4. Saisir un mot de passe fort dans le champ de la fenêtre **Chiffrer un document** (voir la diapositive **Création et communication d'un mot de passe fort**).
5. Saisir à nouveau le mot de passe dans le champ de la fenêtre **Confirmer le mot de passe.**



Chiffrement d'un document Microsoft Excel 2010

1. Ouvrir le document.
2. Sous l'onglet **Fichier,** cliquer sur **Informations.**
3. Ouvrir le menu déroulant **Protéger le classeur,** puis cliquer sur **Chiffrer avec mot de passe.**
4. Saisir un mot de passe fort dans le champ de la fenêtre **Chiffrer un document** (voir la diapositive **Création et communication d'un mot de passe fort**).
5. Saisir à nouveau le mot de passe dans le champ de la fenêtre **Confirmer le mot de passe.**



Création et communication d'un mot de passe fort

Il est important de créer un mot de passe **fort** pour protéger les fichiers chiffrés.

- Créer et utiliser des mots de passe différents pour chaque document chiffré.
- Utiliser au moins huit caractères.
- Les mots de passe doivent comprendre au moins trois des quatre types de caractères suivants : lettre majuscule (de A à Z); lettre minuscule (de a à z); chiffre (de 0 à 9); et caractère spécial (p. ex., !, $, #, _, ~, % et ^)
- Exemple d'un mot de passe faible : 1234motdepasse
- Exemple d'un mot de passe fort : C_35t_Un3_B3ll3_J0urné3

Communication du mot de passe

- Une fois le fichier chiffré, il **faut** envoyer le mot de passe au destinataire désigné du fichier à l'aide d'une méthode « hors bande » (p. ex., si le document est envoyé par courriel, transmettre le mot de passe par téléphone, par télécopieur ou par la poste).
- Personnes-ressources désignées de ConnexionOntario : **Ola Edidi (416 324-0838), Razi Farooqui (416 586-4018), Muhammad Usman (416 586-4058).** Vous pouvez aussi nous envoyer le fichier chiffré et vos coordonnées à l'adresse connecting.security@ehealthontario.on.ca.

Quelles sont les conditions de sécurité à respecter avant d'utiliser la solution DSE?

- Suivre la formation sur la sécurité et la protection de la vie privée.
- Remplir l'évaluation de la sécurité :
  - Examiner le formulaire rempli avec cyberSanté Ontario.
  - Combler les lacunes.
  - Une fois connecté, on vous demandera de remplir une attestation annuelle de conformité (conformément à la politique d'Assurance de DSE.

eHealth Ontario
It's working for you.

Merci pour le temps que vous avez consacré aujourd'hui à cette présentation. Si vous avez des questions ou si vous avez besoin d'aide, n'hésitez pas à communiquer avec l'équipe responsable de la sécurité de ConnexionOntario :
connecting.security@ehealthontario.on.ca

Ontario
eHealth Ontario