Attestation for Sole Practitioner (Physician) to Access ClinicalConnect

Dated: June 4, 2021

Background: *The Personal Health Information Protection Act* (PHIPA) came into force in November 2004. PHIPA pertains to the collection, use and disclosure of Personal Health Information (PHI) by organizations and individuals providing health care in Ontario. PHIPA sets out a number of responsibilities and requirements for health care providers in the delivery of health care in Ontario, and in particular the responsibilities of Health Information Custodians (HICs). PHIPA defines HICs and sets out the requirements for individuals who are considered to be HICs. PHIPA also defines the role of an Agent who is a person who acts for, or on behalf of a HIC, in respect of PHI for the purposes of the HIC.

The original ClinicalConnect Data Sharing Agreement was put in place on January 7, 2010. Since then, Ontario's digital landscape has significantly evolved, including legislative changes with respect to PHIPA. Amendments to PHIPA through Bill 119, the *Health Information Protection Act* (HIPA), came into force on June 3, 2016, with the exception of Part V.1 which specifically addresses the Provincial Electronic Health Record. The HIPA provisions in force at this time apply to all PHI accessed through electronic means, not only PHI viewable through ClinicalConnect.

The Canadian Medical Protection Association *Medical-Legal Handbook for Physicians in Canada* (p.30) states that in addition to long-standing obligations of confidentiality in the provision of patient care, a physician must also comply with obligations established under privacy legislation.

The College of Physicians and Surgeons of Ontario's Policy Statement #8-05 (*Confidentiality of Personal Health Information*) (p.2) states that the College expects physicians to follow the regulations under the *Medicine Act, 1991*, and the rules under PHIPA when collecting, using or disclosing PHI.

The OntarioMD Privacy and Security Guide and Workbook (p.4) states: To comply with PHIPA, practices must:[1]

1. Designate a privacy contact person,
2. Identify the purposes for collection, use and disclosure of PHI,
3. Only collect, use and disclose patients' PHI if they have their consent to do so or if the Act allows them to do so without consent,
4. Only collect, use and disclose patients' PHI if no other information would serve the purpose,
5. Only collect, use and disclose that amount of information necessary to serve the purpose,
6. Take reasonable steps to ensure that patients' PHI is as accurate, complete and up-to-date as needed for its use or disclosure,
7. Establish and maintain appropriate information practices and tell patients about these practices,
8. Develop and make available a written statement,
9. Develop procedures to identify inappropriate use or disclosure of PHI, notify affected patients, and make and keep notes of such a use or disclosure in or linked to the affected patient's personal health record,
10. Train staff, volunteers and others acting on their behalf, and
11. Take reasonable steps to protect personal health information that they transfer to others (for example, including privacy clauses in contracts with their Agents).

[1] OntarioMD Privacy and Security Guide and Workbook Version 1.2

Part 1: Physician Attestation

In accordance with the requirements of the *Personal Health Information Protection Act* (PHIPA):

1. I have appointed a privacy contact person.

2. I am aware of my requirements for the collection, use, disclosure and retention of PHI in accordance with PHIPA and other applicable legislation.

3. I have posted my information management practices which include who individuals can contact with privacy inquiries or complaints, and how they can obtain access to, or request correction of a record of PHI (Privacy Notice/Statement).

4. I am aware of the type of consent required in order to collect, use and disclose PHI (e.g. that assumed implied consent applies in the context of providing or supporting health care to patients).

5. I am aware of 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.

6. I am aware of a patient's right to place a consent directive on the access and use of their PHI for healthcare purposes; the need to verify the identity of an individual who requests that a consent directive be applied; and, the need to retain written instructions in respect to patients' consent directives.

7. I am aware of what to discuss with a patient when the patient requests to make a consent directive request. Examples include: 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; healthcare 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 and the consent directive may result in delays in receiving healthcare, reduced quality of care due to a healthcare provider's lacking complete information about the patient, and a healthcare provider's refusal to offer non-emergency care.

8. I am aware of the requirement, when disclosing a record of PHI which is subject to a consent directive, to notify the recipient(s) that the record is missing PHI which is subject to a consent directive.

9. I am aware of the circumstances in which I may override a consent directive (e.g. with express consent of the patient or their SDM; or where there is reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm).

10. I am aware of the steps that I must take when overriding a consent directive (e.g. documenting the reason for the override).

11. I am aware that PHI in verbal, written or electronic forms, may only be 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.

12. I am aware of the need for myself and my staff (and other Agents) to understand, agree to, and comply with privacy and security training requirements (e.g. initial and ongoing annual).

13. I am aware of the need for myself and my staff (and other Agents) to 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 reasonable portable electronic device used for purposes capable of storing or transmitting data, including the following: smart phones (including iPhone, Android, and BlackBerry), Laptops (including iPads and notebooks), Personal Digital Assistants, Cloud storage, 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').

14. I am aware of the 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.

15. I am aware of the requirements for physical controls (e.g. devices or equipment that can be used for storage of electronic PHI).

16. I am aware of the definition of a privacy breach and the processes required under PHIPA to address privacy breaches. (e.g. IPC's publication: *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*)

17. I am aware of the requirement to implement practices for auditing access to PHI. (e.g. IPC Reference Document: *Detecting and Deterring Unauthorized Access to Personal Health Information*).

18. I am aware of the need for third parties to understand, agree to, and comply with privacy and security requirements (e.g. IPC Reference Document: *Detecting and Deterring Unauthorized Access to Personal Health Information*).

19. I am aware of the need for myself and my staff (and other Agents) to understand that privacy responsibilities continue to apply even after employment/affiliation terminates.

20. I am aware and will ensure that my staff (and other Agents) understand that sanctions for inappropriate use of PHI include reporting to Regulatory Colleges and the IPC in accordance with any requirements under PHIPA.

21. I am aware of the requirement that devices used to access PHI via web-based systems (e.g. ClinicalConnect) are trusted secure devices. 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 like Java and Adobe Flash. Public devices found in hotels and libraries are deemed non-trusted devices.

22. I am aware of the secure destruction requirements for PHI (e.g. IPC Order HO-001 and IPC Reference document on Secure Destruction Practices provides information on destruction requirements), including the maintenance and indefinite retention of a PHI destruction log.

23. I am aware of a patient's right for access to their PHI and the steps my practice must take in response to a patient's request to access their PHI, including verifying the identity of the individual who is requesting access to PHI.

24. I am aware of the requirement to retain PHI for as long as necessary to allow individuals to exhaust any recourse under PHIPA that they may have with respect to a request for access to PHI as well as other legislated retention requirements (e.g. Ontario Regulations made under the *Medicine Act, Limitations Act*, referenced in the CPSO Medical Records Policy Statement).

25. I am aware of the appropriate amount to charge patients for fulfilling access and disclosure of PHI requests (e.g. OMA Physician's Guide to Uninsured Services).

26. I am aware of the requirements for a patient to access their PHI before requesting a correction to that PHI.

27. I am aware of my practice's obligation to correct a record of PHI (while maintaining the original record) if the patient demonstrates that the record is incorrect/incomplete, and provides the information necessary to correct the record.

28. I am aware of the steps required to permit a patient to issue a Statement of Disagreement with respect to a decision not to fulfill a PHI correction request and the requirements to share the Statement of Disagreement with a recipient organization when the record in question is disclosed.

29. I am aware of the steps necessary to respond to a request for access to PHI in the form of a subpoena/summons/warrant, police acting on behalf of a coroner, and related legal contexts.

Part 2: CPSO Licence Information - * indicates mandatory field

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

Part 3: Professional Liability Coverage - * indicates mandatory field

Canadian Medical Protective Association (CMPA) Membership Number*	

✓ ***Provide copy of your Statement of Protection from the CMPA 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 (Physician) Full Name (please print/type)*	
CPSO 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

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

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