

ONE™ Network Access Extended Wide Area Network (eWAN)

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
02	2008-03-17	Incorporates feedback from Jane Dargie	Ruth Vale
01 (renumbered)	2008-02-11	Incorporates comments from Patrick Lo	Ruth Vale
.02	2008-01-18	Incorporates comments from Patrick Lo	Ruth Vale
.01	2008-01-17	First draft	Ruth Vale

Table of Contents

INTRODUCTION..... III

1.0 SOLUTION OVERVIEW..... 4

 1.1 EWAN DESCRIPTION/BACKGROUND..... 4

2.0 SCOPE..... 5

 2.1 IN-SCOPE 6

 2.2 OUT-OF-SCOPE..... 7

3.0 FINDINGS..... 7

 3.1 CLIENT PRIVACY RESPONSIBILITIES..... 8

4.0 SAFEGUARDS IN PLACE TO PROTECT INFORMATION 8

5.0 RISK, MITIGATION, AND TIMEFRAMES..... 9

APPENDIX 1: TERMS AND ACRONYMS..... 12

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™ Network Access (eWAN).

1.0 Solution Overview

Smart Systems for Health Agency (SSHA) provides a high-speed private network infrastructure to the health care community. The latter provides a means of transit for data from health care applications in a predictable and highly supported manner.

SSHA's ONE Network allows health care providers confidently to share information over a high-speed network built for health care. ONE Network is 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. Extended Wide Area Network (eWAN) is one component of ONE Network Access designed for physician offices and small organizations

As part of ONE Network Access, the eWAN service connects professional health care providers including pharmacies, clinics, and private medical facilities, such as long-term care homes. These facilities may in turn enable connectivity from even smaller locations acting as the hub in hub-and-spoke configurations and by means of remote Virtual Private Network (rVPN) routes. In general, eWAN provides connectivity for smaller scale facilities where Wide Area Network (WAN) capacity would be excessive and too expensive to be feasible. The environment uses Small Office Firewall Appliance (SOFA) devices that are interconnected via Cable or Asymmetric Digital Subscriber Line (ADSL), Digital Subscriber Line (DSL) or fixed T1 connections (see the Terms and Acronyms section for a description of T1 connections).

From a functional point of view, the eWAN service provides health care subscribers with connectivity to the health care network in Ontario. They can use VPN access to their clinics via the Internet from offices or at home, thus protecting the client's internal network from external-based threats. While eWAN may be considered a private network located behind a firewall, it is nevertheless fully and integrally connected to the SSHA Managed Private Network (MPN) via the Network Service Provider (NSP) and Firewall layers at SSHA Data Centres.

SSHA procured the eWAN network to provide a secure communications mechanism for SSHA's smaller subscribing clients. With the use of the standard SOFA devices in their typical configuration, there is no expectation of an encrypted VPN. Instead, eWAN can be adjusted so that subscribers can establish the appropriate level of security for their needs. The eWAN network, in its several models, provides the subscriber with a default level of access control to prevent Internet based sources from breaching the perimeter of the network or from gaining access to the subscriber's internal network.

1.1 eWAN Description/Background

The connection between the client and the eWAN network happens by means of a SOFA via cable, ADSL, or telephone lines to SSHA into eWAN. SSHA then acts as that office's sole Internet Service Provider (ISP). Acceptable use policies, security policies, and policies that cover privacy, confidentiality, and freedom of information obligations, form part of the agreement between the client and SSHA in order to provide close oversight and tight administrative controls over the connection.

SSHA is a Health Information Network Provider (HINP) when it provides eWAN services to subscribers. The Agency owns and controls the devices which constitute the eWAN infrastructure.

That infrastructure is composed of multiple client networks utilizing one or more of the SOFA access control devices. These devices produce logs, controlled by SSHA. Several SOFA device models are currently utilized to provide the endpoint security. These devices run versions of the Check Point's SofaWare.

Allstream is the sole provider in the current eWAN architecture and manages all user accounts on the eWAN network. Allstream employs Check Point Virtual Private Network (VPN) technology to authenticate and authorize the user by means of a central user authentication registry and to carry out account validation by means of VPN password management.

A complete eWAN circuit consists of an access facility with a modem (cable or ADSL) and a Small Office Firewall Appliance (SOFA) box that are installed at the client site. The eWAN infrastructure is composed of multiple levels of access control and security mechanisms. The first level of security provides basic connectivity to the network subscribers. While technically the network infrastructure is connected to the Internet, the SOFA connection occurs behind an SSHA primary firewall. Generally, none of the SOFAs used to protect the individual subscriber offices are directly connected to the Internet.

eWAN circuits may be ordered by individual offices or on behalf of cooperating groups of offices. The circuit is ordered from SSHA, provisioned by SSHA from an approved third party vendor, and installed at the client site by the approved vendor. From then on, the system maintenance and security are the responsibility of the health care provider.

The demarcation point between SSHA and the client is the managed SOFA box. The SOFA box provides a standardized level of protection for the client Local Area Network (LAN). The eWAN network community has access points to the Network Service Provider (NSP) layer of the SSHA's infrastructure only and the eWAN traffic must traverse the NSP layer before accessing SSHA products and services.¹

2.0 Scope

The Privacy Team's conclusions were based on reviewing project documentation and on gathering information from SSHA's ONE Network eWAN Product Service Team.

This PIA summary is based on information available to February 2008.

¹ Smart Systems for Health Agency Technology Infrastructure: Network Services Layer, Version 0.04, December 2004, p. 12 and 19-20.

2.1 In-Scope

People:

- The roles and responsibilities of the various stakeholders involved in eWAN.

Process:

- Client and service provider agreements that relate to eWAN. Related SSHA operational policies.
- Installing eWAN circuit connections to health care providers.
 - Operation of the stand-alone SOFA device and rVPN services.
 - SSHA data centre configuration and service administrative processes.
 - SOFA Platform Management, including Allstream's Security Management System (SMS).
 - Logging and automated system alerts of eWAN devices.

Policy:

- Agreements/policies including the schedule specific to eWAN and the acceptable use policy.

Technology:

- Technology employed by eWAN including the security features.

2.2 Out-of-Scope

Process:

- The registration of users for access to eWAN circuitry.

Technology:

- eWAN makes it possible for its subscribers to connect to SSHA's MPN. (The MPN will be addressed in a separate PIA.)

Other:

- Clients' privacy compliance programs.
- The Client environment, including in-house security measures, firewalls, and connectivity within the client's system.

3.0 Findings

In the PIA the privacy team identified the following findings associated with eWAN:

1. Safeguarding network connectivity is a partnership between SSHA and client subscribers who share eWAN network capacity.
2. eWAN must meet the client's privacy expectations.
3. As in any technical environment, a limited number of highly trained Allstream and SSHA staff may have incidental access to network traffic during service provisioning.
4. The SSHA network infrastructure was originally fundamentally dependent on eWAN. However, eWAN will be superseded by newer technology that will reduce the risks identified for eWAN.
5. There is no established assurance mechanism by which eWAN clients can affirm to SSHA, and to each other, that they have established and operate in accordance with a common security standard.
6. SSHA ensures there is a named person (client) within the support documents it prepares. For example, physician will be named if eWAN is deployed to physician's office.
7. SSHA must address existing agreements with Third Party Service Providers who were engaged prior to November 2004 and for which there is privacy and security risk associated with the arrangements.
8. eWAN logging and alert capabilities of SOFAs and Allstream infrastructure are technically limited and provide only limited disclosure of eWAN network activity.
9. SSHA's work to address current security risks associated with eWAN will be ongoing until all clients are moved to ONE™ Network Access – OfficeNet ('OfficeNet').

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 eWAN.

Clients are responsible for attesting that users have a legitimate business need for using eWAN. 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.

The client is responsible for assessing and addressing any privacy risks associated with the applications it uses 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 of its activities relevant to eWAN 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 eWAN 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.
- Remote access registration and control is being created and will reside in-house.
- SOFA boxes provides basic routing and firewall services. It provides minimal default security settings (i.e. no predefined security) and no sniffing capabilities.
- SSHA provides current administrative policies and agreements related to eWAN as part of the Subscriber Agreement package.

5.0 Risk, Mitigation, and Timeframes

The Privacy Team has recommended the following mitigating actions in this PIA to address the privacy risks which it has identified and associated with eWAN:

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
Unauthorized collection, use, or disclosure of traffic moving on eWAN connections: <ul style="list-style-type: none"> • eWAN technology is older and may not provide a successful defence against more current security threats. 	High	Medium	SSHA will phase out this product and all new subscribers are connected via OfficeNet. Current eWAN subscribers will be upgraded to OfficeNet technology.	eWAN is scheduled to be retired by 2010

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
<ul style="list-style-type: none"> HICs may operate unsafely and compromise the security of the eWAN network, associated client networks and attached SSHA networks, such as the MPN. 	Medium	Medium	<p>SSHA has augmented the privacy and security language of subscriber agreements (client agreements) in order to clarify expectations and reinforce the nature of the privacy and security partnership. SSHA has implemented a policy that agreements must be signed before work is begun on new deployments.</p> <p>SSHA has provided its own privacy and security training materials to clients and continues to support client efforts to implement strong privacy and security programs.</p> <p>Clients are responsible for ensuring that their users comply with applicable standards.</p> <p>Privacy has recommended that risks and options associated with eWAN be communicated to existing clients.</p>	<p>Complete</p> <p>Complete</p> <p>Stated in agreement.</p> <p>The eWAN summary (this document) will be posted on the SSHA public website and sent to clients in March 2008.</p>
<ul style="list-style-type: none"> SSHA must enhance its Privacy and Security provisions in agreement with Allstream service provider. 	High	Medium	<p>The Allstream agreement of 2003 was renewed in 2005 without changes. SSHA has completed a standard privacy and security schedule for all provider agreements going forward. The Implementation Plan includes a review of the privacy and security aspects of existing agreements and will make recommendations associated with enhancing those agreements.</p>	<p>Implementation of a review of currently-in-force privacy and security clauses in existing agreements is planned for 08/09.</p>

Risk Description	Risk Impact	Risk Likelihood	Mitigation Action	Completion Date
<p>Unmitigated risks associated with SOFA Appliances</p> <ul style="list-style-type: none"> SOFA appliances do not track activity above the transport layer. Records of events recorded at the transport layer by the SOFA appliance are lost when the logs disappear as a result of power outages. Open SOFA architecture increases risks. 	Medium	Low	<p>The privacy team has recommended that risks associated with eWAN be communicated to clients.</p> <p>ONE products that are new, Network Refresh (Network Refresh Project (NRP)), and OfficeNet have enhanced security capabilities and will replace the eWAN technology for new subscribers.</p>	<p>The eWAN summary (this document) will be posted on SSHA public website and sent to clients in March 2008.</p> <p>Complete.</p>
<ul style="list-style-type: none"> The default setting on the SOFA appliance is to transmit in plain text. SSL encryption is available on request from client. 	High	Medium	<p>Privacy has recommended that the default setting for all SOFA appliances be set to automatically encrypt transmissions.</p>	<p>SSHA is considering this recommendation.</p>

APPENDIX 1: TERMS AND ACRONYMS

Acronym/Term	Definition
ADSL	Asymmetric Digital Subscriber Line
DSL	Digital Subscriber Line
eWAN	extended Wide Area Network
FIPPA	Freedom of Information and Protection of Privacy Act
HIC	Health Information Custodian
HINP	Health Information Network Provider
IPC	Information Privacy Commissioner/ Ontario
ISP	Internet Service Provider
LAN	Local Area Network
Ministry	Ministry of Health and Long Term Care, Ontario
MPN	Managed Private Network
MSA	Master Service Agreement
NRP	Network Refresh Project
NSP	Network Service Provider
Personnel	SSHA staff, consultants, and employees of vendors.
PIA	Privacy Impact Assessment
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
rVPN	Remote Virtual Private Network
SOFA	Small Office Firewall Appliance
SSHA	Smart Systems for Health Agency
T1 Connection	A dedicated data connection supporting data rates of 1.544Mbits per second
TRA	Threat Risk Assessment