Attestation for Sole Practitioner to Access ClinicalConnect

Date: January 2026

To continue to improve the quality and timeliness of health care decision-making and to enhance access to remote medical consultations, ClinicalConnect makes a broad set of personal health information (PHI) available to Participants who are providing health care or assisting in the provision of health care to individuals whose health records Participants can be viewed in ClinicalConnect. ClinicalConnect is an effective and efficient means to allow health care providers in south west Ontario to view their patients' PHI.

In Ontario, the *Personal Health Information Protection Act, 2004* (PHIPA) governs the processing of PHI. It includes rules regarding the collection, use, and disclosure of PHI by health information custodians (HICs). It is a requirement that every ClinicalConnect Participant be a HIC; as such, every Participant is required to have adequate measures in place to ensure compliance with *PHIPA* while using the portal in the delivery, or assisting in the delivery, of health care to individuals.

The ClinicalConnect Program Office requires that all Sole Practitioner HIC Participant Organizations complete the Sole Practitioner Attestation, including producing a copy of the applicant's *Statement of Protection* from the Canadian Protective Medical Association (CMPA), or *Professional Liability Protection* from the Canadian Nurses Protective Society (CNPS) as outlined in this document. This Attestation and proof of professional liability coverage are key pieces of the application process to access ClinicalConnect.

Part 1: Attestation

In accordance with the requirements of Ontario's *Personal Health Information Protection Act, 2004* (PHIPA) and the ClinicalConnect Policies, I attest the following statements on behalf of the Legal Entity named in Part 1 of the Participation Agreement I previously submitted as part of the application process to access ClinicalConnect. I understand that I may be asked to provide evidence or proof to substantiate these attestations should that be necessary (e.g., in the case of a complaint, audit, or other query).

1. I have established policies and practices (information practices) to ensure the appropriate collection, use, disclosure, modification, retention, destruction and ongoing protection of personal health information (PHI) in accordance with PHIPA and other applicable legislation, and to ensure staff (and other Agents) comply with those policies and practices.

2. I have appointed a privacy contact person in accordance with section 15 of PHIPA.

3. I have posted or made available to the public a written statement of my information practices (e.g., a Privacy Notice or Privacy Statement) that complies with section 16 of PHIPA and states who individuals can contact with privacy inquiries or complaints and how they can obtain access to or request correction of a record of PHI.

4. I have established policies and/or practices for managing complaints or challenges to my Legal Entity's compliance with PHIPA, its own policies or privacy best practices.

5. I have established policies and practices regarding the type of consent required to collect, use and disclose PHI for different purposes (e.g., that (assumed) implied consent applies in

the context of providing or supporting health care to patients and the use of shared electronic health records).

6. I have established policies and/or practices regarding the role that a substitute decision-maker (SDM) plays when a patient is not capable with respect to making their own decisions regarding the collection, use or disclosure of their PHI.

7. I have established policies and/or practices for managing interactions with an estate trustee after a patient dies.

8. I have established policies and practices for managing a patient's right to place a consent directive on the access and use of their PHI for health care purposes; the need to verify the identity of the individual who requests that a consent directive be applied or modified; and the need to document verbal directions or retain written instructions in relation to a patient's consent directives.

9. I have policies and/or practices regarding what to discuss with a patient or substitute decision-maker who requests the implementation of a consent directive. For example: the consent directive only applies to PHI the patient has already provided and not to PHI which the patient might provide in the future; PHIPA permits certain collections, uses, and disclosures of the PHI despite the consent directive; health care providers may override the consent directive in certain circumstances, such as where there is reasonable grounds to believe that it is necessary to eliminate or reduce a significant risk of serious bodily harm; that the consent directive may result in delays in receiving health care or a reduced quality of care due to a health care provider's lacking complete information about the patient; and a health care provider's refusal to offer non-emergency care.

10. I have established practices for managing the requirement, when disclosing a record of PHI that is subject to a consent directive, to notify the recipient(s) that the record is missing PHI due to a consent directive.

11. I have established practices for managing the circumstances in which health care providers may override a consent directive (e.g., with express consent of the patient or their substitute decision-maker; or where there is reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm).

12. I have established practices for managing the steps that must be taken when a consent directive has been overridden (e.g., documenting the reason for the override and who provided consent).

13. I have established policies and practices to ensure PHI in verbal, written or electronic forms is only collected, used and disclosed for the purposes of providing or supporting health care within the limits of each staff member's job role, and that these limitations also apply to printed hard copies of PHI.

14. I have established practices to ensure staff (and other Agents) understand, agree to, and comply with privacy and security training requirements (e.g., at the commencement of employment/contract and annually thereafter).

15. I have established policies and/or practices to ensure staff (and other Agents) comply with privacy and security requirements for network resources, desktop computers, mobile computing devices and wireless data transmission including encryption, minimizing data

storage, screen timeout and locking functions, and device storage in a secure location accessible only by the user. (Mobile computing device is defined as any reasonably portable electronic device capable of storing or transmitting data, including the following: smart phones, laptops, tablets, personal digital assistants, USB memory sticks, portable hard disk or solid state data storage devices, numeric, alpha-numeric and two-way pagers, medical or other electronic devices that contain hard disk or solid state data memory and which can be plugged in a USB port, CD/DVD disks or CD/DVD 'burners').

16. I have established policies and practices regarding requirements for the use of passwords and appropriate levels of password protection based on the security risk inclusive of mobile computing devices and for maintaining the security of passwords.

17. I have established policies and/or practices regarding requirements for physical controls of devices or equipment that can be used for storage of electronic PHI.

18. I have established policies and/or practices to ensure staff (and other Agents) comply with separate/additional safeguarding and handling requirements when accessing PHI remotely.

19. I have established policies and/or practices regarding the identification, management, and reporting of privacy breaches and to ensure compliance with processes required under PHIPA in response to privacy breaches. (e.g., Information and Privacy Commissioner of Ontario's (IPC)'s Reference Document: What to do When Faced with a Privacy Breach – Guidelines for the Health Sector).

20. I have established policies and/or practices with respect to auditing access to PHI by employees (and other Agents). (e.g. IPC Reference Document: Detecting and Deterring Unauthorized Access to Personal Health Information)

21. I have established policies and/or practices to ensure third parties understand, agree to, and comply with privacy and security requirements (e.g., IPC Reference Document: Detecting and Deterring Unauthorized Access to Personal Health Information).

22. I have established practices to ensure staff and volunteers (and other Agents) understand that privacy responsibilities continue to apply even after employment/affiliation ends (or a contract terminates).

23. I have established practices to ensure that staff (and other Agents) understand that sanctions for inappropriate use of PHI include reporting to regulatory colleges and the IPC in accordance with requirements under PHIPA, and may also include termination of employment or other contract.

24. I have established practices to ensure staff (and other Agents) use only trusted secure devices to access PHI via web-based systems (e.g., ClinicalConnect). (This means the devices are in a known state running up-to-date patches and anti-virus software. Patches include the operating system, internet browser, and internet browser add-ons such as Java and Adobe Flash. Public devices found in hotels and libraries are deemed to be non-trusted devices.)

25. I have established practices to comply with secure destruction requirements for PHI (e.g., IPC Order HO-001; the IPC Reference Document: Secure Destruction of Personal Information also provides suggested best practices for the destruction of personal information), including the maintenance and indefinite retention of a PHI destruction log.

26. I have established policies and/or practices ensuring a patient's right to access their PHI and for managing the steps taken in response to a patient's request to access their PHI, including verifying the identity of the individual making the request.

27. I have established policies and/or practices to ensure PHI is retained for as long as necessary to allow individuals to exhaust any recourse under PHIPA they may have with respect to a request for access to PHI, as well as other legislated retention requirements according to CPSO's Medical Records Management Policy, or CNO's Practice Standard: Documentation).

28. I have established policies and/or practices regarding the fees that are charged for fulfilling requests for access and disclosure of PHI.

29. I have established policies and/or practices for managing the requirement for a patient to access their PHI before requesting a correction to that PHI.

30. I have established policies and/or practices for managing the correction of a record of PHI (while maintaining the original record) if the patient demonstrates that the record is incorrect or incomplete and provides the information necessary to correct the record.

31. I have established policies and/or practices for managing the process to permit a patient to issue a statement of disagreement with respect to a decision not to fulfill a PHI correction request and to ensure the statement of disagreement is shared with a recipient organization when the record in question is disclosed.

32. I have established policies and/or practices for managing requests for access to PHI in the form of a subpoena, summons or warrant; police acting on behalf of a coroner; and other related legal contexts.

Part 2: Licence Information - * indicates mandatory field

Date of Registration to Practice in Ontario*	
CPSO or CNO Registration Number*	

Part 3: Professional Liability Coverage - * indicates mandatory field

Canadian Medical Protective Association (CMPA), or Canadian Nurses Protective Society (CNPS) Membership Number*	

✓ ***Provide copy of your Statement of Protection from the CMPA (physicians), or Professional Liability Protection from the CNPS (nurse practitioners), valid for current year.***

Sole Practitioner Attestation - * indicates mandatory field
I confirm that the information provided is to the best of my knowledge true, and free from error.

Sole Practitioner Full Name (please print/type)*	
CPSO or CNO Registration Number*	
Sole Practitioner Signature*	
Date*	

Any questions regarding this Attestation can be directed to access@clinicalconnect.ca.

This Attestation includes the following pieces:

1. This Attestation Form
2. Copy of Statement of Protection from the CMPA or Professional Liability Protection from the CNPS

And must be sent together, by email or fax, to the ClinicalConnect Program Office:

Email: access@clinicalconnect.ca
Fax: 905-577-8260