ClinicalConnect™ | CONNECTING SOUTH WEST ONTARIO

ClinicalConnect™: Privacy & Security Self-Assessment

ClinicalConnect Provider Portal

In order to improve the quality and timeliness of health care decision-making, and to enhance access to remote medical consultations, ClinicalConnect will make a wider set of personal health information available to Participants in a new and technical manner. The ClinicalConnect Program Office requires that all organizations, excluding Sole Practitioners Health Information Custodian (HIC) type, who complete an equivalent attestation, complete the Privacy and Security Self-Assessment, a key piece of the application process to be approved to access ClinicalConnect.

Privacy Legislation

In Ontario, the *Personal Health Information Protection Act (PHIPA)* is in place to govern the protection of personal health information (PHI); this includes rules regarding the collection, use, and disclosure of PHI by Health Information Custodians (HICs). ClinicalConnect is an effective and efficient means of providing shared access to patients' PHI within their circle of care. As such, it is important to have the correct measures in place for Participants to ensure compliance with *PHIPA*, while successfully using the portal in the delivery of healthcare to patients.

Privacy Obligations

HICs have a duty to ensure compliance with *PHIPA.* In order to comply successfully the Canadian Standard Association (CSA) Model Code for the Protection of Personal Information can be followed. The Model Code is informed by the following ten principles: *Accountability Accuracy, Identifying Purposes, Safeguards, Consent, Openness, Limiting Collection, Access, Limiting Use, Disclosure and Retention, Challenging Compliance.*

Benefits of Privacy Compliance

Working through the ClinicalConnect Privacy & Security Self-Assessment, using the resources available, will allow Participants to meet *PHIPA* requirements, fulfill the CSA Model Code, and meet the requirements to participate in ClinicalConnect. Breaches of confidentiality can have severe consequences as well as a negative impact on careers and the care patients receive. Having the compliance measures in place allows peace of mind that legislative requirements are being met for your organization. It also helps to build a culture of patient safety, privacy and confidentiality. When patients feel secure that their PHI is being handled confidentially, they are more open with their healthcare team and happier with the care they receive.

ClinicalConnect Privacy & Security Self-Assessment

The ClinicalConnect Privacy & Security Self-Assessment 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.

Please complete the ClinicalConnect Privacy & Security Self-Assessment as per the instructions below:

You may use this working copy of the Privacy & Security Self-Assessment to familiarize yourself with the requirements, then log into the Access Governance System (AGS) to submit your Privacy & Security Self-Assessment when requested to do so by the ClinicalConnect Program Office.

The ClinicalConnect Program Office will review the organization's responses, and will follow up with the organization as required, **within 4-6 weeks** of receiving the document from the organization. Organizations will not be provided with access to the ClinicalConnect until they have satisfied all of the requirements.

Each organization must check off the appropriate check box for therequirements listed. Please refer to the 'ClinicalConnect Privacy & Security Toolkit', available by visiting http://info.clinicalconnect.ca, as a resource to help you meet any requirements that you are not yet compliant with.

ClinicalConnect Privacy & Security Requirements

Requirement	Reference CSA Privacy Model Code	Compliant?	Policy Reference (Optional)
1. Policy identifies organization's Privacy Contact, and provides their contact information.	Principle: Accountability		
2. Policy identifies the purpose(s) for which PHI is collected, used, and disclosed.	Principle: Accountability		
3. Policy clarifies the type of consent required in order to collect, use, and disclose PHI (e.g. assumed implied consent applies in the context of providing or supporting health care).	Principle: Consent		
4. Policy clarifies the role a Substitute Decision Maker (SDM) plays when a patient is not capable.	Principle: Consent		
5. Policy clarifies the role an estate trustee plays when a patient dies.	Principle: Consent		
6. Policy clarifies a patient's/SDM's right to impose a consent directive on the access/use of the patient's PHI.	Principle: Consent		
7. Policy clarifies the steps required to verify the identity of an individual who requests that a consent directive be applied (i.e. to ensure that they are the patient or SDM).	Principle: Consent		

8. Policy clarifies the preference for written consent directive requests. PHIPA permits patients to make verbal consent directive requests. However, it is a Privacy Best Practice for HICs, where possible, to obtain the patient's written instructions in this respect.	Principle: Consent		
9. Policy establishes the need to retain the patient's written consent directive instructions.	Principle: Consent		
10. Policy establishes a list of factors to discuss with a patient when the patient makes a consent directive request. Examples of factors to discuss with the patient 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 emergencies; and the consent directive may result in delays in receiving health care, 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.	Principle: Consent		

11. Policy clarifies the steps staff must take to notify the Privacy Contact and Health Records Department that a patient has provided a staff member with instructions to impose a consent directive upon the patient's PHI.	Principle: Consent		
12. Policy clarifies the steps the Privacy Contact and Health Records Department must take to notify all staff that a patient has imposed a consent directive upon their PHI.	Principle: Consent		
13. Policy clarifies the steps staff must take when they share a record of PHI which is subject to a consent directive, in order to notify the recipient(s) that the record is missing certain information which is subject to a consent directive.	Principle: Consent		
14. Policy clarifies the circumstances in which staff may override a consent directive (e.g. emergencies).	Principle: Consent		
15. Policy clarifies the steps staff must take when overriding a consent directive (e.g. recording the reason for the override).	Principle: Consent		
16. Policy establishes that staff may only collect PHI for purposes of providing or supporting health care, and within the limits of each staff member's job role.	Principle: Limiting Collection of PHI		

17. Policy establishes that staff may only use and disclose PHI for purposes of providing or supporting health care, and within the limits of each staff member's job role.	Principle: Limiting Use, Disclosure, and Retention of PHI		
18. Policy establishes that staff who print hard copies of PHI are responsible to comply with the limitations on the use and disclosure of PHI described in Requirement 17.	Principle: Limiting Use, Disclosure, and Retention of PHI		
19. Policy clarifies that it applies to PHI in all forms – verbal, written, and electronic.	Principle: Limiting Use, Disclosure, and Retention of PHI		
20. Policy clarifies the steps required to verify the identity of an individual who is requesting access to PHI (i.e. to ensure that the individual is the patient or the Substitute Decision Maker).	Principle: Limiting Use, Disclosure, and Retention of PHI		
21. Policy establishes 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 contexts.	Principle: Limiting Use, Disclosure, and Retention of PHI		
22. Policy establishes fees for fulfilling information access requests.	Principle: Limiting Use, Disclosure, and Retention of PHI		
23. Policy establishes fees for disclosures.	Principle: Limiting Use, Disclosure, and Retention of PHI		

24. Policy establishes a procedure for the retention of PHI which satisfies the information retention rules found in: PHIPA section 13(2) regarding pending patient access requests, the *Limitations Act* and the Rules of Civil Procedures regarding lawsuits, regulations to the *Public Hospitals Act*, and the need to resolve legal/College issues.	Principle: Limiting Use, Disclosure, and Retention of PHI		
25. Policy establishes the requirement for a PHI destruction log – as directed by the IPC.	Principle: Limiting Use, Disclosure, and Retention of PHI. The IPC endorses such maintenance as well; see IPC, Order HO-001 (October 2005).		
26. Policy establishes the requirement to retain the destruction log indefinitely – as directed by the IPC.	Principle: Limiting Use, Disclosure, and Retention of PHI		
27. Policy establishes the need for privacy training, ongoing privacy awareness reminders and updates.	Principle: Safeguarding PHI		
28. Policy establishes sanctions for inappropriate use of PHI, up to and including termination of employment/affiliation.	Principle: Safeguarding PHI		
29. Policy establishes that privacy responsibilities continue to apply even after employment/affiliation terminates.	Principle: Safeguarding PHI		

30. Policy addresses information security (which includes network resources, desktop computers, mobile computing devices and wireless data transmission) and addresses mandatory mobile computing devices 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 used for purposes capable of storing or transmitting data, including the following: smart phones (including Blackberry's and iPhone's), Laptops (including Net books), Personal digital assistants, USB memory sticks, Portable hard disk or solid state data storage devices, Numeric, alpha-numeric and 2 way pagers, Medical or other electronic devices that contain hard disk or solid state data memory and which can be plugged into a USB port, CD / DVD disks or CD/DVD 'burners'	Principle: Safeguarding PHI		

31. Policy establishes requirements for the use of passwords and the appropriate level of password protection based on the security risk, including reference to mobile computing devices.	Principle: Safeguarding PHI		
32. Policy establishes requirements for maintaining the security of passwords.	Principle: Safeguarding PHI		
33. Policy establishes requirement for physical controls (e.g. pass card entry to data facility, locked cabinets, monitoring power supply and temperature).	Principle: Safeguarding PHI		
34. Policy defines a privacy breach.	Principle: Safeguarding PHI		
35. Policy addresses the implementation of privacy audits.	Principle: Safeguarding PHI		
36. Policy establishes the need for service agreements with contractors who may have access to PHI which makes them aware of their privacy responsibilities (an agreement for contractors/affiliates to sign)	Principle: Safeguarding PHI		

37. Policy establishes separate/additional requirements for remote (VPN) access.	Principle: Safeguarding PHI		
38. Policy establishes 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.	Principle: Safeguarding PHI		
39. Policy addresses the destruction of information. IPC Order HO-001 and IPC Reference document on Secure Destruction Practices provides information on destruction requirements.	Principle: Safeguarding PHI. See IPC, Order HO-001 (August 2006)		
40. Policy establishes process to address non-clinical observers.	Principle: Safeguarding PHI		
41. Policy establishes processes to address privacy breaches.	Principle: Safeguarding PHI		
42. Policy establishes the requirement for a public-friendly version of the organization's Privacy Policy.	Principle: Openness		
43. Policy acknowledges a patient's right for access to their PHI.	Principle: Individual Access		
44. Policy clarifies the steps the organization must/may take in response to a patient's written access request.	Principle: Individual Access		

45. Policy clarifies the steps the organization must/may take in response to a patient's verbal access request.	Principle: Individual Access		
46. Policy clarifies the organization's requirement to respond to information access requests within 30 days (or up to 60 days upon extension).	Principle: Individual Access		
47. Policy clarifies the limitations to the organization's requirement to fulfill information access requests.	Principle: Individual Access		
48. Policy establishes process by which stakeholders may challenge the organization's compliance with PHIPA, the requirements in this document, or Privacy Best Practices.	Principle: Challenging Compliance		
49. Policy establishes process by which organization will respond to challenges described in Requirement 47.	Principle: Challenging Compliance		
50. Policy establishes the requirement for a patient to access their PHI before requesting a correction to that PHI.	Principle: Accuracy		
51. Policy establishes the organization's obligation to correct a record of PHI if the patient demonstrates that the record is incorrect/incomplete, and provides the organization with the information necessary to correct the record.	Principle: Accuracy		
52. Policy establishes the steps required to correct a record of PHI while maintaining the original record.	Principle: Accuracy		

53. Policy clarifies the organization's requirement to respond to information correction requests within 30 days (or up to 60 days upon extension).	Principle: Accuracy		
54. Policy clarifies the limitations to the organization's requirement to fulfill information correction requests.	Principle: Accuracy		
55. Policy clarifies the steps required to permit a patient to issue a Statement of Disagreement (SOD) with respect to the organization's decision not to fulfill an information correction request.	Principle: Accuracy		
56. Policy clarifies the steps required to ensure that staff are aware of the SOD.	Principle: Accuracy		
57. Policy clarifies the steps required to share a SOD with a recipient organization when the record in question is disclosed.	Principle: Accuracy		