Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Review of the Smart Systems for Health Agency (SSHA):

An Electronic Goods or Services Provider to Health Information Custodians under the *Personal Health Information Protection Act, 2004*

March 16th, 2007

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER/ONTARIO

Review of the Smart Systems for Health Agency (SSHA):
An Electronic Goods or Services Provider to Health Information Custodians under the *Personal Health Information Protection Act, 2004*

The *Personal Health Information Protection Act, 2004* (PHIPA) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC) has been designated as the oversight body responsible for ensuring compliance with *PHIPA*. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians that protect the confidentiality of, and the privacy of individuals with respect to, that personal health information. In particular, *PHIPA* provides that health information custodians may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates or as permitted or required by *PHIPA*.

Responsibilities of Electronic Goods or Services Providers to Health Information Custodians

Section 10(4) of *PHIPA* requires a person who provides goods or services for the purposes of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information to comply with the prescribed requirements, if any. The prescribed requirements are set out in section 6 of Ontario Regulation 329/04 under *PHIPA* (the Regulation).

In subsection 6(1) of the Regulation, the following requirements are prescribed with respect to a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, and who is not an agent of the custodian:

1. The person shall not use any personal health information to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services.
2. The person shall not disclose any personal health information to which it has access in the course of providing the services for the health information custodian.
3. The person shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person who is subject to this subsection.

Subsection 6(2) of the Regulation further defines a "health information network provider" as a person who provides services to two or more health information custodians where the services are provided primarily to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.

In subsection 6(3) of the Regulation, the following requirements are prescribed with respect to a health information network provider in the course of providing services to enable a health information custodian to use electronic means to collect, use, disclose, retain or dispose of personal health information:

1. The provider shall notify every applicable health information custodian at the first reasonable opportunity if,

    i. the provider accessed, used, disclosed or disposed of personal health information other than in accordance with paragraphs 1 and 2 of subsection (1), or

    ii. an unauthorized person accessed the personal health information.

2. The provider shall provide to each applicable health information custodian a plain language description of the services that the provider provides to the custodians, that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information.

3. The provider shall make available to the public,

    i. the description referred to in paragraph 2,

    ii. any directives, guidelines and policies of the provider that apply to the services that the provider provides to the health information custodians to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information, and

    iii. a general description of the safeguards implemented by the person in relation to the security and confidentiality of the information.

4. The provider shall to the extent reasonably practical, and in a manner that is reasonably practical, keep and make available to each applicable health information custodian, on the request of the custodian, an electronic record of,

    i. all accesses to all or part of the personal health information associated with the custodian being held in equipment controlled by the provider, which record shall identify the person who accessed the information and the date and time of the access, and

    ii. all transfers of all or part of the information associated with the custodian by means of equipment controlled by the provider, which record shall identify the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent.

5. The provider shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to,

    i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and

ii. how the services may affect the privacy of the individuals who are the subject of the information.

6. The provider shall ensure that any third party it retains to assist in providing services to a health information custodian agrees to comply with the restrictions and conditions that are necessary to enable the provider to comply with this section.
7. The provider shall enter into a written agreement with each health information custodian concerning the services provided to the custodian that,
    i. describes the services that the provider is required to provide for the custodian,
    ii. describes the administrative, technical and physical safeguards relating to the confidentiality and security of the information, and
    iii. requires the provider to comply with *PHIPA* and the Regulation.

Where a person, who is not acting as an agent of the custodian, supplies goods or services to a custodian, subsection 6(4) of the Regulation states that a health information custodian, in using those goods or services, for the purpose of using electronic means to collect, use, modify, disclose, retain or dispose of personal health information, shall not be considered to be disclosing personal health information to the person who supplies the goods or services. However, this is only the case if the person who supplies the goods and services complies with the requirements of subsection 6(1) and 6(3) of the Regulation and the custodian does not, in returning the goods to the person, enable the person to access personal health information except where subsection 6(1) of the Regulation applies and is complied with.

Description of SSHA

Smart System for Health Agency (SSHA) is an agency of the Ministry of Health and Long-Term Care. Its mandate is to work with the health care sector in the province of Ontario to enable health information custodians to share personal health information. SSHA receives 100 per cent of its funding from the Ministry of Health and Long-Term Care and provides its goods and services free of charge to the publicly-funded health care sector.

According to its enabling regulation[1], the objectives of SSHA are to support effective and efficient delivery, planning and management of health services in Ontario and to support health research by:

1. providing a secure province-wide information infrastructure for the collection, transmission, storage and exchange of information about health matters (including personal information),
2. planning, implementing and encouraging the use of services, products and technologies that will promote the effective use of the information infrastructure, and

[1] O.Reg. 43/02 made under the *Development Corporations Act*, as amended by O.Reg. 54/05

3. collecting, using and disclosing personal information as permitted by sections 15 and 16 of SSHA's enabling regulation as is necessary for the provision of the information infrastructure.

Section 15 of SSHA's enabling regulation pertains to emergency health records. SSHA is permitted to collect, use and disclose personal health information in this context with the consent of the individual and his or her health care provider, however SSHA has not developed emergency health records to date. Accordingly, it does not collect, use or disclose personal health information in this regard.

Section 16 of the enabling regulation pertains to verification of the users of the information infrastructure. SSHA presently performs these activities, which involve personal information, but not personal health information.

According to its website (www.ssha.on.ca), SSHA was created to be a trusted third party to protect the patient information of health care providers. In providing its goods and services to the health care sector, SSHA fulfills different functions. In carrying out these functions, SSHA is obligated to comply with a variety of requirements set out in section 6 of the Regulation. As a person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, SSHA is required to comply with subsection 6(1) of the Regulation. When acting as a health information network provider as defined in section 6(2) of the Regulation, SSHA is required to comply with subsection 6(3) of the Regulation. Further, when acting as a third party retained by a health information network provider to assist in providing services to a health information custodian, SSHA must agree to comply with the restrictions and conditions that are necessary to enable the health information network provider to comply with section 6 of the Regulation, as required under subsection 6(3)6 of the Regulation.

Personal health information is one of the most sensitive types of personal information. As an organization with a mandate that touches the privacy and security of the personal health information of every individual in the province of Ontario and that aspires to becoming a world-class leader in the provision of electronic goods and services to the health sector, SSHA must engender the utmost trust and confidence on the part of the public and the health care provider community. To foster this trust and confidence, it is the IPC's expectation that SSHA should demonstrate leadership in privacy and security manners and adhere to high standards with respect to the privacy and security of personal health information.

Mandate of the IPC with Respect to SSHA

As the government of Ontario moves forward in transforming the delivery of health care services through the use of information technology, there has been recognition of the need to ensure the privacy of individuals with respect to their personal health information. To help ensure a high standard of privacy protection during this transformation, the government of Ontario requested that the IPC review the information practices of SSHA. This request was formalized through an amendment to the Regulation under PHIPA.

Section 6.1 of the Regulation requires SSHA to put in place administrative, technical and physical safeguards, practices and procedures that have been reviewed by the IPC to protect both the privacy of individuals in relation to whose personal health information it provides services and the confidentiality of such information, and that,

(a) permit compliance with *PHIPA* by health information custodians who rely on services supplied by SSHA to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information; and

(b) permit SSHA to comply with section 6 of the Regulation.

Review Process

A preliminary meeting was held to discuss the review process with key representatives of SSHA, including the Chairman of the Board of Directors, the Chief Executive Officer, the Chief Privacy and Security Officer and the Director of Privacy. The process included a review of documentation relating to the safeguards, practices and procedures of SSHA to protect the privacy of the individuals in relation to whose personal health information it provides services and to maintain the confidentiality of that information, as well as a visit to the primary facility where personal health information is kept by SSHA. The IPC provided SSHA with a preliminary checklist of privacy and security measures that the IPC would be looking for during the course of its review. The checklist included the following:

Human Resources

- Confidentiality agreements
- Disciplinary procedures for violations
- Clearly defined roles and responsibilities for privacy and security
- Appointed contact persons for privacy and security
- Ongoing education and training program for all staff, employees, affiliates, volunteers, etc., on security and privacy policies and procedures
- Third party agreements (including agreements with health information custodians as required by subsection 6(3)7 of the Regulation, agreements with researchers and agreements with third parties retained to assist in providing services to health information custodians pursuant to subsection 6(3)6 of the Regulation)

Privacy

- Privacy Policy – privacy policies and procedures in place that describe how SSHA adheres to each fair information practice
- A plain language description of the services provided that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in place to protect against unauthorized use and disclosure and to protect the integrity of the information – provided to health information custodians pursuant to subsection 6(3)2 of the Regulation
- A plain language description of the services provided to each health information custodian, a general description of the safeguards implemented in relation to the security and confidentiality of the personal health information and directives, guidelines and

polices that apply to the services provided to health information custodians – made available to the public pursuant to subsection 6(3)3 of the Regulation
- Privacy Impact Assessments –written copies of the results of assessments of the services provided to health information custodians with respect to how the services may affect the privacy of the individuals who are the subject of the personal health information pursuant to subsection 6(3)5 of the Regulation
- Internal/external privacy audits
- Privacy crisis management protocol – including the procedure for notifying health information custodians, pursuant to subsection 6(3)1 of the Regulation, if SSHA accessed, used, disclosed or disposed of personal health information except as permitted under subsection 6(1) of the Regulation or if an unauthorized person accessed the personal health information
- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Mechanism for reviewing and updating privacy policies and procedures

Security

- Comprehensive security program including physical, technical and administrative measures
- A general description of the safeguards in place to protect against unauthorized use and disclosure and to protect the integrity of the personal health information provided to health information custodians pursuant to subsection 6(3)2 of the Regulation
- A general description of the safeguards implemented in relation to the security and confidentiality of personal health information made available to the public pursuant to subsection 6(3) 3 of the Regulation
- Access control procedures – authentication and authorization
- Perimeter control
- Audit trails – electronic record of all accesses to all or part of the personal health information associated with the custodian being held in equipment controlled by SSHA, which identifies the person who accessed the information and date and time of the access, and all transfers of all or part of the personal health information associated with the custodian by means of equipment controlled by SSHA, which identifies the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent – which is made available to health information custodians pursuant to subsection 6(3)4 of the Regulation
- Internal/external security audits
- Disaster Recovery Plan
- Threat and Risk Assessments – written copies of the results of an assessment of the services provided to the health information custodians with respect to the threats, vulnerabilities and risks to the security and integrity of the personal health information pursuant to subsection 6(3)5 of the Regulation
- Mechanism for reviewing and updating security policies and procedures

A site visit took place following the IPC's review of the documentation provided by SSHA. The purpose of the site visit was to provide SSHA with an opportunity to provide additional

information to the IPC and to clarify their practices and procedures, and to provide the IPC with an opportunity to:

- review the physical, technological and administrative security measures implemented;
- ask questions about the documentation provided; and
- discuss privacy and security matters with appropriate staff at SSHA.

In addition to the document review and site visit, the IPC hired a consulting firm, Deloitte and Touche, to develop criteria to assess compliance with privacy and security standards and to conduct the compliance assessment.

On the basis of the document review, site visit and compliance assessment, the IPC prepared a draft report that was submitted to SSHA for review and comment prior to publication on the IPC website.

Review of SSHA

Documents Reviewed

The IPC received and reviewed over 100 documents from SSHA throughout the review process. Key documentation was in draft form and SSHA was reviewing several critical policies when the review took place. The IPC requested and received additional documentation during the review. Examples of the types of documents that were received and reviewed by the IPC are set out in the Appendix.

Site Visit

Representatives from the IPC attended a training session for SSHA employees on October 21, 2006. A meeting with the Director of Privacy was held on November 1, 2006. IPC representatives conducted a site visit at SSHA's main data centre on November 8, 2005. The site visit included meetings with the following representatives from SSHA:

Director, Operations
Tier 1 Technical Support Manager
Director, Privacy
Senior Policy Analyst (current title is Legal Counsel)
Director, Risk Management
Administrative Assistant, Human Resources
Director, Security
Manager, Security Operations

Findings of the Review

A. INSUFFICIENT PRIVACY AND SECURITY DOCUMENTATION

Staff of SSHA cooperated fully with the IPC in producing documentation for the purposes of the review. Nevertheless, insufficient documentation and a lack of effective document management procedures presented challenges throughout the review process. In some cases, relevant documents were identified by the IPC only because they were referred to in other documents provided by SSHA.

Furthermore, it was generally unclear if and how the documents that were provided related to the various requirements under *PHIPA* and the Regulation. Health information custodians and the general public were not specifically mentioned as the intended audience for any of the documents provided. Most of the documents were marked as confidential, with the intended audience being individuals who are internal to SSHA.

Many of the documents provided were expressed at a high level of generality that often seemed to be restatements and adaptations of external documents such as International Standards Organization (ISO) 17799, 27001, and the Canadian Standards Association (CSA) Privacy Code. The documents generally expressed SSHA's commitment to high level principles and/or processes rather than to specific operational policies and practices. More specific documents that were referred to either did not exist or were provided in draft form only and were not formally approved by management. Examples include:

- Information Security Policy
- Information Security Operating Directives
- Security Standards of Practice
- Operations Security Policies Handbook
- Privacy and Security Enterprise – Incident Response Policy
- Media Disposal Policy

Without formal approval, there is a risk that the draft documents may not be known, understood or followed.

The documents that were provided had not been reviewed or updated in a regular, prescribed manner. Consequently, the current applicability of many policies and procedures was unclear.

Most of SSHA's technology, security, and privacy initiatives have been conducted as stand alone projects rather than as part of an integrated suite of activities designed to support a higher strategic mission. Consistent with this approach, the documentation provided indicated that a comprehensive suite of privacy and security policies and procedures have not been developed or adopted by SSHA. Further, even where privacy and security policies and procedures have been developed or adopted, there are instances where these policies and procedures have not been complied with or have not been followed in a systematic and verifiable manner. For example, while section 4.4 of the Risk Management Policy requires SSHA to report its risk profile to the

audit committee on a quarterly basis, it is our understanding that to date no such reports have been made to the audit committee. Further, while the Enterprise Privacy Policy requires privacy impact assessments to be reviewed and approved by the Risk Management Committee, it is our understanding that no such reviews and approvals have taken place.

In general, it is the IPC's view that SSHA needs to significantly improve the completeness, quality and detail of its privacy and security documentation. In addition, good documentation management processes need to be implemented to ensure that up-to-date documentation on all privacy and security matters is readily available. Good documentation and documentation management processes are essential to support SSHA in its role as a health information technology service provider for the province of Ontario.

B. RESPONSIBILITY FOR PRIVACY AND SECURITY

The Chief Privacy and Security Officer, who heads the Privacy, Security and Risk Management Division, is responsible for the overall privacy program and for maintaining, monitoring compliance with, and ensuring this framework and all relevant policies and procedures are enforced throughout SSHA. This person is responsible for the establishment and delivery of a privacy education and awareness program for SSHA staff, consultants, and employees of vendors. The Enterprise Privacy Program Framework indicates that the Chief Privacy and Security Officer will establish guidelines for the completion of privacy impact assessments for SSHA. The Chief Privacy and Security Officer is the person to whom inquiries or complaints concerning the privacy practices of SSHA may be directed. The Chief Privacy and Security Officer delegates responsibility for the day-to-day management of the privacy program to the Privacy Director.

The Chief Privacy and Security Officer is also responsible for development and management of the information security program and information security management system. In addition to the Chief Privacy and Security Officer, the Chief Technology Officer is responsible for the safeguarding of information in the SSHA infrastructure. The Chief Information Officer is responsible for the safeguarding of personal information in SSHA corporate information systems, and for developing guidelines and implementing procedures to govern the retention and destruction of personal information held in SSHA's personal information banks. The Executive Director of Standards Management and Business Integration and the Electronic Health Record is responsible for ensuring the privacy of personal health information held by SSHA in an electronic health record. It is unclear whether these responsibilities encompass all personal health information transmitted using the SSHA infrastructure.

Although the Chief Privacy and Security Officer and the Privacy, Security and Risk Management Division headed by the Chief Privacy and Security Officer are responsible for the overall privacy and security program at SSHA, they do not have direct operational responsibility for accomplishing SSHA's privacy and security objectives. This has been devolved to end users in organizational units within SSHA who have other operational responsibilities and who are not privacy and security specialists. This decentralization may explain why SSHA has not implemented comprehensive privacy and security policies and procedures and why the privacy

and security policies and procedures that have been implemented, have not been consistently followed.

It should also be noted that at the beginning of the review process, the position of Chief Privacy and Security Officer was vacated. Therefore, at the time of the review, there was a definite lack of clarity about responsibility for the privacy and security program. The vacancy of a key position in SSHA's privacy team may have added additional complexity to the review process. We also note that since, in some cases, privacy and security practices can be in conflict, the designation of one individual who is responsible for both privacy and security may not be a best practice.

It is important that SSHA recruit and retain suitable, skilled staff with the necessary privacy qualifications to establish and maintain a culture of privacy within the organization. It is also important that staff who are ultimately responsible for implementing privacy in the operational units at SSHA, have the necessary training and expertise to do so.

In addition, it is the IPC's view that a complex and high profile organization, such as SSHA, that plays a central role in the e-health strategy for the province of Ontario, must be perceived as a leader in the protection of privacy. To achieve this, we recommend the creation of a senior position within SSHA for a person with a high level of privacy expertise, experience, and authority. This person would assume the role of privacy advocate, advisor and leader for the entire organization and would be responsible not only for embedding a culture of privacy within SSHA but for establishing SSHA's reputation as a leader in the protection of privacy among the health sector and the general public.

It is therefore recommended that SSHA augment its current privacy expertise by recruiting a seasoned privacy expert to provide leadership and oversight for the privacy program at SSHA and by ensuring that key staff members who are responsible for implementing privacy on a day-to-day basis have the necessary training, expertise and authority to carry out this function.

C. ENTERPRISE PRIVACY POLICY

1. General Comments on the Enterprise Privacy Policy

SSHA has completed an Enterprise Privacy Policy in relation to personal information and personal health information that is collected, transmitted, stored or exchanged by and through the information infrastructure that it operates. The Enterprise Privacy Policy is currently available to the public on SSHA's website.

The Enterprise Privacy Policy does not reference all of SSHA's obligations under *PHIPA* and the Regulation. It is also worth noting that, in some respects, SSHA is currently not complying with its own Enterprise Privacy Policy. This will be discussed in greater detail throughout this report.

Since the privacy requirements vary, depending on SSHA's status under *PHIPA*, the Enterprise Privacy Policy should be amended to clearly describe the various possible roles of SSHA under

PHIPA and the Regulation, which depend on the particular services being provided by SSHA to health information custodians in respect of personal health information.

For example, SSHA may be a health information network provider as defined in section 6(2) of the Regulation, a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation or a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information ("electronic service provider") pursuant to section 6(1) of the Regulation. SSHA may fulfill more than one of these roles depending on the nature of the services being provided to health information custodians in the particular context.

In a meeting on November 1, 2006, staff of SSHA acknowledged that as a health information network provider and as a third party retained by a health information network provider to assist in providing services to a health information custodian, SSHA would be required to comply, directly or indirectly, with sections 6(1) and 6(3) of the Regulation and that as an electronic service provider, SSHA would be required to comply with section 6(1) of the Regulation.

Consequently, it is our view that it is insufficient for the Enterprise Privacy Policy to state that SSHA is "a person who provides services to health information custodians." The Enterprise Privacy Policy should describe the circumstances in which SSHA is: a health information network provider; a third party retained by a health information network provider to assist in providing services to a health information custodian; and/or an electronic service provider, as described above. The Enterprise Privacy Policy should further explain the obligations that arise from *PHIPA* and the Regulation with respect to each of these roles and how SSHA is or will be addressing each of these obligations.

In addition, it is recommended that the Enterprise Privacy Policy be amended to reference and define "personal health information" in accordance with section 4 of *PHIPA*, an electronic service provider in accordance with section 6(1) of the Regulation, a "health information network provider" in accordance with section 6(2) of the Regulation and a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation.

The definitions of "collection" and "use" in section 8 of the Enterprise Privacy Policy should be amended to be consistent with the definition of these terms in *PHIPA.* Similarly, a definition of the term "disclosure" should be provided that is consistent with *PHIPA.* Further, the definition of "privacy breach" in section 8 of the Enterprise Privacy Policy should be consistent not only with the *Freedom of Information and Protection of Privacy Act*, but with section 6(3)1 of the Regulation. In this regard, the definition should include any access, use, disclosure or disposal of personal health information by SSHA in contravention of section 6(1) of the Regulation and any other access to personal health information by unauthorized persons.

In addition, while the Enterprise Privacy Policy states that it will be reviewed and updated on an annual basis or more frequently as determined by the Risk Management Committee, it appears that the Enterprise Privacy Policy has not been updated. For example, the Enterprise Privacy

Policy refers to an "Acceptable Use Policy for Client Organizations" and a "Privacy, Security and Acceptable Use Policy for Health Providers and Small Office Practices," but it is our understanding that these two documents are no longer in use by SSHA. It is therefore recommended that the Enterprise Privacy Policy be reviewed and updated on an annual basis in accordance with the stated intention of the Enterprise Privacy Policy.

2. Comments on Specific Provisions of the Enterprise Privacy Policy

Provisions Related to "Privacy Policy Authorities"

Section 5.1 of the Enterprise Privacy Policy states that it, "is developed in accordance with the following authorities *listed in order of precedence*" and then proceeds to set out the legislation, regulations, directives and guidelines that apply to SSHA. This statement should be deleted given there is no "precedence" between the *Freedom of Information and Protection of Privacy Act* and *PHIPA*. SSHA is required to comply with both statutes.

Section 5.1.4 of the Enterprise Privacy Policy references the fact that the Enterprise Privacy Policy is guided by the *Personal Information Protection and Electronic Documents Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. It is unclear why these statutes are referenced as they do not appear to have any application to SSHA. Therefore, these references should be either deleted or clarified.

Provisions Related to "Privacy Accountability"

Section 5.3.1 of the Enterprise Privacy Policy states that SSHA will only access personal health information for the purpose of providing information management and technology services to health information custodians. However, it should further reference the limitations imposed with respect to the use and disclosure of personal health information by sections 6(1)(1) and 6(1)2 of the Regulation which prohibit SSHA from using or disclosing personal health information to which it has access in the course of providing services to a health information custodian.

Section 6.1.3.1 of the Enterprise Privacy Policy states that SSHA will use contractual or other means to ensure that personal information transferred to a third party has an equivalent level of protection. It is recommended that this be amended to further reference the requirements imposed on SSHA pursuant to section 6(1)3 of the Regulation to ensure that its employees or other persons acting on its behalf do not have access to personal health information in the course of providing services to a health information custodian, unless they agree not to use the personal health information except as necessary in the course of providing services and agree not to disclose the personal health information. It is also recommended that section 6.1.3.1 reference the requirement imposed on SSHA pursuant to 6(3)6 of the Regulation, when it is acting as a health information network provider, to ensure that any third party retained to assist in providing services to a health information custodian agrees to comply with the conditions and restrictions that are necessary to enable SSHA to comply with section 6 of the Regulation.

Provisions Related to "Privacy Breaches and Violations"

Section 6.1.6 of the Enterprise Privacy Policy, dealing with "privacy breaches and violations," indicates that staff, consultants and vendors must report to their manager "as soon as possible" when certain enumerated circumstances occur. It is recommended that "as soon as possible" be replaced with "at the first reasonable opportunity" in order to conform to section 6(3)1 of the Regulation. Further, as written, this section only requires staff of vendors to report "privacy breaches and violations" to their manager. It does not require vendors to report the "privacy breaches and violations" to SSHA.

Further, section 6.1.6 of the Enterprise Privacy Policy does not mention the requirement imposed on SSHA pursuant to 6(3)1 of the Regulation, when acting as a health information network provider, to notify every applicable health information custodian at the first reasonable opportunity if SSHA accessed, used, disclosed or disposed of personal health information other than in accordance with section 6(1) of the Regulation or if an unauthorized person accessed the personal health information. It is recommended that section 6.1.6 of the Enterprise Privacy Policy be amended accordingly.

Provisions Related to "Employment and Contracting"

Section 6.1.7 of the Enterprise Privacy Policy, dealing with "employment and contracting," should reference the requirements imposed on SSHA pursuant to section 6(1)3 of the Regulation. Specifically, SSHA must ensure that its employees or other persons acting on its behalf do not have access to personal health information in the course of providing services to a health information custodian, unless they agree not to use the personal health information except as necessary in the course of providing services and agree not to disclose the personal health information.

Section 6.1.7 should further reference the requirements imposed on SSHA pursuant to section 6(3)6 of the Regulation. Specifically, when acting as a health information network provider, SSHA must ensure that any third party retained to assist in providing services to a health information custodian agrees to comply with the conditions and restrictions that are necessary to enable SSHA to comply with section 6 of the Regulation.

Provisions Related to "Openness"

It is recommended that section 6.8.1 of the Enterprise Privacy Policy related to "openness" be amended to reference the obligations imposed on SSHA pursuant to sections 6(3)2 and 6(3)3 of the Regulation. These sections require SSHA, when acting as a health information network provider, to provide each applicable health information custodian with a plain language description of the services provided, including a general description of the safeguards to protect against unauthorized use and disclosure and to protect the integrity of the personal health information. In addition, these sections require SSHA to make available to the public a plain language description of the services provided, a general description of the safeguards implemented in relation to the security and confidentiality of the personal health information and any directives, guidelines and policies that apply to the services provided.

D. ENTERPRISE SECURITY POLICY

1. General Comments on the Enterprise Security Policy

SSHA, in respect of its services, has written an Enterprise Security Policy. This policy is available to the public on the SSHA website. The policy was completed on March 30, 2004, and was scheduled for review in 2005. However, the current policy has not been updated to include SSHA's obligations in regards to *PHIPA* and the Regulation. It is recommended that the Enterprise Security Policy be revised and finalized as soon as possible. It is also worth noting that in some respects SSHA is not complying with it own Enterprise Security Policy. This will be discussed throughout this report.

Since security requirements vary depending on SSHA's status under *PHIPA*, the Enterprise Security Policy should be amended to clearly describe the various possible roles of SSHA under *PHIPA* and the Regulation depending on the particular services being provided by SSHA to health information custodians in respect of personal health information.

The Enterprise Security Policy should describe the circumstances in which SSHA is a health information network provider pursuant to section 6(2) of the Regulation, the circumstances in which it is a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation and the circumstances in which it is an electronic service provider pursuant to section 6(1) of the Regulation. The Enterprise Security Policy should further explain the obligations with respect to security that arise from each of these roles and how SSHA is or will be addressing each of these obligations.

In addition, the Enterprise Security Policy should be amended to reference *PHIPA* and the Regulation and to reference and define an electronic service provider pursuant to section 6(1) of the Regulation, a health information network provider pursuant to section 6(2) of the Regulation and a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation.

The definitions of "collection," "disclosure" and "personal health information" in section 9 of the Enterprise Security Policy should be amended to parallel the definitions of these terms in *PHIPA*. In addition, a definition of the term "use" should be provided that is consistent with *PHIPA*. The definitions of "breach" and "security breach" in section 9 of the Enterprise Security Policy should be consistent with section 6(3)1 of the Regulation. In this regard, the definitions should include any access, use, disclosure or disposal of personal health information by SSHA in contravention of section 6(1) of the Regulation and any other access to personal health information by unauthorized persons.

The Enterprise Security Policy also continually references the responsibilities of staff, consultants and third party service providers with respect to "sensitive information." Section 9 defines sensitive information as, "information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction or loss will cause perceivable damage to someone or something." This definition is vague and subjective and may result in undue confusion about whether or not information is "sensitive." It is therefore recommended

that the definition of "sensitive information" be amended to set out the precise information that SSHA considers sensitive and that this include personal information as defined in the *Freedom of Information and Protection of Privacy Act* and personal health information as defined in *PHIPA*.

In addition, while the Enterprise Security Policy states that it will be reviewed and updated on annual basis or more frequently as determined by the Risk Management Committee, it appears that the Enterprise Security Policy has not been updated. It is recommended that the Enterprise Security Policy be reviewed and updated on an annual basis in accordance with the stated intention of the Enterprise Security Policy.

2. Comments on Specific Provisions of the Enterprise Security Policy

Provisions Related to "Security Policy Authorities"

Section 5.1 of the Enterprise Security Policy states that it has been "developed in accordance with the following authorities" and then proceeds to set out the legislation, regulations, directives and guidelines that apply to SSHA. However, *PHIPA* and the Regulation are not mentioned as legislation governing the security of personal health information by SSHA, despite the fact that there are certain provisions in section 6 of the Regulation relating to security. For example, there is requirement imposed on SSHA pursuant to section 6(3)5 of the Regulation, when acting as a health information network provider, to perform threat, vulnerability and risk assessments and to provide applicable health information custodians with a written copy of the results of these assessments.

Accordingly, it is recommended that section 5.1 of the Enterprise Security Policy be amended to reference *PHIPA* and the Regulation as relevant legislation governing the security of personal health information by SSHA.

Provisions Related to "Terms and Conditions of Employment," "Staff, Consultant and Vendor Obligations and Practices" and "Contracting"

Sections 6.2.2, 6.2.6 and 6.5.3 of the Enterprise Security Policy dealing with "terms and conditions of employment," "staff, consultant and vendor obligations and practices" and "contracting," should be amended to reference the requirements imposed on SSHA pursuant to section 6(1) of the Regulation to ensure that employees or persons acting on its behalf do not have access to personal health information unless they agree not to use the personal health information except as necessary in the course of providing services and agree not to disclose the personal health information.

Sections 6.2.2, 6.2.6 and 6.5.3 of the Enterprise Security Policy should be further amended to reference the requirements imposed on SSHA pursuant to section 6(3)6 of the Regulation, when it is acting as a health information network provider, to ensure that any third party retained to assist in providing services to a health information custodian agrees to comply with the conditions and restrictions that are necessary to enable SSHA to comply with section 6 of the Regulation.

Provisions Related to "Security Breaches, Violations and Other Incidents"

Section 6.4.2 of the Enterprise Security Policy, dealing with "security breaches, violations and other incidents," does not mention the requirement imposed on SSHA pursuant to 6(3)1 of the Regulation, when acting as a health information network provider, to notify every applicable health information custodian at the first reasonable opportunity if SSHA accessed, used, disclosed or disposed of personal health information other than in accordance with section 6(1) of the Regulation or if an unauthorized person accessed the personal health information. It is recommended that section 6.4.2 of the Enterprise Security Policy be amended accordingly.

Provisions Related to "Exchange of Information and Assets"

Section 6.6.2 of the Enterprise Security Policy states that staff, consultants and vendors are responsible for applying "appropriate safeguards" when communicating sensitive information by e-mail, facsimile, telephone or other method.

It is recommended that SSHA implement policies, practices and procedures governing the communication of personal information and personal health information through various technological methods in order to minimize the risk of inadvertent disclosure and in order to ensure that staff, consultants and vendors apply "appropriate safeguards" when using email, facsimile or other technological methods.

In developing these policies, practices and procedures, regard should be given to the *Guidelines on Facsimile Transmission Security* and the *Privacy Protection Principles for Electronic Mail Systems* developed by the IPC. In particular, the statements contained in these documents to the effect that, as a general rule, personal information and personal health information should not be sent by facsimile or email transmission and that in exigent circumstances where such information is required to be sent by these methods that technical safeguards, such as user identification and authentication and encryption, and security procedures, such as password policies and alerting recipients that a facsimile transmission will be sent, should be implemented.

E. DRAFT INFORMATION SECURITY POLICIES, OPERATING DIRECTIVES, STANDARDS OF PRACTICE AND GUIDELINES

A number of the policies, practices and directives that relate to security, including the Information Security Policy, the Information Security Operating Directives and the Information Security Standards of Practice are in draft form, are incomplete and have yet to be approved by the Board of Directors of SSHA. These draft policies, practices and directives purport to serve as a "set of coordinated policies, standards and procedures for the SSHA security program" and purport to give operational expression to the guiding principles and general requirements set out in the higher level documents, such as the Enterprise Security Policy.

This is consistent with what was noted in respect of the privacy and security program as a whole. There are plans to develop and implement certain policies, procedures and practices and to ensure that the requirements in the Regulation are satisfied, but these policies, procedures and

practices have either not been developed or remain in draft form and the obligations imposed on SSHA pursuant to section 6 of the Regulation remain unsatisfied. Without formally approved polices, practices and directives that comply with section 6 of the Regulation, there is a risk that these draft policies, practices and directives will not be viewed as binding and will not be followed. Furthermore, employees may be left with the impression that these draft documents are not important.

In addition, none of these security policies, practices and directives identify and discuss the obligations imposed on SSHA with respect to security that arise from *PHIPA* and the Regulation nor do they identify and discuss how these requirements are or will be fulfilled and who is designated as the person responsible for fulfilling these requirements.

Further, compliance with the Information Security Guidelines, including those related to mobile device security and information disposal for electronic media, is discretionary. As stated in the draft Information Security Operating Directives, an agent of SSHA can "decide whether to follow an information security guideline." Given the risk of disclosure and the risk of compromising the security of the technological infrastructure at SSHA, it is recommended that SSHA consider making compliance mandatory.

In addition, there are no policies, practices and directives relating to the use of wireless network communications, despite the fact that wireless networks are in use at SSHA.

Also, the language in the Information Security Guidelines is vague and may result in employees being unsure of how to comply with the guidelines. For example, the guideline related to mobile device security states, "if you bring them with you to your home or travel with them you must ensure that you award it adequate protection." This raises the issue of what is "adequate protection." Examples of what constitutes adequate protection of mobile devices should be provided to be of assistance in this regard. As a further example, the guideline related to information disposal for electronic media states "if physical destruction is performed by a service provider, security and audit controls must be in place to ensure appropriate protection of the media or other equipment from the time it leaves direct Agency control until it is destroyed." This raises the issue of what "security and audit controls" should be put in place. These controls should be explicitly provided for in the guideline.

The IPC also noted deficiencies in the documentation relating to logical access controls to SSHA network, facilities hosts and other technological resources. SSHA has indicated that access control is role-based, however segregation of duties and of incompatible functions is not formally documented across the agency, making the establishment of a role-based model difficult. Indeed, role-based access is not formally documented and managed. Furthermore, in certain sensitive applications, authentication levels are inadequate. Stronger methods, such as two-factor and context-based authentication, should be considered. Accordingly, it is recommended that SSHA ensure that access controls, including authentication, are formally documented and managed and appropriate to the level of sensitivity of the applications to which they are applied.

Finally, with respect to the Information Security Operating Directives, sections 7.2.4 and 7.3.2.3 require each service or technological asset to be assigned a sensitivity classification according to the magnitude of harm that could result from a security incident or from the loss of integrity or availability of the service or technological asset or from the inability to hold individuals accountable for their actions involving the service or technological asset. Further, the statement of sensitivity contained in the Information Security Operating Directives requires each service or technological asset to be assigned a sensitivity classification according to the magnitude of the following harms: "serious injury or loss of life," "non life-threatening injury," "financial costs," "loss of employment," "legal consequences" and "loss of trust."

Nowhere is the magnitude of harm that could result from a loss of privacy to the individual to whom the personal health information relates or that could result from a breach of confidentiality mentioned. This was acknowledged by staff at SSHA during a teleconference on November 6, 2006, who also acknowledged that the harm categories should be expanded to include the harms that could result to individuals arising from a loss of privacy.

It is recommended that the sensitivity classification assigned to each service or technological asset take into account the magnitude of harm that could result from a loss of privacy to the individual to whom the personal health information relates or that could result from a breach of confidentiality.

F. INFORMATION CLASSIFICATION AND HANDLING POLICY

The Information Classification and Handling Policy states that the information protection scheme contained in this policy, "will support compliance with the *Freedom of Information and Protection of Privacy Act*." Nowhere in this policy is *PHIPA* or the Regulation referenced. It is therefore unclear whether the information protection scheme contained in this policy supports compliance with SSHA's obligations under *PHIPA* and the Regulation as it relates to personal health information.

In addition, it is recommended that the Information Classification and Handling Policy be amended to reference and define personal health information pursuant to section 4 of *PHIPA*. It is also recommended that the definitions of "disclosure" and "use" in section 8 of the Information Classification and Handling Policy be amended to be consistent with the definitions in *PHIPA* and that the definition of "breach" in section 8 be consistent with section 6(3)1 of the Regulation. In this regard, the definition should include any access, use, disclosure or disposal of personal health information by SSHA in contravention of section 6(1) of the Regulation and any other access to personal health information by unauthorized persons.

Further, the definition of "sensitive information" in section 4.1 of the Information Classification and Handling Policy, which is defined as, "information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction or loss will cause perceivable damage to someone or something," is vague and may result in undue confusion as to whether or not information is "sensitive." This is especially important given special safeguards are implemented with respect to "sensitive information." For example access will only be

granted to those whose duties require access to sensitive information and visitor access will be controlled in areas where sensitive information is discussed, developed, reviewed or stored.

As a result, it is recommended that the definition of "sensitive information" be amended to set out the precise information that SSHA considers sensitive and that this include personal information as defined in the *Freedom of Information and Protection of Privacy Act* and personal health information as defined in *PHIPA*.

Further, section 5.5 of the Information Classification and Handling Policy which provides examples of highly sensitive information states that highly sensitive information "may include" personal health information. It is our view that personal health information is always highly sensitive. Therefore, it is recommended that "highly sensitive information" be defined to always include personal health information.

Also, section 5.9.3 of the Information Classification and Handling Policy states that sunset dates must be established whereby records or information will no longer be considered sensitive. However, it should be noted that the application of sunset dates to personal health information may not be appropriate given that the sensitivity of personal health information generally does not diminish with the passage of time. This is subject, of course, to section 9(1) of *PHIPA* which states that *PHIPA* does not apply to personal health information about an individual after the earlier of 120 years after the record containing personal health information was created and 50 years after the death of the individual. It is therefore recommended that any sunset dates related to personal health information be consistent with section 9(1) of *PHIPA*.

Finally, inconsistencies were noted during the course of the review with respect to the classification and handling of "sensitive information." For example, the Information Classification and Handling Policy states that if information is not classified, it must be considered to be of "medium sensitivity" and treated accordingly until it is classified. This is inconsistent with its operational security policies, namely Policy 050603 relating to "Sensitive Information Encryption." Inconsistencies were also noted with respect to the implementation of appropriate controls, such as encryption, based on the classification of information. It is therefore recommended that consistency be ensured in the classification and handling of "sensitive information" and in the implementation of appropriate controls based on such classification.

G. ASSET MANAGEMENT POLICY

The Asset Management Policy does not identify specific procedures for removing personal health information from information technology equipment or network devices when an information technology asset is being used for purposes other than its original intent, used by a different individual, sent for repair or is being prepared for disposal. Sections 3.3.4, 3.3.5 and 3.8 of the Asset Management Policy refer to various processes and procedures including "data removal processes and procedures" and "media destruction processes and procedures," but do not specifically name the processes and procedures being referenced. It is recommended that the

policies and procedures being referred to be specifically named in order to avoid confusion as to how to comply with the Asset Management Policy.

Further, certain provisions in the Asset Management Policy speak to requirements imposed on assets or equipment that contain "sensitive information," yet no definition of "sensitive information" is provided. Once again, this may lead to uncertainty and undue confusion about whether or not information is "sensitive." As a result, it is recommended that a definition of "sensitive information" be provided and that the definition include personal information as defined in the *Freedom of Information and Protection of Privacy Act* and personal health information as defined in *PHIPA*.

Section 3.6 of the Asset Management Policy also states that the Chief Privacy and Security Officer must be contacted immediately if any item that is lost or stolen holds personal, personal health or corporate information "deemed as highly sensitive or medium sensitive data based on the classification scale as detailed in the Information Classification and Handling Policy." It is recommended that section 3.6 of the Asset Management Policy be amended such that the requirement to notify the Chief Privacy and Security Officer is not limited to those cases in which the lost or stolen item contains personal health information that has been classified as highly sensitive or of medium sensitivity. The rationale for this is that when acting as a health information network provider, section 6(3)1 of the Regulation requires SSHA to notify every applicable health information custodian at the first reasonable opportunity if SSHA accessed, used, disclosed or disposed of personal health information other than in accordance with section 6(1) of the Regulation or if an unauthorized person accessed the personal health information. This requirement applies whether or not the personal health information is deemed to be "highly sensitive" or "of medium sensitivity."

H. ACKNOWLEDGEMENT OF CONFIDENTIALITY

It is recommended that an Acknowledgement of Confidentiality Policy be developed and implemented to clearly and comprehensively address such issues as: who is required to sign an Acknowledgement of Confidentiality, when an Acknowledgement of Confidentiality must be signed and how often an Acknowledgement of Confidentiality must be signed.

It is also recommended that the current Acknowledgement of Confidentiality used by SSHA be amended to reference *PHIPA* and the Regulation, to reference and define personal health information in accordance with section 4 of *PHIPA*, to require each person signing the Acknowledgement of Confidentiality to acknowledge that a breach of confidentiality may result in discipline up to and including dismissal and to require each person signing the Acknowledgement of Confidentiality to acknowledge, in accordance with section 6(1) of the Regulation, that the person:

- will not use any personal health information to which the person has access in the course of providing the services except as necessary in the course of providing those services; and

- will not disclose any personal health information to which the person has access in the course of providing the services.

This will permit SSHA to comply with its obligations pursuant to section 6(1)3 of the Regulation, which prohibits SSHA from permitting its employees or anyone acting on its behalf to have access to personal health information unless they agree to comply with the above restrictions.

In addition, the Acknowledgement of Confidentiality should be amended to include a positive obligation on the person signing the Acknowledgement of Confidentiality to immediately notify SSHA if the person signing the Acknowledgement of Confidentiality accessed, used, disclosed or disposed of personal health information other than in accordance with the Acknowledgement of Confidentiality, to immediately notify SSHA upon becoming aware of a breach of the Acknowledgement of Confidentiality and to immediately notify SSHA upon becoming aware that an unauthorized person accessed personal health information. This will ensure that SSHA, when acting as a health information network provider, is able to comply with its duties under section 6(3)1 of the Regulation.

I. ENTERPRISE PRIVACY POLICY ACKNOWLEDGEMENT AND ENTERPRISE SECURITY POLICY ACKNOWLEDGEMENT

It is recommended that a policy be developed and implemented to comprehensively address such issues as: who is required to sign the Enterprise Privacy Policy Acknowledgment and the Enterprise Security Policy Acknowledgement, when these acknowledgements must be signed and how often they must be signed. It is further recommended that the policy require the execution of acknowledgements with respect to the Information Classification and Handling Policy and Enterprise Risk Management Policy. This will ensure consistency with the Information Classification and Handling Policy and Enterprise Risk Management Policy which require employees, consultants, contractors and vendors to adhere to these policies.

It is also recommended that the acknowledgements themselves be amended to reference *PHIPA* and the Regulation, to reference and define personal health information in accordance with section 4 of *PHIPA* and to require each person to acknowledge that a breach of the acknowledgement or a breach of the Enterprise Privacy Policy, Enterprise Security Policy, Information Classification and Handling Policy and Enterprise Risk Management Policy may result in discipline up to and including dismissal.

It is also recommended that the acknowledgements be amended to include a positive obligation on the person signing the acknowledgement to immediately notify SSHA upon becoming aware of a breach of the Enterprise Privacy Policy, the Enterprise Security Policy, the Information Classification and Handling Policy and the Enterprise Risk Management Policy. It should also require each person to immediately notify SSHA if he or she accessed, used, disclosed or disposed of personal health information other than in accordance with these policies or if an unauthorized person accessed the personal health information.

Further, it is recommended that SSHA implement a process to track which employees have signed the acknowledgements and the date of signature to ensure appropriate monitoring and follow up for those employees who have not signed the acknowledgements.

In a teleconference on November 6, 2006, staff of SSHA acknowledged that there was no formal process to track and monitor the execution of these acknowledgements and that it was assumed that employees acted in good faith in signing these acknowledgements. It was further conceded that as a result of this review by the IPC, the Human Resources Department became aware that some employees had not signed these acknowledgements. Based on figures that the IPC received on November 10, 2006, SSHA could not confirm whether 18 per cent of its employees had signed these acknowledgements.

Staff of SSHA also acknowledged that SSHA does not have a discipline policy that sets out the consequences for breaching the acknowledgements, the Enterprise Privacy Policy, the Enterprise Security Policy, the Information Classification and Handling Policy and the Enterprise Risk Management Policy. It is recommended that a policy be developed that sets out the process to be followed in investigating breaches, the possible consequences resulting from such breaches from a labour relations perspective and any aggravating factors that may affect discipline.

J. AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS

In a meeting on November 1, 2006, staff of SSHA could not confirm whether agreements have been entered into with all third parties retained to assist SSHA in providing services to a health information custodian due to the lack of a central repository for such agreements.

Even where agreements have been entered into, both prior to and after the enactment of *PHIPA*, the agreements largely do not reference *PHIPA* and the Regulation, do not reference and define personal health information, do not include personal health information within the definition of "Confidential Information" and do not stipulate the obligations of SSHA and the third party retained to assist SSHA in providing services to a health information custodian under section 6 of the Regulation.

It is therefore recommended that SSHA immediately enter into agreements with all third parties retained to assist SSHA in providing services to a health information custodian and that all the agreements currently in existence with these third parties, whether entered into prior to or after the enactment of *PHIPA*, be amended in the following respects.

The agreements should be amended to address section 6(1) of the Regulation. In particular, the agreements should require third parties retained to assist SSHA in providing services to a health information custodian to acknowledge that the third parties and their employees and persons acting on their behalf will not use personal health information except as necessary in the course of providing services and will not disclose personal health information to which they have access in the course of providing services. The agreement should also stipulate the policies, procedures and practices that will be implemented by these third parties to ensure compliance with these restrictions on use and disclosure of personal health information.

Where SSHA is acting as a health information network provider, the agreements should also address section 6(3)1 of the Regulation by requiring third parties retained to assist SSHA in providing services to a health information custodian to notify SSHA at the first reasonable opportunity if employees or persons acting on behalf of these third parties accessed, used, disclosed or disposed of personal health information other than in accordance with section 6(1) of the Regulation or if an unauthorized person accessed the personal health information. In particular, the agreements should outline the procedure to be used for notifying SSHA (including the person to be notified) and the procedures to be followed with respect to the identification, investigation, containment, notification and prevention of a similar unauthorized access, use, disclosure or disposal of personal health information. The agreements should also set out the responsibilities of SSHA and the third parties for such investigations and for the implementation of containment and prevention measures.

In addition, related to the requirement to notify mandated in section 6(3)1 of the Regulation, the agreements should be amended to set out the respective responsibilities of SSHA and these third parties to monitor for unauthorized access, use, disclosure or disposal of personal health information.

Where SSHA is acting as a health information network provider, the agreements should also be amended to address section 6(3)6 of the Regulation, by setting out the specific restrictions and conditions that third parties retained to assist SSHA in providing services to a health information custodian are required to agree to comply with in order to enable SSHA to comply with section 6 of the Regulation.

The agreements should also require third parties retained to assist SSHA in providing services to a health information custodian to acknowledge that they have read, understood and agree to comply with the Enterprise Privacy Policy, the Enterprise Security Policy, the Information Classification and Handling Policy and the Enterprise Risk Management Policy and these policies should be appended to the agreements. Although some of the current agreements state that the third parties "shall observe all rules, procedures and policies adopted by SSHA from time to time," such statements are vague and may lead to uncertainty as to which rules, procedures and policies third parties are required to comply with. This may lead to non-compliance especially if these rules, procedures and policies are not formally provided to third parties.

A draft Enterprise Privacy Agreement between the Ministry of Health and Long-Term Care and SSHA provides that any third party that SSHA retains (since September 1, 2006) to assist in providing services to custodians or the Ministry must agree in writing to comply with its terms. Its terms include restrictions on disclosure of personal information and personal health information to those who may be subject to the laws of a foreign jurisdiction and other requirements related thereto.

We also note that the government is currently finalizing its draft *Guidelines for the Protection of Information when Contracting for Services*. These *Guidelines* will apply to agencies subject to the *Freedom of Information and Protection of Privacy Act* such as SSHA. Accordingly, we recommend that the requirements and restrictions in the draft Enterprise Privacy Agreement

should be reviewed and finalized in light of these *Guidelines*. Once finalized, the requirements and restrictions in the Enterprise Privacy Agreement should be incorporated into all of SSHA's agreements with third party service providers.

Further, to the extent that the current agreements with third parties, retained to assist SSHA in providing services to a health information custodian, limit or define the term of protection afforded to Confidential Information, it is also recommended that term of protection afforded to Confidential Information that is personal health information be consistent with section 9(1) of *PHIPA*. This section states that *PHIPA* will not apply to personal health information about an individual after the earlier of 120 years after a record containing the information was created and 50 years after the death of the individual.

Finally, it is recommended that a database be maintained of all agreements with third parties retained to assist SSHA in providing services to a health information custodian in order to monitor whether agreements have been entered into with each third party and are up-to-date and in order to act as a central repository for such agreements.

K. AGREEMENTS WITH HEALTH INFORMATION CUSTODIANS

In the Risk Register dated June 7, 2006, and in a meeting on October 25, 2006, staff of SSHA acknowledged that SSHA has not entered into agreements with each health information custodian to whom services are provided. Without these agreements in place, the roles, responsibilities, rights and obligations of SSHA and health information custodians to whom services are provided is unclear. This increases the risk to the privacy of individuals in relation to whose personal health information SSHA provides services and the risk to the confidentiality of such information.

Section 6(3)7 of the Regulation requires SSHA, when acting as a health information network provider, to enter into written agreements with each health information custodian concerning the services provided that describes the services required to be provided, that describes the administrative, technical and physical safeguards relating to confidentiality and security of the personal health information and that requires SSHA to comply with *PHIPA* and the Regulation.

Further, even where SSHA is acting as a health information network provider and has entered into agreements with health information custodians concerning the services provided, whether prior to or after the enactment of *PHIPA*, these agreements do not satisfy all the requirements imposed on SSHA by section 6(3)7 of the Regulation. For example, a Services Hosting Agreement that was provided merely states that SSHA will:

> Use organizational, administrative, physical and technical means to limit physical access to the technological infrastructure that SSHA uses to provide the Services under this Agreement. These include developing privacy and security policies and procedures, implementing physical and logical security controls, conducting privacy and security assessments and providing training to staff on privacy and security matters.

In our view, vague statements, such as the one above, are not sufficient to satisfy section 6(3)7 of the Regulation, which requires SSHA to enter into a written agreement that "describes" the administrative, technical and physical safeguards relating to the confidentiality and security of personal health information. Health information custodians, who are ultimately accountable for the personal health information in relation to which SSHA provides services, require more detailed information relating to safeguards in order to satisfy themselves that the privacy of individuals to whom the personal health information relates is protected.

As has been the case with other technology, security and privacy initiatives at SSHA, the agreements with health information custodians have been treated as project-specific documents. Consequently, the agreements that have been established and negotiated for one project are not readily amenable for use in other projects. However, it is our understanding that SSHA is currently in the process of developing standard language that can be included in all of in its contractual agreements with health information custodians.

Accordingly, it is recommended that SSHA immediately enter into standard form agreements with each health information custodian to whom services are provided and that in future, *prior* to providing services to a health information custodian involving personal health information, that SSHA ensure that standard form agreements have been executed with each applicable health information custodian in accordance with the recommendations set out in this report. SSHA has acknowledged that it has not entered into agreements with each health information custodian to whom services are provided and that even where such agreements have been executed, on a number of occasions, SSHA commenced providing services prior to the execution of these agreements. This is of concern since without formal agreements in place, prior to the provision of services, the privacy and security roles, responsibilities, rights and obligations of SSHA and health information custodians to whom services are provided lack clarity. This increases the risks to the privacy of individuals to whom the personal health information relates.

It is also recommended that all the agreements currently in existence with health information custodians, whether entered into prior to or after the enactment of *PHIPA*, be amended and re-executed in accordance with the recommendations that follow.[2]

The agreements should clearly set out the status of SSHA under *PHIPA* and the Regulation in providing services to the health information custodian in respect of personal health information. Specifically, the agreement should explicitly state whether SSHA is a health information network provider as defined in section 6(2) of the Regulation, a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation or an electronic service provider pursuant to section 6(1) of the Regulation.

[2] This is important given certain provisions in the agreements entered into prior to November 1, 2004, are inconsistent with *PHIPA* and the Regulation. For example, the provisions in certain agreements only require SSHA to provide notice to a health information custodian when SSHA is aware of any unauthorized access or any violations of privacy, "that will directly impact the services provided." There is no such qualification in section 6(3)1 of the Regulation, which requires SSHA to notify applicable health information custodians at the first reasonable opportunity every time there has been an unauthorized access, use disclosure or disposal of personal health information.

The agreements should further set out the obligations imposed on SSHA as a result of its status under *PHIPA* and the Regulation and how SSHA is or will be addressing each of these obligations. In this regard, the agreements should clearly establish the respective security and privacy roles, responsibilities and obligations of SSHA and the health information custodian to whom services are provided including the administrative, physical, and technical safeguards undertaken by SSHA and the health information custodian to protect personal health information.

The agreements should also be amended to include an acknowledgement by SSHA, pursuant to section 6(1) of the Regulation, that it will not disclose any personal health information to which it has access in the course of providing services, that it will not use personal health information except as necessary in the course of providing services and that it will not permit its employees or any person acting on its behalf to have access to personal health information unless the employee or person acting on its behalf agrees to comply with these same restrictions with respect to the use and disclosure of personal health information.

Where SSHA is acting as a health information network provider, it is recommended that the agreements contain provisions describing the services required to be provided, describing the administrative, technical and physical safeguards relating to confidentiality and security of the personal health information and requiring SSHA to comply with *PHIPA* and the Regulation as mandated by section 6(3)7 of the Regulation. It is further recommended that where SSHA is a health information network provider, that the agreements address section 6(3) of the Regulation.

For example, the agreements should set out the procedures that will be followed by SSHA pursuant to section 6(3)1 of the Regulation in identifying, investigating and containing privacy and security breaches, notifying health information custodians about such breaches, and preventing similar breaches from occurring in the future. At a minimum, the procedure should specify the health information custodian or the agent of the health information custodian who will be notified of an unauthorized access, use, disclosure or disposal and should stipulate the information that will be provided by SSHA to the health information custodian including:

- the date and time of the unauthorized access, use, disclosure or disposal;
- a detailed description of the personal health information subject to the unauthorized access, use, disclosure or disposal;
- the circumstances surrounding the unauthorized access, use, disclosure or disposal including who accessed, used, disclosed or disposed of personal health information in an unauthorized manner; and
- the actions taken to contain and to prevent similar unauthorized access, use, disclosure or disposal.

Where SSHA is acting as a health information network provider, the agreements should also append the plain language description that SSHA is required to provide to health information custodians pursuant to section 6(3)2 of the Regulation, describing the services provided and the

safeguards implemented to protect against unauthorized use and disclosure and to protect the integrity of the personal health information.

When acting as a health information network provider, the agreements should also formally define and document the extent and manner to which SSHA will keep and make available to health information custodians electronic records of all accesses and transfers of personal health information in accordance with section 6(3)4 of the Regulation, how a health information custodian may request copies of these electronic records of accesses and transfers, the content of these electronic records and which accesses and transfers will be logged, monitored and reported on by SSHA. The agreements should also formally document when a written copy of the results of the privacy impact assessment and threat, vulnerability and risk assessment will be provided to the health information custodian as mandated by section 6(3)5 of the Regulation.

Finally, it is recommended that a database be maintained of all agreements with health information custodians in order to monitor whether agreements have been entered into with each health information custodian to whom services are provided and are up-to-date and in order to act as a central repository for such agreements.

L. PRIVACY IMPACT ASSESSMENTS

1. Failure to Conduct Privacy Impact Assessments for All Services

From the documentation provided it appears that SSHA, when acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, has either not performed or has not completed assessments with respect to how each of the services provided to health information custodians may affect the privacy of the individuals who are the subject of the personal health information (privacy impact assessments). Further, during the course of the review, it was difficult to determine which privacy impact assessments had been completed given a complete service catalogue of privacy impact assessments had not been compiled prior to the commencement of the review.

Even where privacy impact assessments were conducted, their formats were variable and only partially aligned with the *Privacy Impact Assessment Guidelines* of the Ministry of Government Services, although it is our understanding that an effort is underway to standardize the approach and format.

Further, from the documentation provided, it appears that SSHA, when acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, has not provided health information custodians with a written copy of the results of the privacy impact assessment for each of the services provided in accordance with section 6(3)5 of the Regulation. Even where the written results of a privacy impact assessment have been prepared, for example the Certification and Accreditation reports for the Managed Private Network, ONE Hosting and ONE Network, it appears that these written results have not been “provided” by SSHA to each

applicable health information custodian as required by section 6(3)5 of the Regulation, but rather are only "available on request."

It is recommended that, when acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, prior to providing any services to a health information custodian involving personal health information, SSHA perform privacy impact assessments and provide a written copy of the results of the privacy impact assessment indicating how the services provided may affect the privacy of individuals who are the subject of the information and the actions taken, or to be taken by SSHA, to address the risks to privacy and the timelines for such actions.

Section 6(3)5 of the Regulation requires a written copy of the assessment to be provided to each applicable health information custodian. In our view, merely making these reports "available on request" is insufficient to satisfy section 6(3)5 of the Regulation.

2. "Privacy Reviews" as Opposed to "Privacy Impact Assessments"

Further, in certain circumstances SSHA performs "a privacy review" as opposed to a "privacy impact assessment." It is our understanding that a privacy review is performed when a privacy impact assessment was already undertaken and a review is necessary to determine whether there are any changes in the roles and responsibilities of SSHA that could have an impact on how the services may affect the privacy of individuals. If there is a change in the roles and responsibilities of SSHA and therefore a change in how the services may affect privacy, a further privacy impact assessment is performed.

The IPC is concerned that a privacy review may not identify all the impacts that a product or service provided by SSHA may have on the privacy of individuals. Based on a review of the documentation provided, there are occasions where the risks to the privacy of individuals who are the subject of the personal health information and the strategies to minimize these risks were not discussed in a comprehensive manner. This is discussed in more detail elsewhere in this report. It is therefore recommended that privacy reviews contain a comprehensive discussion of the risks to the privacy of individuals and the strategies to minimize these risks.

It is also recommended that SSHA implement a policy, which is provided to all health information custodians to whom services are provided, setting out those circumstances where a privacy impact assessment will be performed, those circumstances where a "privacy review" as opposed to a privacy impact assessment will be performed and the rationale for performing a "privacy review" as opposed to a "privacy impact assessment." The policy should also stipulate a time frame for providing health information custodians with a written copy of the results of the privacy impact assessment or privacy review.

3. No "End to End" Privacy Impact Assessments

To date, none of the privacy impact assessments conducted by SSHA are "end-to-end" privacy impact assessments and there has been little, if any, interaction between SSHA and health information custodians to ensure such "end-to-end" privacy impact assessments are conducted

for the products or services provided. End-to-end privacy impact assessments address privacy issues in relation to all potential flows of personal health information within a health information network or system, from the point where the data is created to the point where it is finally destroyed, and at every point in between.

In a meeting on October 25, 2006, staff of SSHA indicated that SSHA does not have the authority to conduct "end-to-end" privacy impact assessments and does not have the authority to prohibit health information custodians from receiving services from SSHA unless they have conducted a privacy impact assessment.

It is recommended that SSHA work together with the Ministry of Health and Long-Term Care and the health information custodian community to address this issue in order to ensure that the privacy of individuals whose personal health information is subject to the services provided by SSHA is protected and to ensure the confidentiality of personal health information is maintained. End-to-end privacy impact assessments should be conducted for every product and service provided by SSHA, prior to the product or service being provided. This can only be accomplished by requiring health information custodians to undertake privacy impact assessments on all applications provided to them by SSHA.

In the interim, until such end-to-end privacy impact assessments can be undertaken, it is recommended that SSHA advise the health information custodians, to whom services are provided, of the scope and limitations of the privacy impact assessments conducted by SSHA and the risks to the health information custodians, to SSHA and to the privacy of individuals whose personal health information is subject to the services provided that may result from those limitations. It is recommended that this be communicated in the agreements entered into with the health information custodians to whom services are provided, in the privacy impact assessments themselves and in the written copy of the results of the privacy impact assessment that are required to be provided to each applicable health information custodian pursuant to section 6(3)5 of the Regulation.

4. Incomplete Discussion of Risks to Privacy and Strategies to Minimize these Risks

Where privacy impact assessments or privacy reviews were performed, there are occasions where the risks to the privacy of the individual who is the subject of the personal health information and the strategies to minimize these risks were not discussed in a comprehensive manner.

For example, one Privacy Assessment Summary that was provided indicates that : "once an email message leaves the SMI solution, the transmission of the email is not encrypted." Further, a Design Level Privacy Impact Assessment for a family health network information technology transition project states, "within the interim solution, any email communications occurring with parties outside of the ... Pilot physicians will not be encrypted. All email destined outside the physician group will be open to the internet." While these risks are identified, there does not appear to be a discussion of the effect of these risks on the privacy of individuals to whom the personal health information relates or the strategies to minimize these risks to privacy.

It is therefore recommended that in future, all privacy impact assessments and privacy reviews and the written results of the privacy impact assessment provided to health information custodians contain a comprehensive discussion of the risks to the privacy of individuals and the strategies to minimize these risks.

5. Failure to Identify a Time Frame for Implementing Strategies to Minimize Privacy Risks

Even where strategies to minimize the risks to the privacy of individuals are identified, the time lines for implementing these strategies are not clearly articulated. For example, two Privacy Summary Reports that were provided discuss the fact that some of the obligations imposed on SSHA as a health information network provider pursuant to section 6 of the Regulation have not been completed and are "in progress." No time frame is provided for when the requirements imposed by the Regulation will be addressed.

In future, it is recommended that all privacy impact assessments and privacy reviews and the written results of privacy impact assessments provided to health information custodians, stipulate a time frame for SSHA to implement the recommended strategies to minimize the risks to privacy identified. The absence of the identification of relevant time frames leaves health information custodians, who are ultimately accountable for the personal health information, with no mechanism to hold SSHA accountable for ensuring that strategies are implemented to minimize the risks to privacy of individuals who are the subject of the personal health information.

6. Point in Time Privacy Impact Assessments

The privacy impact assessments drafted by SSHA are "point in time" privacy impact assessments. The results of the privacy impact assessments conducted by SSHA inform health information custodians to whom SSHA provides services of the risks to privacy of individuals who are the subject of the personal health information at a "point in time," the time of drafting. They further inform health information custodians of the strategies that will be implemented to minimize these risks at this same point in time.

For example, the Design Level Privacy Impact Assessment for a family health network information technology transition project was based on the *Freedom of Information and Protection of Privacy Act* and acknowledges that, "Ontario proposes to introduce privacy legislation over the coming months that should apply to SSHA and this Privacy Impact Assessment must be revisited in light of any new obligations that arise." But, despite the fact that SSHA is now required to comply with *PHIPA*, the Design Level Privacy Impact Assessment for this project has not been updated in order to take into account SSHA's obligations under section 6 of the Regulation.

To be truly valuable, the privacy impact assessment process must be iterative. The privacy impact assessment and the written results of the privacy impact assessment provided to health information custodians should be updated throughout the lifecycle of the services provided by SSHA to address the continuing risks to privacy resulting from the services provided, to address

whether the strategies identified to minimize the risks to privacy have been implemented and to report on the effectiveness of these strategies in minimizing or mitigating these risks.

It is therefore recommended that the privacy impact assessments conducted by SSHA and the written results of the privacy impact assessments provided to health information custodians be updated to identify the continuing risks to privacy resulting from the services, to address when or whether recommended strategies were implemented to minimize the risks to privacy previously identified and to address whether these strategies in fact minimized or mitigated the risks identified.

It is further recommended that SSHA develop and maintain a database to monitor whether privacy impact assessments have been conducted for each product or service provided by SSHA, to ensure that the privacy impact assessments that have been conducted are up-to-date, to track whether a copy of the results of the privacy impact assessment have been provided to health information custodians, and to act as a central repository for such privacy impact assessments.

7. Discussion of Obligations Pursuant to Section 6 of the Regulation

Finally, it is recommended that the privacy impact assessments and that the written results of the privacy impact assessments reference *PHIPA* and the Regulation and clearly set out the status of SSHA under *PHIPA* and the Regulation. Specifically, the privacy impact assessments and the written results of the privacy impact assessment should specify whether SSHA is a health information network provider as defined in section 6(2) of the Regulation, a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation or an electronic service provider pursuant to section 6(1) of the Regulation.

The privacy impact assessments and the written results of the privacy impact assessments should also set out the obligations imposed on SSHA as a result of its status under *PHIPA* and the Regulation, how SSHA is or will be addressing each of its obligations and how addressing each of these obligations will minimize the risks to the privacy of individuals.

M. THREAT, VULNERABILITY AND RISK ASSESSMENTS

1. Failure to Conduct Threat, Vulnerability and Risk Assessments for All Services

The documentation provided indicates that the threat and risk assessment process is usually initiated because of an identified need. For example, a threat and risk assessment may be necessary when a new system is introduced or after the occurrence of a recent threat event that may have compromised an information technology system. However, it should be noted that, under the Regulation, SSHA has specific requirements with respect to assessments of the threats, vulnerabilities and risks to the security and integrity of personal health information as a result of the services provided by SSHA (threat, vulnerability and risk assessments), which are not subject to the discretion of SSHA.

From the documentation provided, it appears that SSHA, when acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, has either not performed or has not completed threat, vulnerability and risk assessments.

Even where threat, vulnerability and risk assessments were conducted, their formats were variable and only partially align with the standards set by the government of Ontario.

Further it appears that SSHA, when acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, has not provided health information custodians with a written copy of the results of the threat, vulnerability and risk assessments as required by section 6(3)5 of the Regulation. Even where the written results of threat, vulnerability and risk assessments have been prepared, for example the Certification and Accreditation reports for the Managed Private Network, ONE Hosting and ONE Network, it appears that the written results have not been "provided" by SSHA to the applicable health information custodians as required by section 6(3)5 of the Regulation, but rather are only "available on request."

When acting as a health information network provider or as a third party who provides services to assist a health information network provider, it is recommended that prior to providing any services to a health information custodian involving personal health information that SSHA perform threat, vulnerability and risk assessments. Furthermore, it is recommended that SSHA provide a written copy of the results of these assessments indicating the threats, vulnerabilities and risks to the security and integrity of the personal health information, the actions taken or to be taken by SSHA to minimize or mitigate these threats, vulnerabilities and risks and the timelines for such actions.

Section 6(3)5 of the Regulation requires a written copy of the assessment to be provided to each applicable health information custodian. In our view, merely making these reports "available on request" is insufficient to satisfy this requirement.

2. Failure to Identify a Time Frame for Implementing Strategies to Minimize Threats, Vulnerabilities and Risks

Where strategies to minimize the threats, vulnerabilities and risks to the security and integrity of personal health information are identified, the time lines for implementing these strategies are not clearly articulated.

In future, it is recommended that all threat, vulnerability and risk assessments and the written results of threat, vulnerability and risk assessments provided to health information custodians, stipulate a time frame for SSHA to implement the recommended strategies to minimize the threats, vulnerabilities and risks to the security and integrity of the personal health information identified. The absence of specific time frames leaves health information custodians, who are accountable for the personal health information, with no mechanism to hold SSHA accountable for ensuring that strategies are implemented to minimize the threats, vulnerabilities and risks to the security and integrity of the personal health information.

3. Point in Time Threat, Vulnerability and Risk Assessments

The threat, vulnerability and risk assessments drafted by SSHA are "point in time" threat, vulnerability and risk assessments. The results of the threat, vulnerability and risk assessments, conducted by SSHA, inform health information custodians to whom SSHA provides services of the threats, vulnerabilities and risks to the security and integrity of personal health information at a "point in time," the time of drafting. They further inform health information custodians of the strategies that will be implemented to minimize these threats, vulnerabilities and risks at this same point in time.

However, to be truly valuable, the threat, vulnerability and risk assessment process must be iterative. The threat, vulnerability and risk assessment and the written results of the threat, vulnerability and risk assessment provided to health information custodians should be updated throughout the lifecycle of the services provided by SSHA to address the threats, vulnerabilities and risks to security and integrity of the personal health information resulting from the services provided, to address whether the strategies identified to minimize the threats, vulnerabilities and risks previously identified have been implemented and to report on the effectiveness of these strategies in minimizing or mitigating these threats, vulnerabilities and risks.

It is therefore recommended that the threat, vulnerability and risk assessments conducted by SSHA and that copies of the written results of the threat, vulnerability and risk assessments provided to health information custodians be updated to identify the ongoing risks to the security and integrity of the personal health information resulting from the services, to address when or whether recommended strategies were implemented to minimize the threats, vulnerabilities and risks previously identified, and to address whether these strategies in fact minimized or mitigated the threats, vulnerabilities and risks identified.

It is further recommended that SSHA develop and maintain a database to monitor whether threat, vulnerability and risk assessments have been conducted for each product or service provided by SSHA, to ensure that the threat, vulnerability and risk assessments that have been conducted are up-to-date, to track whether written copies of the results of the threat, vulnerability and risk assessments have been provided to the health information custodians, and to act as a central repository for such threat, vulnerability and risk assessments.

N. PRIVACY TRAINING

SSHA has initiated a privacy training program in respect of SSHA operations. However, this is not a robust, on-going privacy program. All new staff do not routinely receive privacy orientation prior to the commencement of employment and prior to being given access to SSHA systems which may give the employee access to personal health information. It is our understanding that not all individuals working at SSHA have completed *PHIPA*-specific privacy training or role-based privacy training. In addition, until recently, privacy training was not monitored to ensure that all staff have received initial privacy training and ongoing training.

The documentation provided indicates that SSHA has provided training sessions on privacy and security to its employees on numerous occasions, including February 2004, March 2004, July 2004, April 2005, and September, October and November 2006. However, up to January 1, 2006, these training sessions did not address *PHIPA* and the Regulation nor SSHA's privacy and security policies and procedures in a comprehensive manner. In addition, no role-based privacy and security training has been provided to ensure that agents of SSHA understand how to apply the privacy and security policies in their day-to-day work.

Further, only two training sessions up to January 1, 2006, the "Privacy Awareness Session" in April 2005, and "Bill 31 Lunch and Learn" on February 5, 2004, defined "personal health information" and defined "health information custodians" and explained their relevance in the context of SSHA. Only one training session prior to January 1, 2006, the "Privacy Awareness Session" in April 2005, defined "health information network provider" and explained its relevance to SSHA. Only one presentation, the "Smart Systems for Health Security Awareness" Session, discussed the physical, administrative and technical safeguards implemented by SSHA to protect the confidentiality of personal health information and the privacy of individuals with respect to that information and explained to employees, in a very comprehensive and thoughtful manner, their role in implementing these safeguards.

Up until September 2006, the privacy and security training was not mandatory. As a result, according to statistics for the 2005 calendar year provided to the IPC for the purposes of this review, 76 per cent of employees did not attend privacy training and 67 per cent did not attend security training. When privacy and security training was made mandatory in September 2006, only 8 per cent of employees did not attend privacy training and only 37 per cent of employees did not attend security training.

IPC staff participated in introductory privacy training for SSHA employees. The materials for this seminar have since been updated to incorporate some of IPC's suggestions for improvement. However, the introductory privacy training is still inadequate for the purpose of informing employees about their responsibilities concerning personal health information under *PHIPA*. It is recommended that greater emphasis be placed on the responsibilities of employees in the event of a privacy or security breach. For example, very specific information concerning the definition of a breach, procedures for containing a breach, and whom to notify in the event of a breach needs to be included in the training.

It is our understanding that privacy training will eventually be comprised of an introductory session for new employees and those who have not received privacy training, and a supplementary session that staff will be required to attend on an annual basis. These new features of the privacy training program need to be implemented as soon as possible.

Currently, consultants and employees of vendors who have access to personal information, personal health information and sensitive assets do not receive training about SSHA's privacy policies and procedures or training on best practices for ensuring the privacy and security of personal health information. It is recommended that SSHA ensure that SSHA staff, consultants, and employees of vendors are instructed on privacy policies and procedures relevant to their area of responsibility.

It is therefore recommended that SSHA make privacy and security training mandatory and that this training:

- Explain the status of SSHA under *PHIPA* and the Regulation, depending on the particular services provided to health information custodians in respect of personal health information;

- Describe the circumstances in which SSHA is a health information network provider as defined in section 6(2) of the Regulation, the circumstances in which SSHA is a third party retained by a health information network provider to assist in providing services to a health information custodian as described in section 6(3)6 of the Regulation and the circumstances in which SSHA is an electronic service provider pursuant to section 6(1) of the Regulation;

- Explain the obligations that arise from *PHIPA* and the Regulation, depending on its status and how SSHA is or will be satisfying each of these obligations;

- Define the terms "personal health information," "health information network provider," "third party retained by a health information network provider to assist in providing services to a health information custodian," "electronic service provider" and "health information custodian" and explain their relevance in the context of SSHA;

- Explain the duties with respect to the use and disclosure of personal health information imposed on employees of SSHA under section 6(1) of the Regulation;

- Comprehensively explain the protocol of SSHA as it relates to identifying, containing, investigating and preventing unauthorized access, use, disclosure or disposal of personal health information and as it relates to notifying health information custodians of the unauthorized access, use, disclosure or disposal in accordance with section 6(3)1 of the Regulation, when SSHA is acting in its capacity as a health information network provider; and

- Discuss and explain the Enterprise Privacy Policy, Enterprise Security Policy, Enterprise Risk Management Policy and Information Classification and Handling Policy in a comprehensive manner, including where these policies can be found and the requirements imposed by these policies;

- Explain the requirement on employees to notify SSHA if they have accessed, used, disclosed or disposed of personal health information in contravention of the Regulation or if an unauthorized person accessed the personal health information, including whom to contact in the event that this should occur; and

- Discuss the physical, administrative and technical safeguards implemented by SSHA and explain to employees their role in implementing these safeguards.

It is also recommended that a procedure be implemented to track which employees have received privacy and security training in order to ensure that appropriate action can be taken with respect to those who have not received such training.

O. PLAIN LANGUAGE DESCRIPTIONS

Sections 6(3)2 and 6(3)3 of the Regulation require SSHA, when acting as a health information network provider, to provide each applicable health information custodian with a plain language description of the services provided, including a general description of the safeguards to protect against unauthorized use and disclosure and to protect the integrity of the personal health information. In addition, these sections require SSHA to make available to the public a plain language description of the services provided, a general description of the safeguards implemented in relation to the security and confidentiality of the personal health information and any directives, guidelines and policies that apply to the services provided.

While SSHA's website, www.ssha.on.ca/products-services, contains a plain language description of the services provided by SSHA to health information custodians, there does not appear to be a general description of the safeguards in place to protect the security and confidentiality of the personal health information. In addition, the website does not appear to contain any of the policies, directives or guidelines that apply to the services provided by SSHA to health information custodians. The only document that contained a description of the safeguards, entitled, *Products and Services – Privacy and Security*, only contains general statements that SSHA:

- complies with privacy laws and regulations;
- ensures the rights of patients and health care providers are properly protected;
- is subject to oversight by the IPC;
- is subject to *PHIPA* and the *Freedom of Information and Protection of Privacy Act*; and
- maintains physical, procedural, and electronic safeguards to protect information and systems.

In our view, these statements are insufficient for the purposes of sections 6(3)2 and 6(3)3 of the Regulation, which require SSHA to provide a "description" of the safeguards in place to protect against unauthorized use and disclosure and to protect the integrity of the information.

The general statements in the *Products and Services – Privacy and Security* document, including that SSHA "maintains physical, procedural and electronic safeguards to protect information and systems," do not provide comfort to either health information custodians or to members of the public, whose personal health information has been entrusted to SSHA, that the integrity, security and confidentiality of personal health information is being protected.

It is therefore recommended that this document be revised accordingly to describe the general safeguards in place to protect against unauthorized use and disclosure and to protect the integrity of the information and to describe the safeguards implemented in relation to the security and confidentiality of the information. These safeguards can be described in such a manner so as to provide necessary assurance to health information custodians and members of the public that

personal health information is being safeguarded, without compromising security, by providing overly detailed information on the specific safeguards implemented.

Further, section 6(3)2 of the Regulation is explicit in that it requires SSHA, when acting as a health information network provider, "to provide" to each applicable health information custodian, as opposed to make available, a plain language description of the services that SSHA provides to the health information custodians, including a general description of the safeguards to protect against unauthorized use and disclosure and to protect the integrity of the information. This should be compared to section 6(3)3 of the Regulation which requires SSHA "to make available" a plain language description to the public.

As a result, it is recommended that, prior to providing services to a health information custodian, SSHA provide each applicable health information custodian with a plain language description in accordance with section 6(3)2 of the Regulation as opposed to simply making such a plain language description available on the SSHA website.

It is further recommended that SSHA update the "plain language descriptions" required pursuant to sections 6(3)2 and 6(3)3 of the Regulation when necessary to ensure that health information custodians to whom services are provided and Ontarians whose personal health information has been entrusted to SSHA, have current descriptions of the services being provided and that these updated "plain language descriptions" be immediately provided to applicable health information custodians and be immediately made available to the public on the website of SSHA.

It is our understanding that SSHA is preparing a corporate brochure. It is recommended that the brochure contain a plain language description of the services provided and a description of the safeguards that have been put into place to protect against unauthorized use and disclosure of personal health information and to protect the integrity, security, and confidentiality of the information.

It is also recommended that in addition to the Enterprise Privacy Policy and the Enterprise Security Policy, the written results of privacy impact assessments and threat, vulnerability and risk assessments be immediately posted on both the SSHA website: www.ssha.on.ca and on the privacy portal: www.privacy.ssha.on.ca or, alternatively, that these documents be posted on the privacy portal and a direct link be provided from SSHA's website: www.ssha.on.ca to the privacy portal: www.privacy.ssha.on.ca.

In addition, based on a review of the privacy portal and the *Functional Specifications: Privacy, Security and Risk Management Portal* document (*Functional Specifications* document), we have the following comments.

First, the objective of this portal, as set out in section 2.1 of the *Functional Specifications* document, is to provide a vehicle for SSHA to communicate with clients of SSHA. This objective and the layout of the portal as described in the *Functional Specifications* document do not address the communication between SSHA and Ontarians whose personal health information is the subject of the services being provided by SSHA nor do they seem to address the requirement imposed on SSHA, when acting as a health information network provider, to make

available to the public a plain language description in accordance with section 6(3)3 of the Regulation and to make available any directives, guidelines and policies that apply to the services to the extent that they do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information.

Further, while the portion of the portal entitled "Policies and Procedures" contains the Enterprise Privacy Policy and Enterprise Security Policy, from the *Functional Specifications* document, it appears that the layout of the portal will not provide for the posting of a plain language description prepared in accordance with section 6(3)2 of the Regulation for health information custodians to whom services are provided nor the written results of privacy impact assessments and threat, vulnerability and risk assessments conducted in accordance with section 6(3) 5 of the Regulation.

In addition, the "Frequently Asked Questions" as formulated in the *Functional Specifications* document do not address the status of SSHA under *PHIPA* and the Regulation depending on the particular services in respect of personal health information being provided to health information custodians, the obligations that arise from *PHIPA* and the Regulation and how SSHA is addressing each of its obligations arising out of *PHIPA* and the Regulation.

It is therefore recommended that SSHA consider using its privacy portal as a vehicle for fulfilling SSHA's obligations under the Regulation to inform both health information custodians and the general public about its products and services.

P. ELECTRONIC RECORDS OF ACCESS AND TRANSFERS

It is our understanding that it is not a common practice for SSHA to produce electronic logs of accesses to personal health information at SSHA. For example, the Privacy Review for a national home care partnership pilot project states that "it is not reasonably practical for SSHA to produce electronic logs of accesses to personal health information." If SSHA is of the opinion that it is not practical to produce electronic logs of accesses to personal health information, it is recommended that the rationale behind this statement be provided.

When acting as a health information network provider, SSHA is required, pursuant to section 6(3)4 of the Regulation, to ensure that the following electronic records are kept and made available upon request, to the extent and in a manner that is reasonably practical:

- Accesses to all or part of the personal health information associated with the health information custodian being held in equipment controlled by SSHA, which record the person who accessed the personal health information and the date and time of the access; and

- Transfers of all or part of the personal health information associated with the health information custodian by means of equipment controlled by SSHA, which record the person who transferred the personal health information, the person or address to whom the personal health information was sent and the date and time it was sent.

Staff of SSHA have indicated that where SSHA is hosting an application for a client, it can monitor SSHA's infrastructure. However, its ability to monitor and log accesses and transfers will depend on the design of the application and SSHA's involvement in operating or managing that system on behalf of its client. For example, where SSHA is providing hosting services, its role relating to the application may be restricted simply to providing the power, cooling and external connection for the client's server. In such cases, SSHA cannot monitor and log accesses.

As a result, where SSHA is not acting as a health information network provider and is simply providing hosting services, it is recommended that the agreements entered into with health information custodians for whom such services are provided should specify the type of monitoring and logging that SSHA is able to provide, the information that this type of monitoring and logging is able to provide to health information custodians and the limitations on this type of monitoring and logging.

Where SSHA is acting as a health information network provider, it is recommended that the agreements with health information custodians for whom services are provided should formally define and document the extent and manner in which electronic records of accesses and transfers in accordance with section 6(3)4 of the Regulation will be made available, how a health information custodian may request these electronic records from SSHA, the content of these electronic records, which accesses and transfers will be logged, monitored and reported on, the information that this type of monitoring and logging is able to provide to health information custodians, and the limitations, if any, on this type of monitoring and logging.

It is further recommended that SSHA, when acting as a health information network provider, implement practices and procedures relating to monitoring accesses and transfers to enable SSHA to keep and make available to a health information custodian upon request, to the extent and in a manner that is reasonably practical, these electronic records pursuant to section 6(3)4 of the Regulation. This should include defining which accesses and transfers will be logged, monitored and reported on, the extent and manner in which electronic records of such accesses and transfers will be made available to health information custodians, the content of these electronic records of accesses and transfers, and the process to be followed by a health information custodian in making a request for electronic records of accesses and transfers.

Q. INTEGRATED DISASTER RECOVERY AND BUSINESS CONTINUITY FRAMEWORK

It is recommended that an integrated organization-wide business continuity and disaster recovery framework be developed by SSHA. The purpose of the framework would be to identify and mitigate business risks and consequences associated with major failures or disasters, to identify risks to the security, integrity and confidentiality of the personal health information of individuals and to the privacy of individuals who are the subject of the personal health information and to identify mitigation strategies to minimize or mitigate against these risks.

Although not apparent from the documentation provided, it is our understanding, based on a meeting with staff of SSHA, that some organizational units within SSHA have developed

business continuity and/or disaster recovery plans for their particular organizational unit, while others have not. Staff of SSHA confirmed at the meeting on October 25, 2006, that there was no integrated organization wide business continuity or disaster framework currently in place. However, it is our understanding that SSHA has entered into an agreement with a third party to develop such a framework.

R. PRIVACY/SECURITY BREACHES AND INCIDENTS

The ability to monitor, identify and respond to actual or potential privacy and security breaches and incidents are key components of a good privacy and security program. The identification, documentation and investigation of privacy and security incidents must follow a prescribed and rigorous process if evidence is to be obtained, maintained and, if necessary, made available to prosecute violators or others attempting to gain unauthorized access to facilities, networks, or personal health information.

In the course of the review, the IPC noted that documented security monitoring, incident tracking, response and remediation procedures exist, but are not mature, formalized, or utilized enterprise-wide. For example, there are serious gaps in SSHA's ability to monitor security event data. Moreover, the identification of security and privacy incidents is not consistent. Current methods of tracking and reporting security and privacy incidents are also not consistent, and reports contain insufficient details. Privacy incidents are not tracked or reported centrally along with other types of incidents, but are escalated separately in a less than formal process. As a result, it is not evident that SSHA has sufficient capability to detect and isolate incidents, analyze root causes, and respond in a timely manner with an effective plan of action.

In accordance with section 6(3)1 of the Regulation, when SSHA is acting in its capacity as a health information network provider, SSHA must notify every health information custodian at the first reasonable opportunity if SSHA accessed, used, disclosed or disposed of personal health information in an unauthorized manner or if an unauthorized person accessed, used, disclosed or disposed of personal health information.

However, currently such incidents are not identified, contained, investigated, tracked and reported on in a consistent and formal manner, as acknowledged in the SSHA Certification and Accreditation Report for ONE Hosting, "thereby making root cause analysis and recognition of recurring problems difficult." It is our understanding that SSHA is undertaking a request for proposal process to obtain assistance in this area.

Accordingly, it is recommended that SSHA develop and implement comprehensive security monitoring and management policies and practices, combined with robust security procedures and supported with tools and techniques to detect, record, report, investigate, and respond effectively to privacy and security incidents. Constant monitoring of the activities on the network and security status is essential, with appropriate records being kept.

The protocol to respond to privacy and security breaches should:

- identify the person at SSHA to whom employees, consultants, contractors and vendors must report an unauthorized access, use, disclosure or disposal of personal health information;

- stipulate the timeline for making such a report;

- outline the information that must accompany the report including the date and time of the unauthorized access, use, disclosure or disposal, a detailed description of the personal health information subject to the unauthorized access, use, disclosure or disposal and the circumstances surrounding the unauthorized access, use, disclosure or disposal;

- identify the person at SSHA responsible for conducting an investigation and determining whether or not to involve law enforcement agencies and the person at SSHA who is responsible for containment of the unauthorized access, use, disclosure or disposal;
- identify who will be notified of the unauthorized access, use, disclosure or disposal of personal health information, which shall include the applicable health information custodian(s) pursuant to section 6(3)1 of the Regulation; and

- outline the information that will be provided to those notified which should include:

    - the date and time of the unauthorized access, use, disclosure or disposal;

    - a detailed description of the personal health information subject to the unauthorized access, use, disclosure or disposal;

    - the circumstances surrounding the unauthorized access, use, disclosure or disposal; and

    - the actions taken or planned to contain and prevent a similar unauthorized access, use, disclosure or disposal in future.

S. PROCEDURE FOR RECEIVING AND RESPONDING TO PRIVACY QUESTIONS/COMP LAINTS

Section 6.10.2 of the Enterprise Privacy Policy states that SSHA will establish procedures to receive and respond to complaints or inquiries about its practices relating to the management of information. At a meeting on October 25, 2006, staff of SSHA acknowledged that despite this statement in the Enterprise Privacy Policy, such procedures do not exist, but that the contact information for the person to whom inquiries or complaints in relation to privacy should be directed is provided on the website of SSHA.

It is recommended that SSHA implement procedures to receive and respond to complaints or inquiries about its practices relating to personal information and personal health information. This procedure should:

- identify how to make a complaint or ask questions relating to SSHA's compliance with *PHIPA*, the Regulation and the Enterprise Privacy Policy;

- identify and provide contact information for the person at SSHA to whom these complaints or questions may be addressed;

- be made available on the SSHA website: www.ssha.on.ca, the privacy portal: www.privacy.ssha.on.ca and to individuals who make inquiries about the compliant procedure;

- the process for investigating a complaint including sending an acknowledgement advising the individual making the complaint that the complaint has been received, explaining the complaint investigation procedure and advising the individual making the complaint of the process for obtaining further information concerning the complaint; and
- the process for providing a written response, to the individual making the complaint, summarizing the nature and findings of the investigation and outlining the measures taken in response to the complaint, which may include amendment of the Enterprise Privacy Policy.

In addition, it is recommended that SSHA record, track and monitor response times for investigating and resolving privacy questions and complaints and monitor the types of issues, about which questions are raised or complaints made, in order to analyze trends and recommend changes to its Enterprise Privacy Policy and Enterprise Security Policy, based on this analysis.

T. PRIVACY AND SECURITY POLICIES RELATING TO SSHA SERVICES

A number of documents, which discuss privacy issues in relation to certain services offered by SSHA, indicate that SSHA has yet to develop appropriate policies and procedures relating to these services. For example, SSHA does not have a policy for responding to requests for information from law enforcement authorities and other third parties. Another example is the lack of a policy for dealing with orphaned email accounts where email services are being offered by SSHA. SSHA should ensure that all potential privacy and security issues that could arise in the context of providing services are addressed through appropriate policies and procedures prior to offering services. In addition, health information custodians should be made aware of these policies and procedures prior to receiving the services so that they will understand in advance what will happen when these events arise.

U. RETENTION AND DISPOSAL POLICIES AND PROCEDURES

The Enterprise Privacy Policy states that SSHA will develop guidelines and implement procedures with respect to the retention of personal information and that the guidelines will set out minimum and maximum retention periods. This policy states further that the Chief Information Officer will develop guidelines and implement procedures to govern the destruction

of personal information. It is our understanding that retention and disposal policies and procedures in respect of personal health information have not been developed.

SSHA does not have a comprehensive policy for retention and disposal of data. There are only policies and procedures relating to the destruction of specific types of media, such as high-density disks. In addition, at the site visit, SSHA indicated that old back-up tapes are retained in a secure cabinet. However, there are no general policies setting out how long information will be retained, the manner in which it will be retained and how it will be disposed of, when it is no longer needed. Currently there are inconsistent practices and procedures in place in this regard. For example, at certain locations back-up tapes are encrypted, while at other locations they are not. It is therefore recommended that comprehensive retention and destruction policies and procedures be developed and implemented.

V. INTERNAL/EXTERNAL AUDITS

The Enterprise Privacy Policy indicates that compliance with the privacy program will be subject to internal reviews/audits on an annual basis and subject to an external audit at least once every five years. The Enterprise Privacy Policy states further that the Chief Privacy and Security Officer will review the design and assist in overseeing the audits of the privacy program. Audits are intended to be provided to the CEO annually by the Chief Privacy and Security Officer.

Similarly, the Enterprise Security Policy states that it will be subject to an internal audit on an annual basis and an external audit at least once every five years. The Chief Privacy and Security Officer is responsible for designing and overseeing the internal security audit. Audit reports must be provided to the CEO annually by the Chief Privacy and Security Officer. The Information Classification and Handling Policy also indicates that the Chief Privacy and Security Officer is responsible for security audits for the purpose of ensuring compliance with this policy, and for assuring that information classification is completed at the appropriate levels.

It is our understanding that SSHA has not undertaken internal or external audits of its privacy or security program. In fact, currently, SSHA does not have a functioning audit committee or an internal audit department. The failure to conduct internal audits of its privacy and security program contravenes SSHA's Enterprise Privacy Policy and Enterprise Security Policy which require internal audits on an annual basis. It is therefore recommended that SSHA immediately develop and implement a comprehensive privacy and security internal audit program. It is also recommended that SSHA conduct an external audit of its privacy and security program prior to January 1, 2008, in compliance with its Enterprise Privacy Policy and Enterprise Security Policy which require external audits at least once every five years.

W. NON-CREDIBLE CERTIFICATION AND ACCREDITATION SERVICES

SSHA's certification and accreditation program applies generally to the design and deployment of external SSHA programs and services, which may include use by external clients including health information custodians. The certification and accreditation program appears to be central

to SSHA's ability to provide and assure reasonably secure managed network and hosting services to external clients such as health information custodians.

The Enterprise Security Policy defines certification to mean a "procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements." "Accreditation" (in computer security) is defined as "[t]he authorization and approval by a designated authority to a data processing system, computer network, organization, or individual, to process sensitive information or data." However, these fairly common, conventional definitions of accreditation and certification do not appear to have been applied in the context of other documents and to SSHA's certification and accreditation program.

In terms of accreditation, the SSHA documentation provides little or no objective basis that its accreditation program is founded upon any recognized standards. Rather, it seems to refer only to formal senior executive approval of the capability of staff to carry out certifications, or recognition that a certification has been carried out. There is no basis for asserting that the CEO would be recognized as an accreditation authority outside of SSHA.

In terms of certification, while SSHA refers to several external documents and guidelines (such as the Canadian Security Establishment MG-4 and Ministry of Government Services Privacy Impact Assessment) in its documentation, there is little evidence that its certification and accreditation program adheres to any of these standards. Instead, SSHA "certification," to the extent it is defined at all, seems to refer only to the SSHA's opinion or assertion that the managed system in question is sufficiently secure to be trusted and used. At best, the "certification" process may yield insights and advice for clients to consider or follow.

SSHA's certification and accreditation program is strictly an in-house affair. Few SSHA services and products have completed the certification and accreditation process. The documentation reviewed indicated that only ONE Networks and One Hosting have completed this process. In our view, such a program cannot assure trust and confidence in the security of SSHA networks and information systems when:

- the standards of evaluation are not clearly-defined, objective or recognized beyond SSHA;
- the "certification" process can only be performed or recognized in-house, according to variable criteria; and
- the "accreditation" of certifiers is also carried out in-house as a function of executive sign-off, without regard to external standards of evaluation.

It is recommended that SSHA refrain from using the terms "certification" and "accreditation," unless SSHA is able to develop or adopt a set of clearly defined, objective standards for evaluation. Any standards of evaluation that are developed or adopted should be susceptible to external third party use and validation. Once such standards have been developed or adopted, SSHA should seek external validation. The accreditation (and therefore recognition) of certifiers is best left to well-established internationally-recognized criteria and processes, such as those of the International Standards Organization (ISO).

X. RISK TOLERANCE AND MANAGEMENT

SSHA has embarked on a comprehensive and extensive policy initiative to identify, measure, review, prioritize, assign and mitigate a wide range of strategic, operational, program and project-specific risks to the organization and to services it offers through the establishment of a Risk Management Committee and a "risk register." This is a very welcome development and direction, as understanding security risks in a systematic and quantifiable manner provides a strong starting point for developing effective security policies and procedures to mitigate them. While, for the most part, SSHA has done an excellent job identifying and quantifying the many operational risks extant, some issues are still outstanding.

While SSHA has established a "risk register" to identify, measure, review, prioritize, assign and mitigate risks, six risk issues that were identified by SSHA were not included in the "risk register." It is recommended that SSHA record all risks identified in the "risk register" in order to ensure that the "risk register" provides a complete picture of the risks identified by SSHA.

Further, while SSHA established a Risk Management Committee chaired by the Chief Privacy and Security Officer and comprising members of senior management including the Chief Executive Officer to review, address and manage risk tolerance levels, the Risk Management Committee has not met as a group since March 2005. Instead, it appears that informal meetings are held to discuss such issues. It is recommended that meetings of the Risk Management Committee be reconvened in order to review, address and manage risks. This would help to ensure that these risks are formally shared, documented, reported on and resolved.

Also, throughout the risk management documentation reviewed, the risks to individual Ontarians posed by security and privacy breaches are nowhere to be found. That is, virtually all of the identified risks are interpreted exclusively within the lens of their potential impacts upon SSHA as an organization (The one notable exception here is the risk to individuals of unavailability of their personal health information on the network). This is inconsistent with the spirit of *PHIPA*, and we urge SSHA to factor in the many potential impacts upon the individuals as a result of various threats, vulnerabilities and risks.

In addition, a number of documents, including the draft Information Security Policy and the draft Information Security Operating Directives, reference the fact that risk appetite and risk tolerance will be defined by the Board of Directors of SSHA and communicated to organizational units of SSHA.

Further, in a teleconference on November 6, 2006, staff at SSHA acknowledged that to date, the risk tolerance of the Board of Directors has not yet been defined but that there has been "progress" in this regard. Staff at SSHA further confirmed that in some respects SSHA is working backwards given it has already developed a Risk Management Policy and Information Classification Policy based on the Board's likely "risk appetite and risk tolerance."

It is recommended that direction be sought from SSHA's Board of Directors in defining its "risk appetite and risk tolerance." This should be communicated to the organizational units of SSHA.

In addition, the Information Classification and Handling Policy and Enterprise Risk Management Policy should be revisited and amended in light of this definition.

Through the review of the risk management documentation that was provided, it became apparent that there are quite a few serious risks, with either a high likelihood of occurrence and/or high impact which have not been sufficiently addressed or mitigated to date. While these risks cannot be discussed in detail in this report, for security reasons, it is important to note that a significant number of risks fall above the threshold of risk tolerance established by SSHA.

Further, it is not clear from the documentation that sufficient progress has been made in mitigating these risks. It is often unclear precisely what actions or steps are being taken. To compound this problem, it is not clear that the risk management documentation is being updated at regular intervals to effectively assess the current level of risk.

It is not evident from the documentation provided that SSHA has taken steps to comply with all provisions of its own Risk Management Policy which require, for example, that "SSHA must report the Agency's risk profile to the Audit Committee of the board on a quarterly basis," or that "[r]isk management activities and responsibilities must be in all job profiles that have management accountabilities." Furthermore, the review indicated that although the Risk Management group provides guidance, direction and education, it does not monitor compliance to ensure that risk management practices are continually applied in decision-making processes.

Accordingly, it is recommended that SSHA adopt a program to deal credibly with current strategic, operational, program and project-specific risks, before proceeding with development and rollout of new managed programs and services, such as ONE web and ONE mail, and new products, such as the voluntary electronic health record. That is, we urge deferral of plans to proceed with even riskier projects until such time as the current risks are satisfactorily addressed.

Summary of Recommendations

Based on this review, the IPC makes the following recommendations to SSHA. **Recommendations that appear in BOLD should be given priority.** In addition, where the timing for the implementation of a specific recommendation is deemed to be immediate, action must be taken to comply with the *Personal Health Information Protection Act* (*PHIPA*) and the Ontario Regulation 329/04 (the Regulation):

1. **Develop and implement comprehensive, explicit and coordinated sets of policies, standards and procedures for the SSHA security and privacy programs.**

2. Develop and implement appropriate documentation practices and document management procedures for all privacy and security related matters.

3. Establish clearly defined roles and responsibilities for privacy and security matters.

4. **Augment SSHA privacy expertise by recruiting a seasoned privacy expert, with demonstrated experience in implementing a privacy program in a complex and high profile organization, to provide leadership and oversight for the privacy program at SSHA and by ensuring that key staff members who are responsible for implementing privacy on a day-to-day basis have the necessary training, expertise and authority to carry out this function.**

5. Revise the Enterprise Privacy Policy and Enterprise Security Policy to reference all of SSHA's obligations with respect to privacy and security in relation to the various roles that SSHA fulfills under *PHIPA* and the Regulation.

6. Revise the Enterprise Privacy Policy, the Enterprise Security Policy and the Information Classification and Handling Policy to reference and define personal health information; collection, use and disclosure in relation to personal health information; and privacy breach, in accordance with *PHIPA* and the Regulation.

7. Review and update the revised the Enterprise Privacy Policy and the Enterprise Security Policy on an annual basis.

8. Revise the Enterprise Privacy Policy with respect to the privacy policy authorities, privacy accountability, privacy breaches and violations, employment and contracting, and openness, as described in this report.

9. Revise the Enterprise Security Policy with respect to the security policy authorities; provisions related to terms and conditions of employment, staff, consultant and vendor obligations and practices, and contracting; security breaches, violations and other incidents; and provisions relating to exchange of information and assets, as described in this report.

10. Revise and finalize all privacy and security policies, standards and procedures and ensure that they are applied consistently across SSHA and that compliance with these policies, standards and procedures is mandatory for all staff, consultants and vendors.

11. Ensure that access controls, including authentication, are formally documented and managed and appropriate to the level of sensitivity of the applications to which they are applied.

12. Amend the sensitivity classification assigned to each service or technology asset to take into account the magnitude of harm that could result from a loss of privacy of individuals to whom the personal health information relates or that could result from a breach of confidentiality.

13. Amend the definition of "sensitive information" in the Information Classification and Handling Policy to set out the precise information that SSHA considers sensitive and to include personal information as defined under the *Freedom of Information and Protection of Privacy Act* and personal health information as defined under *PHIPA.*

14. Amend the sunset dates in the Information Classification and Handling Policy, whereby records or information will no longer be considered sensitive, to accord with section 9(1) of *PHIPA*, which sets out the time frame in which *PHIPA* applies to records containing personal health information.

15. Amend all policies and procedures to ensure consistency in the classification and handling of "sensitive information" and to ensure consistent application of appropriate controls based on such classification.

16. Amend the Asset Management Policy to identify procedures for removing personal health information from information technology equipment or network devices when an information technology asset is being used for purposes other than its original intent, used by a different individual, sent for repair, or being prepared for disposal.

17. Amend the Asset Management Policy to require all staff to notify the Chief Privacy and Security Officer, if an item holding personal health information is lost or stolen.

18. Develop and implement a policy that specifies by whom, when and how often the Acknowledgement of Confidentiality, the Enterprise Privacy Policy Acknowledgment and Enterprise Security Policy Acknowledgement must be signed.

19. Revise and implement the Acknowledgement of Confidentiality to refer to *PHIPA* and the Regulation; to refer to and define personal health information in accordance with *PHIPA*; to set out the consequences of privacy breaches; to require individuals to comply with the requirements of section 6(1) of the Regulation; to require individuals to notify SSHA if they accessed, used, disclosed or disposed of personal health information other than in accordance with the Acknowledgement; and to

require individuals to notify SSHA if they become aware that an unauthorized person accessed personal health information.

20. Develop and implement a policy that requires the signing of an acknowledgement with respect the Information Classification and Handling Policy and the Enterprise Risk Management Policy.

21. Revise or develop and implement the Enterprise Privacy Policy Acknowledgment, the Enterprise Security Policy Acknowledgement, the Information Classification and Handling Policy Acknowledgement and the Enterprise Risk Management Policy Acknowledgement: to refer to *PHIPA* and the Regulation; to refer to and define personal health information in accordance with *PHIPA*; to set out the consequences of breaches of the policy or the acknowledgement; to require individuals to notify SSHA, if they accessed, used, disclosed or disposed of personal health information other than in accordance with the policy; and to require individuals to notify SSHA, if they become aware of any breaches of the policy.

22. Implement a process to track which employees have signed the acknowledgements mentioned above and the date of signature to ensure appropriate monitoring and follow up for those employees who have not signed the acknowledgements.

23. Develop and implement a policy that sets out the process to be followed in investigating breaches of the above mentioned policies and acknowledgements, the possible consequences of such breaches from a labour relations perspective and any aggravating factors that may affect discipline.

24. Immediately enter into agreements with all third parties retained to assist SSHA in providing services to health information custodians.

25. Amend agreements with all third parties retained to assist SSHA in providing services to health information custodians to specify the policies, procedures and practices that will be implemented to ensure compliance with the requirements set out under section 6(1) of the Regulation.

26. Amend agreements with all third parties retained to assist SSHA in its role as health information network provider to require these parties to notify SSHA at the first reasonable opportunity, if employees or persons acting on behalf of these third parties accessed, used, disclosed or disposed of personal health information other than in accordance with section 6(1) of the Regulation or if an unauthorized person accessed the personal health information; to specify the procedures to be followed with respect to the identification, investigation, containment, notification and prevention of a similar unauthorized access, use, disclosure or disposal; to specify the responsibilities of SSHA and these third parties with respect to monitoring for unauthorized access, use, disclosure or disposal of personal health information; and to specify the restrictions and conditions that these third parties are required to comply with in order to enable SSHA to comply with section 6 of the Regulation.

27. Amend agreements to require third parties retained to assist SSHA in providing services to health information custodians to acknowledge that they have read, understood and agree to comply with the Enterprise Privacy Policy, the Enterprise Security Policy, the Information Classification and Handling Policy and the Enterprise Risk Management Policy and to append these policies to the agreements.

28. Amend agreements with third parties retained to assist SSHA in providing services to health information custodians to ensure that the protection afforded to Confidential Information that is personal health information is consistent with section 9(1) of *PHIPA*.

29. Develop and maintain a database of all agreements with third parties retained to assist SSHA in providing services to a health information custodian in order to monitor whether agreements have been entered into with each third party and are up-to-date and in order to act as a central repository for such agreements.

30. **Immediately develop and enter into standard form agreements with each health information custodian to whom services are provided, in accordance with the recommendations set out in this report.**

31. On a going forward basis, prior to providing services to a health information custodian involving personal health information, ensure that standard form agreements have been executed with each applicable health information custodian as described in this report.

32. Amend and re-execute existing agreements with health information custodians to clearly specify the status of SSHA under *PHIPA* and the Regulation in providing services to the health information custodian in respect of personal health information, the obligations imposed on SSHA as a result of its status and how SSHA will be addressing each of these obligations, and to include an acknowledgement of SSHA's obligations under section 6(1) of the Regulation.

33. Develop and maintain a database of all agreements with health information custodians in order to monitor whether agreements have been entered into with each health information custodian and are up-to-date and in order to act as a central repository for such agreements.

34. Revise policies and practices in accordance with the requirements under section 6(3)5 of the Regulation with respect to performing assessments of how the services provided by SSHA may affect the privacy of individuals who are the subject of the information.

35. Where SSHA is acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, immediately perform or update existing privacy impact assessments in relation to the services provided, and provide health information custodians with written copies of the results of the privacy impact assessments including: the action taken or to be taken by SSHA to address the risks

to privacy, and the timelines for taking such action, as required under section 6(3)5 of the Regulation.

36. On a going forward basis**,** prior to providing any services to a health information custodian, perform privacy impact assessments in relation to the services provided and provide health information custodians with a written copy of the results of the privacy impact assessments.

37. Develop and implement a policy, and provide a copy to all health information custodians to whom services are provided, setting out the circumstances where a privacy impact assessment will be performed, those circumstances where a "privacy review" as opposed to a privacy impact assessment will be performed and the rationale for performing a "privacy review" as opposed to a privacy impact assessment.

38. Work directly with the Ministry of Health and Long-Term Care, the health information custodian community, and other stakeholders to ensure that the privacy of individuals whose personal health information is subject to the services provided by SSHA is protected and to ensure that the confidentiality of that information is maintained, by requiring end-to-end privacy impact assessments, prior to SSHA providing a product or service.

39. Until a process is implemented to require end-to-end privacy impact assessments, advise health information custodians to whom services are provided of the scope and limitations of any privacy impact assessment conducted by SSHA and the risks to health information custodians, SSHA and to the privacy of individuals whose personal health information is subject to the services provided that may result from those limitations.

40. Communicate the scope, limitations and associated risks of any privacy impact assessments conducted by SSHA in the agreements entered into with the health information custodians to whom services are provided, in the privacy impact assessments themselves, and in the written copies of the results of the privacy impact assessments that are required to be provided to each applicable health information custodian pursuant to section 6(3)5 of the Regulation.

41. Include in all privacy impact assessments and privacy reviews and the written results of the privacy impact assessments provided to health information custodians, pursuant to section 6(3)5 of the Regulation, a comprehensive discussion of all the risks to the privacy of the individual who is the subject of the information and the strategies to minimize these risks.

42. Include in all privacy impact assessments and privacy reviews and the written results of the privacy impact assessments, provided to health information custodians, a time frame for SSHA to implement the recommended strategies to minimize the risks to privacy identified.

43. On a regular basis, update the privacy impact assessments conducted by SSHA and the written results of the privacy impact assessments provided to health information custodians to identify the continuing risks to privacy resulting from the services, to address when or whether recommended strategies were implemented to minimize the risks to privacy previously identified and to address whether these strategies in fact minimized or mitigated the risks identified.

44. Develop and maintain a database to monitor whether privacy impact assessments have been conducted for each service provided by SSHA, to ensure that the privacy impact assessments that have been conducted are up-to-date, to track whether copies of the results of the privacy impact assessments have been provided to health information custodians, and to act as a central repository for such privacy impact assessments.

45. Ensure that the privacy impact assessments and the written results of the privacy impact assessments refer to *PHIPA* and the Regulation and clearly set out the status of SSHA under *PHIPA* and the Regulation, the obligations imposed on SSHA as a result of its status under *PHIPA* and the Regulation, how SSHA is or will be addressing each of its obligations, and how addressing each of these obligations will minimize the risks to the privacy of individuals.

46. Revise policies and practices in accordance with the requirements under section 6(3)5 of the Regulation with respect to assessments of the threats, vulnerabilities and risks to the security and integrity of personal health information as a result of the services provided by SSHA.

47. Where SSHA is acting as a health information network provider or as a third party who provides services to assist a health information network provider in providing services to a health information custodian, immediately perform or update existing threat, vulnerability and risk assessments in relation to the services provided, and provide health information custodians with written copies of the results of the threats, vulnerability and risk assessments including: the action taken or to be taken by SSHA to minimize or mitigate these threats, vulnerabilities and risks, and the timelines for taking such action, as required under section 6(3)5 of the Regulation.

48. On a going forward basis**,** prior to providing any services to a health information custodian, perform threat, vulnerability and risk assessments in relation to the services provided and provide health information custodians a written copy of the results of the threat, vulnerability and risk assessments.

49. Include in all threat, vulnerability and risk assessments and the written results of such assessments provided to health information custodians a time frame for SSHA to implement the recommended strategies to minimize the threats, vulnerabilities and risks to the security and integrity of the personal health information identified.

50. On a regular basis, update all threat, vulnerability and risk assessments and the written results of such assessments provided to health information custodians to identify the

ongoing risks to the security and integrity of the personal health information resulting from the services, to address when or whether recommended strategies were implemented to minimize the threats, vulnerabilities and risks previously identified, and to address whether these strategies in fact minimized or mitigated the threats, vulnerabilities and risks identified.

51. Develop and maintain a database to monitor whether threat, vulnerability and risk assessments have been conducted for each product or service provided by SSHA, to ensure that the threat, vulnerability and risk assessments that have been conducted are up-to-date, to track whether copies of the results of the threat, vulnerability and risk assessments have been provided to the health information custodians, and to act as a central repository for such threat, vulnerability and risk assessments.

52. Make privacy and security training mandatory and ensure that this training includes an overview of *PHIPA* and the Regulation as it relates to the work of SSHA, as described in this report and provide updated training when the privacy and security policies and procedures are revised.

53. Implement a procedure to track which employees have received privacy and security training in order to ensure that appropriate action can be taken with respect to those employees who have not received such training.

54. Revise the document entitled, *Products and Services – Privacy and Security* to describe the general safeguards in place to protect against unauthorized use and disclosure and to protect the integrity of the information and to describe the safeguards implemented in relation to the security and confidentiality of the information.

55. When acting as a health information network provider, prior to providing services, pursuant to section 6(3) of the Regulation provide each applicable health information custodian with a plain language description in accordance with section 6(3)2 of the Regulation as opposed to simply making such a plain language description available on the SSHA website.

56. Update the "plain language descriptions" required pursuant to sections 6(3)2 and 6(3)3 of the Regulation when necessary to ensure that health information custodians to whom services are provided and Ontarians whose personal health information has been entrusted to SSHA, have current descriptions of the services being provided.

57. Immediately provide to applicable health information custodians updated, "plain language descriptions" of the services provided by SSHA as required pursuant to sections 6(3)2 of the Regulation.

58. Immediately make available to the public updated, "plain language descriptions" of the services provided; any directives, guidelines and policies that apply to the services; and a general description of the safeguards implemented in relation to the

security and confidentiality of the information on the website of SSHA as required pursuant to section 6(3)3 of the Regulation.

59. When developing the proposed corporate brochure, include a plain language description of the services provided and a description of the safeguards that have been put into place to protect against unauthorized use and disclosure of personal health information and to protect the integrity, security, and confidentiality of the information.

60. Consider using SSHA's privacy portal as a vehicle for fulfilling SSHA's obligations under the Regulation to inform both health information custodians and the general public about its products and services.

61. In addition to the Enterprise Privacy Policy and the Enterprise Security Policy, post the written results of privacy impact assessments and threat, vulnerability and risk assessments on both the SSHA website: www.ssha.on.ca and on the privacy portal: www.privacy.ssha.on.ca or, alternatively, post these documents on the privacy portal and provide a direct link from SSHA's website: www.ssha.on.ca to the privacy portal: www.privacy.ssha.on.ca.

62. Where SSHA is providing hosting services and is not acting as a health information network provider, the agreements entered into, with health information custodians to whom the services are provided, should specify the type of monitoring or logging that SSHA is able to provide, the information that this type of monitoring or logging is able to provide, and the limitations of this type of logging or monitoring.

63. Where SSHA is acting as a health information network provider, the agreements entered into with health information custodians to whom the services are provided should formally define and document the extent and manner in which electronic records of accesses and transfers in accordance with section 6(3)4 of the Regulation will be made available; how a health information custodian may request these electronic records from SSHA; the content of these electronic records; which accesses and transfers will be logged, monitored and reported on; the information that this type of monitoring and logging is able to provide to health information custodians; and the limitations, if any, on this type of monitoring and logging.

64. Where SSHA is acting as a health information network provider, immediately implement practices and procedures relating to monitoring accesses and transfers to enable SSHA to keep and make available to a health information custodian upon request, to the extent and in a manner that is reasonably practical, these electronic records pursuant to section 6(3)4 of the Regulation.

65. Develop and implement an integrated organization-wide business continuity and disaster recovery framework.

66. Develop and implement comprehensive security monitoring and management policies and practices, combined with robust security procedures and supported with tools and

techniques to detect, record, report, investigate, and respond effectively to privacy and security incidents.

67. Develop and implement procedures to receive and respond to complaints or inquiries about SSHA's practices relating to personal information and personal health information.

68. Develop and implement procedures to record, track and monitor response times for investigating and resolving privacy questions and complaints and to monitor the types of issues about which questions are raised or complaints made in order to analyze trends and recommend changes to SSHA's Enterprise Privacy Policy and Enterprise Security Policy, based on this analysis.

69. Ensure that all potential privacy and security issues that could arise in the context of SSHA providing goods and services to health information custodians are addressed through appropriate policies and procedures, prior to offering services, and that health information custodians are made aware of these policies and procedures, prior to receiving these goods or services.

70. Develop and implement comprehensive policies and procedures for the retention and disposal of personal health information.

71. Develop and implement a comprehensive privacy and security internal audit program.

72. Conduct an external audit of both the privacy and security programs prior to January 1, 2008, in accordance with SSHA's own policies.

73. Refrain from using the terms "certification" and "accreditation", unless SSHA is able to develop or adopt a set of clearly defined, objective standards for evaluation that are validated by an independent third party having the appropriate credentials for certification and accreditation.

74. Ensure that all risks that have been identified are recorded and tracked through the risk register.

75. Reconvene meetings of the Risk Management Committee to review, address and manage risks, in order to ensure that these risks are formally shared, documented, reported on and resolved.

76. When assessing risks, take into consideration the many potential impacts upon the individuals, to whom the personal health information relates, as a result of various threats, vulnerabilities and risks.

77. Seek direction from the Board of Directors of SSHA in defining its "risk appetite and risk tolerance" as discussed in this report and communicate this to the organizational units of SSHA.

78. Amend the Information Classification and Handling Policy and Enterprise Risk Management Policy in accordance with the "risk appetite and risk tolerance" of the Board of Directors of SSHA, and in a manner that does not interfere with SSHA's ability to fulfill its obligations under *PHIPA*.

79. Develop and implement a program to deal credibly with the current strategic, operational, program and project-specific risks before proceeding with the development and rollout of any newly managed programs and services, such as ONE web and ONE mail and new products, such as a voluntary electronic health record.

80. Foster a culture of privacy throughout the organization, to help ensure that privacy is woven into all day-to-day operations.

81. For those recommendations where the timing for the implementation is deemed to be immediate, provide a status report to the Ministry of Health and Long-Term Care three months after the date that this report is issued and every three months thereafter, until each of those recommendations have been addressed.

82. For those recommendations where the timing for the implementation has not been deemed to be immediate, provide a plan for implementing the recommendation, including benchmarks and time line for completion, to the Ministry of Health and Long-Term Care six months after the date that this report is issued and a status report every six months thereafter, until each of those recommendations have been addressed.

APPENDIX

Examples of Documents Reviewed

Certifications

One™ Hosting Certification and Accreditation Report, Version 9 (draft), June 8, 2006

One™ Network Certification and Accreditation Report, Version 9 (draft), June 8, 2006

Third Party Agreements

Hosting Services Module Agreement between Smart Systems for Health Agency (SSHA) and a Board of Health

Autism Services Agreement between Smart Systems for Health Agency (SSHA) and a Child and Family Services Organization

Human Resources

SSHA Privacy Orientation, July 2004

Privacy: Making it Real (Training)

Smart Systems for Health Security Awareness: BE SMART, Be Aware, Be Secure (Training)

Risk Management Framework (Training), August 17, 2006

Privacy

Enterprise Risk Management Policy, Version 2 (Draft), October 17, 2006

Enterprise Privacy Policy, Policy No: PSO-002, Version 3, December 7, 2004

Information Classification and Handling Policy, Policy No: PSO-003, Version Date March 30, 2004

Security

Enterprise Security Policy, Policy No: PSO-001, Version Date March 30, 2004

SSHA Position Paper: Safeguarding Sensitive Information, Version 0.04 (Draft), September 19, 2006

iPHIS Security Opinion RDIS, December 12, 2005

Information Security Threat and Risk Assessment SEH Phase 2 ONE Mail Direct, Version 0.05 (Draft), May 4, 2006

Smart Systems for Health Agency End to End Threat and Risk Assessment Iteration 2: TRA for eWAN, Final Version 1.0 (not signed), February 9, 2005

Security Department, PSRD Information Disposal Guideline (for electronic media), Version 1.0 (Approved), September 20, 2005