

MOHLTC and SSHA

Response to *A Privacy Impact Assessment on
the Operations of the Ontario Laboratory
Information System*

February 10, 2008

Table of Contents

- 1.0 Introduction and Overview..... 2**
- 2.0 MOHLTC and SSHA PIA Response..... 3**
 - 2.1 Response Methodology..... 3
 - 2.2 Response to Recommendation 1.....4
 - 2.2.1 Response to Recommendation 1a5
 - 2.2.2 Response to Recommendation 1b7
 - 2.2.3 Response to Recommendation 1c.....8
 - 2.2.4 Response to Recommendation 1d10
 - 2.2.5 Response to Recommendation 1e12
 - 2.2.6 Response to Recommendation 1 (cont'd)13
 - 2.2.7 Response to Recommendation 1 (cont'd)14
 - 2.3 Response to Recommendation 2..... 15
 - 2.4 Response to Recommendation 3..... 16
 - 2.5 Response to Recommendation 4..... 17
 - 2.6 Response to Recommendation 5..... 18
 - 2.6.1 Response to Recommendation 5a 19
 - 2.6.2 Response to Recommendation 5b20
 - 2.6.3 Response to Recommendation 5c.....21
 - 2.7 Response to Recommendation 6.....22

1.0 Introduction and Overview

As of April 1, 2008 the Ontario Smart Systems for Health Agency (SSHA) will begin providing network, audit logging, de-identification and hosting services in respect of the Ontario Laboratory Information System (OLIS) for the Ministry of Health and Long Term Care (MOHLTC).

OLIS is a provincial laboratory information system under development by the MOHLTC. Once fully implemented, OLIS will electronically store test results from Ontario's medical laboratories and make those results available to authorized health care practitioners throughout Ontario. OLIS will eventually improve the quality and efficiency of the health care patients receive, eliminate unnecessary duplication of laboratory tests and reduce medical errors that result from a lack of patient information. Health care practitioners will have faster access to test results, meaning they can diagnose conditions and begin treatment sooner.

OLIS is in the very early stages of implementation and is not currently fully operational. The system is being implemented in a series of carefully planned steps. The first step is for the Foundation Adopters, a small group of hospitals and community laboratories (organizations that will participate in OLIS in the future are generically referred to as "OLIS Adopters"), to begin entering their results into OLIS. To initiate this process, three Foundation Adopter hospitals and three Foundation Adopter community laboratories began sending their lab results to OLIS in late 2007. However, the MOHLTC has not yet deemed OLIS ready for clinical use. As such, no clinical users in Ontario currently have access to OLIS.

As part of SSHA's Privacy Management Program, SSHA has commissioned a privacy impact assessment (PIA) on the OLIS services for which it will be responsible; the PIA is in response to legal requirements under the *Personal Health Information Protection Act, 2004* (PHIPA) applicable to SSHA as a "health information network provider" in relation to OLIS. This PIA, which was completed on January 16, 2008, resulted in the identification of several privacy risks and six recommendations to strengthen the OLIS Privacy Framework.

The current document serves as the MOHLTC's and SSHA's response to the OLIS PIA commissioned by SSHA.

2.0 MOHLTC and SSHA PIA Response

2.1 Response Methodology

Section 2 of this document summarizes the MOHLTC's and SSHA's existing safeguards and activities planned in relation to risks and recommendations identified in the OLIS PIA commissioned by SSHA. These responses are arranged in table format organized under the following headings:

- **Recommendation:** Below are the six recommendations identified in the January 16, 2008, *A Privacy Impact Assessment on the Operations of the Ontario Laboratories Information System*, written by Sextant Software on behalf of the Smart Systems for Health Agency. Where the PIA identifies multiple sub-recommendations, the associated risk mitigation steps and planned activities are described in separate tables. Furthermore, the PIA categorized recommendations as "pre-transition" or "post-transition." Pre-transition recommendations should be implemented by the MOHLTC and SSHA prior to March 31, 2008, when SSHA assumes responsibility for providing OLIS services. Post-transition recommendations are those that can be implemented by the MOHLTC and SSHA after March 31, 2008. The recommendation cell indicates if the recommendation is intended to be implemented pre or post transition.

Note: the transition date, March 31, 2008, is not the date that the MOHLTC will deem OLIS ready for clinical use. There are a variety of factors that figure into this decision, some of which are discussed below. The MOHLTC will only deem OLIS ready for clinical use once the system has been adequately tested and a robust privacy infrastructure is in place.

Note: The terms consent management and consent administration will appear to be used interchangeably in this document. In responding to any recommendations that use the term "Consent Administration" the term Consent Management will be used to delineate the stakeholder-driven activities that OLIS will perform to handle consent directives.

- **Potential Consequences:** The potential consequences of the privacy risks identified in the tables below are the negative situations that may result if the MOHLTC and SSHA do not implement the OLIS PIA's recommendations. The potential consequences provided were established by SSHA following the completion of the PIA.
- **Current Risk Mitigation:** The current risk mitigation descriptions are the steps that have already been taken by the MOHLTC and SSHA to reduce or eliminate the privacy risks and vulnerabilities that the PIA recommendation addresses.
- **Planned Activities:** This section identifies the tasks and strategies the MOHLTC and SSHA have planned to address and implement all of the PIA's recommendations. Scheduled dates of completion for those tasks are provided, where available.

The recommendations below are numbered as they are in the PIA. Refer to the PIA for a detailed description of each recommendation and related issues.

2.2 Response to Recommendation 1	
Recommendation 1	<p>Pre-transition: SSHA should obtain a clear understanding from MOHLTC of its information governance roles and responsibilities for the operation of OLIS, with particular consideration given to:</p> <ul style="list-style-type: none"> a) consent directives management; b) role-based access control model, including roles and their access privileges, and the processes by which they are determined and administered; c) privacy complaints and incident management, especially with regard to liaison with organisational privacy officers; d) disclosures of PHI to third-parties, including disclosure of information in the audit log; and e) retention of data in OLIS repositories and audit log. <p>SSHA should also obtain a legal opinion on the Agency's status under PHIPA with respect to its planned operations of OLIS.</p> <p>Post-transition: SSHA should have a clear understanding of its information governance roles and responsibilities before access to information in the OLIS clinical repository is made broadly available to healthcare practitioners.</p>
Potential Consequences	<ul style="list-style-type: none"> • Reputation risk to SSHA, the eHealth Office and HICs. • Loss of trust of Ontarians in SSHA, the eHealth Office and HICs. • Risk of inappropriate access to OLIS and PHI by unauthorized users, third parties and recipients of audit logs. • Risk of inappropriate disclosure of PHI due to a lack of administrative controls. • Lack of clarity regarding roles and responsibilities surrounding time-critical aspects of OLIS operations. • Risk of delay in response to, and resolution of, privacy complaints and incidents. • Risk of inappropriate retention of PHI. • Risk of inappropriate disclosure of PHI through the audit log. • Lack of clarity regarding SSHA's status under PHIPA when operating OLIS. • Lack of clarity regarding information governance roles and other responsibilities of the SSHA and eHealth office.
Current Risk Mitigation	<p>The current mitigation plan for each of the sub-recommendations identified in PIA Recommendation #1 are described in separate tables below.</p>
Planned Activities	<p>The current planned activities plan for each of the sub-recommendations identified in PIA Recommendation #1 are described in separate tables below.</p>

2.2.1 Response to Recommendation 1a	
Recommendation 1a	<p>SSHA should obtain a clear understanding from MOHLTC of its information governance roles and responsibilities for the operation of OLIS, with particular consideration given to:</p> <p>a) consent directives administration:</p>
Current Risk Mitigation	<p>In its role of providing network, hosting and application management services, SSHA will not be involved in the management of consent directives for OLIS. The current OLIS consent directives management process was developed in 2003, prior to the introduction of the Personal Health Information Protection Act, 2004. The MOHLTC is reviewing this consent directives management process and related OLIS functionality. OLIS has not yet been deemed ready for clinical use and, as such, access to OLIS via hospital, lab and OLIS viewers is not available at this time. The MOHLTC will not deem OLIS ready for clinical use until the following consent directives management related tasks are complete (in addition to the completion of other data protection related tasks described below):</p> <p>a) The consent directives management process has been reviewed;</p> <p>b) The consent directives management process has been formally defined, approved and communicated to OLIS Foundation Adopters; and</p> <p>c) Any changes required to make the OLIS application’s consent directives management process PHIPA-compliant have been made.</p> <p>The current consent directives management process allows patients to request a “block” on one or more of their tests results. This blocking request can be made at the time of specimen collection or any time thereafter. The block will prevent all OLIS users, except for the physician that ordered the laboratory test and any physician “copied” on the test result, from accessing the blocked results. Authorized health care providers may override a block with the consent of the patient or his/her substitute decision maker. The fact that a health care provider has overridden a block is captured in the OLIS audit log, along with the identity of the health care provider who overrode the block, and the date and time of the block override. This consent directives management process, which is described in the draft OLIS Consent Management Process document, an internal current-state consent management overview document developed by the Ministry of Health and Long-Term Care in October 2007, is currently operational (i.e. patients can request that their laboratory tests be blocked, even though access to OLIS is not currently available) and the MOHLTC has made information available on how patients can request a block on their test results to OLIS Foundation Adopters and on the MOHLTC website.</p>
Planned Activities	<ul style="list-style-type: none"> • The MOHLTC is in the process of reviewing the current consent directives management process and identifying any gaps between the current process and PHIPA’s requirements. In addition, this consent directives management review will consider the consent management administration processes established by the Ontario Drug Profile Viewer program to ensure, where possible, consistency across MOHLTC e-Health initiatives. • The MOHLTC will create an OLIS application change request (i.e. a request to the OLIS technical architects to change system functionality) by March 7, 2008, in order to rectify any legal compliance gaps it identifies and increase consistency with the Drug Profile Viewer program consent directives management processes. • The MOHLTC will create an OLIS Consent Directives Management

	<p>Procedure by March 31, 2008, to define how the OLIS application meets, and enables OLIS Adopters to meet, PHIPA requirements. This procedure will also identify the consent directives management roles and responsibilities of all organizations involved in the process, including: OLIS Adopters and the MOHLTC. (Note that the MOHLTC does not currently anticipate SSHA having a role or responsibilities in the consent directives management process.)</p> <ul style="list-style-type: none">• By March 31, 2008, MOHLTC will develop communications materials for patients and OLIS Adopters about the consent directives management process.• The MOHLTC will complete the above tasks prior to deeming OLIS ready for clinical use, at which point OLIS Adopters may begin accessing the system for patient care purposes.
--	--

2.2.2 <u>Response to Recommendation 1b</u>	
Recommendation 1b	SSHA should obtain a clear understanding from MOHLTC of its information governance roles and responsibilities for the operation of OLIS, with particular consideration given to: <ul style="list-style-type: none"> b) role-based access control model, including roles and their access privileges, and the processes by which they are determined and administered;
Current Risk Mitigation	See current risk mitigation discussion in relation to PIA Privacy Risk #2.
Planned Activities	See planned activities discussion in relation to privacy risk #2.

2.2.3 <u>Response to Recommendation 1c</u>	
Recommendation 1c	<p>SSHA should obtain a clear understanding from MOHLTC of its information governance roles and responsibilities for the operation of OLIS, with particular consideration given to:</p> <ul style="list-style-type: none"> c) privacy complaints and incident management, especially with regard to liaison with organisational privacy officers;
Current Risk Mitigation	<ul style="list-style-type: none"> • Both the MOHLTC and SSHA currently have in place privacy complaint management procedures and incident management procedures. • The MOHLTC and SSHA have understandings of their responsibilities with respect to the provision of OLIS services, including in relation to privacy complaints and incident management. Procedures for handling privacy complaints and incidents involving both the MOHLTC and SSHA also exist. • SSHA staff and OLIS project staff at the MOHLTC have been trained in incident management procedures and privacy complaint response. • The MOHLTC has drafted an OLIS System Access Agreement which all participating organizations must enter into prior to accessing OLIS. OLIS community laboratory Foundation Adopters have executed System Access Agreements and it is expected that hospital Foundation Adopters will execute the agreements before March 31, 2008. The System Access Agreement include provisions concerning the following privacy complaints and incident management issues: <ul style="list-style-type: none"> ○ Reciprocal Notification Requirements: in the event that the MOHLTC becomes aware of a privacy incident, it must notify the OLIS Adopter involved/affected. In the event that an OLIS Adopter becomes aware of a privacy incident, it must notify the MOHLTC. This enables both parties to take appropriate steps to investigate and contain the incident, notify the appropriate individuals (including patients in the case of OLIS Adopters), and implement remedial actions. ○ Privacy Complaints Cooperation: The MOHLTC and OLIS Adopters will provide all assistance reasonably requested by the other party in relation to any privacy concerns relating to OLIS, including individuals' complaints, or the Information and Privacy Commissioner of Ontario's reviews or complaints. ○ Appointing an OLIS Contact Person: Each OLIS Adopter must appoint an individual to be responsible for OLIS issues, and provide this individual's contact information to the MOHLTC. • Finally, educational materials about OLIS have been developed and made available to OLIS Adopters as hard-copy brochures, and to the public through the MOHLTC website. The website and brochure provide the public with an overview of OLIS, and instructions for contacting the INFOline with questions and concerns.
Planned Activities	<ul style="list-style-type: none"> • The MOHLTC and SSHA are in the process of drafting an Enterprise Privacy Agreement that will outline each organization's privacy responsibilities in relation to provincial eHealth initiatives, including OLIS. • The MOHLTC and SSHA are in the process of entering into a Service Management Agreement, which will clarify each organization's roles and responsibilities in relation to OLIS.

	<ul style="list-style-type: none">• The MOHLTC will review its existing privacy complaints and incident management procedures to ensure that, where required, they correspond with SSHA's in relation to OLIS. This review will be completed prior to transition on March 31, 2007.• The MOHLTC will, by March 31, 2008, develop additional educational materials for MOHLTC staff and Adopters on the management of privacy complaints and incidents.• The MOHLTC will provide an OLIS Privacy Training refresher course to members of its staff working on OLIS once the privacy complaints and incident management procedures have been reviewed and the OLIS Privacy Policies and Procedures have been developed. This Privacy Training refresher will be completed in Spring 2008.
--	---

2.2.4 <u>Response to Recommendation 1d</u>	
Recommendation 1d	<p>SSHA should obtain a clear understanding from MOHLTC of its information governance roles and responsibilities for the operation of OLIS, with particular consideration given to:</p> <ul style="list-style-type: none"> d) disclosures of PHI to third-parties, including disclosure of information in the audit log;
Current Risk Mitigation	<ul style="list-style-type: none"> • No disclosures of personal health information are currently being made via OLIS, as the MOHLTC has not yet deemed it ready for clinical use. • Disclosures of personal health information via OLIS are regulated by PHIPA. • The MOHLTC has drafted an OLIS System Access Agreement which all participating organizations must enter into prior to accessing OLIS. OLIS community Laboratory Foundation Adopters have executed System Access Agreements and it is expected that hospital Foundation Adopters will execute the agreements before March 31, 2008. The System Access Agreement includes the following provisions relating to the disclosure of personal health information: <ul style="list-style-type: none"> ○ OLIS Adopters’ Responsibilities for Disclosures: OLIS Adopters may only disclose or access personal health information via OLIS as permitted by PHIPA and the System Access Agreement. ○ OLIS Adopters’ Responsibilities for Agents: OLIS Adopters are responsible for their agents’ (e.g. employees, officers, directors, and any other third parties) actions in relation to OLIS and must ensure that these individuals comply with the “End User Acceptable Use Policy” which is attached as Schedule C to the System Access Agreement. Under the End User Acceptable Use Policy, the MOHLTC may require the OLIS Adopter to terminate one or more of its agents’ access to OLIS. Furthermore, the End User Acceptable Use Policy identifies additional privacy requirements; for example, the OLIS Adopter’s agents must enter into an End User Agreement that requires them to: <ul style="list-style-type: none"> ▪ Not disclose their passwords to anyone, including other OLIS users; ▪ Not allow others to use OLIS while they are logged in; ▪ Log out after each session of use; ▪ Notify the site’s system administrator in the event they suspect password security has been compromised, so the password can be changed as soon as reasonably possible; ▪ Only access OLIS from within the OLIS Adopters’ sites with whom they have entered into an End User Agreement; ▪ Not gain or attempt to gain electronic access to OLIS other than through the OLIS Adopters’ connection to the SSHA network and using SSHA’s related equipment; and ▪ Immediately report any privacy incidents to the Adopter. ○ MOHLTC’s Responsibilities for Disclosure: The MOHLTC will not use or disclose any personal health information to which it has access, except as required to fulfill its obligations under the System Access Agreement or as permitted by FIPPA or PHIPA. ○ MOHLTC’s Responsibilities for Agents: The MOHLTC may not permit its employees or any third parties acting on its behalf to access

	<p>personal health information unless the employee or third party agrees to comply with the restrictions that apply to the Ministry under the System Access Agreement.</p> <ul style="list-style-type: none"> • Use of audit log information for OLIS testing purposes is regulated by the System Access Agreement, PHIPA, and applicable SSHA and MOHLTC policies and procedures.
<p>Planned Activities</p>	<ul style="list-style-type: none"> • The MOHLTC will execute System Access Agreements with hospital Foundation Adopters prior to March 31, 2008. • The MOHLTC will draft an OLIS Privacy Policy describing OLIS, the privacy roles and responsibilities of participating organizations, and the administrative, technical and physical safeguards included in OLIS by March 31, 2008. This policy will identify the disclosures of personal health information permitted, including that associated with the audit log. The MOHLTC will not deem OLIS ready for clinical use until this policy is in place. • Any additional requests for OLIS PHI that may be requested to support other MOHLTC initiatives (e.g. Public Health Reportable Diseases or Colo-rectal Screening) will be reviewed to determine compliance with regulatory and PHIPA requirements before data access is granted.

2.2.5 Response to Recommendation 1e

Recommendation 1e	SSHA should obtain a clear understanding from MOHLTC of its information governance roles and responsibilities for the operation of OLIS, with particular consideration given to: <ul style="list-style-type: none"> e) Retention of data in OLIS repositories and audit log.
Current Risk Mitigation	<ul style="list-style-type: none"> • An OLIS-specific record retention schedule does not currently exist. Until the MOHLTC develops one, personal health information in OLIS and its audit log will be retained in compliance with the Drug Profile Viewer Record Retention Schedule. This policy requires that personal health information in the OLIS clinical repository be retained indefinitely, with the audit log retained for 10 years.
Planned Activities	<ul style="list-style-type: none"> • Clinical, operational and legal requirements for record retention and destruction will be established post-transition. • Post-transition, but no later than Summer 2008, the MOHLTC will develop an approach to retaining clinical and audit data. The Record Retention Schedule will address clinical and legal requirements. • The MOHLTC will lead the development of the OLIS Record Retention Schedule and will notify the SSHA of the requirements once developed. The OLIS Record Retention Schedule will address record archiving (see PIA Privacy Recommendation 5B below), as archiving strategy requirements depend on the Record Retention Schedule (i.e. the longer the retention periods, the greater the storage requirements, the greater the need for a long-term archiving strategy, and vice versa).

2.2.6 Response to Recommendation 1 (cont'd)

Recommendation 1 (cont'd)	SSHA should also obtain a legal opinion on the Agency's status under PHIPA with respect to its planned operations of OLIS.
Current Risk Mitigation	SSHA has retained the law firm of Heenan Blaikie to provide legal opinion prior to 31 March, 2008.
Planned Activities	<p>Planned activities will be dictated by the outcome of the legal opinion.</p> <ul style="list-style-type: none"> • SSHA will provide the MOHLTC with a copy of the legal opinion to the MOHLTC eHealth Office prior to it being shared with any other parties. SSHA and the MOHLTC will discuss impacts of the status designation of SSHA. • SSHA will provide a copy of the legal opinion upon request by the Information Privacy Commissioner Office of Ontario.

2.2.7 Response to Recommendation 1 (cont'd)	
Recommendation 1 (cont'd)	Post Transition SSHA should have a clear understanding of its information governance roles and responsibilities before access to information in the OLIS clinical repository is made broadly available to healthcare practitioners.
Current Risk Mitigation	<ul style="list-style-type: none"> • Please see response to Recommendation 1c)
Planned Activities	Upon completion of the Enterprise Privacy Agreement and the Service Management Agreement, SSHA expects to have a clear understanding of its information governance roles and responsibilities.

2.3 Response to Recommendation 2	
Recommendation 2	<p>Post-transition:</p> <p>Because SSHA operations should apply a consistent, unified, and user-centric role-based access control model for all eHealth applications that SSHA will administer, the Agency should request the MOHLTC eHealth Program to provide it with one.</p>
Potential Consequences	<ul style="list-style-type: none"> • Reputation risk to SSHA, the eHealth Office and the HICs. • Loss of trust of Ontarians in SSHA, the eHealth Office and HICS. • Development of unnecessary inefficiencies of process for SSHA if there are unique access control models for different eHealth applications.
Current Risk Mitigation	<ul style="list-style-type: none"> • There is a consent management strategy and approach within the overall eHealth strategy that is awaiting approval. Currently access to OLIS for reviewing results is only allowed through the OLIS web viewer which manages role-based access through the SSHA Registration Management System. Hospital viewer access and expansion of access through the OLIS viewer will be limited until more comprehensive solution is identified that addresses the need for detailed access controls.
Planned Activities	<ul style="list-style-type: none"> • The MOHLTC eHealth Program is forming a Policy working group to explore the implications of requiring all eHealth stakeholders to identify themselves in a consistent and assured manner as part of a broader eHealth access approach. • The MOHLTC eHealth Program is developing the strategy for an eHealth User Registry to support the current eHealth Client and Provider Registry projects. The User Registry will incorporate components of Authentication, Authorization (Role Based Access Controls), Access Logging and account information into a single system that will support all the eHealth applications in the future.

2.4 Response to Recommendation 3	
Recommendation 3	<p>Post-transition:</p> <p>Because SSHA is committed to providing robust, privacy-protective data services; because a privacy breach of a patient's express consent directives could adversely affect the Agency's reputation for protecting the healthcare-related privacy of Ontarians; and because SSHA's operations would benefit from consistent, unified, and user-centric consent directives management for all eHealth applications that the Agency will administer, SSHA should request the MOHLTC eHealth Program to provide the Agency with an approach to consent management that is consistent and unified across all eHealth applications.</p>
Potential Consequences	<ul style="list-style-type: none"> • Reputation risk to SSHA, the eHealth Office and the HICs. • Loss of trust of Ontarians in SSHA, the Health Office and HICS. • Development of unnecessary inefficiencies of process for SSHA if consent management is handled differently for different eHealth applications.
Current Risk Mitigation	<ul style="list-style-type: none"> • The OLIS privacy office is currently reviewing the OLIS consent and blocking controls to evaluate compliance against PHIPA before any broader access is granted to the system. Currently only laboratories that are providing data to OLIS are allowed to view results in order to perform Quality Assurance on the data they transmit. • OLIS currently employs consent repository to manage the requirements for consent for lab results. This function will continue to be employed by OLIS until the creation of an eHealth consent service is created.
Planned Activities	<ul style="list-style-type: none"> • The OLIS privacy office will be examining the current provisions within OLIS for consent management and role-based access controls. The privacy office will provide direction and requirements back to the eHealth office so that requirements for OLIS are included in the finalization of the eHealth consent model. • The MOHLTC eHealth Program is developing a consent directives registry that will operate within the provincial HIAL (Health Information and Access Layer). When operational, the provincial HIAL will handle all requests for information from all the eHealth applications in a unified manner. The consent directives registry within the HIAL will then provide a consistent process for managing consent across all eHealth applications. • The MOHLTC eHealth Program will continue to review and enhance the consent mechanisms within OLIS through the OLIS privacy office and reviews outlined in the responses to Recommendation 1.

2.5 Response to Recommendation 4	
Recommendation 4	<p>Pre-transition: SSHA should consult with the MOHLTC eHealth Program to determine the most appropriate way to mitigate the privacy risks inherent in allowing PHI to remain in the OLIS access report.</p>
Potential Consequences	<ul style="list-style-type: none"> • Reputation risk to SSHA, the eHealth Office and the HICs. • Loss of trust of Ontarians in SSHA, the Health Office and HICS. • Unnecessary use and disclosure of, and risk to, PHI when viewing information of which authorized individuals have accessed patient data in OLIS.
Current Risk Mitigation	<ul style="list-style-type: none"> • There are currently no clinicians viewing the OLIS Access Report as OLIS access is only being granted to participating laboratories. The original requirement to provide the OLIS access report is being reviewed to determine if removing PHI will inhibit an individual from being able to have a definitive view of who has accessed their health information. • The SSHA OLIS Transition Lead has created and submitted a change request to remove PHI from the OLIS access report to the MOHLTC Change Review Board. The board will be reviewing the change request before the end of February 2008.
Planned Activities	<ul style="list-style-type: none"> • The OLIS privacy office will review the requirements of the OLIS access report and the potential exposures of the PHI. An alternative being proposed by SSHA to use LOINC code sets instead of discrete lab test names as a mitigation to the PHI exposure will also be analyzed. Should the decision be made to remove the PHI from the report, the OLIS change request will be finalized and submitted for design before transition occurs.

2.6 Response to Recommendation 5	
Recommendation 5	<p>Pre-transition: SSHA should support the MOHLTC eHealth Program initiative to develop policies and procedures for the OLIS Privacy Implementation Office in order to ensure:</p> <ul style="list-style-type: none"> a) an integrated end-to-end process for managing eHealth privacy and security incidents, including liaison with organisational privacy officers; b) coherent policies and procedures related to retention and archiving of PHI in eHealth applications, including laboratory test results; and c) policies and procedures for protection, retention and disclosure of audit log information
Potential Consequences	<ul style="list-style-type: none"> • Inefficient communication about, and management of, privacy and security incidents. • Reputation risk to SSHA, the eHealth Office and the HICs. • Loss of trust of Ontarians in SSHA, the Health Office and HICS. • Risks are caused by a lack of policies and procedures for protection, retention and disclosure of audit log information. • Risk of re-identification of patients whose information is contained in OLIS.
Current Risk Mitigation	The current mitigation plan for each of the sub-recommendations identified in PIA Recommendation #5 are described in separate tables below.
Planned Activities	The current planned activities plan for each of the sub-recommendations identified in PIA Recommendation #5 are described in separate tables below.

2.6.1 Response to Recommendation 5a	
Recommendation 5a	SSHA should support the MOHLTC eHealth Program initiative to develop policies and procedures for the OLIS Privacy Implementation Office in order to ensure: <ul style="list-style-type: none"> a) an integrated end-to-end process for managing eHealth privacy and security incidents, including liaison with organisational privacy officers;
Current Risk Mitigation	Refer to Current Mitigation Plan described in response to PIA Privacy Recommendation 1C above.
Planned Activities	Refer to Planned Activities described in response to PIA Privacy Recommendation 1C above.

2.6.2 Response to Recommendation 5b

Recommendation 5b	SSHA should support the MOHLTC eHealth Program initiative to develop policies and procedures for the OLIS Privacy Implementation Office in order to ensure: b) coherent policies and procedures related to retention and archiving of PHI in eHealth applications, including laboratory test results;
Current Risk Mitigation	Refer to Current Mitigation Plan described in response to PIA Privacy Recommendation 1E above.
Planned Activities	Refer to Planned Activities described in response to PIA Privacy Recommendation 1E above.

2.6.3 <u>Response to Recommendation 5c</u>	
Recommendation 5c	SSHA should support the MOHLTC eHealth Program initiative to develop policies and procedures for the OLIS Privacy Implementation Office in order to ensure: <ul style="list-style-type: none"> c) policies and procedures for protection, retention and disclosure of audit log information
Current Risk Mitigation	Refer to Current Mitigation Plan described in response to PIA Privacy Recommendation 1D (disclosure) and 1E (retention) above.
Planned Activities	Refer to Planned Activities described in response to PIA Privacy Recommendation 1D (disclosure) and 1E (retention) above.

2.7 Response to Recommendation 6	
Recommendation 6	Pre-transition: SSHA should request the MOHLTC eHealth Program to commission an independent analysis of the OLIS pseudonymisation algorithm and its operations, including a cryptographic review, in order to ensure its robustness and effectiveness.
Potential Consequences	<ul style="list-style-type: none"> • Reputation risk to SSHA, the eHealth Office and the HICs. • Loss of trust of Ontarians in SSHA, the Health Office and HICS. • Risk of re-identification of patients whose information is contained in OLIS.
Current Risk Mitigation	Access to pseudonymised database is restricted and no external, MOHLTC or SSHA stakeholders are accessing the Pseudonymous data. No access will be permitted until a review of the pseudonymisation algorithm and a risk profile of the data is complete.
Planned Activities	<ul style="list-style-type: none"> • At the request of the MOHLTC, SSHA is in the process of commissioning an independent analysis of the pseudonymisation algorithm and its operations including a cryptographic review of the algorithm in order to ensure its robustness and effectiveness. • At the request of the MOHLTC, SSHA has commissioned Dr. Khaled El-Eman of the University of Ottawa to conduct a risk analysis of the data elements in the pseudonymous repository and the orders repository will be conducted to identify the potential risks of cross linking and profile building on the de-identified elements. The risk analysis will identify any areas of risk where policies will need to be implemented to mitigate any potential exposures that could occur as a result of data profiling. • The MOHLTC will continue to restrict access to the pseudonymised database until the cryptographic and risks reviews are complete.