

ONE[®] Portal

PIA Summary

Document Identifier: 1146

Version: 1

Document Control

Revision History

Date	Version	Revision
Mar 2008	1	Final Copy
Mar 2008	0.01	Initial Draft

© 2008, Smart Systems for Health Agency
Copying without permission is prohibited. All rights reserved.

Table of Contents

1.0 Introduction	1
2.0 Solution Overview.....	1
2.1 Project Description/Background	1
3.0 Scope	2
3.1 In-Scope	2
3.2 Out-of-Scope	3
4.0 Findings.....	3
4.1 Client Privacy Responsibilities	3
5.0 Safeguards in Place to Protect Information.....	4
6.0 Risks, Mitigations and Timeframe.....	4
7.0 Appendix 1: Terms and Acronyms	6

1.0 Introduction

Smart Systems for Health Agency (SSHA or the 'Agency') is an Agency of the Ministry of Health and Long-Term Care (the 'Ministry'). SSHA's mandate is to work with Ontario's health care sector to enable health information custodians (HICs) to share personal health information (PHI). SSHA is 100% funded by the Ministry and SSHA provides its products and services free of charge to the publicly-funded health care sector.

SSHA is obliged to comply with the requirements regarding privacy and security established by the regulations made under Ontario's *Personal Health Information Protection Act, 2004*, S.O 2004, c.3, as amended (PHIPA), and by the *Freedom of Information and Protection of Privacy Act*, R. S.O. 1990, c. F.31 (FIPPA).

In providing its products and services ('Solutions') to the healthcare sector, SSHA fulfills different functions. The specific requirements under PHIPA that SSHA must satisfy depend on the particular function SSHA is fulfilling. Regardless of the function or role it is playing SSHA's policy is to have in place administrative, technical and physical safeguards, and practices and procedures that protect privacy appropriately.

The cornerstone of SSHA's privacy program is its *Privacy and Data Protection Policy*. As part of its privacy program SSHA has a number of policies, procedures, and guidelines designed to help ensure effective application of privacy principles.

Achieving privacy protection requires the active involvement of SSHA, its clients, their end users and Ontarians. SSHA is committed to working with its clients to protect privacy.

As part of its privacy program, SSHA conducts Privacy Impact Assessments (PIAs) for the Solutions it provides. SSHA uses PIAs to assess how a particular Solution may affect privacy. The end result of the PIA process is to provide documented assurance that all privacy issues have either been adequately addressed or, in the case of outstanding privacy issues, brought forward to senior management for further direction.

This document summarizes the results of SSHA's PIA related to ONE Portal.

2.0 Solution Overview

SSHA's ONE Portal Solution provides a means for creating information sharing forums using a common technology infrastructure to create portals that reside in the SSHA Data Centre.

2.1 Project Description/Background

SSHA's mandate is to provide a secure, province-wide information infrastructure that enables health care professionals to collect store, use, and exchange personal information (PI) and personal health information (PHI). ONE Portal is a secure electronic communications mechanism to facilitate communication among public health professionals, especially during public health emergencies.

ONE Portal provides a set of platforms (software and applications) that allow for the creation of information sharing forums where healthcare providers can access and post information that is of interest to a specific group of users. ONE Portal provides for integration of, and access to, e-community

content to users through a single point of access. Two examples of existing forums (referred to as “portal instances” or “portals”) that run on ONE Portal platforms are:

- *PublicHealthOntario.ca*, which offers articles of interest on public health programs and communicable diseases, plus links to other relevant web sites for staff within the office of the Chief Medical Officer for Health, Public Health Division, and 37 Public Health Units across the province; and
- *eHealthOntario.ca* which provides consistent, timely, and trusted health information to health care providers in hospitals, long-term care homes, Community Care Access Centres, and others in the health sector.

Portal instances based on ONE Portal provide a secure environment that allows users to access an array of content and tools, like collaboration tools that allow users to create or maintain content (for example, posting documents and announcements, creating and modifying task lists, discussion threads, calendars, etc.) and studio tools (for example, tools that allow for the creation of on-line forms and conducting of on-line surveys, etc.); integrated third-party applications; and links to other web sites and on-line information.

The hardware underlying ONE Portal resides in the SSHA Data Centre and SSHA provides on-going operations, server management, application management, and other support services, enabling Ontario healthcare providers free to focus on developing and accessing information, rather than technical on issues.

User access to different functions within a portal instance can be restricted by requiring membership to the particular community the portal was created for, as well as by access rights, for example, users can be limited in their rights to view or edit information published in the portal.

The Personal Health Information Protection Act (PHIPA) is not applicable to SSHA with regard to ONE Portal. The Freedom of Information and Protection of Privacy Act (FIPPA) applies to SSHA with regard to ONE Portal in two ways. First, FIPPA applies because registration of portal users involves verifying their identity, which involves gathering PI; second, FIPPA applies because SSHA uses tracking technology to collect information from website visitors, including IP addresses, which are considered sensitive and is afforded the same protection as PI.

3.0 Scope

The SSHA Privacy Team conclusions are based on reviewing project documentation and on information gathered from SSHA’s ONE Portal Project Team.

This PIA summary is based on information available as of October 2007.

3.1 In-Scope

The following was assessed as part of the PIA:

- The roles and responsibilities of various stakeholders involved in ONE Portal (for example, SSHA, subscribers, users, etc.).

- The business and technical processes and data flows of ONE Portal.
- Related SSHA policies specifically referred to in the PIA

3.2 Out-of-Scope

The following were not assessed for the PIA:

- Performance monitoring and reporting related to SSHA's infrastructure.
- SSHA hosting facility infrastructure.
- Use of SSHA's Storage Area Network (SAN) for ONE Portal services. (SAN is the subject of a separate PIA.)
- ONE® ID. (This Solution is the subject of a separate PIA.)
- The institutional environment of users and subscribers.

4.0 Findings

The SSHA Privacy Team identified the following findings associated with ONE Portal.

1. SSHA does not have custody or control over the information posted in communities.
2. The purpose for collection on IP addresses is not clearly identified.

4.1 Client Privacy Responsibilities

Ensuring privacy and compliance with relevant and applicable legislative requirements requires a joint effort involving both SSHA and Clients (subscribers). Clients' roles and responsibilities regarding privacy are addressed in the Master Service Agreement and Service Level Agreement.

The Client must also comply with applicable laws, regulations, and professional standards relating to the protection of PI and PHI. As well, the Client is responsible for ensuring that users comply with applicable laws, regulations, and professional standards. Portal users with content management privileges are accountable for their postings and are responsible for ensuring personal information or personal health information is not included in information on the portal.

End-to-end privacy compliance can only be achieved if SSHA and subscribers are in a privacy partnership.

5.0 Safeguards in Place to Protect Information

SSHA has a number of general controls in place that help ensure privacy that are relevant to the ONE Portal, including:

- SSHA’s Privacy and Security Division is charged with overseeing compliance with SSHA’s privacy and security polices and procedures.
- SSHA’s Privacy and Data Protection Policy (the Policy) requires all SSHA personnel to be familiar with the Policy. Furthermore, all personnel are required to sign an *Acknowledgement and Agreement* form relating to the Privacy and Security Standard of Conduct acknowledging their familiarity with SSHA’s privacy and security standards of conduct and affirming their responsibility to uphold them.
- SSHA staff and consultants must sign a confidentiality agreement and submit to a criminal reference checks prior to joining, or doing work for, SSHA.
- SSHA’s Privacy and Security Division conducts privacy reviews and provides design support assistance in the development of solutions. This ensures privacy controls are included in the design of Solutions.
- Privacy and security training is mandatory for all SSHA staff.
- SSHA has strict reporting requirements relating to privacy breaches.

As well, SSHA has the following safeguards (controls) in place that apply specifically to ONE Portal:

- The ONE Portal staging and production environments are hosted and operated in the SSHA Data Centre, which is robust, sophisticated and state-of-the art, featuring multiple system redundancies for high reliability and availability, as well as security and privacy protections.
- SSHA has developed a set of processes and materials to assist Clients in using different features of ONE Portal, such as user guides, data forms, on-line training, etc.
- Access policies can be enabled to ensure that access to specific resources within a portal instance is restricted.
- All portal URLs use the industry standard SSL protocol (128-bit encryption). As a result, traffic between the portal user’s device and the portlet server is encrypted.

6.0 Risks, Mitigations and Timeframe

To address privacy risks associated with ONE Portal, in the PIA the Privacy Team recommended the following mitigating actions:

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
Unauthorized use and disclosure if users post PI/PHI in their postings on the portal.	Medium	Low	SSHA to continue to provide online training to Community Managers on the use of portal.	Ongoing

			<p>Policy statement is posted on the portal reminding users not to post PI/PHI on the portal.</p>	<p>Existing communities has the statement. New communities will have this statement posted to remind users to not to post PI/PHI on their community.</p>
<p>Denial of privacy rights of Ontarians if users are not aware of collection of IP addresses by SSHA.</p>	<p>Low</p>	<p>Low</p>	<p>SSHA should post a privacy statement on its web sites and portals regarding the use of tracking technologies, telling visitors what information is being collected, the purpose for the collection, and the information handling practices and procedures (including contact information) for those interested in raising a privacy concern.</p>	<p>Fall 2008</p>

7.0 Appendix 1: Terms and Acronyms

Acronym/Term	Definition
CMS	Clinical Management System
DPV	Drug Profile Viewer
eHO	eHealthOntario.ca
HIS	Hospital Information System
MCC	Markham Computing Centre
MCMS	Microsoft Content Management System
NAS	Network Attached Storage
OLIS	Ontario Laboratory Information System
PHI	Personal Health Information
pHO	PublicHealthOntario.ca
PI	Personal Information
PIA	Privacy Impact Assessment
SAN	Storage Area Network
SCC	Streetsville Computing Centre
SMTP	Short Message Transfer Protocol
SSHA	Smart System for Health Agency
SSO	Single Sign-on
UAT	User Acceptance Testing