Electronic Health Record Consent Directive and Consent Override Policy

Policy Level Approval:	Chief Executive Officer
Policy Category:	Enterprise Policy
Policy Number:	INF-003.02-P
Sensitivity Level:	Public
Policy Sponsor(s):	Chief, Strategy, Planning, Privacy & Analytics
Original Date of Approval:	September 30, 2020
Date of Posting: This Policy is effective on the date of its posting or as otherwise noted in the Policy	July 22, 2025
Version Approval Date:	June 10, 2025
Next Scheduled Review (Fiscal Year YY/YY):	28/29

1 Purpose, Objectives and Scope

1.1 Purpose

This Policy and its procedures address the process to be followed in:

- Receiving, documenting, implementing, testing, auditing and monitoring individuals' requests to withhold or withdraw, in whole or part, the individual's consent to the Collection, Use and disclosure of their Personal Health Information (**PHI**) by means of the Electronic Health Record (**EHR**), by a Health Information Custodian (**HIC**) for the purpose of providing or assisting in the provision of health care to the individual (**Consent Directive**);
- Receiving, documenting and implementing an individual's request to modify or withdraw such Consent Directives; and
- Overriding a Consent Directive.

1.2 Objectives

1.2.1 This Policy and its procedures support Ontario Health's (**OH**'s) management of consent in compliance with the *Personal Health Information Protection Act, 2004* (**PHIPA**), Ontario Regulation 329/04 (**O. Reg. 329/04**), and the requirements set out in the Information and Privacy Commissioner of Ontario's (**IPC**) *Manual for the Review and Approval of Prescribed Organizations* (**IPC PO Manual**).

1.3 Scope

1.3.1 This policy applies to non-union Employees, people leaders, board members, unionized Employees, secondees, consultants, individuals acting on behalf of OH (**OH Agents**) and HICs who access or contribute PHI to the EHR.

1.3.2 This Policy and its procedures apply to Consent Directives in respect of PHI accessible by means of the EHR developed or maintained by OH under its authority as a Prescribed Organization pursuant to O. Reg. 329/04. For more information on the scope of the EHR, please see the EHR Plain Language Description and List of Repositories.

1.4 Compliance, Audit and Enforcement

1.4.1 Compliance with this Policy in its entirety is mandatory unless an exception to a specific section is approved by the Chief Privacy Officer (**CPO**) or delegate in writing. Failure to comply with the requirements of this Policy may result in disciplinary action up to and including revocation of appointment, termination of employment or termination of contract without notice or compensation.

1.4.2 Compliance will be audited in accordance with and as per the frequency outlined in the *Privacy Audit and Compliance Policy*.

1.4.3 At the first reasonable opportunity upon identifying or becoming aware of a breach of this Policy, Employee(s) and other OH Agents must notify the Privacy Office by reporting the

breach to Enterprise Service Desk by Phone: 1-866-250-1554; or Email: oh-servicedesk@ontariohealth.ca

1.4.4 Breaches of this Policy will be managed in accordance with the *Privacy Incident Management Policy and Procedure*.

1.4.5 Compliance will be enforced in accordance with the *Progressive Discipline Policy.*

1.5 Terminology

1.5.1 The words “include” and “including” when used are not intended to be exclusive and mean, respectively, “include, without limitation,” and “including, but not limited to”.

1.5.2 Words and terms in this Policy that have meanings differing from the commonly accepted definitions are capitalized and their meanings are set out in the Definition and Acronyms section (section 10).

2 Policy

2.1 Consent Directive Policy

2.1.1 PHIPA provides that an individual may at any time make a directive that withholds or withdraws, in whole or in part, the individual’s consent to the Collection, Use and Disclosure of the individual’s PHI by means of the EHR by a HIC for the purposes of providing or assisting in the provision of health care to the individual.

2.1.2 As a Prescribed Organization, OH implements, withdraws or modifies a Consent Directive when requested to do so by an individual in accordance with the requirements prescribed in the regulations.

2.1.3 OH takes reasonable steps to test to ensure that requests to make, modify or withdraw a Consent Directive have been properly implemented.

2.1.4 OH communicates the following information to the public relating to Consent Directives:

- The specificity a which PHI may be made subject to a Consent Directive, including whose Collection, Use and Disclosure of the information may be restricted;
- Any data elements that may not be made subject to a Consent Directive; and
- The name and/or title, mailing address and contact information of the Employee(s) or other OH Agent(s) to whom such requests may be submitted and the manner and format in which individuals may submit requests to make, modify or withdraw Consent Directives.

2.1.5 OH keeps an electronic record of all instances where a Consent Directive is made, modified or withdrawn in accordance with the requirements set out in Appendix “A.”

2.1.6 OH continually audits and monitors the electronic record of all instances where a Consent Directive is made, modified or withdrawn in accordance with the *EHR Privacy Auditing and Monitoring Policy*, and logs such audits in accordance with the requirements set out in Appendix “A.”

2.2 Requirements to Make, Modify, or Withdraw a Consent Directive

2.2.1 An individual or substitute decision-maker (**SDM**) may make, modify, or withdraw a Consent Directive in writing by submitting an EHR Consent Directive Request Form to OH by regular mail or fax as follows:

Mail: Chief Privacy Officer
Privacy Office, Ontario Health
500-525 University Ave
Toronto, ON M5G 2L3
Fax: 416-586-4397 or 1-866-831-0107

2.2.2 Alternatively, an individual or SDM may use the encrypted web form available on OH's website to make, modify, or withdraw a Consent Directive.

2.2.3 Prior to implementing a Consent Directive, OH takes reasonable steps to confirm that the individual who submitted the EHR Consent Directive Request Form is the individual to whom the PHI relates or is that individual's SDM.

2.2.4 The EHR Consent Directive Request Form must contain sufficient detail to enable OH to implement the directive. The individual or SDM making the request must complete all required fields on the EHR Consent Directive Request Form, which are indicated by an asterisk (*). For example, the EHR Consent Directive Request Form must contain one of the following: an Ontario Health Card number (**HCN**), medical record number (**MRN**) and name of the organization that issued the MRN, or a Client Health and Related Information System (**CHRIS**) client number to enable OH to locate the correct individual's records in the EHR.

2.2.5 If the EHR Consent Directive Request Form does not contain sufficient detail to enable OH to implement the directive with reasonable efforts, OH offers assistance to the individual or SDM in reformulating the directive to comply with PHIPA.

2.2.6 If the EHR Consent Directive Request Form contains sufficient detail to enable OH to implement the directive, and sufficient proof of authority has been provided, OH implements the directive in accordance with PHIPA and its regulations and sends a confirmation letter to the individual or SDM making the request.

2.2.7 If OH is unable to implement a directive due to the EHR Consent Directive Request Form containing insufficient detail or where the authority of the individual making the request cannot reasonably be confirmed, OH notifies the individual in writing.

2.3 Level of Specificity of a Consent Directive

2.3.1 In accordance with O. Reg. 329/04 made under PHIPA, where an individual makes a Consent Directive, it applies to all of the individual's PHI that is accessible by means of the EHR, unless it is reasonably possible for OH to apply the Consent Directive only to the specific PHI that has been identified by the individual, in which case OH then implements the Consent Directive only to that PHI.

2.4 Application to PHI added to the EHR in the future

2.4.1 Where an individual has made a Consent Directive and additional PHI is subsequently added to the EHR in relation to that individual, OH implements the Consent Directive with respect to the additional information in accordance with PHIPA.

2.5 Data elements that may be Collected, Used or Disclosed by a HIC for the purpose of uniquely identifying an individual and may not be made subject to a Consent Directive

This section specifies the data elements that may be Collected, Used or Disclosed by a HIC for the purpose of uniquely identifying an individual in order to Collect PHI by means of the EHR that may not be made subject to a Consent Directive provided by the individual.

2.5.1 A HIC may Collect, Use and Disclose the following prescribed data elements for the purpose of uniquely identifying an individual in order to Collect PHI under ss. 55.5(1) of PHIPA:

A Health Number;

- Either or both of a number or version code assigned to an insured person by a province or territory in Canada other than Ontario for the purposes of a health care insurance plan within the meaning of the *Canada Health Act*;
- A medical record number or other unique number assigned by a health information custodian to uniquely identify individuals receiving health care from the custodian;
- A unique number relating to an individual on a form of identification that:
    - has been issued by a government or governmental agency, and
    - bears the name of the individual.
- The name or names of an individual, including a legal name, an alternate name or an alias;
- The date of birth of an individual;
- The administrative gender of an individual;
- The address of an individual;
- A telephone number of an individual;
- The primary or preferred language of an individual;
- A binary value indicating if an individual is deceased; and
- The date of death of an individual.

2.5.2 In accordance with ss. 18.4(4) of O. Reg. 329/04, the data elements listed above may not be made subject to a Consent Directive.

2.6 Collection of PHI for purposes other than provision of health care to the individual

2.6.1 In accordance with PHIPA, OH may provide PHI that is held within the EHR to a coroner in relation to an investigation conducted under the *Coroners Act*, regardless of whether the PHI is subject to a Consent Directive.

2.6.2 In accordance with PHIPA, the Chief Medical Officer of Health (**CMOH**) or a medical officer of health within the meaning of the *Health Protection and Promotion Act* (**HPPA**) may Collect PHI by means of the EHR for purposes related to their duties under the HPPA or the *Immunization of School Pupils Act*, regardless of whether the PHI is subject to a Consent Directive.

2.6.3 In accordance with PHIPA, the Minister may direct the Disclosure of PHI that is accessible by means of the EHR to a person, as if the Minister had custody or control of the information, subject to the conditions and restrictions of section 55.10 of PHIPA.

2.7 Consent Directives made prior to Part V.1 of PHIPA coming into force

2.7.1 If prior to the enactment of s. 55.6 of PHIPA an individual made a Consent Directive in respect of PHI held within the EHR and that PHI was created and maintained by OH under the authority of s. 6.2 of O. Reg. 329/04, then OH will continue to implement the individual's directive as it existed prior to s. 55.6 coming into effect.

2.8 Providing Notice of Consent Directives

2.8.1 If a HIC seeks to Collect PHI for the purposes of providing or assisting in the provision of health care to the individual and that PHI is subject to a Consent Directive, OH is required to notify the HIC that the individual has made a Consent Directive without providing any PHI that is subject to the Consent Directive, in accordance with ss. 55.6 (7) of PHIPA. In addition, OH ensures that no PHI that is subject to the Consent Directive is provided to the HIC unless a Consent Override is performed.

3 Policy - Overrides of Consent Directives

3.1.1 OH permits a HIC to override a Consent Directive in the circumstances set out in s. 55.7 of the PHIPA (**Consent Override**). Specifically, OH permits a HIC to override a Consent Directive only where the HIC that is seeking to Collect the information:

- Obtains the express consent of the individual to whom the information relates;
- Believes, on reasonable grounds, that the Collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the individual to whom the PHI relates and it is not reasonably possible for the HIC that is seeking to Collect the PHI to obtain the individual's consent in a timely manner; or
- Believes, on reasonable grounds, that the Collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or a group of persons.

3.1.2 OH only permits a HIC to override a Consent Directive where the Disclosure is permitted by the HIC with custody and control of the PHI in question.

3.1.3 Where the technology supports, the user interface provides HICs with the ability to override a Consent Directive once the required conditions are met (as outlined in s. 3.1.1 and 3.1.2 above).

3.1.4 The Digital Excellence in Health Portfolio within OH is responsible for ensuring that HICs with access to the EHR are able to override a Consent Directive. Regular application health checks are performed to ensure continuity of service and trigger incident management processes as needed.

3.1.5 Where a Consent Override is performed, the HIC who has Collected the information is responsible for documenting the Consent Override in accordance with the HIC's internal policies and procedures, including recording the purpose for the Consent Override and retaining any supporting documentation.

3.1.6 OH keeps an electronic record of all instances where a Consent Directive is overridden by a HIC in accordance with the requirements set out in Appendix "A."

3.1.7 OH audits and monitors the electronic record of all instances where a Consent Directive is overridden by a HIC in accordance with the *EHR Privacy Auditing and Monitoring Policy*, and logs such audits in accordance with the requirements set out in Appendix "A."

3.2 Identifying Consent Overrides

3.2.1 The Digital Excellence in Health Portfolio within OH is responsible for maintaining and ensuring continuity of service of the systems that record and identify Consent Overrides performed using EHR technology.

3.2.2 Application Management Support, Product Management, and SQL Operations are responsible for preparing and providing reports of Consent Overrides to Privacy Operations in accordance with this Policy and its procedures.

3.3 Providing Notice of Consent Overrides

3.3.1 OH notifies the HIC in the event that the HIC overrides a Consent Directive.

3.3.2 Where PHI that has been made subject to a Consent Directive has been Collected by a HIC pursuant to a Consent Override, OH immediately provides written notice, in accordance with the requirements prescribed in the regulations, to the HIC that Collected the PHI.

3.3.3 Upon receiving notice from OH of a Consent Override, the HIC that Collected the PHI is responsible for:

- Confirming the purpose for the Consent Override (i.e., to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to another person or group of persons);
- Notifying the individual to whom the PHI relates; and
- Giving written notice to the IPC where required by PHIPA.

3.3.4 Upon request and subject to availability, OH provides further relevant information to the HIC that Collected the PHI as result of a Consent Override to support the HIC in fulfilling

its notice obligations to the individual to whom the PHI relates or the IPC where applicable.

3.4 Reporting Consent Overrides to the IPC

3.4.1 OH submits to the IPC, at least annually, a report based on or containing any information, other than PHI, that is kept in the electronic record that the Prescribed Organization is required to keep of every instance where PHI that is accessible by means of the EHR that is the subject of a Consent Directive is Disclosed pursuant to a Consent Override since the time of the last report, as required by paragraph 16 of s. 55.3 of PHIPA.

3.4.2 The form and manner of the report must be in accordance with that specified by the IPC.

3.5 Requests for Electronic Records of Consent Directives and Consent Overrides

3.5.1 OH provides, upon the request of a HIC that requires the records to audit and monitor its compliance with PHIPA, the electronic records that OH keeps pursuant to paragraphs 5 and 6 of s. 55.3 of PHIPA.

3.5.2 OH provides to the IPC, upon request, the electronic records that OH keeps under PHIPA for the purposes of Part V.1 of PHIPA.

4 Process for Receiving Requests for Consent Directives

4.1 General

This section establishes the process to be followed by OH in receiving requests to make, modify or withdraw Consent Directives in accordance with s. 55.6 of PHIPA.

The CPO or delegate is responsible for overseeing OH's intake, review, implementation, and logging of requests to make, modify or withdraw Consent Directives.

4.2 Intake & Review

4.2.1 Upon receipt of an *EHR Consent Directive Request Form*, the CPO or delegate designates a member of the Privacy Team to be responsible for the request (hereinafter "Designated Member of the Privacy Team"). The Designated Member of the Privacy Team is responsible for recording the request in the tracking log and saving the relevant documentation in accordance with the requirements set out in Appendix "A."

4.2.2 As soon as possible after receipt of the *EHR Consent Directive Request* Form by OH, the Designated Member of the Privacy Team:

- Records the request in the tracking log;
- Saves the *EHR Consent Directive Request Form* in the secure drive;

- Reviews the *EHR Consent Directive Request Form* and any supporting documentation submitted to determine whether sufficient proof of authority has been provided;
- Reviews the *EHR Consent Directive Request Form* to determine whether it contains sufficient detail to enable OH to implement the directive with reasonable efforts; and,
- If the *EHR Consent Directive Request Form* does not contain sufficient detail to enable OH to implement the Consent Directive with reasonable efforts, the Designated Member of the Privacy Team will follow section 4.3 below.

4.3 Offering Assistance to the Individual or SDM in Reformulating a Consent Directive

4.3.1 As soon as possible after the Designated Member of the Privacy Team reviews the *EHR Consent Directive Request Form* and determines that it does not contain sufficient detail to enable OH to implement the Consent Directive with reasonable efforts, the Designated Member of the Privacy Team contacts the individual or SDM using their preferred method of contact and information provided on the *EHR Consent Directive Request Form* to offer assistance in reformulating the request.

4.4 Implementing a Consent Directive in the EHR

4.4.1 As soon as possible and no later than ten (10) calendar days after receiving sufficient detail and proof of authority from the individual or SDM making the request, the Designated Member of the Privacy Team uses the information provided on the EHR Consent Directive Request Form and the appropriate consent application tool to implement the Consent Directive in the EHR in accordance with the individual or SDM's instructions.

4.4.2 Once the Consent Directive is implemented in the EHR, the Designated Member of the Privacy Team ensures the following details are recorded (if not already):

- The first and last name of the individual or SDM who made, withdrew or modified the Consent Directive;
- The instructions that the individual or SDM provided regarding the Consent Directive;
- The HIC, agent or other person to whom the directive was made, withdrawn or modified; and,
- The date and time that the Consent Directive was made, withdrawn or modified (i.e., the time the Consent Directive was implemented in the EHR).

4.4.3 The CPO or delegate is responsible for ensuring that the required details are recorded in accordance with the requirements set out in Appendix "A."

4.5 Testing Consent Directives

4.5.1 OH takes reasonable steps to test to ensure that requests to make, modify or withdraw a Consent Directive have been properly implemented in the EHR.

4.5.2 As soon as possible after the Consent Directive is implemented in the EHR, and no later

than ten (10) calendar days following the receipt of the request, the Designated Member of the Privacy Team uses the appropriate consent application tool to test the Consent Directive and ensure that it has been properly implemented in accordance with the individual's instructions.

The Designated Member of the Privacy Team uses the appropriate consent application tool and information provided on the EHR Consent Directive Request Form to create testing parameters applicable to the individual's instructions and performs the testing. The Designated Member of the Privacy Team documents the completion of the testing.

Where testing indicates that the Consent Directive has not been properly implemented (for example, the Disclosure of information is allowed where it should be blocked), the Designated Member of the Privacy Team modifies the Consent Directive accordingly following the procedure in s. 4.4, and then re-tests the Consent Directive following the procedure in this s. 4.5.

Documentation that must be completed and provided: Where testing indicates that the Consent Directive has been properly implemented in accordance with the individual's instructions, the Designated Member of the Privacy Team is responsible for recording the completion of testing in the tracking log.

4.5.3 Documentation that must be provided and to whom: Should any recommendations arise from testing, the Designated Member of the Privacy Team is responsible for notifying the CPO or delegate as soon as possible. Upon receiving notice of any such recommendations, the CPO or delegate is responsible for reviewing the recommendations and designating employee(s) or other OH Agent(s) to be responsible for implementing the recommendations where appropriate.

4.6 Confirmation (Notice of Implementation)

4.6.1 As soon as possible and no later than seven (7) calendar days after the Consent Directive is implemented in the EHR, the Designated Member of the Privacy Team prepares a letter to the individual or SDM who made the request notifying them that the Consent Directive has been implemented, and includes the following information:

- The name of the individual to whom the PHI relates;
- The details of the Consent Directive implemented, including the type of data subject to the directive (i.e., the EHR repository), and the specificity of consent applied to each type of data and
- The date the Consent Directive was implemented in the EHR.

4.6.2 As soon as possible and no later than seven (7) calendar days after the Consent Directive is implemented in the EHR, the Designated Member of the Privacy Team must send the written confirmation letter to the individual or SDM using the contact information provided on the *EHR Consent Directive Request Form*.

4.6.3 ***Documentation that must be completed and provided:*** Once the confirmation letter has been sent to the individual or SDM, the Designated Member of the Privacy Team must record completion of this step.

4.7 Providing Notice of Consent Directives

This section establishes the process to be followed by OH in notifying a HIC that an individual has made a Consent Directive where the HIC seeks to Collect the individual's PHI.

4.7.1 OH provides notice of a Consent Directive to a HIC seeking to Collect an individual's PHI by way of an electronic alert presented to the HIC in the clinical user interface. When a HIC attempts to view an individual's PHI that is subject to a Consent Directive, an electronic alert is presented to the user in the clinical user interface to notify the HIC that a Consent Directive is in place blocking access to the PHI. The electronic alert (i.e. notice of Consent Directive) must convey to the HIC that some or all of the records they are seeking to access are blocked due to a Consent Directive.

4.7.2 OH ensures that no PHI that is subject to the Consent Directive is provided to the HIC unless a Consent Override is performed.

4.7.3 The Director, Product Management, Digital Excellence in Health is responsible for maintaining and ensuring continuity of service of the systems that identify Consent Directives in the EHR and present the electronic alert to the HIC in the clinical user interface when a Consent Directive is present.

4.7.4 The Director, Product Management, Digital Excellence in Health is responsible for ensuring that a HIC has been notified of a Consent Directive through the electronic means described in this section 4.7.

5 Procedures related to Consent Overrides

5.1 Process for Performing Consent Overrides

5.1.1 HICs or agents of HICs with access to the EHR may use EHR technology available through a clinical user interface to override a Consent Directive in the EHR (perform a "Consent Override").

5.1.2 The HIC or agent of the HIC seeking to Collect the PHI blocked by a Consent Directive uses available means to indicate the purpose for which they seek to Collect the PHI in order to perform the Consent Override (i.e. must select an override reason).

5.1.3 Where the HIC or agent of the HIC selects "express consent", they also indicate whether such consent has been provided by the individual to whom the PHI relates or that individual's SDM.

5.1.4 Once the HIC or agent of the HIC has made the required selections in the clinical user interface, the PHI subject to the Consent Directive will be made available to the HIC for a limited period of time.

5.1.5 Where a Consent Override is performed, the HIC who has Collected the information must document the Consent Override in accordance with the EHR Health Care Provider Guide and the HIC's internal policies and procedures, including recording the purpose for the Consent Override and retaining any supporting documentation.

5.2 Process to Provide Notice of Consent Overrides

This section sets out the process that OH follows in notifying HICs about Consent

Overrides, as required by ss. 55.7(6) of PHIPA.

5.2.1 Each business day, OH generates Consent Override reports that include all Consent Overrides performed since the period of the last such report, and clearly state the following in relation to each Consent Override:

- The name of the individual to whom the PHI relates;
- The name of the HIC that Collected the PHI;
- The name of the agent of the HIC who Collected the PHI, if available;
- A description of the type of PHI that was Collected (i.e., the EHR repository);
- The purpose for the Consent Override (i.e. the override reason), as indicated by the HIC at the time of the Consent Override; and
- The date and time of the Consent Override.

5.2.2 Designated employees within Application Management Support, Product Management, and SQL Operations are responsible for generating reports each business day identifying Consent Overrides in accordance with 5.2.2 above and providing such reports to the Privacy Operations team.

5.2.3 For each Consent Override in the report, Privacy Operations must immediately provide written notice of the Consent Override to the HIC who Collected the PHI as a result of the Consent Override in accordance with the requirements prescribed in the regulations, and at a minimum, the notice will include the information listed in section 5.2.1 above.

5.2.4 Privacy Operations must immediately provide notice of the Consent Override(s) to the HIC in the form of an encrypted document sent by email or make it available to the HIC through a secure portal.

5.2.5 Privacy Operations is responsible for logging all instances where a notice of a Consent Override is provided to a HIC pursuant to ss. 55.7(6) of PHIPA in accordance with the requirements set out in Appendix “A”.

5.3 HIC Requests for Further Information

5.3.1 If a HIC requests further information from OH for the purposes of providing notice of a Consent Override to the individual to whom the PHI relates or to the IPC, OH takes reasonable steps to retrieve the requested information and, where available, promptly provides the requested information to the HIC.

6 Process for Reporting Consent Overrides to the IPC

6.1.1 The Privacy Office is responsible for logging all instances where a report of Consent Overrides is provided to the IPC pursuant to paragraph 16 of s. 55.3 of PHIPA in accordance with the requirements set out in Appendix “A”, and saving documentation related to the report in the secure drive.

6.1.2 Upon request by the Privacy Office, designated employees within Application Management Support, Product Management, and SQL Operations are responsible for

preparing the report of Consent Overrides and providing the report to the Privacy Office as soon as reasonably possible.

6.1.3 The report is based on or contains any information, other than PHI, that is kept in the electronic record that OH keeps of every instance where PHI that is accessible by means of the EHR that is the subject of a Consent Directive is Disclosed pursuant to a Consent Override since the time of the last such report to the IPC, as required by paragraph 16 of section 55.3 of PHIPA.

6.1.4 Upon receipt, the Privacy Office, including Privacy Operations, is responsible for reviewing the report and providing it to the CPO or delegate for further review and approval.

6.1.5 The CPO or delegate is responsible for reviewing the report to ensure that the contents of the report and the form and manner in which the report will be provided to the IPC is in accordance with that specified by the IPC.

6.1.6 The CPO is responsible for approving the report, and delegating employees or other OH Agents to be responsible for providing the report to the IPC.

6.1.7 The report of Consent Overrides is in written form and provided to the IPC as an encrypted document delivered by email, unless otherwise specified by the IPC. The report is provided to the IPC as soon as reasonably possible on an annual basis, unless otherwise specified by the IPC. The CPO is responsible for determining the date on which the report is provided.

7 Process for Responding to Requests for Electronic Records of Consent Directives and Consent Overrides

7.1 Requests from Health Information Custodians

This section sets out the process that is followed by OH in responding to requests from HICs pursuant to paragraph 9 of s. 55.3 of PHIPA for the electronic records of Consent Directives and Consent Overrides that OH is required to keep pursuant to paragraphs 5 and 6 of s. 55.3 of PHIPA.

7.1.1 Privacy Operations is responsible for receiving requests for electronic records from HICs, recording each request in the tracking log in accordance with the requirements set out in Appendix “A,” and saving documentation related to the request in the secure drive.

7.1.2 Upon request from Privacy Operations, Application Management Support and/or Product Management is responsible for preparing the electronic records requested by the HIC, and providing the electronic records to Privacy Operations as soon as reasonably possible.

7.1.3 Privacy Operations is responsible for reviewing the electronic records to ensure that they are responsive to the HIC’s request and include the content required in accordance with PHIPA.

7.1.4 Privacy Operations is responsible for providing the requested information to the HIC. As soon as reasonably possible and no later than thirty (30) calendar days from the date OH received the request from the HIC, Privacy Operations provides the electronic records to the HIC either as an encrypted document sent by email or makes the

electronic records available to the HIC through a secure portal. Where OH requires more than 30 days to gather the requested information, OH's CPO or delegate notifies the HIC that an extension of time is needed and provides the reason why.

7.1.5 Privacy Operations is responsible for recording the request in the tracking log in accordance with the requirements set out in Appendix "A" and saving documentation related to the request in the secure drive.

7.2 Requests from the IPC

This section sets out the process that is followed by OH in responding to requests from the IPC pursuant to paragraph 8 of section 55.3 of PHIPA for the electronic records that OH keeps, pursuant to paragraphs 5 and 6 of section 55.3 of PHIPA.

7.2.1 The Privacy Office is responsible for receiving requests for electronic records from the IPC, recording each request in the tracking log in accordance with the requirements set out in Appendix "A," and saving documentation related to the request in the secure drive.

7.2.2 Upon request from the Privacy Office, Application Management Support and/or Product Management is responsible for preparing the electronic records requested by the IPC and providing the electronic records to the Privacy Office as soon as reasonably possible.

7.2.3 The Privacy Office, including Privacy Operations, is responsible for reviewing the electronic records to confirm that they are responsive to the IPC's request and providing the electronic records to the CPO or delegate for further review and approval.

7.2.4 The CPO or delegate is responsible for reviewing the electronic records to ensure that they are responsive to the IPC's request and include the content required pursuant to PHIPA and provides approval before the records are sent to the IPC.

7.2.5 Prior to providing the electronic records to the IPC, the CPO or delegate notifies the HIC(s) that are named in the electronic records, or whose agent or electronic service provider is named in the electronic records, that OH will be providing the electronic records to the IPC.

7.2.6 The CPO or delegate is responsible for providing the requested information to the IPC as soon as reasonably possible and no later than thirty (30) calendar days from the date OH received the request from the IPC. Where OH requires more than 30 days to gather the requested information, the CPO or delegate notifies the IPC that an extension of time is needed and provides the reason why.

7.2.7 The electronic records are provided to the IPC in written form as an encrypted document delivered by email, unless otherwise specified by the IPC.

8 Logging Requirements

8.1 Logging

8.1.1 OH maintains logs of the following, in accordance with the detailed requirements listed in Appendix "A":

- All instances where a notice of a Consent Directive is provided to a HIC pursuant to ss. 55.6(7) of PHIPA;
- All instances where a notice of a Consent Override is provided to a HIC pursuant to ss. 55.7(6) of PHIPA;
- All instances where a Report of Consent Overrides is provided to the IPC pursuant to paragraph 16 of s. 55.3 of PHIPA;
- All requests from HICs, made pursuant to paragraph 8 of s. 55.3 of PHIPA, for the electronic records OH maintains pursuant to paragraphs 5 and 6 of s. 55.3 of PHIPA;
- All requests from the IPC, made pursuant to paragraph 9 of s. 55.3 of PHIPA, for the electronic records OH i maintains pursuant to paragraphs 5 and 6 of s. 55.3 of PHIPA; and
- The audits, required by paragraph 7 of s. 55.3 of PHIPA, of the electronic records that OH keeps under paragraphs 5 and 6 of s. 55.3 of PHIPA.

8.1.2 OH maintains the logs identified in 8.1.1 in accordance with the detailed requirements listed in Appendix “A”.

8.1.3 The CPO or delegate is responsible for ensuring that OH maintains the logs identified in s. 8.1.1 of this Policy in accordance with PHIPA and the IPC PO Manual.

9 Responsibilities

9.1 Chief Privacy Officer

9.1.1 Overseeing OH’s intake, review, implementation, and logging of requests to make, modify or withdraw Consent Directives.

9.1.2 Designating a member of the OH Privacy Office to manage Consent Directives, Consent Overrides and associated notifications and reports in accordance with this Policy.

9.1.3 Reviewing and approving reports and notifications in respect of Consent Overrides and Consent Directives as requested by the IPC.

9.2 Health Information Custodians

9.2.1 Accessing, performing and/or managing PHI, Consent Directives and Consent Overrides in compliance with this Policy and all applicable EHR policies, and in accordance with PHIPA.

9.3 Designated Members of the Privacy Office (including Privacy Operations)

9.3.1 Receiving, reviewing, recording, managing, tracking, testing, responding to and logging requests for Consent Directives and Consent Overrides, and related reports and notifications in accordance with this Policy.

9.4 Employees and other OH Agents

9.4.1 Notifying and forwarding any requests for Consent Directives to OH's Privacy Office.

9.5 Digital Excellence in Health Portfolio

9.5.1 Maintaining and ensuring continuity of service of the systems that record and identify Consent Overrides performed using EHR technology.

9.5.2 Ensuring that a HIC has been notified of a Consent Directive through the electronic means described above.

9.6 Designated employees within Application Management Support, Product Management, and SQL Operations

9.6.1 Preparing and providing reports of Consent Overrides to Privacy Operations in accordance with this Policy and its procedures.

9.6.2 Generating Consent Override reports in accordance with this Policy.

10 Definitions and Acronyms

Defined terms are capitalized throughout this document.

Term / Acronym	Definition
CHRIS	Client Health and Related Information System
CMOH	Chief Medical Officer of Health
Collect	Has the meaning set out in section 2 of PHIPA with respect to PHI; and in respect of PI has the same meaning. "Collect" means to gather, acquire, receive, or obtain the information by any means from any source, and "Collection" and "Collected" has a corresponding meaning.
Consent Directive	Means a directive, made in accordance with s. 55.6 of PHIPA, that withholds or withdraws, in whole or in part, an individual's consent to the Collection, Use and Disclosure of their PHI by means of the EHR by a HIC for the purposes of providing or assisting in the provision of health care to the individual.
Consent Override	Means the permitted disclosures described in section 55.7 of PHIPA.
CPO	Chief Privacy Officer

Term / Acronym	Definition
Disclose	Has the meaning set out in s. 2 of PHIPA with respect to PHI in the control of a HIC or a person; and in respect of PI has the same meaning. "Disclose" means to make the information available or to release it to another HIC or to another person, but does not include to Use the information, and "Disclosure" has a corresponding meaning.
EHR or Electronic Health Record	Has the meaning set out in s. 55.1 of PHIPA and generally means the electronic systems that are developed and maintained by OH pursuant to Part V.1 of PHIPA for the purpose of enabling HICs to Collect, Use and Disclose PHI by means of the systems.
Employee	A person employed and compensated by OH as an Employee, and is classified as either permanent full-time, permanent part-time, temporary full-time, temporary part-time, paid student or casual, as set out in the *Employee Classification Guideline*. A consultant or contractor is not an Employee.
Health Card Number, or HCN	Has the same meaning as 'health number' as defined in PHIPA and means the number, the version code or both of them assigned to an insured person within the meaning of the Health Insurance Act by the General Manager within the meaning of that Act.
HIC or Health Information Custodian	Has the meaning set out in s. 3 of PHIPA and generally means a person or organization that has custody or control of personal health information for the purpose of health care or other health-related duties. Examples include physicians, hospitals, pharmacies, laboratories and the MOH, but does not include OH.
HPPA	*Health Protection and Promotion Act and the regulations thereunder, as may be amended or relaced from time to time.*
IPC	Information and Privacy Commissioner of Ontario
IPC PO Manual	IPC Manual for the Review and Approval of Prescribed Organizations
MRN	Medical Record Number
O. Reg. 329/04	Ontario Regulation 329/04 made under PHIPA
OH	Ontario Health, the agency of the Government of Ontario to which this Policy applies.
OH Agent	A person that acts for or on behalf of OH for the purposes of OH, and not for the Agent's own purposes, whether or not the Agent has the authority to bind OH, whether or not the Agent is employed by OH, and whether or not the Agent is being remunerated.

Term / Acronym	Definition
PHI or Personal Health Information	Has the meaning set out in section 4 of PHIPA. Specifically, it is "identifying information" in oral or recorded form about an individual that: • Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family; • Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual; • Is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019; • Relates to payments or eligibility for health care or eligibility for coverage for health care in respect of the individual; • Relates to the donation by the individual of any body part or bodily substance of the individual or that is derived from the testing or examination of any such body part or bodily substance; • Is the individual's health number; and/or • Identifies an individual's substitute decision-maker. PHI also includes identifying information about an individual that is not PHI listed above but that is contained in a record that includes PHI listed above. Information is "identifying" when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.
PHIPA or *Personal Health Information Protection Act, 2004*	The Ontario health privacy law. It establishes rules for the management of PHI and the protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services. References to PHIPA include the regulation made thereunder, as may be amended or replaced from time to time.
PI or Personal Information	Has the meaning set out in section 2 of FIPPA. Specifically, it means recorded information about an identifiable individual, including: • information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual; • information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; • any identifying number, symbol or other particular assigned to the individual; • the address, telephone number, fingerprints or blood type of the individual; • the personal opinions or views of the individual except where they relate to another individual; • correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about the individual; and the individual's name where it appears with other personal information relating

Term / Acronym	Definition
	to the individual or where the disclosure of the name would reveal other personal information about the individual. Personal Information also includes information that is not recorded and that is otherwise defined as Personal Information when considering the manner of collection, notice to public, privacy impact assessments and safeguards.[1]
Prescribed Entity or PE	An entity that is prescribed in Ontario Regulation 329/04 for the purposes of s. 45 of PHIPA, to which a HIC is permitted to Disclose PHI, without the consent of the individual to whom the information relates, for the purpose of analysis or compiling statistical information for the management, evaluation, or monitoring of the allocation of resources to, or planning for, all or part of the health system, including the delivery of services.
Prescribed Organization or PO	The organization prescribed in Ontario Regulation 329/04 as the organization for the purposes of Part V.1 of PHIPA. The Prescribed Organization has the power and the duty to develop and maintain the EHR in accordance with Part V.1 of PHIPA and the regulations made thereunder.
Prescribed Person or PP	A person that is prescribed in the regulations for the purposes of s. 39(1)(c) of PHIPA, to which a HIC is permitted to Disclose PHI, without the consent of the individual to whom the information relates, to such person who maintains a registry of PHI for purposes of facilitating or improving the provision of health care or that relates to the storage or donation of body parts or body substances.
Prescribed Registry or PR	A registry of PHI that is prescribed in Ontario Regulation 329/04 maintained for the purpose of enabling or improving the provision of health care or that relates to the storage or donation of body parts or bodily substances.

[1] Section 38 (1) FIPPA

Term / Acronym	Definition
Privacy Incident	Any event where the Privacy Office is notified or becomes aware that a Privacy Breach may have occurred. This includes events that are reviewed/investigated and: 1.confirmed to be a Privacy Breach 2.confirmed not to be a Privacy Breach 3.it cannot or has not been determined if a Privacy Breach occurred (Suspected Privacy Breach). **Note:** Privacy Incidents include events involving PI and PHI, as well as De-identified Information and Business Identity Information as these events require investigation in accordance with this Policy to confirm if they are Privacy Breaches as defined below. OH shall investigate these incidents involving De-identified Data and Business Identity Information, considering factors such as the 1) risk of re-identification and related de-identification guidelines for De-identified Data, as well as 2) the context for handling data that OH received as Business Identity Information, to confirm that it does not constitute PI, respectively.

Term / Acronym	Definition
Privacy Breach	A Privacy Breach includes: 1) Privacy Breach of PHI or PI (Privacy PHI/PI Breach) means an event where: • The Collection, Use, or Disclosure of PHI or PI is not in compliance with PHIPA or its regulation, or with FIPPA or its regulations (i.e., without legal authority); and/or • The Viewing, handling or otherwise dealing with PHI provided to OH is not in compliance with PHIPA, or its regulation; • PHI or PI is stolen, lost or subject to unauthorized Collection, Use or Disclosure or where records of PHI or PI are subject to unauthorized copying, modification, or disposal. **Note:** A Privacy PHI/PI Breach does not include a breach of De-identified Information, or Business Identity Information, if the event does involve PI or PHI. 2) Privacy Breach of Privacy Policy or Agreement (Privacy Policy/Agreement Breach) means an event where: • There is a contravention of OH's privacy policies, procedures, or practices; and/or • There is a contravention of a privacy-related[2] term or condition in a: ○ data sharing agreements, ○ research agreements, ○ confidentiality agreements, or, ○ agreements with third-party service providers retained by OH to handle PHI or PI, ○ written acknowledgements acknowledging and agreeing not to use PHI or PI which has been de-identified and/or aggregated, to identify an individual; and • Does not include a privacy breach of PHI or PI **Note:** A Privacy Policy/Agreement Breach may include a breach that involves De-identified Information or Business Identity Information, if the breach relates to privacy controls in an agreement or a privacy policy, procedure or practice related to handling of De-identified Information or Business Identity Information.
SDM or Substitute Decision Maker	Has the meaning set out in s. 5 of PHIPA and in relation to an individual, means, unless the context requires otherwise, a person who is authorized under PHIPA to consent on behalf of the individual to the collection, use or disclosure of PHI about the individual.

[2] A privacy-related term or condition, includes terms or conditions that relate to privacy requirements from law (including, for example, FIPPA, PHIPA and GOLA), the IPC PP/PE Manual, the IPC PO Manual, IPC guidelines and orders, OH's privacy information practices or other controls to protect the privacy of individuals or the confidentiality of their PI and PHI.

Term / Acronym	Definition
Use	In relation to PHI or PI in the custody or under the control of a HIC or a person, "Use" means to view, handle or otherwise deal with the information, but does not include to Disclose the information, and "Use", as a noun, has a corresponding meaning. For the purposes of PHIPA, the providing of PHI between a HIC and an agent of the HIC is a Use by the HIC, and not a Disclosure by the person providing the information or a Collection by the person to whom the information is provided.

11 Review Cycle

This Policy is to be reviewed by Ontario Health at least within 3 years of its effective date or earlier if required in accordance with the *Privacy Audit and Compliance Policy.*

12 References and/or Key Implementation Documents

- *Personal Health Information Protection Act, 2004*
- *Canada Health Act*
- *Immunization of School Pupils Act*
- *Health Protection and Promotion Act*
- Ontario Regulation 329/04
- IPC PO Manual
- EHR Consent Directive Request Form
- EHR Privacy Auditing and Monitoring Policy
- Privacy Audit and Compliance Policy
- Privacy Incident Management Policy and Procedure

13 Appendices

- Appendix "A": Contents of Logging

14 Policy Consultations

The following were consulted in the development of this Policy:

- Staff from the Privacy Office and other OH Agents responsible for drafting, maintaining and/or reviewing the privacy policies in reference to OH's privacy requirements; and
- Working Group members of the Privacy Program Advisory Committee (version 1 of Policy).

15 Policy Review History

Date of Review MM/YYYY	Itemize section changed and description of change (if no changes made, indicate N/A	New policy number	Date of Approval DD/MM/YYYY	Approver
1/7/2025	• Updated IT contact information. • Added/edited information throughout Policy as per the updated IPC Manuals; • Updated roles and responsibilities to reflect changes in organizational structure; • Updated compliance will be enforced in accordance with the *Progressive Discipline Policy;* • Added accountabilities for Ontario Health Directors, Employees and Agents. • Revised definitions of Personal Health Information, Privacy Breach and Privacy Incident	INF-003.02-P	06/10/2025	CEO

16 Policy Repeal

1) Date of Repeal:
2) Reason for Repeal:
3) Date of Approval of Repeal:
4) Approver:

Appendix A: Contents of Electronic Records and Logs

Keeping an Electronic Record of Consent Directives

OH keeps an electronic record of all instances where a Consent Directive is made, modified, or withdrawn, as required by paragraph 5 of s. 55.3 of PHIPA.

The electronic record must identify:

- The individual or SDM who made, withdrew or modified the Consent Directive;
- The instructions that the individual or SDM provided regarding the Consent Directive;
- The health information custodian, agent or other person to whom the directive was made, withdrawn or modified; and,
- The date and time that the Consent Directive was made, withdrawn or modified.

Keeping an Electronic Record of Consent Overrides

OH keeps an electronic record of all instances where a Consent Directive is overridden by a HIC, as required by paragraph 6 of section 55.3 of PHIPA.

The electronic record must identify:

- The HIC that Disclosed the information;
- The HIC that Collected the information;
- Any agent of the HIC who Collected the information;
- The individual to whom the information relates;
- The type of information that was Disclosed;
- The date and time of the Disclosure;
- The purpose of the Disclosure (i.e. to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information related, or to prevent harm to another person or group of persons).

Log of Notices of Consent Directives

OH logs all notices of Consent Overrides that are provided to HICs, which serves as a notice of Consent Directive (since a Consent Override cannot be performed unless a Consent Directive is in place). See Log of Notice of Consent Overrides below.

Log of Notices of Consent Overrides

OH maintains a log of notices of Consent Overrides that have been sent to HICs pursuant to ss.

55.7(6) of PHIPA.

The log sets out the following:

- The Employee(s) or other OH Agent(s) who sent the notice;
- The HIC to whom the notice was sent;
- The date the notice was sent;
- The HIC that Disclosed the PHI as a result of the override;
- The name of any agent of the HIC who Collected the information, if available;
- The individual to whom the PHI relates;
- The type of PHI that was Collected;
- The date and time of the Collection; and
- The purpose of the Collection (i.e. to provide health care or facilitate the provision of health care to the individual with the consent of the individual, to prevent harm to the individual to whom the information relates, or to prevent harm to a person other than the individual to whom the information relates to a group of persons).

Log of Reports of Consent Overrides to the IPC

OH maintains a log of annual reports provided to the IPC based on or containing any information, other than PHI, that is kept in the electronic record that OH keeps of every instance where PHI that is accessible by means of the EHR that is the subject of a Consent Directive is Disclosed since the time of the last report pursuant to paragraph 16 of ss. 55.3 of PHIPA.

For each annual report, the log sets out the following:

- The Employee(s) or other OH Agent(s) who sent the report to the IPC;
- The Employee(s) or other person(s) acting on behalf of the IPC to whom the report was sent;
- The date the report was sent; and
- The date by which the next annual report must be sent to the IPC.

Log of Requests for Electronic Records of Consent Directives and Consent Overrides from HICs

OH maintains a log of the electronic records that are provided to HICs pursuant to paragraph 9 of s. 55.3 of PHIPA.

For each request for electronic records received from a HIC, the log sets out the following:

- The Employee(s) or other OH Agent(s) who received the request for electronic records;
- The date the request for electronic records was received by OH;
- The HIC who made the request for electronic records;

- The types of electronic records that were requested by the HIC;
- The employee(s) or other OH Agent(s) who responded to the request;
- The types of electronic records that were provided to the HIC;
- The agent of the HIC to whom the electronic records were provided;
- The form the electronic records were provided to the HIC;
- The manner the electronic records were provided to the HIC; and
- The date the electronic records were provided to the HIC.

Log of Requests for Electronic Records of Consent Directives and Consent Overrides from the IPC

OH maintains a log of the electronic records that are provided to the IPC pursuant to paragraph 8 of s. 55.3 of PHIPA.

For each request for electronic records received from the IPC, the log sets out the following:

- The employee(s) or other OH Agent(s) who received the request for electronic records;
- The date the request was received;
- The employee(s) or other person(s) acting on behalf of the IPC who submitted the request;
- The types of electronic records that were requested by the IPC;
- The employee(s) or other OH Agent(s) who responded to the request;
- The types of electronic records that were provided to the IPC;
- The employee(s) or other person(s) acting on behalf of the IPC to whom the electronic records were provided;
- The form in which the electronic records were provided to the IPC;
- The manner in which the electronic records were provided to the IPC; and
- The date when the electronic records were provided to the IPC.

Log of Audits of Electronic Records of Consent Directives and Consent Overrides

OH maintains a log of all audits conducted on the electronic records OH is required to maintain of Consent Directives and Consent Overrides pursuant to paragraphs 5 and 6 of s. 55.3 of PHIPA.

For each audit conducted, the log must set out the following:

- The nature and scope of the audit;
- The Employee(s) or other OH Agents who conducted the audit;

- The date the audit was conducted;
- The results of the audit;
- Any follow-up action that is required to be taken as a result of the audit;
- The Employee(s) or other OH Agent(s) responsible for taking the follow-up action;
- The date the follow-up action was completed;
- The Employee(s) or other OH Agent(s) or other third parties to whom the results of the audit must be communicated;
- The Employee(s) or other OH Agent(s) responsible for communicating the results of the audit.

Indicators to be Reported to the IPC

OH ensures that it records and maintains the information needed to prepare the indicators regarding Managing Consent in the EHR required by the IPC PO Manual and outlined below:

- The number of instances in which a Consent Directive has been made, modified or withdrawn since the prior review by the IPC.
- The number of instances in which a notice of a Consent Directive has been provided to a HIC in accordance with ss. 55.6 (7) of PHIPA since the prior review by the IPC.
- The number of instances in which a HIC has overridden a Consent Directive pursuant to s. 55.7 of PHIPA since the prior review by the IPC and the number of occasions on which each of ss. 55.7(1), (2) or (3) of PHIPA was invoked to override the Consent Directive.
- The number of instances in which a notice of a Consent Override has been provided to a HIC in accordance with ss. 55.7(6) of PHIPA since the prior review by the IPC.
- The dates on which reports of Consent Overrides were made to the IPC pursuant to paragraph 16 of s. 55.3 of PHIPA since the prior review by the IPC.
- The number of requests received from HICs pursuant to paragraph 9 of s. 55.3 of PHIPA for the electronic records of Consent Directives and Consent Overrides since the prior review by the IPC.
- The number of requests received from the IPC pursuant to paragraph 8 of s. 55.3 for the electronic records of Consent Directives and Consent Overrides since the prior review by the IPC.