

ONE™ Network (Network Refresh)

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	2008-03-19	Approved by Michael Power	Michael Power
0.2	2008-03-18	Incorporates feedback from Jane Dargie and Brian Spencer	Ruth M. Vale
0.1	2007-11-22	First draft	Ruth M. Vale

Table of Contents

INTRODUCTION.....1

1.0 SOLUTION OVERVIEW.....2

 1.1 ONE NETWORK ENTERPRISE DESCRIPTION/BACKGROUND2

2.0 SCOPE.....3

 2.1.1 *In Scope*.....3

 2.1.2 *Out-of-Scope*.....4

3.0 FINDINGS4

 3.1 CLIENT PRIVACY RESPONSIBILITIES5

4.0 SAFEGUARDS IN PLACE TO PROTECT INFORMATION5

5.0 RISK, MITIGATION AND TIMEFRAME8

INTRODUCTION

Smart System for Health Agency ('SSHA' or '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) 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™ Network Enterprise.

1.0 Solution Overview

ONE Network Enterprise comprises several technologies that work together to support transmission requirements for data.

1.1 ONE Network Enterprise Description/Background

SSHA is undertaking a technology refresh project (Network Refresh Project) to enhance Ontario's Health Information Network. This project will significantly expand bandwidth of the network and will also improve the reliability, security, privacy, and quality of the ONE Network Enterprise service. Expanded bandwidth and a scalable design will address the short and long term connectivity needs of the Ontario Ministry of Health and Long Term Care. Hydro One Telecom (HOT) will design, implement and operate the fibre-optic core of the network based on SSHA's architecture requirements. Services include network monitoring and infrastructure security.

The current, legacy product is the Wide Area Network (WAN) service provided through the Agreement with EDS/Bell. The new ONE Network Enterprise service provides a complete portfolio of WAN, Virtual Private Network (VPN) and Internet products. This high-availability Core network is based on Multi Protocol Label Switching (MPLS) technology running over dedicated Dense Wavelength Division Multiplexing (DWDM) wavelengths on optical fibre rings. Each of the core links supports transfer rates of 2.5 Gbps today and is scalable to multiple 10 Gbps in the future. A second tier Access Network, again running over dedicated fibre optic links, provides points-of-presence at most major clients.

Where a dedicated fibre link to a hospital or to other client facility is unavailable, the link will be achieved through the use of Transparent LAN Services (TLS) procured from a third party common carrier. In these cases, all non-Internet traffic through the TLS link will be encrypted using IPSec between the CPE router controlled by HOT and an IPSec concentrator located at the interface with the MPLS network.

Internet service will be provided to clients through the MPLS network, but will be kept totally separate from private health network traffic through the use of MPLS Layer II tunnels.

The Off-Net Access Network connected to the base network connects health care providers who require a Digital Subscriber line (DSL)/Cable or DS-1 based service access.

Internet services will be routed through a VPN connection (Martini –Draft, at a Layer II level¹) and be directed straight to the internet based router. Internet connections will not be routed through the core network.

The Network Refresh Project (NRP) has worked with the Local Health Integration Networks in order to ensure that all of the client sites will be migrated from SSHA's Managed Privacy Network (MPN) WAN circuits to the HOT ONE Network Enterprise network. The project continues to complete site surveys detailing the specifics of configuration and application requirements for each site, to facilitate rapid migration to the new network in a transparent manner that does not affect the users.

¹ 2006-08-28_NRP Services Overview with MCC

The applications and technologies currently used at each site will be carried up the upgraded bandwidth.

2.0 Scope

The Privacy Team's conclusions were based on reviewing project documentation and on gathering information from SSHA's Network Refresh team.

This report is based on information current to December 2007.

2.1.1 In Scope

People:

- The roles and responsibilities of the various stakeholders involved in NRP and ONE Network Enterprise.

Process:

- Partnership agreement between SSHA and HOT.
- Related SSHA operational policies.
- Processes associated with implementation of ONE Network Enterprise (Network Refresh) including processes to order circuits, deployment and support.
- Migration of current sites.
- Integration, of SSHA internal processes and HOT network processes.

Policy:

- Agreements/policies including the schedule specific to ONE Network Enterprise (Network Refresh) and the acceptable use policy.

Technology:

- Technology employed by ONE Network Enterprise (NRP) including the security features offered by the ONE Network Enterprise (NRP) technology.
- High level business requirements of architecture and design.
- Network build of the core and access to the core.
- Enablement of network operations centre (NOC) access for SSHA.

2.1.2 Out-of-Scope

Process:

- SSHA Security Operations Centre and Network Operations Centre.
- Clients' internal processes for using ONE Network Enterprise (Network Refresh).

Technology:

- Detailed design of the HOT network.

Other:

- Clients' privacy compliance programs and physical environment.

3.0 Findings

Inherent in the design of the network architecture is the principles that every effort has been made to limit, reduce and prevent access by network support personnel (both SSHA and HOT) to the client data stream. This objective has been achieved to a remarkable degree. The provision of this network does not involve the collection, use or disclosure of, or access to patient information. User information is collected in the registration process, but the provision of services in itself is a technical exercise with primary emphasis placed on accountability, appropriate safeguards and proactive incident management.

The Privacy Team identified the following additional findings associated with ONE Network Enterprise (Network Refresh).

1. SSHA and its clients and vendors have a privacy and security partnership.
2. SSHA does not have custody or control over ONE Network Enterprise (Network Refresh) 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.

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 ONE Network Enterprise (Network Refresh).

Clients are responsible for attesting that users have a legitimate business need for using ONE Network Enterprise (Network Refresh). 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.

The demarcation point between the client network and SSHA provided services represents the primary vulnerability for access to the client stream. Clients are responsible to ensure that physical access to their site and to the demarcation point in particular, is appropriately safeguarded.

Lastly, the client is responsible for assessing and addressing any privacy risks associated with the application and its own support processes. It is assumed that the client is undertaking these activities.

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 Network 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 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.
- Remote access registration and control is being created and will reside in-house.
- SSHA provides current administrative policies and agreements related to ONE Network as part of the Subscriber Agreement package.
- Privacy and Security safeguards have been embedded in the Agreement between HOT and SSHA. The agreement addresses:
 - a. Security screening for HOT personnel and subcontractors is underway.
 - b. Privacy training has been conducted by SSHA for specified HOT personnel.
 - c. HOT personnel to abide by SSHA privacy and security policies.
 - d. Confidentiality agreements.
 - e. HOT to cooperate with SSHA's Threat Risk and privacy assessments.
 - f. All SSHA confidential data streams to stay in Ontario.
 - g. All information on HOT networks transmitted within Canada.
 - h. Disclosure only as required by law, legal compliance.
 - i. Design to meet SSHA security needs, HOT to conduct security audits.
 - j. HOT has undertaken an ISO-based assessment with respect to information systems security.
 - k. HOT is in the process of completing a statement about the security controls in place at their organization and active in the network being built to support SSHA activity.
 - l. The CFO is appointed the senior privacy officer at HOT.
 - m. A privacy program is in development at HOT.

- n. Incident and problem resolution are addressed in the agreement.
- o. Detailed privacy and security obligations are provided in the agreement.
- p. HOT Security practices assessment to be conducted by independent third party within 12 months after acceptance. HOT will also periodically conduct a security assessment as part of technology review process, report to be delivered to SSHA within 30 days of delivery to HOT. This security work is in progress.
- q. SSHA has read-only access to HOT monitoring tools for anomaly detection and traceback, signature detection, worm detection, traffic analysis and transit analysis, black hole routing, sinkhole routing. A dashboard provides for drilling down to particular circuit, managed element, SSHA site, client site. SSHA to have interface to Hot Ticket management system for any incidents, and to daily & periodic incident reports.
- r. ONE Network Access (Network Refresh) is designed and operated in a manner intended to eliminate or minimize the possibility of an unauthorized person obtaining access to the system, or any person being able to compromise the client data being transmitted.
- s. Agreement Schedules include Incident management and problem management procedures.
- t. On request from SSHA, SSHA will receive weekly and monthly security reports citing unusual usage patterns in the core network – in the future this will include reports on intrusions and breaches (actual and attempted), detection and removal of viruses and malicious content.

5.0 Risk, Mitigation and Timeframe

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
<p>HOT and SSHA are working to complete the integration of their privacy programs where relevant to ONE Network. The lack of integration may impact the operational effectiveness of the parties working together to address any privacy issues such as any incidents arising.</p>	<p>Medium</p>	<p>Medium</p>	<p>HOT has initiated a privacy program plan.</p> <p>SSHA has provided privacy training to HOT members of the project management team.</p> <p>Process development has included Incident and Problem Management protocols.</p>	<p>This is a continuous improvement exercise which SSHA is monitoring through the Privacy Risk Management Program through its standard review cycles.</p>
<p>SSHA has still to review and assess the privacy impacts of SSHA's Network Operations Centre and, in particular, the related auditing and monitoring capacity.</p>	<p>Medium</p>	<p>Medium</p>	<p>SSHA will review the NOC from a privacy perspective.</p> <p>Security work is underway.</p>	<p>Scheduling underway.</p>

APPENDIX 1: TERMS AND ACRONYMS

Acronym/Term	Definition
DWDM	Dense Wavelength Division Multiplexing
DSL	Digital Subscriber Line
EPP	Enterprise Privacy Policy
HIC	Health Information Custodians
Layer 2	Refers to the OSI model of Network architecture
LAN	Local Area Network
INP	Ontario Government Information Network services
MOHLTC	Ministry of Health and Long Term Care
MPLS	Multi Protocol Label Switching protocol
NRP	Network Refresh Project
PI	Personal Information
PHI	Personal Health Information
PIA	Privacy Impact Assessment
SSHA	Smart Systems for Health Agency
TLS	Transparent LAN Services
TRA	Threat Risk Assessment
WAN	Wide Area Network
VPN	Virtual Private Network