Ontario
eHealth Ontario

Summary of Security obligations for sites accessing the EHR with ONE ID or ClinicalConnect accounts

This document is intended to provide a summary of the security requirements to connect to the EHR as a Viewer using ONE ID or ClinicalConnect accounts. Applying effective security measures to protect patient data is of critical importance to reduce risk and ensuring public confidence in Ontario's EHR. Visit the Getting Connected Site and start your onboarding process and contact us at connecting.security@ehealthontario.on.ca if you have any questions.

1. Your **Security Officer** (i.e. person in charge of Computer Security) must complete the Security Webinar, which provides an introduction to the security requirements of the EHR and serves as your Security Officer Training. (View the eLearning Module online) or (Download it).
2. Have your **Legally Responsible Person** review the responsibilities of **Local Registration Authorities (LRA)** and **Sponsors** and assign individuals or groups to these roles. Ensure they complete the Privacy and Security training for LRAs and Sponsors. New LRAs must complete ONE ID or ClinicalConnect LRA training.
3. Ensure you have an Information Security Policy that meets the EHR Security Policies or adapt the sample Information security Policy available to you within *Appendix D* of the EHR Security Reference Guide.
4. Ensure your organization is compliant with the behavioral, technical and administrative security requirements:

Behavioral Requirements

Have your Clinical End Users complete the Privacy and Security training for Clinical End Users; this will allow them to understand their requirements and help your organization become compliant.

Technical Requirements

Ensure that:

a. Only Health Information Custodian approved tools are used to connect to the EHR solution.
b. All devices accessing the EHR solution remotely have encryption applied to the Hard Disk.
c. Clinical End Users have passwords applied to Health Information Custodian approved tools used to access the EHR at device logon. These must be at least eight characters long and include at least three of the following:
    - One number
    - One uppercase letter
    - One lowercase letter
    - One special character
d. Ensure that browsers and operating systems are kept up-to date.
e. When communicating PHI to the Program Office, such as during Access and Correction Requests, ensure that the information is encrypted by using features in products such as Microsoft Office, or utilize the ONE Mail service.
f. Implement an antivirus product and ensure it is kept up to date.
g. If you offer guest Wi-Fi, ensure the guest network is segmented from your Office network.

Administrative Requirements

h. Maintain a record of all Electronic Service Providers who support your participation in the EHR and communicate to them the security requirements (e.g. IT Help desk).
i. Maintain and implement a security incident response process and procedure. A security incident management template can be found in *Appendix C* of the EHR Security Reference Guide.