

Ontario Laboratory Information System

PIA Summary

© 2007, Smart Systems for Health Agency
Copying without permission is prohibited. All rights reserved.

Table of Contents

1.0 Solution Overview 1

 1.1 Project Description/Background 1

 1.2 Sources of Information on Privacy and OLIS..... 2

2.0 Purpose and Scope of the PIA 3

 2.1 Purpose 3

 2.2 In-Scope 3

 2.3 Out-of-Scope 3

3.0 Findings..... 4

 3.1 General statement from the findings of the PIA..... 4

4.0 Technical Safeguards in Place to Protect Information..... 5

5.0 Risks, Mitigation and Timeframe 10

1.0 Solution Overview

This PIA was commissioned by the Smart Systems for Health Agency (SSHA) as part of preparations to transfer technical operations of the Ontario Laboratory Information System (OLIS) to SSHA in March of 2008. Its purpose is to identify any privacy issues that the Agency should address in order to ensure ongoing protection of personal health information in OLIS when these operations are transferred.

This PIA is one of several that have been performed on OLIS. Previously, the eHealth Program has performed PIAs at the conceptual, logical, and physical stages of OLIS development and implementation. This PIA focuses on the OLIS application itself: how the application is used; how its databases are maintained; the ways in which data flows into those databases from hospital, public and community medical laboratories; the ways in which data flows out of those databases to fulfil information access requests; how privacy-related processes such as access control, and consent and data blocking work; and, how audit information recorded by SSHA can be used to answer questions about who has accessed a patient's records in OLIS.

1.1 Project Description/Background

OLIS is a central database of lab test results for Ontario residents and others who have been treated as patients in Ontario hospitals, clinics, and medical practices. It provides authorized healthcare providers with access to the results of laboratory tests that were ordered and processed on the patients to whom they are providing healthcare services.

OLIS consists of three primary repositories:

1. a **clinical repository** used to record lab results reported from community, public, and hospital-based medical labs.
2. a **pseudonymous repository** that contains de-personalized information derived from the clinical repository and is used for planning and research.
3. an **orders reporting repository** that has been constructed to allow the MOHLTC to better manage its program of Ministry-funded lab tests. The repository contains a record for each lab test order in the Clinical Repository that is covered by OHIP. This repository does not contain test results.

Three ancillary repositories are needed to support various aspects of OLIS operations:

4. an **enrolment Repository** was designed to record access credentials for healthcare practitioners authorised to access OLIS. Currently, all of the data that would otherwise be stored in this repository is delivered in real-time by the SSHA Registration Management Service, ONE ID.
5. a **Consent Repository** used for recording the consent directives of those individuals who wish to restrict access to some or all of their lab tests to only those healthcare practitioners who have ordered the test or who are explicitly named on the order as recipients of test results ("copy-to").

6. a **Vendor Products Repository** will store information that identifies vendor applications, such as hospital information systems, that have passed OLIS conformance tests and that can therefore be used to exchange information with the OLIS application.

All these repositories will be hosted and operated by SSHA.

Access to OLIS is provided through Hospital Information Systems (HIS). Clinics and physician offices will be able to access OLIS via Clinical Management Systems (CMS) or practice management systems that are connected to OLIS. Labs access OLIS via Laboratory Information Systems (LIS). Healthcare providers will also be able to access lab results in OLIS directly via a web browser.

At present, lab results in OLIS come from one community medical laboratory. Currently, three hospital corporations are connected to OLIS. The connection allows access to OLIS by healthcare providers within each hospital and also allows copies to be generated of all test results from the hospitals' own in-house labs. In the future, all community and public laboratories and hospital laboratories will feed data into OLIS

From its inception until now, OLIS has been managed and operated by the OLIS Office of the MOHLTC eHealth Program. During this time, the OLIS systems and servers have been hosted in the SSHA Markham and Streetsville data centres and managed by Hewlett Packard under contract to Accenture, the software developer of OLIS. SSHA has provided the network services that allow medical laboratories and hospitals to connect to OLIS.

1.2 Sources of Information on Privacy and OLIS

The findings of this PIA are based in part on information provided by a review of project documentation provided by the MOHLTC eHealth Program, SSHA, and consultants currently working on OLIS. It is also based on interviews the authors conducted with MOHLTC and SSHA staff and consultants, SSHA information privacy and security division staff, MOHLTC eHealth Office staff, MOHLTC Legal Branch staff, and Anzen Consulting staff. The authors have also contrasted the privacy protective features of OLIS with those of two other systems: British Columbia's equivalent to OLIS, the Provincial Laboratory Information System (PLIS), and the Ontario Drug Profile Viewer (DPV). The former comparison highlights some privacy-protective features that OLIS could benefit from in future. The latter highlights operational variations related to privacy and their potential impact on future SSHA operations.

Readers who are unfamiliar with health information privacy legislation in Ontario may find useful a guide to Ontario's Personal Health Information Protection Act (PHIPA) that has been provided by the Information and Privacy Commissioner of Ontario. *A Guide to the Personal Health Information Act*, available at <http://www.ipc.on.ca/index.asp?navid=46&fid1=400>

A general description of clinical repositories of laboratory test results and the role they play in supporting electronic health record deployments can be found in *Laboratory Information Systems: Providing On-Line Test Results to Speed Diagnosis and Care*. It is available at: http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/Infosheet_E_Lab_Final.pdf

Finally, MOHLTC has an OLIS web site which provides a basic explanation of OLIS and what patients can do to protect the privacy of their information. The web site can be found at www.health.gov.on.ca/olis

2.0 Purpose and Scope of the PIA

2.1 Purpose

The purpose of this PIA is to provide SSHA with information that will allow the Agency to be proactive in ensuring the protection of personal health information contained in OLIS during and after the transfer of technical operations to SSHA. It also serves to fulfil its legal obligation under PHIPA to provide such an analysis for the systems it provides as a health information network provider.

2.2 In-Scope

The following components fall within the scope of this PIA:

- a discussion of relevant terminology used in OLIS;
- a description of the OLIS systems and infrastructure, the OLIS databases, and the server environment that supports these systems;
- a description of the data that is contained in the OLIS databases and how that data flows into and out of OLIS;
- a description of the technical safeguards that will be implemented to protect against unauthorized access, use, disclosure, modification or loss, including the technical mechanisms that support access control, consent management, masking and locking of data, audit and enforcement;
- a current state privacy analysis using the Ontario Information and Privacy Commission's *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* as a framework for the analysis; and
- a discussion of privacy-related risks in the technical operation of OLIS and how SSHA can effectively mitigate these risks.

2.3 Out-of-Scope

Data for OLIS is obtained from the MOHLTC Registered Persons Database (RPDB), the MOHLTC Corporate Providers Database (CPDB), the MOHLTC Public Health Laboratories, hospital laboratories that are operated by Ontario hospital corporations, and community medical laboratories that provide services to Ontarians and to Ontario healthcare practitioners. All of these data sources are required to have privacy protections and information management practices in place that meet the requirements of the legislation that pertains to their operations. The following are therefore out of scope of this PIA:

- sources from which PHI is obtained (e.g., public, community, and hospital labs);

- the circumstances in which collection of PHI takes place (e.g., the clinical procedures in a specimen collection centre);
- the recipients of PHI from OLIS and their subsequent use of that information (with the exception of processes related to user registration, authentication, and authorization: these remain within scope);
- Hospital Information Systems (HIS) operating in Ontario. These systems should be the subject of PIAs performed by the hospitals that run them;
- Laboratory Information Systems (LIS) operating in Ontario labs;
- the privacy-protective practices of healthcare providers and healthcare organizations except where they relate explicitly to the functioning of OLIS; and
- the privacy-protective policies and processes of the MOHLTC Registered Persons Database (RPDB) and Corporate Providers Database (CPDB), as these databases, used by OLIS, are subject to systematic privacy and security reviews by MOHLTC.

A PIA is also no substitute for a thoroughgoing security assessment as would be obtained in a Threat and Risk Assessment (TRA). SSHA has engaged McDonnell Doane and Associates to perform such a TRA. This work is expected to be finished in early 2008.

3.0 Findings

3.1 General statement from the findings of the PIA

Work has been undertaken by the developers of OLIS and by the MOHLTC eHealth Office to protect the personal health information collected, used, disclosed and retained by OLIS from theft, loss and unauthorized access, disclosure, copying, use or modification.

SSHA has pro-actively commissioned this PIA and an accompanying TRA to ensure that a thorough privacy assessment was completed in advance of the Agency assuming responsibility for the ongoing technical operations, application development and maintenance of OLIS and to give the Agency adequate time to respond to any recommendations that would be forthcoming from these assessments. While the authors of this PIA found some privacy risks that require mitigation, (see section 5.0 below), these risks are manageable and resolvable. Provided that all of this report's recommendations are acted upon, the authors are confident that SSHA will be able to meet its obligations in ensuring the safe and privacy-protective operation of the OLIS repositories.

The analysis identified six privacy risks and six recommendations have been made in the PIA to mitigate these risks. These are described below in section 5.0.

4.0 Technical Safeguards in Place to Protect Information

Description of Control	Rationale for Control	Control Category
<p>Access control. OLIS provides access control mechanisms to ensure that potential users of OLIS are identified and registered, to ensure that users are authenticated whenever they access OLIS, and to ensure that users are authorized to access whatever information or systems services they are attempting to access. There were some potential privacy issues related to the current implementation of access control and these led to a recommendation discussed in item 2 of the next section (section 5.0).</p>	<p>Access control is an essential safeguard in protecting data subject privacy in any online database system. All users of IT systems should be identified as a matter of best practice. Access control is also essential for preventing access to personal health information by unauthorized users.</p>	<p>Preventative</p>

Description of Control	Rationale for Control	Control Category
<p>Consent Directives. Patients can expressly withhold or withdraw their consent to use or disclose information related to their lab tests. An OLIS “blocking” feature enables patients to restrict access to lab information associated with one or more requisitions (i.e. tests ordered and the associated results). Patients may block information in one of three ways:</p> <ol style="list-style-type: none"> 1. by requesting a hospital to block hospital test results. 2. by requesting a Specimen Collection Centre or a healthcare practitioner's office to attach a <i>Restricting Access to Patient Records in OLIS</i> form to the lab requisition and sample <i>before</i> it is sent to the laboratory. Laboratory staff members enter the patient's blocking request into OLIS. 3. by direct request to MOHLTC to restrict access to the results <i>after</i> the lab test has been completed. Patients may fill out the <i>Restricting Access to Patient Records in OLIS</i> form from MOHLTC's OLIS website (www.health.gov.on.ca/olis) and submit it by mail or fax to INFOnline staff. The MOHLTC provides a consent management subject matter expert, who is also a health care practitioner, to oversee blocking requests that are received through the MOHLTC INFOnline. <p>Consent directives can subsequently be revoked by a patient who fills in a <i>Reinstating Access Patient Records in OLIS</i> form and mails or faxes it to the MOHLTC INFOnline. While patients are permitted to block specific lab test orders and their associated results, when access is reinstated (i.e., the block is removed), it is removed from all previously blocked information. It cannot be removed selectively.</p> <p>The approach to blocking currently adopted has limitations and these have led to a recommendation discussed in item 3 of the next section (section 5.0).</p>	<p>Patients have the right under Ontario law (Personal Health Information Protection Act, 2004) to withdraw or withhold their consent to the collection, use, or disclosure of their personal health information, subject to certain constraints.</p>	<p>Preventative</p>
<p>Network Security. To protect the confidentiality and integrity of PHI in transit, all data are encrypted in transit to and from OLIS. SSHA also employs a robust firewall cluster to manage ingress and egress from the SSHA network. Network intrusion detection is also operational.</p>	<p>Network security protects systems from unauthorized access and protects network traffic from unauthorized interception and monitoring.</p>	<p>Preventative</p>
<p>Encryption. As noted above, all the data that flows to and from OLIS is encrypted during transmission. The confidentiality and integrity of PHI in storage is not currently protected by encryption. While the strong physical security surrounding the database servers in the SSHA data centres and the network firewall protections in place obviate the necessity for database encryption, it would nevertheless be a useful security feature to add to OLIS. Database encryption secures data against unauthorised</p>	<p>Encryption of data in transmission protects it from unauthorized interception. Encryption of data in storage protects its confidentiality and integrity from unauthorized access or</p>	<p>Preventative</p>

Description of Control	Rationale for Control	Control Category
<p>access by database administrators, data centre staff, third-party vendors, and others with access to the underlying databases. It also simplifies and enhances the security of data backup. As a practical matter, there is little the Agency can do in the short term regarding the hand-over of fully developed systems that do not use database encryption. But the Agency is well positioned to take a leadership role in offering database encryption services to future eHealth applications while they are still in development. By doing so, the enhanced security and operational benefits of database encryption will accrue to data subjects, healthcare providers, the public, and the Agency.</p>	<p>modification, and protects its confidentiality if lost or stolen.</p>	
<p>Physical security. SSHA hosting environment has robust physical security measures in place, including: physical security perimeter patrol, physical access controls, monitored entry/exit points, restricted access to the data centre environments protected by access cards and biometrics, video monitoring, and security guard on duty round-the-clock. Physical security separation of OLIS servers from other areas of the SSHA data centre is also be enforced.</p>	<p>Required to ensure data confidentiality and integrity and system availability.</p>	<p>Preventative, detective</p>
<p>Audit Logging. SSHA audit and monitoring services will provide immutable logging (i.e., logs that are tamper-proof), network monitoring, and application monitoring. Audit log entries are created and maintained for all transactions (including the date, time and user identification) related to any patient in the database. The ability to identify the date/time for any transaction is available on a real time basis. The ability to identify the user related to an OLIS transaction depends upon whether the user is a direct or organisational user of OLIS: direct users are fully identified as registered SSHA users; while organisational users will be identified only indirectly by means of client transaction ID and institution ID of the institution from whence the transaction originated. SSHA would need to contact the institution in order to determine which organisational user initiated the transaction to which the client transaction ID referred.</p> <p>SSHA lacks clear rules regarding disclosure of information in the audit log and retention of audit log information. OLIS also does not appear to have a comprehensive suite of preformatted standard reports and reporting tools that could ensure rapid accounting for and delivery of information on straightforward privacy-related queries such as: as: what information has a specified user accessed during a specified time period; what information has been accessed by a specified institution during a specified time period; and how many patients' data records have been accessed by a specified user during a specified time period.</p>	<p>Required to ensure compliance with access policy and acceptable use by users and to provide a basis for compliance checking.</p>	<p>Detective, corrective.</p>

Description of Control	Rationale for Control	Control Category
This has led to the recommendation described in item 5 of the next section (section 5.0).		
Archiving. Rules for archiving OLIS data have not yet been developed. See the discussion in section in item 5 of the next section (section 5.0).	Health data must be retained for many years.	Corrective.
Integrated Privacy and Security Incident Management. SSHA has a fully developed security and privacy incident management system. The OLIS System Access Agreement, which all adopters must enter into, requires adopters to also notify the MOHLTC that a privacy breach has occurred, when it occurred, the nature of the incident, and the steps the adopter has taken to contain it. Future work must be done by SSHA to integrate OLIS into this system or ensuring effective integration with hospitals reporting OLIS privacy breaches. Incident management must also align with the privacy framework currently being developed for the OLIS Privacy Implementation Office. This has led to the recommendation described in item 5 of the next section (section 5.0).	Security incident can develop very rapidly and robust procedures must already be in place to deal effectively with a rapidly unfolding security incident. Privacy incidents may arise from security incidents and the two need to be closely coordinated.	Detective, corrective
Data accuracy controls. When an order is received by OLIS, the patient and all healthcare practitioners named on the order (ordering, admitting, and “copied to” practitioners) are validated against data in RPDB and CPDB. Once entered in OLIS, patient and practitioner identity information cannot be changed nor removed from the transaction. The transaction can be cancelled but not deleted or assigned to other individuals. When specimen information is added, there is an additional identity validation performed for the laboratory. For each transaction performed after the initial order entry, OLIS verifies that the ordering practitioner and patient information has not changed and will reject a transaction otherwise.	The accurate identification of patients on lab orders is essential for patient safety. The accurate identification of healthcare providers is essential for timely delivery of results and for safeguarding patient confidentiality.	Preventative, detective
Operational Change Management and Security Patch Management. SSHA operational software and systems change management procedures will apply to all aspects of OLIS technical operations after transition.		Preventative, corrective
Continuous availability. The SSHA hosting environment provides for continuous secure data backup and immediate failover to the alternate SSHA hot backup site, Storage Area Networks, and comprehensive disaster recovery. Network intrusion detection and server-based malware detection are also in place.	Emergency access to PHI essentially requires that OLIS remain operational on a nearly continuous basis.	Preventative, detective, corrective
Processes and Methodologies Used To Assess and Manage Security Risks. At the time this PIA was written, a Threat/Risk Assessment of OLIS was being carried. The information security division of SSHA has also performed extensive security assessments of various components of OLIS at several junctures and continues this	Manage risks effectively.	Preventative, detective

Description of Control	Rationale for Control	Control Category
work.		
Administrative, Contractual, and Operational Measures to Safeguard PHI. The PIA describes a privacy framework that includes a range of privacy policies and procedures to provide additional protections and contractual remedies for breaches. This work is currently under development by the OLIS Privacy Implementation Office.	Users, staff and contractors must be made aware of their responsibilities to held accountable.	Preventative, corrective.

	Risk Description	Mitigation Action	Completion Date
		information in the OLIS clinical repository is made broadly available to healthcare practitioners.	

Risk Description	Mitigation Action	Completion Date
<p>2 Access Control. Several issues arise from the manner in which access control is currently carried out in OLIS:</p> <p>a) Patient Provider Relationships. The term "circle of care" refers to the relationship that exists between a patient and his or her healthcare providers. There is no mechanism in OLIS that requires a user to attest that an active patient-provider relationship exists prior to the patient's information in the clinical repository being accessed by a healthcare provider who is an authorized OLIS user. By contrast, in British Columbia, access to that province's lab information system will require users to first attest that there is an active provider-patient relationship prior to their initial access to the patient's lab information, and every such attestation will be recorded in that system's audit log. As healthcare practitioners have codes of ethics, they are powerfully dissuaded from attesting to the presence of a patient-provider relationship where none exists as they know that this attestation is recorded in the system's audit log. This, in turn, dissuades users from making an unauthorized access to a patient's PHI. Such a mechanism is missing from OLIS. The experience gained in BC and other Canadian jurisdictions could usefully inform future OLIS development, and SSHA can capitalize on this experience.</p> <p>b) Role-Based Access Control. OLIS uses a role-based access control model, but its implementation is somewhat limited. OLIS does not currently admit fine-grained access control by role. All healthcare practitioners, for example, have the same access privileges in OLIS. Lab users also have different access rules than other users but in certain hospitals, this cannot be readily enforced, as the OLIS system cannot differentiate between healthcare providers and hospital lab technicians in some connected hospitals. As noted above, a role-based access control policy is an information governance issue that MOH eHealth Program needs to resolve before the Agency's responsibilities are clear.</p> <p>c) Federated User IDs. Organisational systems such as HIS, LIS and CMS that are connected to OLIS all transmit a "client transaction ID" along with each transaction (e.g., a query, update, etc.) that identifies the organisational user who initiated the transaction. This client transaction ID will be a number that has no meaning or association outside the organisation and must be used as a key into the organisation's audit logs which in turn may identify users by means of a user ID that has no meaning or association outside the organisation. OLIS does not support, nor does the</p>	<p>Recommendation 2</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>	<p>Post-transition</p>

Risk Description	Mitigation Action	Completion Date
<p>eHealth Program provide, a province-wide identifier for healthcare practitioners in Ontario. As a result, institutions such as hospitals that are connected to OLIS cannot provide a user ID which is consistent from one institution to another. This has several implications. There is no uniform method by which audit log references to a transaction from a user who accesses OLIS via a HIS, LIS or CMS can be resolved to an actual identity. SSHA and MOHLTC are wholly reliant upon each specific institution being able to reliably determine who initiated a transaction based a transaction ID from the organisation's own logs. Moreover, several transactions in the OLIS audit logs may all relate to a single user. This may complicate the process of reliably informing patients of who has accessed their records.</p> <p>At least one other province provides all healthcare users of interoperable EHR applications with a consistent and unique identifier that can be used for all applications. Such a scheme would simplify SSHA registration and auditing operations for OLIS and, ultimately, all other eHealth applications as well.</p> <p>d) Monitoring and Responding to Unauthorised Uses. OLIS does not have robust "application intrusion detection" mechanisms that could access patterns by OLIS users in order to detect possible signs of misuse (e.g.: access by a user to many thousands of lab results over a short period of time). Even if robust intrusion detections mechanisms were in place, the Agency's security and privacy incident management system is not yet integrated with hospitals in a way that would allow rapid and effective involvement of hospital privacy officers or others if such an incident were in progress. The Agency will need to ensure that effective procedures are in place to swiftly liaise with hospital privacy officers where appropriate and permitted under whatever information governance structure is adopted for OLIS.</p> <p>e) Reliance on SSHA Network Access Controls. While access to OLIS will take place either via the OLIS web portal or via a workstation connected to a hospital or lab system, (which, in turn, are connected to the SSHA network), inexpensive commercial remote access software running on a desktop computer with connectivity to OLIS would potentially allow a user to connect remotely to OLIS from anywhere over the Internet. In the absence of access tokens (OLIS users rely solely on a user name and password), there may be residual risks that are not well understood at present. Resolution of the issue needs to be tied to MOHLTC policy, as it is not an issue specific only to OLIS. The</p>		

Risk Description	Mitigation Action	Completion Date
<p>TRA discusses the issue of multi-factor authentication for remote access.</p> <p>f) Consistent Access Control Strategy and Policy Across All eHealth Projects</p> <p>There is currently no overarching access control strategy articulated by the eHealth Program. For example, the approach to access control varies between OLIS and DPV, even though both programs make PHI on a large number of patients available to healthcare practitioners in Ontario hospitals, and both systems have direct users (although DPV has no organisational users). SSHA would benefit operationally from a consistent strategy and unified access control policy for eHealth applications that, in future, it will be tasked with operating. Reduction in complexity of administration will also reduce risk of an unauthorised access to PHI through the kind of administrative error or misinterpretation that unintentionally grants a user inappropriate access privileges.</p>		

Risk Description	Mitigation Action	Completion Date
<p>3 Consent Directives Management. While OLIS provides “blocking” capability as per PHIPA requirements, the implementation of this functionality lacks some of the rigour that Ontario residents might otherwise expect to ensure that their wishes regarding disclosure of PHI are respected. At present, any authorized user can override a block and access any individual’s laboratory test results. While this transaction is logged, there are no mechanisms currently in place to: notify the patient or their substitute decision-maker that the override occurred; notify a responsible person (such as a hospital privacy officer) of the incident for purposes of follow-up to ensure that the override and resulting access was done for purposes of providing care to the patient; permit only specified users, as per the permissions of their assigned role, to override a block with the consent of the individual (or without as in the case of Emergency Department physicians); or ensure the privacy protection of those individuals identified as requiring additional protection (e.g., persons in the entertainment business, politicians, or abused spouses or children).</p> <p>At present, the only way that an individual would become aware of the fact that their block was overridden without their consent would be to request a report of all accesses to their PHI in OLIS. If an access appears to have occurred without consent, the result could be a complaint, filed by the individual, of a privacy breach. The impact on SSHA, as the operator of OLIS, could then be a challenge by the IPC, by the press, or by the public's legislative representatives, as to whether the Agency has adequate protections in place to ensure the healthcare-related privacy of Ontarians, despite the Agency's strong commitment to provide robust, privacy-protective data services.</p> <p>It should also be noted that the consent directives approach adopted by OLIS differs from that adopted by MOHLTC's DPV System. As the eHealth Program expands, the presence of multiple consent directives management systems will lead to increased frustration and confusion amongst the public and healthcare practitioners, and a significant increase in the overhead for those organizations and/or programs responsible for administering and maintaining consent directives.</p>	<p>Recommendation 3</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>	<p>Post-transition</p>

Risk Description	Mitigation Action	Completion Date
<p>4 Reporting of Who Has Accessed a Patient's Lab Results. OLIS can provide a report to an individual who makes a request to see who has accessed the individual's PHI in OLIS. How this has been implemented, however, creates potential privacy issues. A report of who has accessed lab results can be generated for any patient by any practitioner authorised to access OLIS. In addition to date, identification of the practitioner who ordered the test, etc., the report also lists details of exactly what the test was (e.g., HIV test, TB test). No audit report or alert is generated when a practitioner produces this report. Because the access report currently contains PHI (i.e., the test(s) performed), someone generating the report could therefore be considered to have accessed patient PHI. This exceeds the intent and purpose of the access report which is merely to identify who has accessed an individual's PHI, <i>not</i> to list what tests were performed. In other jurisdictions (e.g., BC), the name of the accessing user is not provided as part of the report, only a unique but otherwise meaningless identifier, but the name is available to the requestor after the fact. This is done, in part, to protect the identity of healthcare practitioners who have sometimes been threatened by the patients they care for or by the patient's family members. Further, the service for responding to a request for an access report is centralized, with the ability to generate such reports being restricted to a limited set of individual who have been assigned a specific role.</p> <p>The fact that any authorized OLIS user can request the access report and that the report provides the name of the test that was performed might also result in an inadvertent breach of privacy, as there is no need to provide clinical information on such a report. Because there are no limitations on who can generate the report, it leaves the system open to abuse by authorized users who use this system feature in an unauthorized manner. The information contained in the report should answer the question "who has accessed my personal health information in OLIS?" and nothing more.</p> <p>The lack of strict access control on who can generate the access report could negatively impact SSHA, as the operator of OLIS, if a privacy breach occurs.</p>	<p>Recommendation 4 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>	<p>Pre-transition</p>

Risk Description	Mitigation Action	Completion Date
<p>5 Operational Aspects of OLIS Privacy Policies and Procedures. OLIS privacy policies and procedures must be such that the Agency can effectively operationalize and harmonize them with its own privacy policy and procedures. Failure to do so would have obvious adverse consequences for the Agency's technical operation of OLIS. In order to prepare for the transition of OLIS technical operations on March 31, 2008, SSHA should be working constructively with the Privacy Implementation Office currently being set up by the MOHLTC eHealth Program able to integrate OLIS privacy policies and procedures with its own. Three aspects of privacy policy merit special attention :</p> <p>a) Retention and archiving of test results in the clinical repository. It is an accepted privacy principle that personal information be retained only for as long as is needed to serve the purposes for which the information was collected. Lab test results in the clinical repository vary widely in the lifetime of their clinical usefulness. Some results have little or no long-term value while others are relevant for the lifetime of the patient. It is not a trivial matter to determine how long to retain results in the clinical repository. OLIS currently lacks a clear policy for retention and archiving of clinical data and long-term retention and archiving cannot be operationalized until SSHA has guidance on data retention and disposal from the MOHLTC.</p> <p>b) Privacy and Security Incident Management. OLIS is not yet fully integrated with SSHA incident management system (the Enterprise Security and Privacy Incident Management (ESPIM) system). OLIS incident management procedures will need to fit mature SSHA processes. SSHA processes will need to be further developed to ensure faster and more effective liaison with responsible hospital authorities when handling privacy and security incidents. This will be especially true in the future when hospital privacy officers must deal not only with OLIS, but with a variety of other eHealth projects, many of them operated by SSHA.</p> <p>c) Disclosure and Retention of Audit Log Information. All data, including PHI, which goes into or comes out of any OLIS repository also ends up in the Transaction Manager audit log, as this audit log contains a detailed transactional account of all the data flowing into or out of OLIS. So detailed is this audit log that it contains a copy of every piece of PHI contained in OLIS, including patient names and other identifiers and test results. Several aspects of this audit log are</p>	<p>Recommendation 5 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. 	<p>Pre-transition</p>

Risk Description	Mitigation Action	Completion Date
<p>potentially problematic from a privacy perspective. Firstly, SSHA lacks clear rules regarding disclosure of information in the audit log. Secondly, SSHA lacks clear rules regarding retention of this information (i.e., how long should OLIS audit log data be kept?) Thirdly, the OLIS audit log contains a large volume of PHI and this information is not encrypted. In retrospect, the recording of information such as patient names in an audit log may not have been a best-practice from the point of view of privacy protection. This could be ameliorated by other technical safeguards such as encryption, but the OLIS audit log is not encrypted. The Agency must therefore protect the audit log at least as rigorously as the OLIS repositories themselves. Finally, OLIS appears to lack a comprehensive suite of standard preformatted reports and reporting tools that could ensure rapid answers to such privacy-related queries as: what information has a specified user accessed during a specified time period; what information has been accessed by a specified institution during a specified time period; and how many patients' data records have been accessed by a specified user during a specified time period.</p> <p>The first and second items above are matters of information governance and can only be answered once the information governance issues discussed in risk 1 above are resolved. The rest are technical in nature and can be addressed by SSHA's privacy and security team.</p>		

Risk Description	Mitigation Action	Completion Date
<p>6 Pseudonymisation. An algorithm was created that allows records in the clinical repository to be stripped of information that could be used to identify patients, healthcare providers, or lab service providers while at the same time allowing each record to be reliably linked to others for the same patient or healthcare practitioner or lab for the purposes of providing a longitudinal history of an individual's lab test results and for statistical research. There are three potential privacy-related risks that arise from the current implementation of the pseudonymous repository:</p> <p>a) Robustness of the Pseudonymisation Algorithm. Issues have been identified by SSHA's information security division that may undermine the effectiveness of the pseudonymisation process. The bespoke algorithm is non-standard in that it does not use industry-standard algorithms applied according to industry-standard protocols. It also has not been subject to independent review by a cryptographic expert. There may be implications for SSHA if the Agency assumes the ongoing operations of this algorithm and it is later revealed to be flawed. An independent review would clearly illustrate due diligence on the part of the Agency while at the same time allaying fears that the algorithm may be inadequate.</p> <p>b) Risk of Re-identification of Pseudonymised Records. A sufficient amount of personal data remains in each record in the pseudonymous repository (data such as gender, birth year and the first three characters of the patient's postal code) to potentially enable a researcher or healthcare administrator with access to individual records from the pseudonymous repository to re-identify patients by inference, especially if the records were matched against identifying records from other databases. This risk can be mitigated effectively by increasing the so-called "minimum cell size"; i.e., of ensuring that a certain minimum number of records contributed to any statistical result. This prevents the re-identification of patients whose identities would otherwise be discernable from a query result drawn from a single record.</p> <p>c) Data Matching Pseudonymous Against Records in the Orders Reporting Repository. The potential risk of re-identification of patient records in the pseudonymous repository by matching them against another database is increased considerably by the potential to match these records against those in the orders reporting repository. Each record in the orders reporting repository contains all the patient identifiers</p>	<p>Recommendation 6 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.</p>	<p>Pre-transition</p>
	<p>Recommendation 6 (cont.) SSHA should request the MOHLTC eHealth Program to provide the Agency with a data access policy for the pseudonymous repository that applies safeguards so as to mitigate the risk of data matching (e.g., enforcement of minimum cell size in response to queries).</p>	<p>Post-transition</p>

Risk Description	Mitigation Action	Completion Date
<p>that are in the clinical repository. As more than 95% of lab tests are Ministry funded, at least 95% of the test orders in the pseudonymous repository have a matching record in the orders reporting repository. Matching up the records would be straightforward: for the matching to fail, two individuals of the same gender and age, living in the same geographic area, would need to have the exact same lab tests ordered at the same time—an event with very low probability. Hence anyone with access to both repositories could readily reverse the pseudonymisation of about 95% of the records in the pseudonymous repository.</p> <p>Both repositories are in the SSHA data centres and operation of both will be transitioned to SSHA on March 31, 2008. Risk of data matching by users with access to these two repositories will therefore be minimised <i>provided</i> an effective data protection policy is in place to govern access. Privacy-protective operation of the repositories by SSHA, combined with effective information governance and policy, will soundly mitigate the privacy risks, real or perceptual, that arise from the potential for data matching. By providing statistical data in response to queries that meet the criteria of a well constructed data access policy, as opposed to merely providing copies of records from the pseudonymous repository, risk of data matching against individual records is minimised.</p> <p>SSHA currently lacks a policy on the provision of pseudonymised data to third parties or any suitable agreements to prevent, or even deter, re-identification from taking place. This may place the Agency in an awkward position, should a re-identification ever occur. A privacy-protective data access policy for the pseudonymisation repository is therefore needed, as addressed in Recommendation 1d above. This would likely need to be done in conjunction with a broader Agency strategy for developing, in a principled and privacy-protective way, a capability for providing pseudonymisation services and fully anonymised responses to research questions for a variety of PHI repositories that the Agency may ultimately be charged with operating.</p> <p>d) Other Considerations</p> <p>As mentioned above, SSHA could provide a pseudonymisation service to other Ministry programmes in a privacy-protective and secure fashion, using independently reviewed and approved cryptographic algorithms and methods. There are several long-term advantages to do so. Effort spent on the pseudonymisation algorithm and related processes would be capitalised across multiple eHealth</p>		

Risk Description	Mitigation Action	Completion Date
<p>programmes. Once perfected, the privacy-protective features would be available for application to other repositories without the recurring risks of developing such features from scratch (or worse, failing to do so). Also, large volumes of non-nominal clinical data could be made available to medical researchers in a rigorous and fully privacy-protective fashion (e.g., as part of a programme of research approved by a university Ethics Review Board) and such data could advance medical research in Ontario universities and Centres of Excellence. SSHA should consider the possibility of offering such a pseudonymisation service as a part of its service offerings to clients.</p>		

APPENDIX 1: TERMS AND ACRONYMS

Acronym/Term	Definition
Circle of care	<p>PHIPA expands the permissible sharing of client health information within the client's health care team – the circle of care. The circle of care concept is generally defined by reference to paragraphs 3(1)1 to 3(1)4 of PHIPA. Those paragraphs define the following custodians:</p> <ol style="list-style-type: none"> 1. A health care practitioner or a person who operates a group practice of health care practitioners. 2. A service provider within the meaning of the Long-Term Care Act, 1994 who provides a community service to which that Act applies. 3. A community care access corporation within the meaning of the Community Care Access Corporations Act, 2001. 4. A person who operates one of the following facilities, programs or services: <ol style="list-style-type: none"> i. A hospital within the meaning of the Public Hospitals Act, a private hospital within the meaning of the Private Hospitals Act, a psychiatric facility within the meaning of the Mental Health Act, an institution within the meaning of the Mental Hospitals Act or an independent health facility within the meaning of the Independent Health Facilities Act. ii. An approved charitable home for the aged within the meaning of the Charitable Institutions Act, a placement co-ordinator described in subsection 9.6 (2) of that Act, a home or joint home within the meaning of the Homes for the Aged and Rest Homes Act, a placement co-ordinator described in subsection 18 (2) of that Act, a nursing home within the meaning of the Nursing Homes Act, a placement co-ordinator described in subsection 20.1 (2) of that Act or a care home within the meaning of the Tenant Protection Act, 1997. iii. A pharmacy within the meaning of Part VI of the Drug and Pharmacies Regulation Act. iv. A laboratory or a specimen collection centre as defined in section 5 of the Laboratory and Specimen Collection Centre Licensing Act. v. An ambulance service within the meaning of the Ambulance Act. vi. A home for special care within the meaning of the Homes for Special Care Act. vii. A centre, program or service for community health or mental health whose primary purpose is the provision of health care.
Clinical Management System (CMS)	Generally, this term is used in reference to those software products that have been approved as meeting specified security, technology and functionality standards for managing electronic medical records and practice management information for physicians.
CMS	See <i>Clinical Management System</i>
Consent directive	In Ontario, consent is assumed to be implied enabling sharing of personal health information within the individual's "circle of care". A consent directive is the specific and informed direction that an individual provides which contains the individual's wishes with respect to the disclosure of his or her personal health information. In relation to OLIS, this means restrictions on access by users other than those identified on the lab order.
CPDB	See <i>Corporate Providers Database</i>

Corporate Providers Database (CPDB)	A database maintained by the Provider Services Branch of MOHLTC to store information on all health care providers transacting business with the Ministry. This is used within OLIS to validate identities of healthcare practitioners and healthcare facilities that use OLIS or connect to it.
De-identification	Removal from records of any information that identifies an individual or which could reasonably be utilized, either alone or with other information, to identify the individual. De-identified data may be anonymised (in which case, no identifiers of any kind remain) or pseudonymised (in which case, a random but consistently applied identifier allows current pseudonymised records to be correlated with future pseudonymised records for the same patient).
DPV	<i>See Drug Profile Viewer</i>
Drug Profile Viewer (DPV)	The Drug Profile Viewer enables the secure sharing of provincial drug claims information of those persons who receive benefits through the Ontario Drug Benefit Program and the Trillium Drug Program. At present, health care providers in 181 hospital emergency departments in Ontario have access to this information.
EHR	<i>See Electronic Health Record</i>
Electronic Health Record (EHR)	An Electronic Health Record (EHR) provides each individual in Canada with a secure and private lifetime record of his/her key health history and care within the healthcare system. The record is available electronically to authorised healthcare providers and the individual anywhere and anytime in support of high quality care. (EHRS Blueprint, V2.2, Canada Health Infoway, p.5.)
Health Information Custodian (HIC)	[PHIPA subsections (3) to (11)] means a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work
Health Information Network Provider	[PHIPA O. Reg. 329/04, s. 6 (2).] "Health information network provider" or "provider" means a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.
HIC	<i>See Health Information Custodian</i>
HIS	<i>See Hospital Information System</i>
Hospital Information System	A comprehensive, integrated information system designed to manage the administrative, financial and clinical aspects of a hospital.
HL7	Health Level 7 is a set of international standards for defining clinical and administrative data in healthcare to support electronic messaging and transaction processing. The "7" comes from layer 7 in a popular conceptual model of how computer networks process data; layer 7 is the application layer, the highest level at which programs communicate with one another. Further information can be found at www.hl7.org .
HN	Ontario Health Number

Laboratory Information System	Software which receives, processes and stores information required by a medical laboratory. In addition to supporting administrative processes, it serves to assist in the receipt, resulting and distribution of laboratory orders and test results. These systems often must interface with laboratory testing instruments and, often, other information systems such as hospital information systems.
Laboratory Inspection and Licensing database	MOHLTC's repository of information related to laboratory licences. This is used within OLIS to ensure that a laboratory is licensed to perform the tests that are reported to OLIS.
LILI	See <i>Laboratory Inspection and Licensing</i>
LIS	See <i>Laboratory Information System</i>
MOHLTC	Ministry of Health and Long-term Care
OLIS	Ontario Laboratory Information System
Personal Health Information (PHI)	[PHIPA section 4(1) subsection (3) and (4)] means identifying information about an individual in oral or recorded form, if the information, (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, (b) relates to the providing of healthcare to the individual, including the identification of a person as a provider of healthcare to the individual, (c) is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual, (d) relates to payments or eligibility for healthcare, or eligibility for coverage for healthcare, in respect of the individual, (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, (f) is the individual's health number, or (g) identifies an individual's substitute decision-maker.
PHI	Personal Health Information
PHIPA	<i>Personal Health Information Protection Act</i> , S.O., 2004
PHL	Public Health Laboratories of the MOHLTC Laboratory Services Branch
Privacy	The right of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. (<i>Privacy and Freedom</i> , A. F. Westin, New York: Atheneum, 1968. p. 42-43.)
Record	Means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record. (Personal Health Information Protection Act, S.O. 2004. s. 2.)
SSHA	Smart Systems for Health Agency