

ONE[®] Hosting

PIA Summary

Document Identifier: 1144

Version: 1

Document Control

Revision History

Date	Version	Revision
Apr 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
3.0 Scope	2
3.1 In-Scope	2
3.2 Out-of-Scope	3
4.0 Findings.....	3
4.1 Client Privacy Responsibilities	4
5.0 Safeguards in Place to Protect Information.....	4
6.0 Risks, Mitigations and Timeframe.....	5
7.0 Appendix 1: Terms and Acronyms	7

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[®] Hosting.

2.0 Solution Overview

ONE Hosting solution and services allow health care providers to have their application hosted at the two geographically dispersed SSHA datacentres while making use of various technology options. Services that may be provided range from infrastructure, connectivity, server management, system management, customized security management, database services, project services and registration services. ONE Hosting consists of ONE Hosting Core and ONE Hosting Managed.

ONE Hosting Core:

ONE Hosting Core is a client managed service that enables organizations to have their application hosted at SSHA's data centres while maintaining ownership, administration, and control of their equipment. Core clients can either provide their own equipment or have it procured on their behalf by SSHA.

ONE Hosting Core client services reside in the Hosting Service Provider (HSP) zone. The HSP zone provides a network path for hosting SSHA client organization systems and services. The HSP firewalls

serve to separate the various client organization networks from each other and provide a secure path through which necessary communications can travel.

ONE Hosting Managed:

ONE Hosting Managed Services are services for which SSHA has full operational and administrative responsibility. Managed Hosting service enables organizations to select from a menu of standard offerings integrated into the secure and robust SSHA infrastructure. The solution is jointly developed by SSHA and the client.

ONE Hosting Managed services and systems reside in the Application Service Provider (ASP) zone and applications found within the ASP zone. ASP firewalls serve to separate the various Data Centre networks from each other and provide a secure path through which necessary communications can travel.

3.0 Scope

The SSHA Privacy Team conclusions are based on reviewing project documentation and on information gathered from SSHA's Hosting Team.

This PIA summary is based on information available as of February 28th, 2008.

3.1 In-Scope

People:

- Roles and responsibilities for SSHA ONE Hosting clients, vendors and users.

Process:

- Processes associated with implementation of ONE Hosting solution including process to place an order for ONE Hosting, deployment and support.

Policy:

- Agreements and policies related to ONE Hosting including schedule specific to ONE Hosting.

Technology:

- Technology employed by ONE Hosting including the security features offered by the ONE Hosting technology.

3.2 Out-of-Scope

People:

- Roles and responsibilities of clients' users who are contractually obligated to the client.

Process:

- Client processes for signing up for ONE Hosting.

Policy:

- Client policies relating to the use of ONE Hosting solution.

Technology:

- The leveraged SSHA components upon which ONE Hosting is dependent including:
 - The SSHA Managed Private Network (MPN). This is subject of a separate PIA.
 - The SSHA ONE ID. This is subject of a separate PIA.
- The ONE Hosting Web services.

Other:

Client privacy compliance programs and physical environment

4.0 Findings

The SSHA Privacy Team identified the following findings associated with ONE Hosting:

1. When providing ONE Hosting Core Services, SSHA is not able to record or log users with access to the client's application. It's the client's responsibility to develop this functionality in their application.
2. The Personal Health Information Protection Act and its Regulations apply. SSHA is acting in the capacity of both Health Information Network Provider (HINP) and Electronic Service Provider (ESP) while providing hosting services.
3. SSHA could have incidental access to PHI when performing service associated with managed hosting, i.e., troubleshooting, installation, and back-up services.
4. SSHA and clients must sign ONE Hosting agreement(s) before the commencement of Hosting services.

4.1 Client Privacy Responsibilities

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

SSHA's clients are responsible for complying with applicable laws, regulations, and professional standards relating to the protection of PI and PHI and conducting appropriate PIAs. As well, clients are responsible for ensuring that their users comply with applicable laws, regulations, and professional standards.

Clients must use organizational, administrative, physical, and technical means to protect user identifications, passwords, secure tokens, and other authentication credentials assigned to the client, or users, to enable them to use ONE Hosting solution.

Clients are responsible for attesting that users have a legitimate business need for using the applications hosted at SSHA. As well, the Client is responsible for obtaining any necessary consent required under applicable laws and regulations before collecting, using, or disclosing the personal information of users.

5.0 Safeguards in Place to Protect Information

SSHA has a number of controls in place to help ensure that privacy impacts relevant to ONE Hosting are addressed, including:

- SSHA has implemented a Privacy Program.
- SSHA's Privacy and Security Division is charged with overseeing compliance with SSHA's privacy and security policies 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's Privacy and Security Division conducts privacy reviews and provides design support for the development of Solutions. This ensures privacy controls are included in the design of Solutions.
- SSHA has strict reporting requirements relating to privacy breaches.
- The Security Operations Center logs and monitors activities of any system in the SSHA network but has no authority to access information residing on (or passing through) these systems.
- SSHA has implemented an Enterprise Security and Privacy Incident Management Program (ESPIM).
- Privacy and Security training is mandatory for all SSHA staff.
- Client direction would be sought and documented before SSHA staff accessed PHI, if such activities were not initially provided for in Master Service Agreements signed with clients.

- SSHA has implemented a security program and related physical, organizational and logical controls to protect data that it hosts or that is transmitted over its network.
- SSHA has established processes to handle and perform backup and recovery of data.
- The servers used to host applications are protected by firewalls configured to restrict access to authorized users and mitigate harm to any such server from an attack launched from the Internet.
- SSHA could have incidental access to PHI when performing service associated with managed hosting, i.e., troubleshooting, installation, and back-up services. SSHA has a reasonable set of system and Personnel controls in place to ensure that individuals act appropriately. SSHA Personnel are screened and are expected to sign standard of conduct agreement at the time of hiring. All SSHA staff receive comprehensive training on privacy and security. System administrators have unique user identities and passwords. Logons are authenticated so that user identity is assured prior to access.
- SSHA uses intrusion detection tools configured to provide alerts to SSHA when certain sets of circumstances take place that indicate a possible intrusion.

6.0 Risks, Mitigations and Timeframe

To address privacy risks associated with ONE Hosting, the Privacy Team has recommended the following mitigating actions. SSHA has projects underway to address the risks identified below.

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
<ul style="list-style-type: none"> • Unauthorized access, use, and disclosure if clients and SSHA have not agreed upon the role and responsibilities for each party while performing hosting services • Non-compliance with the privacy legislation due to this risk. 	Medium	Low	SSHA and client sign the ONE Hosting agreements.	Ongoing
<ul style="list-style-type: none"> • Unauthorized internal access to personal health information hosted by SSHA. 	Medium	Low	Privacy and Security training is mandatory for all SSHA staff.	All SSHA staff has received the mandatory training. Newly hired staff are required to complete the training within 30 days of the date of

			SSHA to provide continuous privacy training and awareness to its existing employees.	hire. Ongoing
--	--	--	--	----------------------

7.0 Appendix 1: Terms and Acronyms

Acronym/Term	Definition
ASP	Application Service Provider
ESP	Electronic Service Provider
ESPIM	Enterprise Security and Privacy Incident Management
FIPPA	Freedom of Information Protection of Privacy Act
HIC	Health Information Custodian
HINP	Health Information Network Provider
HSP	Hosting Service Provider
MPN	Managed Private Network.
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PIA	Privacy Impact Assessment
SSHA	Smart System for Health Agency