Report to the Information and Privacy Commissioner of Ontario (IPC) on the Ontario Smart Systems for Health Agency's Compliance with the IPC's Privacy and Security Recommendations

Prepared by:
David H. Flaherty, Ph.D.

David H. Flaherty Inc.
Privacy and Information Policy Consultants
1939 Mayfair Drive
Victoria, BC V8P 1R1
Canada
250-595-8897
250-595-8884 (fax)
David@Flaherty.com

October 20, 2007

Table of Contents

Executive Summary

The Table of Contents on the previous page lays out the contents of this report.

This report from an independent consultant addresses the state of readiness of Smart Systems for Health Agency (SSHA) to complete the transition of the Ontario Electronic Master Patient Index (EMPI) from Cancer Care Ontario (CCO) to SSHA and the state of SSHA's progress with respect to implementation of the 82 recommendations of the Information and Privacy Commissioner of Ontario (IPC).

The first major finding of this report is that there are no privacy and security reasons to hinder complete transfer of the operations of the EMPI from CCO to SSHA (recognizing that the control of the EMPI will continue to rest with the Ontario MOHLTC).

The IPC conducted a privacy review of SSHA between October 2006 and March 2007, which made 82 recommendations to improve SSHA's data protection practices. The privacy review was conducted at the request of the government of Ontario in order to ensure a high level of data protection as it moves forward in transforming health care services through the use of information technology.

The overall conclusion of this report is that SSHA has made demonstrable progress towards full compliance with the privacy and security recommendations of the IPC, and that SSHA currently understands privacy and security issues both in terms of conceptualization and the need to operationalize a wide variety of policies and procedures over time. However, SSHA must continue to examine the adequacy of the human and financial resources at the disposal of its Privacy and Security Division. The consultant is of the view that the current cadre of personnel will be hard pressed to meet the important demands of the Ontario MOHLTC and the IPC going forward, especially with respect to the detailed implementation of many policies, processes, and procedures that SSHA now has in place, or has on the verge of being in place.

The March 16, 2007 IPC Review of SSHA

Section 6.1 of Ontario Regulation 329/04 under the Ontario *Personal Health Information Protection* Act (PHIPA) mandated the IPC review of SSHA. The IPC found major deficiencies in the following 24 categories, which led to 82 specific recommendations on the following topics:

- INSUFFICIENT PRIVACY AND SECURITY DOCUMENTATION
- RESPONSIBILITY FOR PRIVACY AND SECURITY
- ENTERPRISE PRIVACY POLICY
- ENTERPRISE SECURITY POLICY
- DRAFT INFORMATION SECURITY POLICIES, OPERATING DIRECTIVES, STANDARDS OF PRACTICE AND GUIDELINES
- INFORMATION CLASSIFICATION AND HANDLING POLICY
- ASSET MANAGEMENT POLICY
- ACKNOWLEDGEMENT OF CONFIDENTIALITY
- ENTERPRISE PRIVACY POLICY ACKNOWLEDGEMENT AND ENTERPRISE SECURITY POLICY ACKNOWLEDGEMENT
- AGREEMENTS WITH THIRD PARTY SERVICE PROVIDERS
- AGREEMENTS WITH HEALTH INFORMATION CUSTODIANS
- PRIVACY IMPACT ASSESSMENTS [7 subheadings]
- THREAT, VULNERABILITY AND RISK ASSESSMENTS [3 subheadings]
- PRIVACY TRAINING
- PLAIN LANGUAGE DESCRIPTIONS
- ELECTRONIC RECORDS OF ACCESS AND TRANSFERS
- INTEGRATED DISASTER RECOVERY AND BUSINESS CONTINUITY FRAMEWORK
- PRIVACY/SECURITY BREACHES AND INCIDENTS
- PROCEDURE FOR RECEIVING AND RESPONDING TO PRIVACY QUESTIONS/COMP LAINTS
- PRIVACY AND SECURITY POLICIES RELATING TO SSHA SERVICES

- o RETENTION AND DISPOSAL POLICIES AND PROCEDURES
- o INTERNAL/EXTERNAL AUDITS
- o NON-CREDIBLE CERTIFICATION AND ACCREDITATION SERVICES
- o RISK TOLERANCE AND MANAGEMENT

The July 25, 2007 SSHA Briefing to the IPC and its Aftermath

SSHA briefed the IPC on the above date with respect to its progress on implementing the 82 recommendations, its recent reorganization, and its establishment of its Privacy Change Initiative Project Management Office (PCIPMO). As listed below, SSHA organized the IPC recommendations into nine basic streams and a larger number of sub-streams with its own timing estimate for compliance for each. It also reported on its progress to date on such issues as leadership, culture, planned developments for the next quarter, and next steps. One immediate consequence, as discussed in the next section, was a letter to SSHA from Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario.

The Issue of the Transfer of the Enterprise Master Patient Index (EMPI) from Cancer Care Ontario (CCO) to SSHA

The intent is that SSHA will act as an agent on behalf of the Ontario Ministry of Health and Long-Term Care (MOHLTC) in operating the EMPI. SSHA will hire existing staff from Cancer Care Ontario (CCO) and house them within a single, secure location at SSHA's downtown Toronto offices. It will physically separate EMPI staff from its other program areas by having a segregated office. SSHA is also committed to adopting most of the existing privacy and security policies and procedures developed at CCO for the EMPI. In the case of differing standards, SSHA will adopt the higher standard.[1] See Appendix 3.

In her letter to SSHA of July 30, 2007, Dr. Ann Cavoukian, Ontario's Information and Privacy Commissioner, indicated that her support for the EMPI transfer would not be forthcoming until her office reviewed two Privacy Impact Assessments (PIAs) for the EMPI transition that SSHA had commissioned. She also indicated that she had retained the present consultant to provide "confirmation from a trusted, independent third party that SSHA is on target for satisfactorily completing the implementation of 70 per cent of the IPC's recommendations by September 30, 2007 and 84 per cent of our recommendations by March 31, 2008, and that once the transfer [of the EMPI] has taken place, the privacy and security safeguards for the EMPI will be equivalent to those in place at CCO."[2] She expected the consultant "to act as our trusted, independent third party to obtain these assurances."

[1] Letter from Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, to Michael Power, SSHA, July 30, 2007.

[2] Letter from Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, to Michael Power, SSHA, July 30, 2007. These percentage figures for compliance were in the SSHA briefing of the IPC on July 25, 2007.

The Commissioner noted that IPC recommendation 79 further emphasized the importance of a follow-up review of SSHA compliance. It reads:

> 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 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.

Based on this recommendation, the Commissioner concluded that it would clearly be difficult for the IPC to support the transition of the EMPI to SSHA in the absence of a follow-up review.

The IPC Instructions to David H. Flaherty to Conduct an Independent Review

The consultant shall conduct a comprehensive and independent review of:

(a) the state of SSHA's compliance with any and all of the IPC recommendations, which were set out in the Review, including whether or not, in his sole and independent view, the representation of SSHA that ten per cent of the recommendations are already implemented; 90 percent are in progress; 70 per cent will be completed by September 30, 2007 and that 84 per cent will be completed by March 31, 2008, is substantiated in whole or in part by his review

(b) the adequacy of safeguards set in place by SSHA in regard to the EMPI and, in particular, whether or not they are equivalent or superior to those that have been in place at CCO in regard to the EMPI.

The consultant has endeavoured to follow these instructions to the fullest extent possible. He has also kept the IPC informed of relevant developments through periodic written and oral briefings.

SSHA Briefings for David H. Flaherty, Aug. 20-23, 2007 and Sept. 11-13, 2007

August 20, 2007: Subject Matter of Meetings

Addressing the IPC Recommendations
EMPI Status
IPC Recommendations 2, 38, 14, 28, 64, 4, 1, 24, 29, 26, 27, 18-23

August 21, 2007: Subject Matter of Meetings

Site Visit to the SSHA Component of the Hewlett Packard Data Centre, Markham, Ontario
EMPI Transition Strategy

SSHA's Access Controls Management for the EMPI
Privacy Impact Assessments for the EMPI

August 22, 2007: Subject Matter of Meetings

Information Security
Threat Risk Assessment for the EMPI

Sept. 11, 2007: Subject Matter of Meetings

Privacy Assurance Process
Privacy Impact Assessment Methodology
Enterprise Privacy Policy
Privacy Culture
Privacy and Security Awareness Month
Privacy Complaints
SSHA Vendor Agreements and Privacy Breach Process
SSHA Client Agreements

Sept. 12, 2007: Subject Matter of Meetings:

EMPI Transition Team
Information Security Team
Privacy Training
Privacy and Security Standard of Conduct
EMPI Threat Risk Assessment

Sept. 13, 2007: Meetings with:

President and Chief Executive Officer, and Vice-President, Privacy and Security
Vice-President, Privacy and Security
Director, Information Security, and an IT Security Consultant, about the Threat Risk Assessment for the EMPI

In addition to these on site meetings, the consultant also interacted with various SSHA personnel by means of telephone, e-mail, and in person discussions since the initiation of this review process. He has received admirable cooperation and assistance.

SSHA supplied the consultant with voluminous documentation for its compliance activities. See appendices 1 and 3. In each instance, the consultant provided candid comments on these materials to SSHA as he was reviewing them, at least until the final deliverables at the end of September/early October 2007.

Snapshot of the Report

The basic finding of this report is that SSHA has made very good progress towards full compliance with the privacy and security recommendations of the IPC. Details will follow later in the body of this report and in references to SSHA documentation of its compliance efforts. In particular, SSHA has dealt at least adequately with all of the highlighted recommendations that were for immediate action in the IPC report.

The second major finding of this report is that there are no privacy and security reasons to hinder complete transfer of the operation of the EMPI from Cancer Care Ontario to SSHA (recognizing that the control of the EMPI will continue to rest with the Ontario MOHLTC).

SSHA already houses most of the operations of the EMPI, including holding EMPI data in servers at the two SSHA data centres. In addition, EMPI staff is already working at borrowed SSHA offices, and SSHA's operation of access control for EMPI users. Positive general arguments in favour of the complete transfer include the prospect of SSHA addressing and managing data quality issues with EMPI data and also enhancing information security.[3]

Points of Emphasis in the Report

At present, SSHA's Ontario Network for e-Health (ONE) provides, as a health information network provider under PHIPA, such services as ONE Network, ONE Mail (secure e-mail), and ONE Hosting. However, SSHA further states that a number of its other products and services, including ONE ID, ONE Pages, and ONE Portal, do not involve any collection, use, or disclosure of personal health information. ONE Support, SSHA also states, collects minimal personal health information for its registration services. At present, SSHA has custody of relatively little personal health information.

However, the EMPI is only the first of several significant, large administrative databases that the Ontario MOHLTC appears intent on moving into the custody of SSHA as its agent, which will mean that SSHA will begin to receive, use, disclose, and retain much more personal information than it has in the past. The Ontario Laboratory Information System (OLIS) already houses its data in SSHA data centres and will likely transfer full custody to SSHA. Of course, this heightens even further the emphasis that the IPC has placed on the need for robust data protection and security at SSHA for all of its operations, including those involving personal information and personal health information.

With respect to the EMPI itself, there is considerable pressure from the Ontario MOHLTC and health information custodians for an active Client Registry (CR) that can be rolled out to hospitals and other health information custodians across the province over time.[4] There are also significant digital imaging

[3] See the discussion below and Sextant [Ross Fraser and Pat Jeselon], "A Privacy Impact Assessment (PIA) on the Ontario Enterprise Master Patient Index Application," prepared for SSHA, draft, Aug. 17, 2007, revised August 22, 2007, 66 pp.; and Ontario, SSHA, Information Security Department, Privacy and Security Division, "Conceptual Threat and Risk Assessment. EMPI Transition," 70 pages, plus 1 appendix. Author: Mugino Saeki, Sept. 12, 2007.

[4] SSHA has renamed the EMPI as the Client Registry.

(PACS) operations across Ontario that would like to use such a provincial client registry for the purpose of accurately and uniquely identifying patients.

SSHA has the potential to be the provincial leader in ensuring robust privacy and security standards for provincial e-Health applications and for sharing its expertise, on an interactive basis, with health information custodians. In my judgment, SSHA's privacy and security specialists have a solid understanding of what needs to be achieved on an ongoing basis with respect to implementation. The new CEO and executive team, supported by a new Board of Directors, are driving this leadership role and want to achieve best industry standards in these two critical domains of privacy and security.[5]

At present, it is also important to emphasize that no more than five per cent of SSHA's staff has ever authorized access to identifiable personal information or personal health information. They do not "need to know" such information to do their jobs. Thus, to take an easy example, the CEO and the VP, Privacy and Security, do not have such access. Ninety-nine per cent of the time, the Information Security staff of seven persons similarly does not access personal information. The reality is that compared to a hospital, or other health information custodian under the authority of PHIPA, very few SSHA staff has such access. It is much like a Fort Knox that protects and secures its gold bullion for purposes of controlled disclosures to authorized borrowers. Like Fort Knox, SSHA is no longer legally responsible for its gold bullion (various forms of information) once it is legitimately withdrawn. SSHA can also be compared to a central bank with significant privacy and security concerns for multiple purposes, including fraud prevention, but SSHA does not own or operate its own branches at present; its clients and customers, especially hospitals, are independent of SSHA. Nor, it might be added, does SSHA have the sophisticated methods of fraud detection that banks currently have in place, which benefit privacy and security requirements as well, through real-time auditing.[6]

Fortunately, for purposes of controlled data sharing among health information custodians, such as hospitals, and their agents, like SSHA, the umbrella of PHIPA creates the legal regime controlling the entire enterprise of the delivery of Ontario health care for purposes of collection, use, disclosure, and retention of personal information in any form (excluding SSHA employee information). Thus the privacy and security rules that require detailed implementation by SSHA and health information custodians of every type exist across the Ontario health care landscape.

SSHA is an agent of the Ontario MOHLTC and also acts in various capacities for health information custodians, in particular, under PHIPA. SSHA can only do what it is told to do by its political and bureaucratic masters, who, in most cases, remain the bureaucratic and legal *controllers* of the personal information that is in the *custody* of SSHA.

Highlights of SSHA Performance on the IPC's Privacy and Security Recommendations

SSHA has promulgated an integrated "Privacy and Security Standard of Conduct" (18 pp.) that, with very few exceptions, all SSHA personnel, including executives, full-time and part-time employees,

[5] See "Message from the CEO," ONE News, Sept. 2007, p. 1, which begins: "Protecting privacy is critical for our business. SSHA hosts and transports more personal health information than any other organization in Ontario."

[6] The largest Canadian bank is only now introducing such auditing for its tellers' uses of personal information.

consultants, contract employees, as well as employees of vendors who work for SSHA, have to sign.[7] Almost 600 staff of full-time equivalents and consultants is required to comply (as will all new hires in future). The Standard is a component of SSHA's Privacy and Security Training and Awareness strategy. [Recommendations 9, 10, 18, 19, 22, 23, 52, 53.] Almost all staff signed and returned the acknowledgement form by October 1, 2007.

SSHA has developed, and made available to the consultant, the following set of comprehensive privacy and data protection policies, which are more than adequate for current purposes of compliance with the IPC's recommendations: [Recommendations 1, 3, 5, 6, 7, 8.]

- The SSHA Privacy and Data Protection Policy (16 pp.).
- The following existing policies are subordinate to this 'mother' policy and must be read in conjunction with it.[8]

    1. SSHA Health Information Network Provider [Privacy] Policy (14 pp.) [SSHA's dominant role].
    2. SSHA Electronic Service Provider [Privacy] Policy (12 pp.) [SSHA's infrequent role].
    3. SSHA Third Party Retained by a Health Information Network Provider [Privacy] Policy (to assist Health Information Custodians) (14 pp.) [SSHA's infrequent role].

SSHA has a strong information security team of seven cross-trained staff, with considerable and relevant experience in other sectors, especially banking. It has released a revised Information Security Policy and related procedures.[9] [Recommendations 1, 2, 3, 5, 7, 9, 10, 11.]

SSHA has developed, and is rolling out for all staff in October and November, 2007, two separate modules of online training on privacy and security fundamentals.[10] [Recommendations 4, 10, 52, 53.] In the experience of the consultant, the quality of the presentation is sufficiently robust and engaging, especially with respect to illustrating the multiple roles of SSHA under PHIPA. The two courses are mandatory for everyone who works on SSHA premises – from senior executives, through to part time staff, consultants and contractors.[11] [Recommendation 10, 52.]

The two new modules of privacy and security training at SSHA are role based. In compliance with the IPC's recommendation 52, SSHA has made privacy and security training mandatory and ensured that it includes an overview of PHIPA and its Regulations as they relate to SSHA's work and multiple

[7] See Ontario, SSHA, "Privacy and Security Standard of Conduct," Document Identifier: 00895, Version: 1, Owner: Michael Power. (19 pp.)

[8] The Privacy Office at SSHA is also in the process of developing a comparable 'daughter' policy for the Ontario *Freedom of Information and Protection of Privacy Act* and an employee privacy policy. SSHA is also adopting and adapting the Cancer Care Ontario privacy policy for the EMPI application, where SSHA will be acting as an agent of the Ontario MOHLTC.

[9] See Ontario, SSHA, "Information Security Policy," Policy No. PSO-001, Document Identifier 867, Version 3.0, Owner: Director of Information Security (16 pp.), March 30, 2007.

[10] See SSHA, "Privacy Training. Presentation to David Flaherty, Sept. 12, 2007." Black binder with a complete presentation deck copy of PowerPoint, 7 slides, and a complete copy of the training modules, and additional material to be catalogued later as required. It is called the *Learning Management System*.

[11] Michael Power, VP, Privacy and Security, adds that "the courses are a crucial part of the extensive work we are undertaking to position SSHA as a leader in e-Health." SSHA, ONE News, Sept. 2007, p. 1.

roles.[12] With respect to IPC recommendation 53, SSHA has implemented procedures to track staff who have, and have not, received privacy and security training. The training is thorough, systematic, and sufficiently robust and involved considerable investment of talent and resources. All staff are expected to complete the training by December 1, 2007.

SSHA declared September, 2007 to be Privacy and Security Awareness Month featuring a novel set of posters, coffee mugs, and coffee events on specific floors. This was a component of its desire to promote and advance an organizational culture of privacy at SSHA.[13] It wants to promote strongly the positive behaviours it expects of all personnel as described in the Standard of Conduct. The tagline of the posters is therefore, "get caught," doing something good. The initiative is being resourced to continue to 'catch' people and to keep the collateral fresh and rotated on an ongoing basis. There is also a privacy and security direct dial hotline available from everyone's phone at SSHA and an e-mail address for the same purpose.[14]

SSHA's Privacy and Security Division has developed an Enterprise Security and Privacy Incident Management (ESPIM) system.[15] [Recommendation 66.]

SSHA's Privacy and Security Division has also developed a Privacy Complaint, Inquiry, Compliment, and Suggestion Handling Policy.[16] [Recommendations 67, 68.]

SSHA has developed new and revised Privacy Assurance Services, which include a new set of roadmap, documentation, and processes with respect to the conduct of End-to-End Privacy Impact Assessments and Threat Risk Assessments.[17] See the lengthy list of "Privacy Assurance Service Processes" in Appendix 1 below. The goal was to respond to the recommendations of the IPC to the effect that SSHA was not always assuring appropriate privacy review of multiple issues. [Recommendations 34-37, 41-45,

[12] The consultant reviewed the following training materials both online and in hard copy: 1) the five roles and responsibilities of SSHA under Ontario privacy legislation; 2) training on "privacy fundamentals" for SSHA new hires and consultants, 2007 (33 PowerPoint slides); 3) "Privacy Fundamentals Feedback: New Hires /Consultants, In-Class Training, January to June 2007," Version 1.0, August 23, 2007, 4 pp.; 4) "SSHA Role Based Privacy Training for Client Registry Operations Team," [EMPI], Sept. 2007, working draft, 36 PowerPoint slides; [use in EMPI section as well]; 5) "Role Based Privacy Training. Privacy Training for SSHA Contact Centre Support Staff, 2007," v2, 38 PowerPoint slides; 6) "Privacy Fundamentals," online training course module, 19 screens, including review questions, click on buttons for additional information, and a final quiz; 7) "Privacy Legislation," online training course module, 30 screens, including image, information, and click on buttons for additional content, links to relevant privacy policies and procedures, and review questions; 8) "Privacy Incident Handling," online training course module, 41 screens, including image, information, and click on buttons for additional content, review questions, and reference materials; and 9) "Privacy Fundamentals Quiz," online training course module, 20 screens of questions.

[13] See SSHA, "Privacy and Security Awareness Campaign," September, 2007, PowerPoint, 21 pp. including copies of the new posters (which were also delivered in hard copy to the Ontario IPC); and SSHA, "Privacy Culture. Presentation to David Flaherty, September 11, 2007," 8 PowerPoint slides, in a small white binder with 3 tabs.

[14] E-mail communication, Jane Dargie, Director, Privacy, SSHA, to David H. Flaherty, August 30, 2007.

[15] See Ontario, SSHA, "Enterprise Security and Privacy Incident Management (ESPIM) Plan and Capability," Aug. 23, 2007. PowerPoint, nine slides.

[16] See SSHA, Privacy Team, "Complaints, Inquiries, Compliments and Suggestions," Sept. 11, 2007, PowerPoint in a white binder, with six tabs.

[17] See SSHA, Information Security Team, "Privacy Assurance Service Process, Presentation to David Flaherty, Sept. 11, 2007, PowerPoint, 6 slides; SSHA, "Privacy Process & Privacy Impact Assessment (PIA) in Product/Service Design at SSHA," large white binder with 30 tabs; and Ontario, SSHA, Information Security Department, "End-to-end Threats and Risk Assessment (TRA) Process at SSHA. Understanding Information Security Assurance and Compliance." Version 1.0 (August 20, 2007), 13 pp.

61, 69: Privacy Assurance Services/ Privacy Impact Assessments**.**] Thus the Privacy team has developed *processes* to help staff of the agency know when privacy issues exist that need to be addressed. These are particular concerns for project teams, legal services, communications, and client services at SSHA. The key decision for privacy assurance at SSHA is whether to conduct, or update, a Privacy Impact Assessment. For this purpose, a series of thirty-one checkpoints exist.

The privacy assurance service will confirm that the solutions SSHA is developing are privacy compliant and identify and communicate the risks and mitigation plans to appropriate parties. The primary vehicle for this purpose is PIAs that are executed before services are provided, documented, updated as required, and reported to the appropriate clients, including the Ontario MOHLTC and health information custodians.[18]

As further discussed below, the two new lawyers in the Legal Department of SSHA have developed new client agreements for health information custodians, including hospitals and physicians.[19] [Recommendations 30-33]

SSHA is reworking its vendor, service provider, and partner agreements and its RFP procurement language for privacy and security purposes. [Recommendations 24-29.] See the discussion below.

Finally, the Risk Management Committee of senior executive has now held two meetings; it reports to the Audit Committee of the Board of Directors. [Recommendations 75, 77.]

In passing, it should be satisfying to the IPC that SSHA has made sufficient progress on most of the 82 recommendations in a relatively short period of time.

Highlights of Privacy and Security Issues Associated with the EMPI Transition

As noted above, SSHA is already operating and hosting, registration, help desk, and access control functions for the EMPI (which is not yet being used as an active client registry).

Anzen Consulting Inc., working with CCO, prepared a series of privacy policies for the EMPI application that are especially well done. SSHA intends to adopt all of these policies for its own management of the EMPI. See Appendix 3. Most of them need to be updated to reflect the fact that SSHA will now be the "agent" of the MOHLTC (not CCO). Sextant Software developed the security policy for the EMPI. This policy will be replaced by SSHA's security program.

The current Wait-Time and EMPI Privacy Lead at CCO is an Anzen consultant who does the work on a part-time basis. SSHA will consider bringing over this resource for the EMPI during a transition period. SSHA will simply transfer from CCO the relatively mature privacy management in place for the EMPI.

[18] See SSHA, Information Security Team, "Privacy Assurance Service Process, Presentation to David Flaherty, Sept. 11, 2007, PowerPoint, 6 slides.

[19] See legal-sized file of client agreements revised by the Legal Department of SSHA (estimate of 100 pp.)

The SSHA Information Security team dedicated a full-time staff person, for a year, to prepare a sophisticated Threat Risk Assessment for the EMPI at CCO.[20] This TRA describes more than the usual run of security issues for the EMPI installation at SSHA, including issues of security governance, and recommends that SSHA assign a full-time security person for the EMPI at SSHA for a period of one year. SSHA has also retained a consultant to do vulnerability testing for the EMPI.

SSHA commissioned two Privacy Impact Assessments of the EMPI transition to SSHA, both of which were reviewed carefully for purposes of this report.[21] The PIA commissioned by SSHA on the EMPI serves to provide privacy and security guidance on the scope of the EMPI for applications beyond the Wait Times Information System, its only current user. The SSHA revisions to both PIAs also include the mitigation strategies and plans that SSHA is currently contemplating, as part of its transition planning, to manage these risks. These mitigation strategies are a work in progress and change daily as consultation processes continue with software suppliers and client registry specialists from other provincial governments and the private sector to address many issues.

SSHA described the processes it followed to develop these mitigation strategies as follows:

- SSHA performed information gathering with various jurisdictions, and held discussions with Initiate and Sierra Systems.
- A workgroup consisting of five persons from the MOHLTC's e-Health Program, CCO, and SSHA met several times to discuss the proposed responses to each of the recommendations.
- Draft responses were circulated to the workgroup itself for comments and feedback.
- Review of draft responses was completed with the authors of the two PIAs – it is important to note that the feedback from the authors resulted in further clarifications, but did not require any substantive changes to the SSHA responses.
- Updated drafts of the PIAs were circulated to the workgroup.
- Final draft text was provided to the Steering Committee for the EMPI transition.
- Final versions were provided to the Steering Committee.
- SSHA is now developing the detailed work plans to support the implementation of the mitigations.[22]

The consultant reviewed each of the risk mitigation strategies and planned activities that SSHA has under development for the transitioned EMPI with respect to each of the recommendations from the PIA for the EMPI application. The consultant concluded that there are reasonable and plausible

[20] See Ontario, SSHA, Information Security Department, Privacy and Security Division, "Conceptual Threat and Risk Assessment. EMPI Transition," 70 pages, plus 1 appendix. Author: Mugino Saeki, Sept. 12, 2007.

[21] See Sextant [Ross Fraser and Pat Jeselon], "A Privacy Impact Assessment (PIA) on the Ontario Enterprise Master Patient Index Application," prepared for SSHA, draft, Aug. 17, 2007, revised August 22, 2007, 66 pp.; and Robert G. Parker, "Smart Systems for Health. Enterprise Master Patient Index Privacy Impact Assessment," prepared for SSHA, August 18, 2007, v#8, 18 pp.

[22] SSHA e-mail to David Flaherty, September 28, 2007, as edited for clarity.

responses, including the creation or existence of a Data Quality Plan, the Data Standards Workgroup, and a Client Advisory Group.[23] SSHA is also conducting a privacy gap analysis.

At present, the EMPI has a very small staff of about a dozen, so transitioning them to the current privacy and security environment at SSHA will not be a major undertaking. In addition, SSHA intends to house them in a secure, separate office facility (for which the consultant did a site visit). It will also mandate role-based privacy training for EMPI staff.

It is very important for readers of this report to understand that the EMPI, as a creation of the Ontario MOHLTC, is still evolving.[24] It will take at least a year for it to become a truly active, and interactive, Client Registry in use by some hospitals as it is rolled out across Ontario. The incremental character of this development is at least advantageous for ensuring robust privacy, confidentiality, and security, since the managers of the EMPI will be learning from both the CCO and SSHA experiences. SSHA should also undertake its anticipated internal and external auditing activities of its own compliance and keep the Ontario IPC informed and updated about relevant developments.

In the judgment of this consultant, the transition planning for the EMPI that SSHA began in December, 2006 is sufficiently well organized and systematic. The process is also well documented.[25]

It is also important for the IPC to understand that the transition planning for the EMPI move is being managed by the e-Health lead for the Ontario MOHLTC, the Chief Information Officer of CCO, and the new Vice-President of SSHA for Solutions, Delivery and Management. The Chief Executive Officers of both CCO and SSHA are also monitoring, and in agreement with, the proposed transition. The Ontario e-Health leadership has approved the creation of a Data Quality Working Group for the EMPI at SSHA.

The SSHA PIA for the EMPI itself raised the broad risk of the emergence of the unique number assigned to each new record in the EMPI as a de facto, new Unique Personal Identifier for the Ontario population once two-way integration exists with hospitals for the Client Registry.[26] This is an issue of potential, broad scale surveillance of residents of Ontario that SSHA needs to keep in its sights in future as it keeps this PIA up to date as a living document.

A Short List of the Current Problematic Areas for both SSHA and the EMPI

- The fact that SSHA has not yet identified someone to serve in the critical leadership post of Director of the EMPI (Client Registry) at SSHA;

[23] See Sextant [Ross Fraser and Pat Jeselon], "A Privacy Impact Assessment (PIA) on the Ontario Enterprise Master Patient Index Application," prepared for SSHA, Aug. 17, 2007, revised August 22, 2007, 66 pp., with Responses from SSHA, September 27, 2007, especially pp. 59-96 passim (which also includes a CCO response to the initial PIA).

[24] There are about 500 users at present.

[25] See Ontario, SSHA, EMPI Transition IPC Audit, Meeting Notes, Aug. 21, 22, 2007 (4 pp. in 2 files).

[26] See Sextant [Ross Fraser and Pat Jeselon], "A Privacy Impact Assessment (PIA) on the Ontario Enterprise Master Patient Index Application," pp. 36-37.

- The adequacy of resourcing for ongoing privacy and security management at SSHA in terms of both personnel and budget in light of the significant and growing responsibilities that SSHA has in these two areas of critical importance. SSHA anticipates growing to about 500 employees. The privacy and security team currently has about 13 staff and additional ad hoc consultants;

- The capacity/ability of the Privacy and Security team at SSHA to deliver a level of service, over time, to meet the expectations of the IPC, the Ontario MOHLTC, and individuals receiving health care services in Ontario;

  The team intends an increasingly operational focus, including audits and compliance monitoring;

- The need for the SSHA privacy and security team to engage in marketing, communications, outreach, and networking for Ontario e-Health with respect to its activities and accomplishments;

- The prospect of the Ontario MOHLTC changing priorities and roles for SSHA as the e-Health strategy for the province continues to evolve, which may distract the Privacy and Security Division from its ongoing and burdensome program of implementation;

  The Division itself is moving towards becoming more of an operational shop than a project shop and will be working on its own structural reorganization with an outside consulting firm;[27]

- The need for SSHA, especially with respect to large administrative data bases like the EMPI and OLIS, to adopt as many privacy by design/privacy enhancing technologies as possible, especially with respect to enhanced online, real-time auditing of users of these systems. Canadian banks, for example, have sophisticated fraud detection tools, especially including monitoring of online staff and user activities, that might be appropriate for SSHA to adopt as well and to offer to its clients;

- The fact that SSHA already manages access to the EMPI for users through a registration system;

  Initial audit logs exist for users logging on and off the system;

  Initiate Systems Inc.'s software monitors actual uses of the EMPI once users are online;

  This auditing capacity needs to be enhanced and made operational.

SSHA's Detailed Responses to the Grouped Recommendations of the IPC

SSHA organized the 82 recommendations of the IPC into a series of nine groups or streams and 24 sub-groups, and this report is organized accordingly. It will contain as much information and

[27] Interview with Michael Power, Vice-President, Privacy and Security, SSHA, and Jane Dargie, Aug. 20, 2007.

footnoted documentation about each major subgroup to justify the judgment of the consultant about the extent of SSHA's progress.

The major finding of the report is that most of the SSHA work to meet the IPC recommendations has been done to accomplish these obligations. SSHA established a Privacy Change Initiative Project Management Office (PCIPMO), guided by the Director of Privacy, that managed plans for responding to the nine streams of IPC recommendations. One long-term goal is to have every SSHA business unit play a defined role in strengthening the culture of privacy and retaining in-house knowledge and expertise on data protection.

The PCIPMO governance and reporting structure is under the direction of the MOHLTC's e-Health Office and its Change Management Oversight Committee.[28] As noted elsewhere, SSHA reports to the MOHLTC on a monthly basis with respect to its efforts to comply with the IPC's recommendations.

The IPC report was a catalyst for opening up budgetary resources, executive direction, and added focus on privacy and security at SSHA. Demonstrating compliance with the IPC's recommendations has been a very high priority for SSHA since it received the initial report in mid-March, 2007.

SSHA organized the IPC recommendations into nine main topics:

1. Privacy
    a. Policy and Procedures
    b. Training Content
2. Security
    a. Policy and Procedures
    b. Incident Management
    c. Training Content
3. Risk Management
    a. Risk Management Program
    b. Business Continuity Plan and Disaster Recovery Plan
4. Asset Management
    a. Policy and Procedures
5. Products and Services
    a. PIA Updates
    b. TRA Updates

[28] Ontario, SSHA, "SSHA IPC Review Response. Information and Privacy Commissioner/Ontario." V1.0, July 25, 2007. PowerPoint, 25 pp, slide 10.

   c. Supporting Controls
   d. Documentation and Communication

6. Framework

   a. Policy
   b. Method
   c. Supporting Controls
   d. Training Solution

7. Governance

   a. Culture
   b. Roles and Responsibilities
   c. Reporting, Monitoring and Compliance

8. Client Management

   a. Agreements
   b. Client Communications
   c. Supporting Controls

9. Vendor Management

   a. Agreements
   b. Vendor Privacy Program

SSHA also very usefully mapped each of the 82 IPC recommendations to each of these sub-streams: from as few as one to as many as 16 recommendations were associated with each one; 16 of the total of 24 sub streams related to five or fewer recommendations.

During its response process, SSHA developed a detailed mapping of its actions with respect to each of 82 recommendations in a document that continues to evolve and that it intends to release to the public and to its clients.[29] In each instance, SSHA quotes the IPC recommendation and then follows with:

1. SSHA's Understanding of this recommendation;

2. Key privacy principles;

3. SSHA's approach;

4. List of deliverables.

[29] See SSHA, "SSHA Response to IPC Review Recommendations," Document Identifier: 00951, Version: 0.02, 08-30-2007, 97 pp.

Most of this text is at a fairly high and general level, and this consultant has often collected more detailed information about the state of compliance during his work with SSHA (which is reflected in some measure in the contents of this report). As noted elsewhere in this report, SSHA has responded well to the most significant, and to most of, the detailed recommendations. Where additional progress is required on a recommendation, the process has begun, and it is understandable that consultation with multiple external and internal parties is required, such as with the implementation of a Business Continuity and Disaster Recovery Plan [Recommendation 65], and recommendations 71 (internal audit) and 73 ('certification' and 'accreditation' language), to give examples. It is also highly relevant that SSHA is reporting its detailed progress on implementation each month to the Ontario MOHLTC. [Recommendation 81.]

The consultant concluded that actually counting the number of recommendations completely or partially completed was not a productive exercise, not least because some recommendations are so much more important for privacy and security compliance than others. He is satisfied, for example, that SSHA has already complied with most of the priority recommendations in the IPC report. [Recommendations 1, 4, 19, 24-26, 35, 47, 57-58, 64, and 81-82.] The consultant decided that a "counting" exercise did not produce meaningful results in the context of the main concerns of this report.

The priority recommendations with respect to agreements with third parties (vendors, service providers, and partners) are a work in progress: "The draft content of the new Privacy and Security schedule is now with SSHA's General Counsel for final review. The new agreement is expected to be used for new third party providers by the end of the 2007 calendar year. SSHA will review existing agreements and develop a strategy for implementing the new language by the end of the 2007 calendar year."[30] [Recommendations 24-28.]

With respect to priority recommendations 30 and 32 concerning agreements with health information custodians, SSHA has amended all of its standard form contracts, is sending unilateral amendments to about 3,000 clients with signed contracts, and has reduced the number of its undocumented relationships: "The physical mail out to all health information custodians is expected to be complete by end of the 2007 calendar year."[31] [Recommendations 57 and 58.]

With respect to priority recommendation 58 and recommendations 54 and 61, SSHA has updated the safeguards and plain language descriptions on its web site,[32] the SSHA Privacy and Data Protection Policy will be posted on the website within two weeks, and the Privacy Impact Assessment summaries are expected on the website by end of the 2007 calendar year, which will align with the Health Information Custodian notification process.[33]

While recommendation 11 with respect to auditing was not a priority recommendation, number 64 was. It concerned the role of SSHA as a health information network provider being able to monitor accesses and transfers so as to make these electronic records available to a health information custodian upon request. SSHA reports that a "consultant has been engaged to prepare a discussion paper which looks holistically at the products and services SSHA offers, the monitoring and logging

[30] E-mail, Jane Dargie to David H. Flaherty, October 12, 2007.

[31] E-mail, Jane Dargie to David H. Flaherty, October 12, 2007.

[32] http://www.ssha.on.ca/products-services/index.asp

[33] E-mail, Jane Dargie to David H. Flaherty, October 12, 2007.

which is available for these products and services, and some discussion about asset classification. (This relates back to recommendations 11, 12, 62, 63, and 64.) The information gathering exercise is 90 per cent complete and the paper is due in October."[34] SSHA adds that: "The consulting exercise we have run was intended to

ascertain: what we are currently logging and monitoring; what and how we could log and monitor anything else that would be useful in connection with section 6(3)4 of the Regulation; and what is reasonable to log and monitor in an infrastructure environment. The consulting paper documents the outcome of all of this work."[35]

IPC Recommendation 2: Document File Management

The Privacy and Security Division is developing and implementing documentation practices and management procedures for all privacy and security related matters (over 7,000 electronic records).[36] Records are catalogued in the Microsoft Access Data Entry Catalogue and searchable by either Access Viewer or Microsoft SharePoint, which will allow enterprise wide sharing of department records. Individual staff members do their own cataloguing based on a set of instructions and guidance.

IPC Recommendations 24-29: Outsource Provider Agreements with Vendors and Other Third Parties

SSHA is targeting vendors, service providers, and partners in any relationship wherein it relies on them to provide products and services, in whole or in part, to support SSHA services. Bell is an example of a vendor. The agency wants to ensure that privacy and security are more visible in every future contractual relationship of this type, that outsource providers meet prescribed privacy and security obligations, and that standard privacy and security language is in relevant agreements.[37]

Procurement will implement an RFP template for new vendors, which, even in draft form, is a very valuable tool, because it includes 40 questions about privacy and security for vendors (proponents) to answer.[38] The new language will be superimposed on template agreements for every vendor and supplier, going forward and backwards, with Procurement also managing a tracking database.

Procurement at SSHA will revisit existing vendors one by one. It will also do a risk assessment for the type of service that a vendor offers to SSHA in order to focus on those that are privacy sensitive. Vendors from the United States are an additional issue: "As part of our review of vendor agreement language, SSHA is considering all sources and making any adjustments to processes as required to

[34] E-mail, Jane Dargie to David H. Flaherty, October 12, 2007.

[35] E-mail, Jane Dargie to David H. Flaherty, October 14, 2007.

[36] See Ontario, SSHA, SSHA Privacy Office, "Document File Management," from Privacy Team, Aug. 24, 2007, PowerPoint 34, slides [updated version with new slide 21, Sept. 11, 2007].

[37] SSHA Briefing from Ruth Vale, Sept. 11, 2007 (work in progress).

[38] The major topics treated include applicability, outsource provider information, privacy preparedness, information handling standards, access to SSHA premises, removal of information, privacy and security training, assurance of safeguards, non-disclosure, co-operation, assignment and subcontracting, and security screening of personnel.

ensure that we operate at a best practice level. This includes reviewing any and all advice provided at the provincial level,"[39]

Planned and future agreements with outsource providers will include a new Privacy and Security Schedule where personal information of clients or patients is involved. In a second phase of implementation, SSHA will supplement its existing agreements with current, medium and high risk outsource providers where personal information is involved.[40] This scheduling is now complete.

IPC Recommendations 30-33: SSHA's Agreements with Health Information Custodians

The SSHA legal team is also producing standard agreements with health information custodians, including physicians, for example, to amend and supplement existing ones. The intent is to communicate what SSHA is doing and to report on several SSHA obligations for such matters as breach notification, tracking agreements (via a database), and monitoring. SSHA is sending out a notice of its unilateral decision to amend more than 4,000 vendor agreements.

Conclusions and Recommendations

The overall conclusion of this report is that SSHA does understand privacy and security issues both in terms of conceptualization and the need to operationalize a wide variety of policies and procedures over time. Although its track record is weak in this regard in its formative years, the commitment appears to be there to turn over a new leaf. The Ontario MOHLTC, health information custodians, and the IPC should continue to be vigilant in this regard with respect to SSHA's compliance with its privacy and security obligations and requirements.

This report also concludes that the current senior executives and the Privacy and Security Division have a sufficient grasp of the privacy and security issues facing SSHA in the e-Health domain and of its huge responsibilities to Ontarians. On the face of the evidence available to him, the consultant concludes that the security team is currently stronger than the privacy team in terms of experience, both at SSHA and elsewhere. SSHA must continue to examine the adequacy of the human and financial resources at the disposal of the Privacy and Security Division. The consultant is of the view that the current cadre of personnel will be hard pressed to meet the demands of the Ontario MOHLTC and the Ontario IPC going forward, especially with respect to the detailed implementation of the many policies, processes, and procedures that SSHA now has in place, or has on the verge of being in place. A good illustration of this burden is the 31 processes in place for Privacy Assurance, including the management of a sophisticated set of Privacy Impact Assessments for multiple services that SSHA offers.

While this report does conclude that SSHA has made sufficient progress in responding to the recommendations of the IPC and that its intentions are honourable in this regard, there is still an element of faith involved with respect to actual implementation and follow through over time, especially in light of the history of underperformance at SSHA in this regard.

[39] E-mail, Jane Dargie to David H. Flaherty, October 14, 2007.

[40] SSHA Briefing from Ruth Vale, Sept. 11, 2007 (work in progress).

The website of SSHA is generally not informative, especially with regard to how it manages its responsibilities under PHIPA for privacy and security. Its separate privacy portal website was the best privacy product of the early years of SSHA.[41] The IPC recommended an enhancement of the contents of the privacy portal. [Recommendations 60, 61.] In response to certain IPC recommendations, SSHA does intend to update its website but that does not appear to have occurred to date.[42] In addition, SSHA states that it will use the main contents of its privacy portal on its website.[43]

On a second concern of this report, the consultant concludes that the case for transitioning the EMPI from CCO to SSHA is open and shut. SSHA already holds the data securely, has engaged in careful transition planning, has made staffing plans, and has in place adequate security safeguards in regard to the EMPI .

In his initial response to the IPC review in a letter on March 20, 2007, new SSHA CEO William Albino stated that "[i]n the future, we would appreciate having your Office review and approve our safeguards, practices and procedures every three years to ensure that we are continuing to fully meet the standards set out in PHIPA and are providing the level of privacy protection that Ontarians expect." This suggestion strikes this consultant as an admirable one, but the time period proposed between reviews of SSHA is excessive for present purposes, given the prospective speed of implementation of e-Health applications in Ontario, the number of privacy and security problems that the IPC reported on in its March, 2007 review of SSHA, and the lack of robust solutions in place in Ontario for meeting the privacy and security challenges posed by the implementation of e-Health applications, especially the issue of resourcing and commitment at all levels of health care. SSHA can, in part, respond on its own to these problems by implementing its own internal and external privacy and security auditing programs.

[41] See "SSHA Response to IPC Review Recommendations," 2.60.3 for its decision to close the privacy portal.

[42] See "SSHA Response to IPC Review Recommendations," 2.54.3, 2.58.3, 2.59.3, and 2.61.4.

[43] E-mail, Michael Power to David H. Flaherty, October 16, 2007: "We will review the content on both the portal and the main site to identify and keep useful materials. We will consolidate these privacy and security materials on a page on the main SSHA site. I expect that we will add material arising out of the IPC review (e.g. summaries of the refreshed product PIAs once they're signed off.)"

Appendix 1: Partial List of Documents Provided to David H. Flaherty by SSHA with respect to the SSHA Review and the EMPI Transition

1. List of the SSHA Executive Team members as of August 23, 2007 (1 p.)

2. Documentation pertaining to recommendations 2, 74, and 75 of the Ontario IPC.

    a. "Document File Plan. Access Document."

    b. "Guidelines for registering documents, Access version .01, 20060628, 15 pp.

    c. "Document Management-Our Responsibilities."

    d. InfoSec_Services_v1_20070613: Organizational chart for Information Security Services, 1 p.

    e. InfoSec_site_scope_notes_v1_20070614: related organizational chart, 1 p. that appears to focus on record keeping.

    f. "Information Security Records Site (File Plan) Scope Notes," 9 pp. [describes sets or categories of records and who has access to them].

    g. Ontario, SSHA, Risk Management Committee, Meeting Minutes, May 23, 2007, 1 p.

    h. SSHA, "Strategic Risk Register, Snapshot," 1 p. Blank template in an Excel spreadsheet listing 15 factors or components.

Documentation pertaining to recommendations 1, 3, 4, 19, 21, and 80:

a. "Privacy and Security Awareness Month." August 24, 2007, PowerPoint, 20 slides.

3. Ontario, SSHA, SSHA Privacy Office, "Document File Management," from Privacy Team, Aug. 24, 2007, PowerPoint 34, slides [updated version with new slide 21, Sept. 11, 2007].

4. Ontario, SSHA, "Get Caught" Posters about privacy and security," 5 pp.

5. Ontario, SSHA, "Privacy and Security Standard of Conduct," Document Identifier: 00895, Version: 1, Owner: Michael Power. (19 pp.)

6. Ontario, SSHA, "Making a Difference for Patients. SSHA Annual Report, April 1, 2005 to March 31, 2006." (42 pp.) This appears to be the latest annual report available.

7. Ontario, SSHA, "SSHA IPC Review Response. Information and Privacy Commissioner/Ontario." V1.0, July 25, 2007. PowerPoint, 25 pp.

8. Deloitte Consulting, Smart Systems for Health Agency, "Operational Review Final Report," Nov. 6, 2006 (99 pp.)

9. Ontario, SSHA, "Information Security Policy," Policy No. PSO-001, Document Identifier 867, Version 3.0, Owner: Director of Information Security (16 pp.), March 30, 2007.

10. White Binder from SSHA's briefing to David Flaherty on August 23, 2007, "Information Security Responses to IPC Recommendations," including:

    a. "Information Security Dept. Privacy and Security Division." PowerPoint, 19 slides.

    b. "IPC Report-Security Portfolio Work plan. July 16 to Aug. 31, 2007. Status as at August 22, 2007." (5 pp.)

    c. "Information Security Response to IPC Recommendations. Privacy and Security Division," Version 1.2 (Portfolio owner: Marc Stefaniu), (20 pp.)

    d. Ontario, SSHA, Information Security Department, "End-to-end Threats and Risk Assessment (TRA) Process at SSHA. Understanding Information Security Assurance and Compliance." Version 1.0 (August 20, 2007), 13 pp.

    e. Ontario, SSHA, "Enterprise Security and Privacy Incident Management (ESPIM) Plan and Capability," Aug. 23, 2007. PowerPoint, 9 slides.

11. EMPI Documentation received from SSHA

    a. Adam Mazer, "Client Registry (EMPI), Presentation to the IPC [David Flaherty], Aug. 21-22, 2007. PowerPoint, 23 slides.

    b. "One ID Direct. Ontario Network for e-Health," Aug. 21, 2007, PowerPoint, 13 slides. [how access controls work]

    c. Ontario, SSHA, EMPI Transition IPC Audit, Meeting Notes, Aug. 21, 22, 2007 (4 pp. in 2 files).

    d. Sextant [Ross Fraser and Pat Jeselon], "A Privacy Impact Assessment (PIA) on the Ontario Enterprise Master Patient Index Application," prepared for SSHA, Aug. 17, 2007, revised August 22, 2007, 66 pp., with Responses from SSHA, September 27, 2007, 96 pp.

    e. Robert G. Parker, "Smart Systems for Health. Enterprise Master Patient Index Privacy Impact Assessment," prepared for SSHA, August 18, 2007, v#8, 18 pp., with Responses from SSHA, September 27, 2007, 43 pp.

12. [re Tier level of Markham Data Centre from VP, IT]: Site Infrastructure, White Paper, "Industry Standard Tier Classifications Definite Site Infrastructure Performance," by W. Pitt Turner IV,

John H. (Hank) Seader, and Kenneth G. Brill (The Uptime Institute, Inc., Sante Fe, New Mexico, 2005, 4 pp.)

Documents Received, Viewed, or Read in Toronto, Sept. 10-14-2007. Updated versions are listed if they were received at a later date.

13. Legal-sized file of client agreements revised by the Legal Department of SSHA (estimate of 100 pp.)

14. SSHA, "SSHA Privacy Policy Framework. Presentation to David Flaherty, Sept. 11, 2007," PowerPoint, 5 slides.

15. SSHA, "Enterprise Privacy Policy," Draft version 0.4, June 25, 2007, 15 pp. Also accompanied by daughter policies for the various roles of SSHA under PHIPA (Aug. 27, 2007, 22 pp.)

16. SSHA, Information Security Team, "Privacy Assurance Service Process, Presentation to David Flaherty, Sept. 11, 2007, PowerPoint, 6 slides.

17. SSHA, "Privacy and Security Awareness Campaign," September, 2007, PowerPoint, 21 pp. including copies of the new privacy and security posters (which were also delivered in hard copy to the Ontario IPC). Also in white binder on Privacy Culture.

18. SSHA, Privacy Team, "Privacy Complaints, Inquiries, Compliments and Suggestions Handling," Sept. 11, 2007, 4 PowerPoint slides in a white binder, with 6 tabs, including: [IPC Recommendations 67 and 68]

    a. SSHA, Privacy Division, "Privacy Complaint, Inquiry, Compliment, and Suggestion Handling Policy," Version 0.1, September 9, 2007, 4 pp.

    b. SSHA, Privacy Division, "Privacy Complaint, Inquiry, Compliment, and Suggestion Handling," Version 0.01, September 11, 2007, 11 pp. [describes processes and procedures for these purposes].

19. SSHA, "Privacy and Security Standard of Conduct, Status Update," Sept. 12, 2007, small white binder. With 5 tabs and PowerPoint, 9 slides. Includes a full copy of the Standard.

20. SSHA, "Privacy Process & Privacy Impact Assessment (PIA) in Product/Service Design at SSHA," large white binder with 30 tabs (which are described in some detail below under Privacy Assurance Service Processes). Also a set of 25 PowerPoint slides, which describe in detail the nature, purposes, goals, value, processes, components, resourcing, and execution of a Privacy Impact Assessment.

21. SSHA, "Privacy Culture," Presentation to David Flaherty, September 11, 2007, 8 PowerPoint slides, in a small white binder with 3 tabs, including:

a. "Privacy is Everyone's Business," a presentation by Jane Dargie, Director, Privacy, to introduce the new Standards of Conduct, August 17, 2007, 9 PowerPoint slides;

b. SSHA, Change Management Office Business Case, August 17, 2007. 4 pp. describing a cultural assessment project for SSHA being undertaken with Deloitte through October, 2007, using its CulturePrint Assessment Tool for "best practice" change management.

c. Karen Pastakia, SSHA, "Culture Assessment Overview," August 22, 2007, 10 PowerPoint slides.

22. Second Round of 'Get Caught' Posters, Sept. 13, Series 2.

23. Ontario, SSHA, Information Security Department, Privacy and Security Division, "Conceptual Threat and Risk Assessment. EMPI Transition," 70 pages, plus one appendix. Author: Mugino Saeki, Sept. 12, 2007. DHF read, but did not retain a copy because of its sensitivity.

Documents, in addition to those listed above, received in September and early October, 2007:

24. SSHA, "IPC Report. Security Portfolio Work plan," Status as of September 14, 2007, 4 pp. spreadsheet.

Privacy Impact Assessments

23. SSHA, Privacy Office, "SSHA Privacy Impact Assessment Policy," Document Identifier: 1002, Version 1, September 28, 2007, 10 pp.

24. SSHA, Privacy Office, "Privacy Project Information," 1 p. form [to manage privacy office workload]

25. SSHA, Privacy Office, "Privacy Scope Analysis," [to determine the amount of work that needs to be done to complete a Privacy Impact Assessment], 4 pp. See also below.

26. SSHA, Privacy Office, "Privacy Threshold Analysis," [to determine the need for a Privacy Impact Assessment], 7 pp. See also below.

27. SSHA, Privacy Office, "Information/Documentation Required for PIA," 2 pp. [lists of topics].

28. SSHA, Privacy Office, "Privacy Impact Assessment. Information Gathering Process Guide," 27 pp. [A template for a PIA and its contents.]

29. SSHA, Privacy Office, "PIA and PIA Update," 1 p. [schedule].

30. SSHA, Privacy Office, "Privacy Impact Assessment Update for the ….," 4 pp. [Table of Contents]

31. SSHA, Privacy Office, "Privacy Impact Assessment. Solution Overview," (2007), Version 0.03, April 3, 2007, 6 pp. [outline of topics for a Table of Contents].

32. SSHA, Privacy Office, "Privacy Impact Assessment. Findings and Risk Analysis," (2007), Version 0.5, April 18, 2007, 11 pp.

33. SSHA, Privacy Office, "Privacy Impact Assessment. Executive Summary," (2007), 9 pp.

34. SSHA, Privacy and Security Office, "PIA/TRA Summary," 2007, 4 pp. Version 0.03, April 3, 2007.

35. SSHA, Privacy Office, "PIA Tracking Tool," Excel spreadsheet [to keep track of PIAs].

Privacy Policies

36. SSHA, Privacy and Security Office, "SSHA Privacy and Data Protection Policy," Document Identifier: 00999, Version 1, Approved September 28, 2007, 16 pp.

37. SSHA, Privacy and Security Office, "SSHA Health Information Network Provider Policy," Document Identifier: 00998, version 1, Version September 28, 2007, 14 pp.

38. SSHA, Privacy and Security Office, "SSHA Electronic Service Provider Policy," version 1, September 28, 2007, 12 pp., Document ID: 1000.

39. SSHA, Privacy and Security Office, "SSHA Third Party Retained by a Health Information Network Provider Policy," Document Identifier: 1001, Draft, September 25, 2007, 14 pp.

Privacy Assurance Service Processes: series of 1 page documents housed in a white binder and in electronic form [Recommendations 35-42, 45 dealing with Privacy Impact Assessments.]

40. SSHA, Flowchart, "Privacy Assurance Service Process," [for when a Privacy Impact Assessment is required], 1 page.) VSD file.

41. SSHA, Process No. 1, Client [describes 3 entry points to the Privacy Assurance Service, in this case when a client requests an SSHA product/service].

42. SSHA, Process No. 2, EPMO [Enterprise Project Management Office]: [describes the second entry point when SSHA decides to enhance an existing product/service].

43. SSHA, Process No. 3, Privacy: [describes the third entry point when there is a change to privacy legislation or an obligation to review products/services].

44. SSHA, Process No. 4, Client: [clients request products/services from SSHA].

45. SSHA, Process No. 5, Client Relation: [Client Relations team at SSHA activates its internal client engagement process.]

46. SSHA, Process No. 6, EPMO: [directions for project managers for an approved project to determine whether privacy resources are required]. [IPC Recommendation 36.]

47. SSHA, Process No. 7, Privacy, 2 pp.: [How the privacy office manages requests for privacy resources and tracks progress.] [IPC Recommendation 36]

48. SSHA, Process No. 8, Communication: [how the privacy team engages communications to support publication of relevant project information on the SSHA website and how to communicate with external stakeholders].

49. SSHA, Process No. 9, Privacy: [about the PIA tracking tool/database that the privacy team will manage].

50. SSHA, Process No. 10, Privacy: [describes the Privacy Threshold Analysis form (7 pp.) that the privacy analyst completes with the project team].

51. SSHA, Process No. 11, EPMO: [In future, project team will fill out the Privacy Threshold Analysis form for analysis by the privacy office.]

52. SSHA, Process No. 12, Privacy: [Privacy analyst determines whether to prepare or update a PIA]. [IPC Recommendation 37].

53. SSHA, Process No. 13, Privacy: [Privacy analyst may have to conduct a Privacy Scope Analysis with respect to the scope, complexity and duration of the PIA exercise].

54. SSHA, Process No. 14, EPMO: [Sharing the Privacy Scope Analysis with the project manager].

55. SSHA, Process No. 15, Privacy: [Privacy analyst initiates the PIA process.] [IPC recommendation 45.] This includes a two-page listing of "Information/Documentation Required for TRA/PIA," covering such relevant topics as business, systems and applications, databases and data exchange, existing security measures, other documents of potential use, and examples of potential source documents.

56. SSHA, Process No. 16, Privacy [describes the three components of a complete PIA].

57. SSHA, Process No. 17, Privacy [communication of privacy risks to business owners]. Includes a spread sheet for describing privacy risks, and SSHA, Risk Management, "Risk Management Monitoring and Reporting Initiative. Phase 1: Privacy and Information Security," September 5, 2007, 6 pp.

58. SSHA, Process No. 18, Risk Management team [describes its responsibilities].

59. SSHA, Process No. 19, Privacy [about the publication of summaries of PIAs]. Includes the SSHA, Privacy and Security Office, "PIA/TRA Summary," 2007, 4 pp. Version 0.03, April 3, 2007.

60. SSHA, Process No. 20, Communications [about the relationship of communications and privacy team about new information or updates to products and services].

61. SSHA, Process No. 21, Privacy [concerns advice to the privacy team from communications about website updates].

62. SSHA, Process No. 22, Legal [concerns the role of the Legal department in the PIA]. [IPC recommendations 22 and 56.]

63. SSHA, Process No. 23, Client Relation [states that no. 24 is not in the scope of the privacy assurance process}. [query]

64. SSHA, Process No. 24, Client [process for ensuring agreements are in place before providing products and services to clients].

65. SSHA, Process No. 25, Privacy [instructions for a privacy analyst to update a PIA]. Includes SSHA, Privacy Office, "Privacy Impact Assessment Update for the ….," 4 pp. [Table of Contents]

66. SSHA, Process No. 26, Privacy [process for documenting when a PIA does not need to be updated.]

67. SSHA, Process No. 27, Privacy [process for updating PIAs]

68. SSHA, Process No. 28, Client [how to direct queries and complaints, etc. from SSHA clients.]

69. SSHA, Process No. 29, Client Relation. [managing complaints and inquiries from SSHA clients.]

70. SSHA, Process No. 30, Privacy [documentation of response to inquiries in the PIA database.]

71. SSHA, Process No. 31, Legal [SSHA products or services will not be deployed to clients until legal agreements are in place.]

Privacy Training Materials

72. SSHA, "Privacy Training. Presentation to David Flaherty, Sept. 12, 2007." Large black binder with a complete presentation deck copy of seven PowerPoint slides, and a complete copy of the two training modules, and additional material.

73. SSHA, Privacy Office, "PIA and Privacy Assurance Training for PM," 1 p., [sign up sheet for training].

74. The five roles and responsibilities of SSHA under Ontario privacy legislation.

75. Training on "privacy fundamentals" for SSHA new hires and consultants, 2007 (33 PowerPoint slides).

76. "Privacy Fundamentals Feedback: New Hires /Consultants, In-Class Training, January to June 2007," Version 1.0, August 23, 2007, 4 pp.

77. "SSHA Role Based Privacy Training for Client Registry Operations Team," [EMPI], Sept. 2007, working draft, 36 PowerPoint slides; [use in EMPI section as well].

78. "Role Based Privacy Training. Privacy Training for SSHA Contact Centre Support Staff, 2007," v2, 38 PowerPoint slides.

79. "Privacy Fundamentals," on-line training course module, 19 screens, including review questions, click on buttons for additional information, and a final quiz.

80. "Privacy Legislation," online training course module, 30 screens, including image, information, and click on buttons for additional content, links to relevant privacy policies and procedures, and review questions.

81. "Privacy Incident Handling," on-line training course module, 41 screens, including image, information, and click on buttons for additional content, review questions, and reference materials; and 9) "Privacy Fundamentals Quiz," online training course module, 20 screens of questions.

Appendix 2: Related Review Activities of David H. Flaherty, including interviews and site visits

Interviews with staff of Anzen Consulting: Dr. Miyo Yamashita, Don MacPherson, and Megan Brister.

Interview with Pat Jeselon, Privacy Consultant, Toronto.

Sept. 13, 2007: Interview with Gail Paech, Assistant Deputy Minister and Lead, e-Health Program, Ontario Ministry of Health and Long-Term Care.

Appendix 3: EMPI Documentation Prepared for Cancer Care Ontario and the Wait Time Strategy and the SSHA Response

a. "Privacy Policy. Ontario Enterprise Master Patient Index," Revised February 2007, 17 pp. *SSHA adopting.*

b. "Cancer Care Ontario's IT Security Program," PowerPoint briefing materials, 20 slides. SSHA will replace with its own Security Policy.

c. "Enterprise Master Patient Index Office. Privacy Training and Awareness Procedure," last revision Oct. 30, 2006, 10 pp. *SSHA adopting.* SSHA will also incorporate its own privacy and security training.

d. "Enterprise Master Patient Index Office. Audit and Compliance Procedure," last revision, Oct. 30, 2006, 7 pp. *SSHA adopting.*

e. "Enterprise Master Patient Index Office. Enterprise Master Patient Index [User] Access Procedure," last revision May 11, 2007, 6 pp. *SSHA adopting.*

f. "Enterprise Master Patient Index Office. Privacy Breach Management Procedure," last revision, Oct. 30, 2006, 7 pp. *SSHA adopting.*

g. "EMPI Office End User Audit Reporting Checklist," 1 p. *SSHA adopting.*

h. Wait Time Strategy, "Privacy Orientation. Enterprise Master Patient Index Office Staff," PowerPoint 18 slides. SSHA will use its own notice process.

i. Wait Time Strategy, "Enterprise Master Patient Index Office. Password Policy and Procedure," last revision April 23, 2007, v5. 3 pp. *SSHA adopting.*

j. Wait Time Strategy, "Answers to Frequently Asked Questions on the Privacy Practices of the Ontario Enterprise Master Patient Index. Privacy Officers," 7 pp., v. 004, January 30, 2007. *SSHA will adopt as part of its communication strategy.*

k. Wait Time Strategy, "Answers to Frequently Asked Questions on the Privacy Practices of the Ontario Enterprise Master Patient Index. Hospital Administrators," 5 pp., v. 004, January 30, 2007. *SSHA will adopt as part of its communication strategy.*

l. Wait Time Strategy, "Answers to Frequently Asked Questions on the Privacy Practices of the Ontario Enterprise Master Patient Index. Patients," 7 pp., v. 004, January 30, 2007. *SSHA will adopt as part of its communication strategy.*

m. Wait Time Strategy, "Enterprise Master Patient Index Privacy Overview." Nov. 21, 2006, 2 pp. *SSHA will adopt as part of its communication strategy.*

n. “Enterprise Master Patient Index Office, Data Handling Policy and Procedure,” v2, April 30, 2007.” 2 pp. *SSHA adopting.*

o. Wait Time Strategy, “Privacy Toolkit Overview,” 30 Jan. 2007, v 003, 3 pp.. *SSHA adopting.*

p. “EMPI Registration and Enrollment Information.” 1 p. [Initiate Auditor credentials for individuals.] *SSHA adopting*.

q. “EMPIO Acceptable Use Agreement.” SSHA will use its Privacy and Security Standard of Conduct.

r. “Authorized PHIPA Agent Agreement. Agents. Obligations to Protect Privacy, Confidentiality and Security of Personal Health Information.” 2 pp. *SSHA adopting*.

s. “Enterprise Master Patient Index Office’s Privacy Acknowledgement [Form].” 2 pp. Version 2. January 8, 2007. [Individuals are required to read and sign this form.] *SSHA adopting*.

t. “CCP Confidentiality Agreement.” SSHA will use its own Privacy and Security Standard of Conduct.

u. “Enterprise Master Patient Index Access/Termination Form.” 2 pp. Version Date November 2, 2006. [For members of the project team and staff.] *SSHA adopting*.

v. “Enterprise Master Patient Index Remote Office Privacy Checklist,” 2 pp. *SSHA adopting.*

w. “WTIS-EMPI Privacy and Security Orientation,” 1 p. Spring, 2007. [A notice of training opportunities in the spring of 2007.] SSHA will use its own notification process.

x. “EMPI. Policies and Procedures Inventory, July 19, 2007.” Microsoft Excel Spreadsheet, 1 p. [A list of 20 CCO documents with a notation as to its status with SSHA for the EMPI transition. Compared to this present list.]

Appendix 4: Table of Abbreviations

CCAC	Community Care Access Centre (Ontario)
CCO	Cancer Care Ontario
CR	Client Registry (SSHA's new name for the EMPI)
CRO	Client Registry Operations (new name for the EMPIO)
CPO	Chief Privacy Officer
DI	Diagnostic Imaging
EHR	Electronic Health Record
EMPI	Enterprise Master Patient Index
EPMO	Enterprise Privacy Management Office (SSHA)
HINP	Health Information Network Provider
IPC	Information and Privacy Commissioner of Ontario
MOHLTC	Ontario Ministry of Health and Long-Term Care
OLIS	Ontario Laboratory Information System
ONE	Ontario Network for e-Health
PACS	Picture Archiving and Communications System
PIA	Privacy Impact Assessment
PHIPA	Ontario *Personal Health Information Protection Act*
RFP	Request for Proposal
SDM	Substitute Decision-Maker
SSHA	Ontario Smart Systems for Health Agency
TRA	Threat Risk Assessment

Appendix 5: Brief Bio of the Consultant, David H. Flaherty

David Flaherty is a specialist in the management of privacy and information policy issues. He served a six-year, non-renewable term as the first *Information and Privacy Commissioner for the Province of British Columbia* (1993-99). He wrote 320 Orders under the *Freedom of Information and Protection of Privacy Act*. He also pioneered the development of site visits to public bodies (hospitals in particular) as a form of privacy auditing.

Dr. Flaherty began his involvement with privacy issues as an assistant to Alan F. Westin at Columbia University in 1964. Dr. Flaherty's first book was ***Privacy in Colonial New England*** (1972). In 1974 he started comparative public policy work in Europe and North America that led to a series of books, including ***Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*** (1989). Dr. Flaherty has written or edited fourteen books.

Dr. Flaherty is an Honours graduate of McGill University (1962) and has an MA and Ph.D. from Columbia University. His teaching career from 1965 to 1993 included Princeton University, the University of Virginia, and the University of Western Ontario, where he was professor of history and law from 1972 to 1999 and is now Professor Emeritus. He was the first director (1984-89) of its Centre for American Studies. He has held fellowships and scholarships at Harvard, Oxford, Stanford, and Georgetown Universities. In 1992-93 Dr. Flaherty was a Fellow of the Woodrow Wilson International Center for Scholars in Washington, DC and a Canada-US. Fulbright Scholar in Law. Dr. Flaherty was an adjunct professor in political science at the University of Victoria from 1999 to 2006.

As a consultant, Dr. Flaherty's services for clients include strategic advice on the management of privacy issues and of relationships with privacy authorities, privacy advocates, and the general public; conducting overall assessments of privacy compliance (privacy reviews, audits, site visits, knowledge transfer); preparing Privacy Impact Assessments; managing privacy breaches; and developing privacy management plans.

In the fall of 1999 Dr. Flaherty served as a Special Adviser to the Deputy Minister of Industry Canada in support of Bill C-6, the *Personal Information Protection and Electronic Documents Act*. Along with Stephanie Perrin, Heather Black, and Murray Rankin, Dr. Flaherty is a co-author of the Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, Toronto, January, 2001). He also co-authored the Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals (A Report prepared by the Ontario Hospital e-Health Council's Privacy and Security Working Group – July 2003). **www.oha.com**

Dr. Flaherty is a member of the External Advisory Committee to the Privacy Commissioner of Canada. Since 2000, he has been the Chief Privacy Advisor to the Canadian Institute for Health Information (CIHI).