

ONE[®] Mail Partnered

PIA Summary

Document Identifier: 1145

Version: 2

Document Control

Revision History

Date	Version	Revision
June 2008	2	Revisions based on feedback from LHIN
Nov 2007	1	Final Copy

© 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 1

 3.1 In-Scope 1

 3.2 Out-of-Scope 1

4.0 Findings 1

 4.1 Client Privacy Responsibilities 1

5.0 Safeguards in Place to Protect Information..... 1

6.0 Risks, Mitigations and Timeframe 1

7.0 Appendix 1: Terms and Acronyms..... 1

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 Mail Partnered Solution.

2.0 Solution Overview

. SSHA's ONE Mail Partnered solution is a secure e-mail service available to health care providers and health care organizations and institutions that have a pre-existing e-mail environment.

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 PHI. To fulfil this mandate SSHA offers a suite of Solutions, including ONE Mail Partnered, a secure e-mail service.

The ONE Mail Partnered solution links together the e-mail systems of ONE Mail Partnered subscriber Health Information Custodians (HICs) across Ontario. This solution facilitates the secure and confidential electronic delivery of messages between HICs, helping them provide better health care services to Ontarians. The ability to send PHI via e-mail, as opposed to slower, more traditional methods like faxing or courier, means that health care providers have more timely and cost-effective access to patient care information.

Health care professionals wishing to use ONE Mail Partnered must subscribe for SSHA's Managed Private Network (MPN) solution. (A separate Privacy Impact Assessment (PIA) has been completed for the MPN.) Through the MPN, subscribers are able to connect to the Internet, as well as to the Government of Ontario Network (GoNet/INP), and to Ontario's broader health care sector. The ONE Mail Partnered solution links the e-mail environments of MPN subscribers and provides all IT services necessary to route e-mail securely between subscribers, and to or from non-subscribers via the Internet. E-mail messages sent between MPN subscribers are encrypted to provide security and do not traverse the Internet. It is possible for unsecured and unencrypted PHI to be routed to the internet.

E-mail messages routed to One Mail Partnered users from non-users, or e-mail messages sent by ONE Mail Partnered users to non-users, cannot be encrypted. So, subscribers must ensure that safeguards around their e-mail servers are in place and that logon mail applications they use (like Outlook and web-based mail) have authentication mechanisms that ensure that only authorized individuals use the system.

For the purposes of PHIPA, SSHA is considered a Health Information Network Provider (HINP) with regard to ONE Mail Partnered, so SSHA must comply with PHIPA provisions applicable to HINPs. As well, because SSHA collects personal information related to some users of ONE Mail Partnered, SSHA must comply with FIPPA.

3.0 Scope

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

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

3.1 In-Scope

The following was assessed as part of the PIA:

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

3.2 Out-of-Scope

The following was not assessed for the PIA:

- Performance monitoring and reporting related to the SSHA infrastructure.
- SSHA hosting facility infrastructure.
- ONE Mail Direct 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.)

4.0 Findings

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

1. FIPPA applies.
2. PHIPA applies.
3. SSHA does not have custody or control over ONE Mail Partnered user-generated traffic that passes through SSHA's environment.
4. SSHA and ONE Mail Partnered subscribers have a privacy and security partnership.
5. SSHA logs transactions only (date, time, addresses, etc). E-mail files are stored on the client's mail server.
6. SSHA system administrators have incidental access to email 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.
7. ONE Mail clients who send emails, knowingly or inadvertently, to recipients not selected from the ONE Pages directory risk sending PI or PHI via unsecure means.

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 (including, when applicable, obtaining consent before using ONE Mail Partnered 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 Partnered can appropriately be transmitted (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 identification, passwords, secure tokens, and other authentication credentials assigned to the Client or users to enable them to connect to One Mail Partnered.

Clients are responsible for attesting that users have a legitimate business need for using One Mail Partnered, that they are associated with the provision of health care related services, and that they meet eligibility requirements for using One Mail Partnered. As well, the Client is responsible for obtaining any necessary consent required under applicable laws and regulations before collecting, using, or disclosing the PI of users.

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 controls in place to help ensure that privacy impacts relevant to ONE Mail Partnered 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 systems.
- Privacy and Security training is mandatory for all staff.

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

- The servers used by SSHA to provide ONE Mail Partnered 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 Partnered. (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 Partnered users is encrypted. (An e-mail message(s) to or from a ONE Mail Partnered user to someone who is not a ONE Mail Partnered user is not encrypted.)
- SSHA employs anti-spam and anti-virus technologies.
- Any time a user attempts to access ONE Mail Partnered, SSHA takes steps to confirm the user is an authorized user of ONE Mail Partnered (for example, requesting their user name and password).
- SSHA has the following administrative policies and agreements related to ONE Mail Partnered. 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.

6.0 Risks, Mitigations and Timeframe

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

Risk Description	Mitigation Action	Completion Date
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).	Fiscal 2008/2009.
Denial of the privacy right to report incidents due to lack of information about an incident	SSHA to ensure that clients are aware of its incident management program.	The deployment package (provided to clients) review includes a strategy

<p>management program.</p>		<p>for building awareness of SSHA's incident management program.</p> <p>The deployment package review and enhancement is to be completed by March 2008.</p>
<p>Unauthorized disclosure of PI and/or PHI if the ONE Pages directory is not used appropriately for sending e-mails.</p>	<p>SSHA to continue to make clients aware of the use of ONE Pages directory for sending and receiving e-mails containing PI and/or PHI.</p>	<p>Ongoing – This is part of the user training conducted by SSHA .</p>

7.0 Appendix 1: Terms and Acronyms

Acronym/Term	Definition
FIPPA	Freedom of Information Protection of Privacy Act
HIC	Health Information Custodian
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