Personal Information Privacy Assessment of CHIPP Projects

Prepared For:

Office of Health and the Information Highway, Health Canada

by PRIVA-C™

Final Report

October 15th, 2002

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 1

2. METHODOLOGY 2

3. CHIPP Program Privacy Assessment 3

3.1. OVERVIEW 3

3.2. CROSS-PROJECT DIMENSION ASSESSMENT 3

3.2.1. Scoring Methodology Applied 3

3.2.2. Analysis of Patient Dimension 4

3.2.3. Analysis of People Dimension 5

3.2.4. Analysis of Process Dimension 7

3.2.5. Analysis of Security Dimension 8

3.2.6. Analysis of Information Management Dimension 10

3.3. MITIGATING PRIVACY RISK THROUGHOUT THE CHIPP PROGRAM 11

3.3.1. Mitigation Through Leadership 11

1. EXECUTIVE SUMMARY

In April 2000 Health Canada launched CHIPP. It is a two-year shared cost incentive program to promote the use of advanced information and communications technologies (ICT) to bring better health and health services to Canadians. The main areas of focus for this initiative are telehealth and electronic health records. In total twenty-nine projects were approved.

To assist in determining each project's compliance with privacy requirements, PRIVA-*C*™ was engaged by Health Canada to conduct an individual high-level privacy assessment on each of the twenty-nine (29) Canadian Health Infostructure Partnership Program (CHIPP) projects.

This privacy gap assessment report serves as findings for current state analysis of all the projects in order to provide Health Canada with an overview of their privacy programs. Each of the twenty-nine (29) CHIPP funded projects were asked to complete an Information Privacy Survey and to be prepared for a follow-up interview based on their responses. The Information Privacy Survey is a self-assessment tool to evaluate privacy and security elements in each project. This survey allows project managers to assess compliance with all applicable legislation and regulations pertaining to the protection of personal information, assess the technical safeguards for the protection of personal information, examine policies and processes that pertain to the protection of personal information and determine a project's compliance with the principles of the Canadian Standards Associations (CSA) Model Code for the protection of personal information. The completed Information Privacy Surveys were utilized to identify the strengths and potential gaps within the privacy programs of each project. These results were presented using a chart to assess and identify any observable trends.

The findings across all projects are presented in the Cross-Project Dimension Assessment of Section 4 and include CHIPP-wide recommendations into the five operational privacy areas including: Patients, People, Process, Security and Information Management. Recommendations include (but are not limited to):

- Ongoing patient education efforts on the projects' information handling practices
- Customized privacy and security training at each site
- Onsite privacy resource
- Privacy and security incident resolution procedures
- Security Audit or TRA conducted at least once a year or whenever a new system is being introduced in the existing environment
- Suggested strategies for managing the risk of faxing

At the time of this report, nineteen projects have completed the survey and thirteen of them were interviewed. Therefore, this report will provide separate findings for privacy assessments of the projects that have completed the survey and been interviewed, and projects that have completed the survey without a follow-up interview. For those projects with no interviews, the individual privacy gap assessment will include findings (based on survey responses), but will not include recommendations, as without an interview to confirm/clarify responses, appropriate recommendations are difficult to make.

2. METHODOLOGY

Each of the twenty-nine (29) CHIPP funded projects was asked to complete an Information Privacy Survey. Once the survey was received from the individual projects a follow-up was scheduled to clarify and expand on their responses. Based on the project and their survey responses, these interviews lasted from a few minutes to an hour and a half. Most interviews were completed around the one-hour mark. The interviews that completed a Privacy Impact Assessment (PIA) did not have to complete the survey; they had the option to send in their PIA document. Certain projects sent additional information along with their survey, such as privacy-related policies.

The Information Privacy Survey analyzes a project's privacy practices based on five key dimensions:

- **Patients** - Refers to the relationship between the project and its patients.
- **People** - Refers to the relationship between the project, its employees and business partners.
- **Process** - Refers to how the project administers its privacy and security program.
- **Security** - Refers to the physical, technical, communications, database and operational safeguards used to protect personal information under the custody or control of the project.
- **Information Management** - Refers to the project's information handling practices.

This final report is based on an assessment of all the projects that have completed a survey and/or PIA. An individual report was written for each project, which submitted a completed survey and/or PIA. The report analyzes the project's strengths and gaps within each of the five dimensions and summarizes the project's current and planned solutions, such as tools and procedures for protecting personal information. Recommendations are based on the remedial actions the project should employ to facilitate compliance with applicable legislation and privacy best practices.

The CHIPP program as a whole is also analyzed and recommendations to mitigate privacy risk from a project management level within Health Canada are provided.

3. CHIPP Program Privacy Assessment

3.1. Overview

The CHIPP projects consist of large-scale, collaborative projects in the areas of telehealth and electronic patient records systems.

Each of the projects presents its own uniqueness and issues in terms of usage of patient information; those that electronically transfer and store patient info (an EHR) and those that are involved in video consultations but do not store patient data (telehealth).

The issue with EHR type projects is that they are centered around what info is collected and who is going to have access to it. For telehealth consultation projects, the issue is not information access as much, but how the sessions are scheduled and whether or not they should be taped. The following analysis has taken these issues into consideration.

3.2. Cross-Project Dimension Assessment

3.2.1. Scoring Methodology Applied

For the purposes of assessing gaps, questions that were answered "No" versus "Yes" were given different scores as illustrated here. If the privacy practice does exist, projects responded with a "Yes". The three levels of "Yes" responses available serve to indicate the quality of the practice in relation to best practices.

Response	Meaning	Gap Score
No	The privacy practice in question currently does not exist within the project.	4
Yes - 1	The practice exists, but it is poor in quality.	2
Yes – 2	The practice exists, but it is average in quality.	1
Yes - 3	The practice exists, and is up to the standard of best practices.	0

The dynamic excel tool applies these scores to each question asked in the surveys, resulting in a final gap score for each project based on "Yes" and "No" responses. For example, a "No" response indicates that the particular privacy practice in question does not exist within the project, representing a gap.

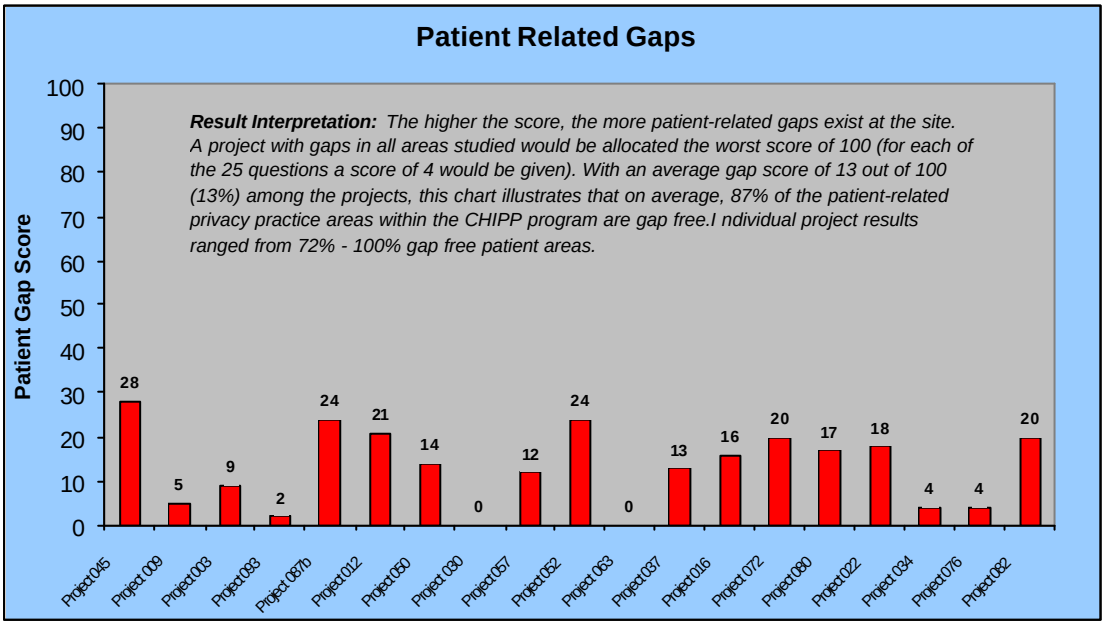
The tool produces charts as a result of the score each project received, and these charts are used as a means of guiding the analysis. It is important to note that the survey is somewhat subjective in that projects may use different rating criteria when assessing if a "Yes" measure rates a "1" or a "2". The project interviews post-survey completion is intended to reduce this subjectivity as much as possible. Also impacting the comparability of projects' scores is that most projects are in different stages of implementation and are all faced with unique external and internal environmental influences. For example, Project 012 answered many of the questions based on the practices of the territorial Health and Social Services department. In addition, Project 009 was in the initial stages of implementation and was not in a position to answer all of the questions.

PRIVA-*C*™ took the individual project's circumstances into consideration when conducting assessments.

The results for projects which were not interviewed should be examined with the knowledge that confirmation and clarification of responses has not yet occurred. It should be noted that the following graphs contain two separate scores for Project 087. Project personnel stated they would not be able to complete just a single survey for the project, due to the different clinical streams and partner sites involved. One survey was for Project 087a component and the other survey was completed for Project 087b component.

Note: **A thorough analysis could not be conducted on Project 087a component as for the majority of the measures; personnel responded "No" and stated "Nothing additional to sites existing policies added for Telehealth Services". Without a follow-up interview, we were unable to accurately assess these practices or to draw a conclusion on the project's privacy practices. Therefore, the following Dimension Assessment only reflects Project 087b component of Project 087.**

3.2.2. Analysis of Patient Dimension



Number of Measures	25
Mean Gap Score	12
Medium Gap Score	12.5
Low Score	0
High Score	28

Findings

Generally, very strong privacy practices with respect to the patient dimension of privacy exist throughout the projects. (See Result Interpretation in graph above.) Common strengths include:

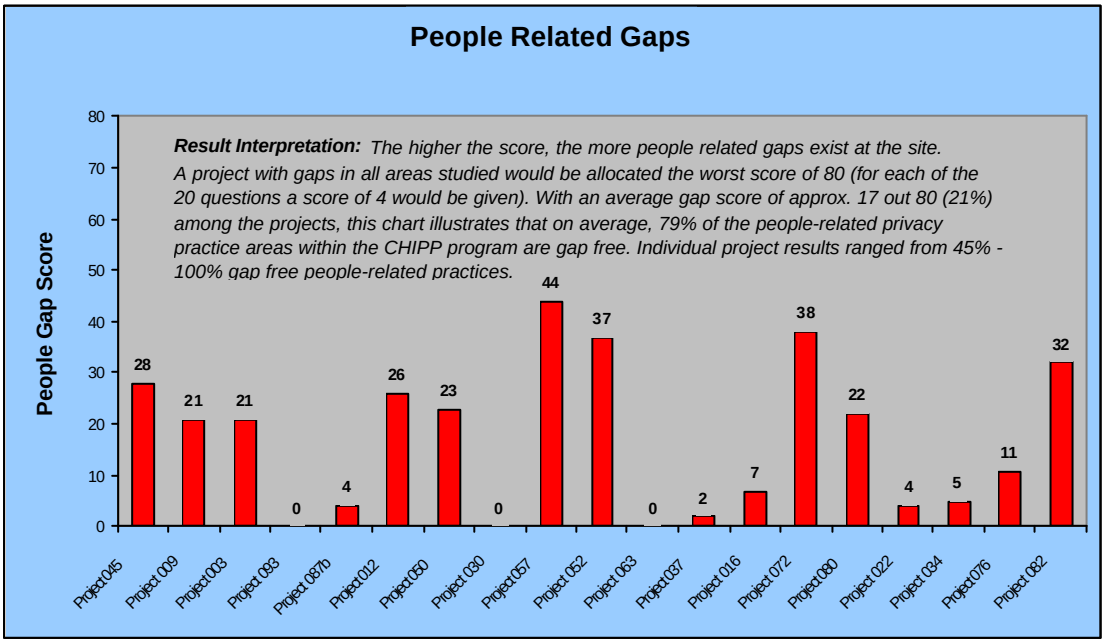
- Obtaining patient consent where appropriate
- Providing notice to the patient of information uses
- Identifying the purposes for collecting the information to the patient
- Some projects have excellent public communications plans in place that utilize informative brochures and effective websites.

Recommendations

- *Improve Communication at Collection Points* - Many projects do not have a comprehensive patient privacy communications strategy in place. Particularly important is the use of a brochure, wall posting, or verbal script upon initial information collection (e.g.: a patient's first use of the system) that informs patient of all uses and disclosures of his/her personal information.

- *Ongoing Education* - The projects' often involve technology and procedures that are new to many patients, and adequate education will make patients comfortable with the process and assure them that their information will be safeguarded. All projects, which have not done so already, are advised to utilize their websites and other collateral (e.g. brochures, posters) as communication mediums for ongoing patient education on the project's privacy practices.

3.2.3. Analysis of People Dimension



Number of Measures	20
Mean Gap Score	16
Medium Gap Score	16.5
Low Score	0
High Score	38

Findings

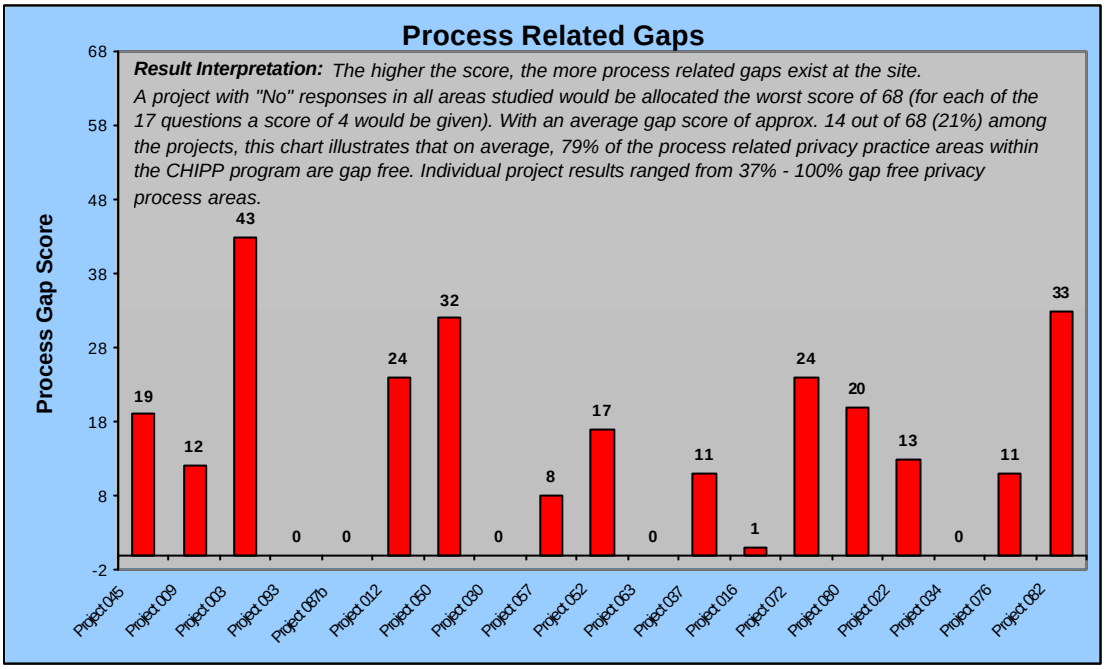
Overall, the people dimension of information privacy is also being handled well by the CHIPP projects, but there is more room for improvement in comparison to the patient area.

- The majority of projects have indicated information privacy, security, and confidentiality are major priorities for the senior management team.
- For those projects dealing with multiple remote sites, site coordinators have been appointed and division managers oversee the operations of the remote sites they are responsible for.
- All projects have some type of privacy related HR policies, but there is a mixture of what each project utilizes. Common policies found throughout most of the projects include acceptable use policies and procedures to revoke or change access privileges.
- Projects do include privacy requirements in contracts with third parties, but few of the projects actively audit and review the third party's privacy practices for compliance.
- Most projects have appointed an external individual, such as a hospital privacy personnel or regional privacy officer as their "privacy resource", to handle any privacy question or compliant the patient body may have.

Recommendations

- *Customized Privacy and Security Training at Each Site* - Although most project personnel are exposed to general privacy-related training at some point, the training is generic/not project specific. Each project should deliver training focused on their own unique information handling and security issues, and a specialized component should be delivered to information handling and management personnel.
- *Privacy Resource Onsite* - An individual within the project should be appointed as the contact point within the project to who project personnel and patients can address privacy concerns or questions. This individual could then go to external resources when required. This will standardize the process and lead to consistent issue resolution.
- *Privacy and Security Job Component*– Privacy and security requirements and responsibilities should be built in to projects' employee job descriptions and regular performance reviews.

3.2.4. Analysis of Process Dimension



Number of Measures	17
Mean Gap Score	15
Medium Gap Score	12.5
Low Score	0
High Score	43

Findings

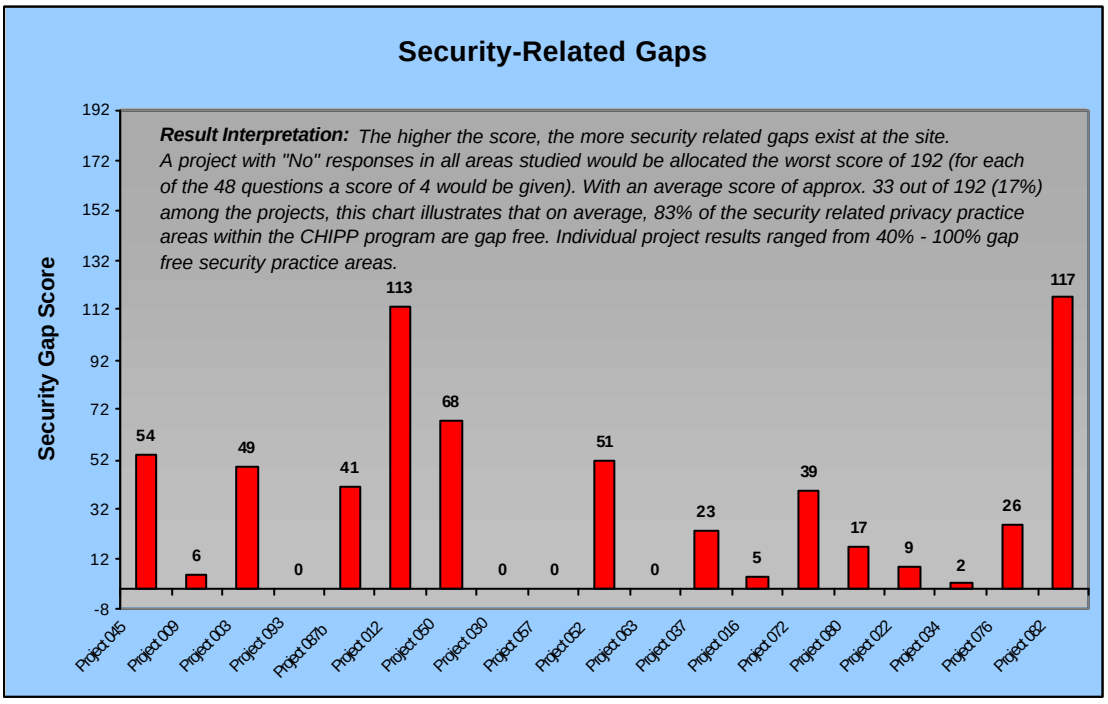
The CHIPP projects have several sound processes in place to safeguard patient information, however weaknesses are present and resulting improvements are recommended in a few areas.

- In general, projects are using the privacy policies of the site they are based out of (the host site or hospital), and specific policies related directly to the project have not been created. (Note that project personnel were not sure of the existing privacy related policies at remote sites that may be part of the project.)
- Only a few projects have a designated person or procedure in place to deal with the mass media. Projects should designate a contact person to manage public relations and ensure all personnel direct any public relations issues to this individual.
- Only 4 of the projects involved in the study have conducted a formal Privacy Impact Assessment on their initiative.

Recommendations

- *Tailored Privacy Policies* - The privacy policies currently used by each site should be evaluated for their relevance to the project and adapted as necessary to cover all unique information handling processes existent in the project.
- *Privacy Relations* - All projects should have a designated contact individual to deal with privacy and security related questions and enquiries from the mass media.
- *Privacy Incident Procedures* - Projects will need to develop a process to identify and respond to security and privacy breaches or incidents. This process should also detail how to communicate security or privacy violations to the appropriate individuals, including the data subject, law enforcement authorities and/or relevant project managers. (See Recommendations for Mitigating Privacy Risks throughout CHIPP Program in Section 4.3 for more information.)
- *Enforce Privacy Impact Assessments* - As all projects are information system initiatives, routine Privacy Impact Assessments (PIAs) should be conducted on all projects.

3.2.5. Analysis of Security Dimension



Number of Measures	48
Mean Gap Score	34
Medium Gap Score	23.5
Low Score	0
High Score	117

Findings

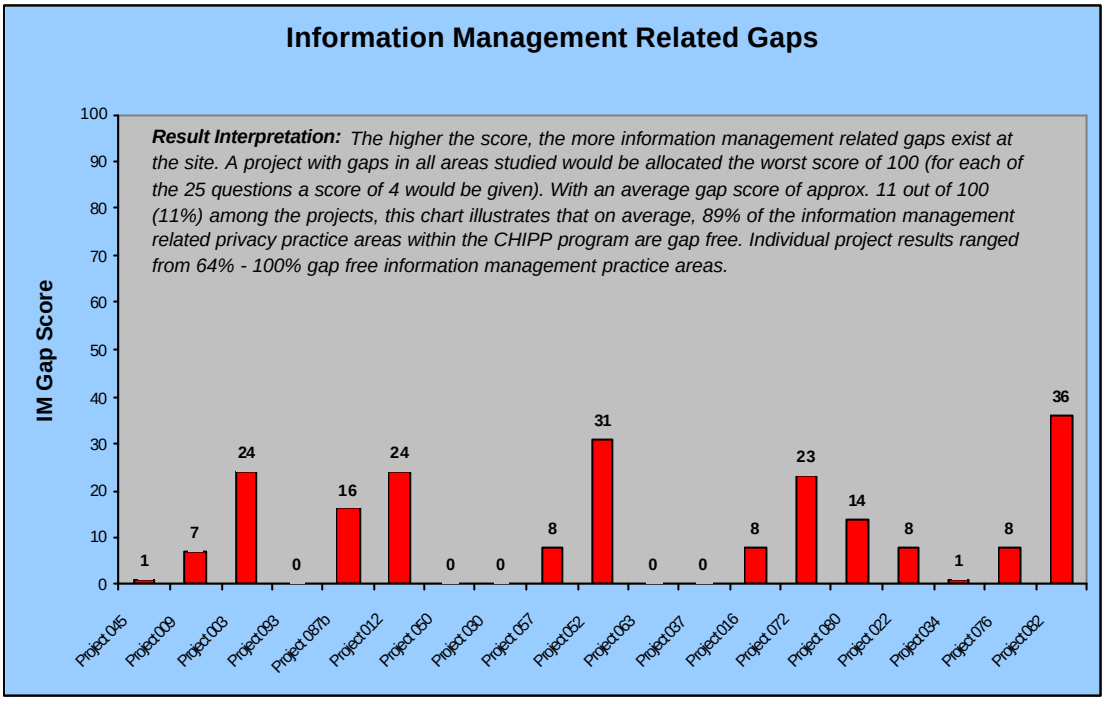
The projects employ varying levels of safeguards to protect patient information.

- The projects use secure networks with safeguards such as firewalls, network monitoring and surveillance mechanisms.
- For the most part, physical security measures such as restricted zones (e.g. main IT computer room) with access controls for areas housing sensitive equipment and data are in place.
- Those projects conducting tele-consultations have ensured that the sessions take place in soundproof rooms.
- Where applicable, unique user IDs and access controls are in place to access all sites. Most projects have conducted an inventory of network devices, video media and equipment, software, communications hardware, and databases.

Recommendations

- *Security Policies* – Security policies must be developed and implemented. For tele-consultation projects, existing security policies must be customized to address the security risks.
- *Data backup* – All backup media with sensitive information should be stored in a secure off site location.
- *Physical Security* – Equipment for tele-consultation or EHR should be stored in locked rooms or other methods to prevent theft.
- *Security Audit/TRA* – Security Audit or TRA must be conducted at least once a year or whenever a new system is being introduced in the existing environment.
- *Safeguards* - All tele-consultation projects should ensure consultations take place in a secure and soundproof room.

3.2.6. Analysis of Information Management Dimension



Number of Measures	24
Mean Gap Score	12
Medium Gap Score	8
Low Score	0
High Score	31

Findings

The privacy performance within the information management area is widespread, but generally very good. There are several projects requiring significant improvements (especially compared to their patients and people dimensions, and several with very few gaps at all.)

- Most EHR type projects have an audit function and different user access levels based on user roles.
- Projects that conduct live video consultations do not tape the sessions. The exception is found in one project where sessions are taped, but used for educational purposes only (to train surgeons).
- Some projects do not have an inventory of their data holdings that identify the primary and secondary purposes of the information.
- For many of the projects (such as tele-consultation ones) information is exchanged by use of a fax machine.

Recommendations

- *Access Polices/Procedures* – Policies/procedures for distributing access privileges, based on job function and revoking/altering privileges are required upon job changes, must be in place at all projects.
- *Guidelines for Collection* - A CHIPP-wide policy guiding when it is appropriate to record video consultations and other services is required so that practices are consistent across the CHIPP program. The guidelines should also indicate how to inform and gain consent from patients before taping occurs.
- *Inventory of Data Holdings* - All projects should have an inventory of their data holdings that identify the primary and secondary purposes of the information.
- *Mitigating Fax Risk* - Projects should manage the risk of faxing by:
    - Avoiding it when possible (e.g. mail personal information that is not time sensitive)
    - Pre-programming regularly used numbers into fax machines
    - Instituting confirmation procedures to ensure fax receipt by external party (e.g.: calls to confirm receipt within 5 minutes of sending fax)

3.3. Mitigating Privacy Risk throughout the CHIPP Program

3.3.1. Mitigation Through Leadership

Supporting numerous, independent projects is a complex role for the Office of Health and the Information Highway and its CHIPP Project Leads. The Office must take a leadership role in guiding privacy practices among the sites. Currently, sites regularly report status to the Project Leads, but there is a lack of ongoing privacy-related direction. The Office of Health and the Information Highway currently has a great opportunity to leverage the current relationship with the projects as a means to provide privacy leadership and mitigate risk through regular monitoring of practices within projects.

The following recommendations outline suggested means for mitigating Health Canada's privacy risk exposure:

Privacy Accountability

- Establish regular procedures for privacy reviews at each project by Health Canada personnel. The reviews will serve as tools to monitor projects' compliance with federal and provincial privacy legislation and with the principles of the *Canadian Standards Association Model Code for the Protection of Personal Information*. (Compliance with this legislation was stipulated as a mandatory requirement for the projects' original proposals.)

Privacy Enforcement

- Health Canada personnel should also facilitate the delivery and comprehension of the attached Privacy Gap Assessment reports for each project to key personnel within the project, so action can be taken to close gaps identified.

- Health Canada should encourage the completion of Privacy Impact Assessments (PIAs) within those projects which have not yet completed the assessment. Guidelines on how to

conduct PIAs is available in some jurisdiction such as the Ontario Management Board Secretariat Privacy Impact Assessment Guidelines, British Columbia Ministry of Management Services Corporate Privacy Impact Assessment Guidelines , and Government of Alberta Privacy Impact Assessment Guidelines. In the absence of PIA guidelines, projects may want to utilize the *Treasury Board Secretariat's PIA Policy and Guidelines.*

Facilitate Shared Learning

- Projects with a privacy best practice (in any operational area) should be identified and their best-practice process collected into an aggregated "Lessons Learned" file. The information should then be disseminated among all projects to facilitate a shared learning environment for improved privacy practices among all projects and reinforcement of commendable practices.

Privacy Assistance

- Health Canada should provide privacy guidance to projects with respect to all privacy policies and procedural inquiries projects may have. The appropriate contact information should be distributed to sites so that appropriate project personnel know whom to contact with privacy-related questions.