ClinicalConnect Privacy & Security Attestation

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. ClinicalConnect is an effective and efficient means of providing shared access to patients' PHI within their circle of care and is used by health care organizations across South West Ontario.

In Ontario, the *Personal Health Information Protection Act, 2004 (PHIPA)* governs the protection 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 legally required to have the correct measures in place to ensure compliance with *PHIPA* while using the portal in the delivery of health care to patients.

The ClinicalConnect Program Office requires that all Participant organizations (excluding Sole Practitioner HIC type who complete an equivalent attestation) complete the Privacy & Security Attestation, a key piece of the application process to access ClinicalConnect. Working through the Privacy & Security Attestation will assist Participants to meet *PHIPA* requirements and also the requirements to participate in ClinicalConnect.

Please complete the ClinicalConnect Privacy & Security Attestation as per the instructions below:

The ClinicalConnect Privacy & Security Attestation must be completed and submitted using the ClinicalConnect Access Governance System (AGS), as part of a Health Information Custodian's application to become a Participant in ClinicalConnect. You may use this working copy of the Privacy & Security Attestation to familiarize yourself with the requirements before logging into AGS to submit your organization's Privacy & Security Attestation when requested to do so by the ClinicalConnect Program Office. The organization's Privacy Contact must check off the appropriate check box for each of the attestation statements listed.

After the Privacy & Security Attestation has been submitted through AGS, the ClinicalConnect Program Office will review the organization's responses and follow up with its Privacy Contact as required within 4 weeks. An organization will not be provided with access to ClinicalConnect until it has satisfied all the requirements.

ClinicalConnect Privacy & Security 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 my organization:

Attestation Statements
1. The organization has 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 its staff (and other Agents) comply with those policies and practices.
2. The organization has appointed a privacy contact person in accordance with section 15 of PHIPA.
3. The organization has posted or made available to the public a written statement of its 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. The organization has established policies and/or practices for managing complaints or challenges to the organization's compliance with PHIPA, its own policies or privacy best practices.
5. The organization has 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. The organization has 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. The organization has established policies and/or practices for managing interactions with an estate trustee after a patient dies.

8. The organization has 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. The organization has established 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. The organization has 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. The organization has 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. The organization has 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. The organization has 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. The organization has 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. The organization has 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. The organization has 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. The organization has established policies and/or practices regarding requirements for physical controls of devices or equipment that can be used for storage of electronic PHI.
18. The organization has established policies and/or practices to ensure staff (and other Agents) comply with separate/additional safeguarding and handling requirements when accessing PHI remotely.
19. The organization has 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) publication titled *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector*)
20. The organization has 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. The organization has 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. The organization has 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. The organization has 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. The organization has 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. The organization has established practices to comply with secure destruction requirements for PHI (e.g. IPC Order HO-001; the IPC reference document titled "*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. The organization has 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. The organization has 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 (e.g. Ontario Regulations made under the *Medicine Act, Limitations Act*, referenced in the CPSO Medical Records Policy Statement).
28. The organization has established policies and/or practices regarding the fees that are charged for fulfilling requests for access and disclosure of PHI.
29. The organization has established policies and/or practices for managing the requirement for a patient to access their PHI before requesting a correction to that PHI.

30. The organization has 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. The organization has 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. The organization has 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.