

ONE™ Network Access (OfficeNet)

PIA Summary

Copyright Notice

Copyright © 2008 Smart Systems for Health Agency (SSHA).

All rights reserved.

Trademarks

Windows is a trademark of Microsoft Corporation.

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Revision History

Version No.	Version Date	Summary of Change	Changed By
1.0	2008-03-18	Approved by Michael Power	Urooj Kirmani
0.3	2008-03-17	Changes based on Jane Dargie's Feedback	Urooj Kirmani
0.2	2008-03-14	Changes based on Brian Spencer's feedback	Urooj Kirmani
0.1	2008-03-11	Initial Draft	Urooj Kirmani

Table of Contents

- 1.0 SOLUTION OVERVIEW.....4**
- 2.0 SCOPE.....5**
 - 2.1 IN-SCOPE.....5
 - 2.2 OUT-OF-SCOPE5
- 3.0 FINDINGS6**
 - 3.1 CLIENT PRIVACY RESPONSIBILITIES6
- 4.0 SAFEGUARDS IN PLACE TO PROTECT INFORMATION7**
- 5.0 RISKS, MITIGATION, AND TIMEFRAMES.....8**

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 the OfficeNet.

1.0 Solution Overview

OfficeNet is a new technology under ONE™ Network Access suite of products. OfficeNet will enhance the existing extended Wide Area Network (eWAN) product currently deployed to SSHA clients. SSHA intends to migrate all existing eWAN clients to the new OfficeNet service by fiscal year 2009/2010.

ONE Network Access provides health care providers with connectivity to the SSHA Private Network as well as to the Internet. It allows health care providers to share confidentially information over a high-speed network built for health care. It is also used by health care organizations to access applications hosted by SSHA, ONE Hosting, and as a custom connection for their specific information sharing needs, such as Health Card validation by hospitals. Typical clients for ONE Network Access include health care organizations that require secure way to share and/or access information. The OfficeNet solution uses Cisco Integrated Service Routers (ISR) that are deployed at client locations with Virtual Private Network (VPN) Tunnels connected to the VPN Concentrators at the SSHA Data Centres.

OfficeNet adds the following functionality to SSHA's eWAN product:

- Product Enhancements and Pricing:
 - Standard Asymmetric Digital Subscriber Line (ADSL) (1Mb) service is being replaced with a RSDSL (7Mb) service.
 - Standard Cable (1Mb) service is being replaced with 5 and 8Mb services.
 - The new ADSL and Cable services will be deployed with Routers rather than only a Firewall, at reduced price points.
 - Additional cost reductions were agreed to via re-structured quantity discount plans.
- Security:
 - All health related traffic will be encrypted (IPSec) in VPN Tunnels between the Client CPE Device and VPN Concentrator.
 - Centralized Virtual Private Network (VPN) Concentrator solution within the SSHA Data Centres to consolidate access control, routing and firewall services.
 - Intrusion Detection and Prevention (IDP), DDOS (Distributed Denial of Service), Policy Based Routing and Strict Firewall Rules. DPI (Deep Packet Inspection), Antivirus are available when needed.
- Enhanced Network Management capabilities allow SSHA a view into all network elements for problem isolation purposes and performance management data collection.
- Process Improvements:
 - Elimination of the SSHA 1FL Order requirement (to Bell Canada) by including it in the order process with Allstream.
 - Elimination of the second order currently required with the eWAN order process.

SSHA has designed the connection to be highly reliable, available and secure in order to support the needs of the sector for sharing of health care information with the confidence that information will reach the target audience in a timely manner and without being compromised.

OfficeNet offers five office models labelled A-E as opposed to the model office 0-5 offered by e-WAN. Office Models are a method of pre-defining connectivity configurations intended to meet the client application needs. The OfficeNet models provide additional security.

2.0 Scope

The Privacy Team's conclusions were based on reviewing project documentation and on gathering information from SSHA's OfficeNet Project Team.

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

2.1 In-Scope

People:

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

Process:

- Processes associated with implementation of OfficeNet including process to order OfficeNet, deployment and support.

Policy:

- Agreements/policies related to OfficeNet including schedule specific to OfficeNet and acceptable use policy.

Technology:

- Technology employed by OfficeNet including the security features offered by the OfficeNet technology.

2.2 Out-of-Scope

People:

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

Process:

- Clients' processes for signing up for ONE Network Access.

Policy:

- Clients' policies relating to the use of ONE Network Access.

Technology:

- The leveraged SSHA components upon which OfficeNet is dependent.
- The client environment serviced by ONE Network Access including in-house security measures, firewalls and connectivity within the system.
- The SSHA MPN. This is subject of a separate PIA.
- The SSHA ONE ID. This is subject of a separate PIA.

Other:

- Clients' privacy compliance programs and physical environment.

3.0 Findings

The Privacy Team identified the following findings associated with ONE Network Access (OfficeNet):

1. SSHA and its clients and vendors have a privacy and security partnership.
2. SSHA does not have custody or control over ONE Network Access network traffic.
3. SSHA has control and custody over the logs produced by devices it owns.
4. The Personal Health Information Protection Act and its Regulations apply.
5. A breach initiated at client source is the responsibility of the Health Information Custodian.
6. There is no established mechanism by which clients can affirm to SSHA that they have established and operate a common security standard.
7. All health related traffic will be encrypted (IPSec) in VPN Tunnels between the Client CPE Device and VPN Concentrator. Allstream and SSHA staff during monitoring of the network may come in contact with network traffic, which may or may not contain PI/PHI. There may be exceptional circumstances, where a highly technical staff may get access to the information traversing the network.

3.1 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 OfficeNet.

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

4.0 Safeguards in Place to Protect Information

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

- SSHA has implemented a Privacy Program which has been reviewed by the Information and Privacy Commissioner of Ontario (IPC).
- 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 staff.
- SSHA uses intrusion detection tools configured to provide alerts to SSHA when certain sets of circumstances take place that indicate a possible intrusion.
- SSHA could have incidental access to PHI when performing service associated with OfficeNet i.e., troubleshooting, installation, and back-up services. SSHA has implemented system and personnel controls to ensure that individuals act appropriately. SSHA personnel are screened and are expected to sign off on standard of conduct agreements at the time of hiring as well as all SSHA staff have received training on privacy and security.

- SSHA has employed string perimeter security of its data centres including biometric scanning.
- Cisco ISR Router provides routing and firewall services. It provides more granular level of security (i.e. no predefined security) and no sniffing capabilities.
- Remote access registration and control is being created and will reside in-house.
- CPE Device Certificate issuance process and control is being moved in-house.

5.0 Risks, Mitigation, and Timeframes

To address privacy risks associated with OfficeNet, 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
Reduced capacity to coordinate management of privacy and security incidents between SSHA and client.	Medium	Low	SSHA to ensure that clients are aware of the incident management program and the roles and responsibilities of each of the parties for investigating a breach.	Enterprise Security and Privacy Incident Management Program (ESPIM) has been deployed at SSHA to tackle privacy/security incidents. The ESPIM program will be socializing the program to SSHA clients in Fiscal 08/09
Unauthorized use or disclosure of personal health information by SSHA while performing support activities for OfficeNet	Medium	Low	Privacy and Security training is mandatory for all SSHA staff. SSHA to provide continuous privacy	As of November 30 th , 2007 all SSHA staff has completed online Privacy and Security Training. The training is mandatory for any new staff. Role based

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
			training and awareness to its existing employees.	training will be rolled out in fiscal year 08/09. As well, privacy awareness campaign is planned for fiscal 08/09.
Accidental destruction of audit logs in the absence of retention schedule	Medium	Very Low	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 (It is currently under development).	Retention schedule is under development. It is expected to be completed in fiscal 08/09.

APPENDIX 1: TERMS AND ACRONYMS

Acronym/Term	Definition
ADSL	Standard Asymmetric Digital Subscriber Line
DDOS	Distributed Denial of Service
DPI	Deep Packet Inspection
ESPIM	Enterprise Security and Privacy Incident Management
eWAN	Extended Wide Area Network
FIPPA	Freedom of Information Protection of Privacy Act
HIC	Health Information Custodian
HINP	Health Information Network Provider
IDP	Intrusion Detection and Prevention
IPC	Information and Privacy Commissioner
IPSec	Internet Protocol Security
ISR	Integrated Service Router
MOHLTC	Ministry of Health and Long Term Care
MPN	Managed Private Network
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PI	Personal Information
PIA	Privacy Impact Assessment
SSHA	Smart Systems for Health Agency
SSO	Single Sign-on
VPN	Virtual Private Network