

ONE™ Pages

PIA Summary

Copyright Notice

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

All rights reserved.

Table of Contents

| | | |
|------------|--|----------|
| 1.0 | SOLUTION OVERVIEW | 1 |
| 1.1 | PROJECT DESCRIPTION/BACKGROUND..... | 1 |
| 2.0 | SCOPE..... | 2 |
| 2.1 | IN-SCOPE | 2 |
| 2.2 | OUT-OF-SCOPE..... | 3 |
| 3.0 | FINDINGS..... | 3 |
| 3.1 | CLIENT PRIVACY RESPONSIBILITIES..... | 3 |
| 4.0 | SAFEGUARDS IN PLACE TO PROTECT INFORMATION..... | 4 |
| 5.0 | RISK, MITIGATION, AND TIMEFRAMES..... | 5 |

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

1.0 Solution Overview

ONE Pages is a value-add component offered in conjunction with SSHA's ONE™ Mail (Direct or Partnered) solution. ONE Pages allows ONE Mail users to access an electronic directory (ONE Pages directory) containing business contact information, including first name, last name, organization name, department, and business e-mail addresses of people who use ONE Mail. Individuals listed in the ONE Pages directory may send and receive personal information (PI) and PHI over SSHA's secure network. Making such contact information available electronically, to those using the ONE Mail system, helps ensure that PHI needed for health care decisions flows to the proper person, or organization, leading to improved health care.

Users of ONE Mail who have concerns about the confidentiality of their contact information being published, or who fear they might be highly susceptible to harassment, unwanted contact, or unsolicited communications, can opt out of being listed in the ONE Pages directory. ONE Mail users who opt out of being listed in the ONE Pages directory can still access ONE Pages.

1.1 Project Description/Background

SSHA is mandated with designing, building, and deploying a trusted, secure e-mail service for transmission of PI and PHI. ONE Pages is a key component of SSHA's trusted e-mail service because the ONE Pages directory allows users to identify intended e-mail recipients, greatly minimizing the risk that PI or PHI might be sent to someone who is not a ONE Mail and ONE Pages Registrant.

Contact information of users listed in the ONE Pages directory (including first and last name, organization they are affiliated with, department they are in, and their business e-mail address) is available to anyone who has access to ONE Mail unless the user has opted not to be listed in the ONE Pages directory.

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

Registering ONE Pages Users

Registration for use of ONE Mail (Direct or Partnered) is a pre-requisite for being listed in the ONE Pages directory. ONE Pages users must be registered, using ONE™ ID Direct or ONE ID™ Partnered, to enable them to access the directory. The registration process is considered out of scope for the purpose of this PIA Summary. Further information with respect to the ONE ID service, ONE Mail Direct, and ONE Mail Partnered can be found on the SSHA website (www.ssha.on.ca).

Once registered, users are enrolled in ONE Pages and they have access to the ONE Pages directory.

Data Seeding of the ONE Pages Directory

Data seeding is a process by which the ONE Pages directory is populated with pertinent information about users. Data related to ONE Mail Direct subscribers who participate in ONE Pages comes through the ONE ID Direct registration process. Once SSHA provisions a ONE Mail Direct mailbox for the user, the user's business contact information is shown in the ONE Pages directory.

For ONE Mail Partnered users, the subscriber controls the list of people in their organization that will appear in the ONE Pages directory. Data regarding these users comes to SSHA from the subscribers' in-house directory after being cleansed (by the subscriber) of data the subscriber does not want included in the ONE Pages directory.

Data Refresh

The data refresh process refers to updating the ONE Pages directory.

For ONE Mail Direct subscribers, the individual user must submit a change request form to the organization sponsoring the user (the subscriber). The change request is then sent by the subscriber to SSHA for updating the ONE Pages directory.

In the case of information from ONE Mail Partnered subscribers, individual users must ask their sponsoring organization to change the information in the sponsoring organization's (the subscriber's) internal directory. The subscriber is responsible for updating its internal directory, which SSHA automatically retrieves, posting changes to the ONE Pages directory every 12 hours, or more frequently if required.

Data Deletion

If a subscriber stops using ONE Mail, or if a user decides he or she no longer wants to be listed in the ONE Pages directory, SSHA deletes all data in ONE Pages relating to that user. For ONE Mail Direct users the subscribing organization informs SSHA that the user wants to be deleted from the ONE Pages directory and directs SSHA to deactivate the user's ONE Pages listing.

When a user from a ONE Mail Partnered subscriber is to be deleted from ONE Pages the subscribing organization removes the user from its internal directory and when ONE Pages automatically updates information from that subscriber's internal directory (as it does every 12 hours) the user is deleted from the ONE Pages directory.

2.0 Scope

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

The PIA was based on information current to November 2007.

2.1 In-Scope

The following were assessed as part of the PIA:

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

- Related SSHA policies, including the *ONE Pages Acceptable Use Policy*, *Information Collection Policy*, and the *SSHA Information Retention and Storage Policy*.

2.2 Out-of-Scope

It should be specifically noted that the following were not assessed for the PIA:

- Performance monitoring and reporting related to SSHA's infrastructure.
- The SSHA hosting facility infrastructure.
- ONE Mail Direct and ONE Mail Partnered. (Note: both of these are the subject of separate PIAs.)
- ONE ID. (This Solution is the subject of a separate PIA.)
- The institutional environment of users and subscribers.
- SSHA's Storage Area Network (SAN). (Note: SAN is the subject of a separate PIA.)

3.0 Findings

In the PIA, the Privacy Team identified the following findings associated with ONE Pages:

1. The aggregate data held in the ONE Pages directory may be considered sensitive even though the ONE Pages data may not be considered to be PI.
2. PHIPA-related implications could arise with respect to the use of the ONE Pages directory if the directory is inaccurate and/or obsolete and consequently there is unauthorized, though unintentional, disclosure of PHI and a privacy breach under PHIPA.
3. The process for deactivating e-mail accounts and subsequent access to ONE Pages is documented. Some staff are trained on this process, however, not all SSHA staff who work in this area, ONE Pages, have received formal training on the deactivation process and procedure.

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. In addition, *ONE Pages Acceptable Use Policy* prohibits inappropriate and illegal use of information contained in the ONE Pages directory.

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 the ONE Pages Solution 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.
- All SSHA Personnel are required to complete mandatory Privacy and Security training.
- SSHA staff and consultants must sign a confidentiality agreement and submit to a criminal background check prior to joining or doing work for SSHA.
- SSHA's Privacy Team 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 requirement relating to privacy breaches.

As well, SSHA has the following safeguards (controls) in place that are specific to ONE Pages:

- Safeguards Designed to Ensure Appropriate Use of the ONE Pages Directory
ONE Pages Acceptable Use Policy provides subscribers with general and specific instructions on acceptable use of the ONE Mail infrastructure. In addition, a description of inappropriate and illegal use of sensitive information in the ONE Pages directory, required, and recommended safeguards for protection of the technology itself are provided. The subscribing organizations are responsible for ensuring that users that are sponsored are using ONE Pages responsibly.

From time-to-time, SSHA receives requests on behalf of subscribers from third parties for ONE Pages directory data relating to a particular subscriber. When this occurs, SSHA seeks permission from the subscriber to release the information. If the third party request relates to information related to various subscribers, SSHA seeks permission from each subscriber.

- Safeguards Designed to Prevent Bulk Harvesting of Information from the ONE Pages Directory
SSHA has implemented controls to prevent the bulk harvesting of contact information from the ONE Pages directory. Technically, SSHA hampers the ability to bulk harvest by limiting the number of records generated from each search to 10 per page. This limitation makes it difficult for individuals to harvest the data.

As well, the *Acceptable Use Policy* related to ONE Pages specifically prohibits subscribers and users from bulk harvesting information.

➤ Safeguards Related to Handling Privacy Incidents that can Arise with Regard to ONE Pages

Incident management is the process used when information on the user registration and enrolment forms, or information from the ONE Pages directory, is revealed to those not authorized to get such information. In the case of ONE Pages, incidents can include:

- stealing or misplacement of completed registration and enrolment forms;
- perpetration of identity theft as a result of stolen personal information collected in the registration process;
- improper disposal of documents (for example, registration and enrolment forms) in other words, disposing of documents in a manner other than shredding;
- improper or unauthorized use of information collected on registration and enrolment forms, (for example, use of information for updating a human resources contact base).

SSHA is in the process of implementing an incident management process.

➤ Administrative policies and Agreements Regarding ONE Pages

SSHA has the following administrative policies and agreements related to ONE Pages:

- 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.

➤ Subscriber and User Education

SSHA has prepared the following educational information for ONE Pages subscribers:

- information regarding roles and responsibilities
- support training for IT staff

SSHA has prepared the following educational information for ONE Pages users:

- ONE Pages Online Help
- ONE Pages User Guide
- A Virtual Tour of ONE Pages

5.0 Risk, Mitigation, and Timeframes

There are no unaddressed Privacy risks to SSHA's ONE Pages solution. For a breakdown of risk mitigation actions taken, refer to the previous section of this document.

APPENDIX 1: TERMS AND ACRONYMS

| Acronym/Term | Definition |
|--------------|--|
| FIPPA | Freedom of Information and Protection of Privacy Act |
| HIC | Health Information Custodian |
| IPC | Information Privacy Commissioner/Ontario |
| IP | Internet Protocol |
| LDAP | Lightweight Directory Access Protocol |
| MIIS | Microsoft Identity Integration Server |
| Ministry | Ministry of Health and Long-Term Care |
| MSA | Master Services Agreement |
| Personnel | SSHA staff, consultants, and employees of vendors. |
| PIA | Privacy Impact Assessment |
| PI | Personal Information |
| PHI | Personal Health Information |
| PHIPA | Personal Health Information Protection Act |
| SAN | Storage Area Network |
| SLA | Service Level Agreement |
| SMTP | Simple Mail Transfer Protocol |
| SSHA | Smart Systems for Health Agency |