SECURITY REQUIREMENTS FOR SOLE PRACTITIONERS SIGNING THE PHYSICIAN AGREEMENT

Version 1.0 – Jan 14, 2019

1. Definitions

"**EHR Solution**" refers to any of the following: ConnectingOntario Clinical Viewer, ClinicalConnect Viewer, OLIS-EMR, ONE Portal, ONE Access or any other viewer used to access EHR under the custody of eHealth Ontario.

2. Summary

This document contains the minimum security requirements for individual healthcare professionals (the Sole Practitioner) who are health information custodians (HICs), as defined in the *Personal Health Information Protection Act* and who signed the eHealth Ontario ("eHealth") Physician Agreement ("Agreement") and will use ONE ID accounts to view information through the EHR Solution. Unless defined in this document, capitalized words have the meaning set out in the Physician Agreement.

These are the minimum EHR Security Policy and Standards requirements for connecting to the EHR Solution; therefore, Sole Practitioners must be 100% compliant. For more information on each requirement, refer to *EHR Security Reference Guide for Viewing Organizations using ONE ID or ClinicalConnect accounts.*

3. Security Requirements

3.1 Information Security Policy

3.1.1 The Sole Practitioner must develop, implement, and maintain information security policies standards and/or procedures for their organization that uphold the principles of the EHR Security Policy and Standards.

3.2 Acceptable Use of Information and Information Technology

3.2.1 A password must have the following characteristics:

- Contain a minimum of eight characters and include a combination of upper and lower case letters, numbers and/or special characters (e.g. !, $, #, _, ~, %, ^)
- Must not be obvious, easily guessable, or found in a common words dictionary
- Must not use acronyms, birthdays, sequential numbers, names of family members, birthdays, anniversaries or pets
- Never include three consecutive characters (e.g. "AAA")

3.2.2 Password must NEVER be disclosed to anyone or written down.

3.2.3 Change your passwords frequently, at least every 90 days.

3.2.4 On suspicion or confirmation that a user's password has been disclosed or compromised, that user must immediately change their password and notify their internal point of contact identified in the security incident management process.

3.3 Managing devices and procedures used to participate in the EHR Solution

3.3.1 Use only systems/devices and processes acquired for practice by the Sole Practitioner to participate in the EHR Solution, either locally or from a remote location (e.g. practice-related workstations or remote access tools with controls for disk encryption, passwords and antivirus).

3.3.2 All persons must ensure that if PHI resides on a mobile device (e.g. phones, laptops, tablets) that is used to access the EHR Solution and that device is taken offsite, it must be encrypted, or the device itself must utilize full disk encryption.

3.4 Securely communicating with eHealth

3.4.1 The Sole Practitioner must have processes to encrypt the contents of the sensitive email or use approved, secure file transfer solutions such as ONE Mail, that apply encryption of email in transit to other ONE Mail users.

3.5 Electronic Service Providers (ESPs)

3.5.1 The Sole Practitioner must maintain documentation related to support contracts, agreements, and service levels for all providers of electronic services who support their organization's participation in the EHR.

3.5.2 The Sole Practitioner must assess the potential risks posed by all new ESPs prior to entering into a contract, and identify methods for mitigating any identified risks.

3.6 Information Security Incident Management

3.6.1 The Sole Practitioner must establish an internal point of contact (e.g. service desk, office manager, office administrator) to whom actual or suspected incidents are reported and investigated.

3.6.2 Ensure that all users, their agents and ESPs are aware of their responsibility to immediately report actual or suspected security incidents.

3.6.3 Follow the Privacy Breach Management Policy process for incidents that result in a privacy breach.

3.7 Network & Operations

3.7.1 The Sole Practitioner must implement and manage network controls in a way that separates and protects internal computers (your network) from the Internet (perimeter).

For example, if your organization provides "guest Wi-Fi" Internet access to patients, ensure this guest network is separate from the Sole Practitioners internal network, thus preventing unauthorized individuals from accessing the Sole Practitioner's network.

3.8 Malware

3.8.1 The Sole Practitioner must ensure implementation of malware detection on all systems/devices used by the Sole Practitioner to participate in the EHR Solution.

3.8.2 The Sole Practitioners must ensure their malware detection and patches are up-to-date on all systems/devices.

3.9 Physical Security

3.9.1 The Sole Practitioner must ensure that workspaces are protected against unauthorized physical access. Methods for preventing physical access may include, but are not limited to:

- Segmenting public and office work spaces
- Using locked cabinets to store equipment and sensitive information
- Fitting vulnerable doors and windows with locks or bolts
- Installing and monitoring closed-circuit television (CCTV)
- Installing intruder detection systems on external doors and testing accessible windows regularly

3.9.2 The Sole Practitioner must ensure that procedures are in place to address the destruction of information in line with the guidance from the Information Privacy Commissioner.

3.10 Identity Validation and Enrolment Management

The Sole Practitioner (or delegate) is responsible for:

3.10.1 Validating the identity of any of the Sole Practitioner's agents who will have access to EHR Information on the Sole Practitioner's behalf, using a combination of documentary and contextual evidence, including the review of at least one piece of government-issued Photo ID.

3.10.2 Ensuring that all registrants are 16 years of age or older.

3.10.3 Maintaining identity records in alignment with known facts (e.g. update to correct errors; revoke duplicate accounts).