

# ONE™ Mail Direct

## PIA Summary

# Copyright Notice

Copyright © 2007 Smart Systems for Health Agency (SSHA).

All rights reserved.

# Table of Contents

<b>1.0</b>	<b>SOLUTION OVERVIEW</b> .....	<b>4</b>
1.1	PROJECT DESCRIPTION/BACKGROUND .....	4
<b>2.0</b>	<b>SCOPE</b> .....	<b>5</b>
2.1	IN-SCOPE.....	5
2.2	OUT-OF-SCOPE .....	5
<b>3.0</b>	<b>FINDINGS</b> .....	<b>5</b>
3.1	CLIENT PRIVACY RESPONSIBILITIES .....	6
<b>4.0</b>	<b>SAFEGUARDS IN PLACE TO PROTECT INFORMATION</b> .....	<b>6</b>
<b>5.0</b>	<b>RISK, MITIGATION, AND TIMEFRAMES</b> .....	<b>8</b>

## INTRODUCTION

Smart System 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 under Ontario's *Personal Health Information Protection Act, 2004*, S.O 2004, c.3, as amended (PHIPA), and 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 health care 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 is required to have in place administrative, technical and physical safeguards, and practices and procedures to ensure compliance with PHIPA. SSHA's compliance with PHIPA is reviewed by the Information and Privacy Commissioner of Ontario (IPC).

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.

Because SSHA's Solutions are used by SSHA's Clients (for example, HICs), ensuring privacy and compliance with PHIPA must be seen as a joint effort involving both SSHA and its Clients. To help ensure so-called end-to-end compliance, SSHA has a number of specific policies, procedures, and safeguards and is committed to working with its Clients to achieve end-to-end privacy compliance.

As part of its privacy program, SSHA is required to conduct Privacy Impact Assessments (PIAs) for the Solutions it provides. PIAs are used to assess how a particular Solution may affect the privacy of individuals. The end result of the PIA process is to provide documented assurance that all privacy issues have been identified and that they 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 PIA related to SSHA's ONE™ Mail Direct Solution.

## 1.0 Solution Overview

---

SSHA's ONE Mail Direct solution is a secure e-mail service intended for non-institutional health care providers and for health care institutions that do not want to participate in ONE™ Mail Partnered (another SSHA Solution that requires users to have a pre-existing e-mail environment). ONE Mail Direct also includes firewall protection, intrusion detection, data centre facilities, content and virus scanning, a variety of platforms, systems, and web services, as well as allowing ONE Mail Direct users access to the ONE Pages directory, which is a separate Solution that is discussed in a separate PIA.

### 1.1 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 PHI. To fulfill this mandate, SSHA offers a suite of Solutions, including ONE Mail Direct, its secure e-mail service.

ONE Mail Direct was created for non-institutional health care providers (such as physicians, smaller hospitals, laboratories, pharmacies, mobile worker, etc.) that do not have the capacity, or desire, to develop an independent e-mail system. Using ONE Mail Direct allows health care providers to exchange PHI via e-mail rather than via fax or courier, saving time and money. Ontarians, in turn, benefit from improved delivery of health care services because health care providers have more timely access to information.

ONE Mail Direct allows health care providers to securely and reliably send PI and PHI because the Solution is hosted in SSHA's secure data centres that include security features such as firewalls, intrusion detection, and anti-spam and anti-virus protection.

For the purposes of the PHIPA, SSHA is considered a Health Information Network Provider (HINP) with regard to its ONE Mail Direct Solution, so SSHA must comply with PHIPA provisions applicable to HINPs. As well, because SSHA collects the personal information of ONE Mail Direct users, SSHA must comply with the Freedom of Information Protection of Privacy Act (FIPPA).

When a health care professional, or a qualifying health care organization, decides to become a subscriber of ONE Mail Direct, the individual, or someone on behalf of the organization, enters into an agreement that contains provisions setting out the parties' rights and obligations regarding privacy and security.

When a subscriber is an organization, the organization designates sponsors within its organization who identify individuals within the organization who will be registered ONE Mail Direct users. In the case of individual health care professionals who subscribe for ONE Mail Direct, the individual is the user. All users of ONE Mail Direct go through an in-person registration process that requires them to provide personal information to SSHA. As well, users also undergo an identity check (to provide identity assurance). Currently, the ONE Mail Direct identity assurance process offers a medium to high level of assurance.

## **2.0 Scope**

---

The Privacy Team's conclusions were based on reviewing project documentation, information it received verbally, and by e-mails from the ONE Mail Direct Project Team.

This PIA summary is based on information available through November 2007.

### **2.1 In-Scope**

The following were assessed as part of the PIA:

- The roles and responsibilities of various stakeholders involved in ONE Mail Direct (for example, SSHA, subscribers, users, etc.).
- The business and technical processes and data flows of ONE Mail Direct.
- Related SSHA policies specifically referred to in the PIA.

### **2.2 Out-of-Scope**

The following were not assessed for the PIA:

- Performance monitoring and reporting related to SSHA's infrastructure.
- SSHA hosting facility infrastructure.
- Other e-mail systems used between ONE Mail Direct clients.
- ONE Mail Partnered Solution. (This solution is the subject of a separate PIA.)
- SSHA's ONE™ Pages Solution. (This solution 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.
- SSHA's Storage Area Network (SAN). (This Solution is the subject of a separate PIA.)

## **3.0 Findings**

---

In the PIA the Privacy Team identified the following findings associated with ONE Mail Direct:

1. SSHA captures personal information in the process of registering users for ONE Mail Direct. As a result, FIPPA applies.
2. SSHA controls the registration data.

3. ONE Mail Direct users' e-mail data is hosted in SSHA's environment.
4. SSHA does not have control over data transmitted via e-mail using ONE Mail Direct.
5. SSHA system administrators have incidental access to e-mail headers and e-mail message content as part of fulfilling their responsibilities. SSHA has a reasonable set of system and Personnel controls in place to ensure that individuals who act as administrators do so appropriately.
6. PHIPA and FIPPA apply.
7. SSHA and subscribers to ONE Mail Direct have a privacy and security partnership.

### **3.1 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 (including, when applicable, obtaining consent before using the ONE Mail Direct solution to transmit information). As well, the Client is responsible for ensuring that users comply with applicable laws, regulations, and professional standards.

The Client is also responsible for determining whether any material transmitted using One Mail Direct can be transmitted appropriately (with or without additional safeguards), given the nature and sensitivity of the materials being transmitted. If the client determines any additional safeguards are required when transmitting materials, the Client must implement such safeguards.

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 connect to One Mail Direct.

Clients are responsible for attesting that users have a legitimate business need for using One Mail Direct and that they are associated with the provision of health care related services and that they meet eligibility requirements for using One Mail Direct. 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.

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

## **4.0 Safeguards in Place to Protect Information**

---

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

- 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 systems in the SSHA network but has no authority to access information residing on (or passing through) these system.
- Privacy and Security training is mandatory for all staff.

As well, SSHA has the following safeguards in place that apply specifically to ONE Mail Direct:

- The servers used by SSHA to provide ONE Mail Direct 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.
- An incident management process is in place to handle privacy incidents related to ONE Mail Direct. (SSHA is in the process of implementing an Enterprise Security and Privacy Incident Management Program.)
- SSHA system administrators have incidental access to e-mail headers and e-mail message content as part of fulfilling their responsibilities. SSHA has a reasonable set of system and Personnel controls in place to ensure that individuals who act as administrators do so appropriately. SSHA Personnel are screened and are expected to sign off on standard of conduct agreements at the time of hiring. 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.
- An e-mail message(s) exchanged between One Mail Direct users is encrypted. (An e-mail message(s) to or from a One Mail user to someone who is not a One Mail user is not encrypted.)
- SSHA employs anti-spam and anti-virus technologies.
- Any time a user attempts to access One Mail Direct, SSHA takes steps to confirm the user is an authorized user of One Mail Direct (for example, requesting their user name and password).
- SSHA has the following administrative policies and agreements related to ONE Mail Direct. They are provided as part of deployment package:
  - Information Collection Policy – this policy provides the subscriber with general and specific instruction to explicitly communicate to users why their information is being collected.
  - Information Retention and Storage Policy – this policy provides subscribers and users with general and specific instruction on how to store and retain registration and enrolment forms.

- Master Service Agreement (MSA) – prior to going live, SSHA and subscribers agree to an appropriate Master Service Agreement.

## 5.0 Risk, Mitigation, and Timeframes

To address privacy risks associated with One Mail Direct, in the PIA the Privacy Team has recommended the following mitigating actions:

Risk Description	Mitigation Action	Completion Date
Unauthorized/accidental access and disclosure of personal registration information collected during the registration process, i.e., name and identity documents (drivers licence, birth certificate, etc.).	Privacy and security training is mandatory for all SSHA Personnel.	Completed November 2007.
	Communicate to client and end users via deployment package and training material the purpose of collecting their personal information.  Notification of the purpose of collection is on the registration form.	Deployment package (provided to clients) for ONE Mail Direct that details the collection process is under review for enhancement and expected to be completed before March 2008.
Accidental destruction of audit logs in the absence of retention schedule.	Record management controls were put in place for system audit logs. SSHA retains the logs indefinitely until such time as a retention schedule is completed (is currently under development).	Expected to be completed before March 2008.
Denial of the privacy right to report incidents due to lack of information about an incident management program.	SSHA to ensure that clients are aware of its incident management program.	The deployment package (provided to clients) review includes a strategy for building awareness of SSHA's incident management program. The deployment package

<b>Risk Description</b>	<b>Mitigation Action</b>	<b>Completion Date</b>
		review for enhancement is to be completed by March 2008.

## APPENDIX 1: TERMS AND ACRONYMS

Acronym/Term	Definition
FIPPA	Freedom of Information Protection of Privacy Act
HIC	Health Information Custodian
MDSM	ONE Mail Direct Service Module
MSA	Master Service Agreement
Personnel	SSHA staff, consultants, and employees of vendors.
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PIA	Privacy Impact Assessment
SSHA	Smart System for Health Agency
TRA	Threat Risk Assessment