Privacy Compliance Tool

Checklist

Prepared by:

Ombudsman Manitoba

October 2003

PRIVACY COMPLIANCE TOOL

CHECKLIST

INTRODUCTION:

This “Checklist” should be used in conjunction with the Privacy Compliance “Guide”. The “Guide” provides general information and explanations that are helpful in completing the “Checklist”,[1] contains many relevant legislative references, and provides some “best practices” that may be useful for building privacy awareness into organizations and projects.

The purpose of the “Checklist” is to provide a diagnostic process for privacy compliance that covers the basic requirements of sound information privacy practices. It is designed to assist organizations evaluate the privacy compliance of a program, a specific initiative, a policy or an information system. Each of the main sections or Elements of the “Checklist” reflects a major privacy process or issue (e.g. limiting *use*, *disclosure*, and retention). By answering the specific questions related to each privacy element, managers and supervisors will be able to review practices and determine what action may be needed to initiate or improve compliance.

Users are asked to offer an **Explanation** for each answer and to provide **Attachments** or an action plan if applicable. **Action Plans** provide detail on corrective or developmental actions that need to be taken (e.g. develop a training program to provide privacy and security awareness for staff).

The “Checklist” also contains the basic requirements for compliance and may be used by the Ombudsman’s Office as a basis for privacy audits or investigations.

Please note that throughout the text of the “Checklist” and “Guide”, certain words or terms may be italicized to indicate that they are defined in *Appendix 1* to the “Guide”. Italics are also used for some subheadings and for references to statutes. We have also provided the “Checklist” in summary form (“Checklist at a Glance”) as an overview of the process and a tally of responses to the questions.

Some words of advice:
take the time to read over the “Guide” before using the “Checklist”.

[1] The following Privacy Impact Assessments and Diagnostic Tools assisted in the preparation of this Privacy Compliance Tool: Office of the Privacy Commissioner for Personal Data, Hong Kong, “Privacy Safe” 2000 (available http://www.pco.org.hk/); Ontario Management Board Secretariat: Electronic Service Delivery Privacy Standard (2000) and Privacy Impact Assessment Guidelines (1999) (available at www.gov.on.ca/mbs); Privacy Commissioner of Ontario: Privacy Diagnostic Tool (2001) (available at: www.ipc.on.ca); Privacy Commissioner of Alberta: Privacy Impact Assessment Template (2001) (available at http://www.oipc.ab.ca/).

TABLE OF CONTENTS

CHECKLIST FOR THE PRIVACY COMPLIANCE TOOL:

PROJECT INFORMATION

Date:
March 10, 2006

Name of Organization and Program Area:

Manitoba Health, on behalf of the Manitoba User Community of HSPnet (MBUC), comprised of health authorities, health service providers, and post-secondary educational institutions that will use HSPnet-MB for coordination and improvement of health sciences practicum placements.

CONTACT INFORMATION

Name:
Theresa Roberts, HSPnet Director

Telephone and FAX:
Phone (604) 925-6077
Fax (604) 926-1357

Address:
c/o BC Academic Health Council
1770 West 7th Ave Suite 402
Vancouver BC V6J 4Y6

E-mail:
theresa@tcroberts.com

CONTACT INFORMATION

Name:
Terry Goertzen
Workforce Policy and Planning
Manitoba Health

Telephone and FAX:
Phone (204) 786-7165

Address:

E-mail:
wau@gov.bc.ca

(**NOTE:** the "contact" should be the person most qualified to respond to questions regarding the compliance assessment.)

DESCRIPTION OF PROGRAM/SYSTEM OR OTHER INITIATIVE

This assessment relates to the Health Sciences Placement Network (HSPnet), a web-enabled application that supports the placement of health sciences students (from post-secondary educational institutions or *Placing Agencies*) into clinical practica or fieldwork opportunities (*placements*) in regional health authorities and other health service provider agencies (*Receiving Agencies*) in Manitoba. Students to be placed are generally enrolled in schools within Manitoba, although HSPnet will allow Receiving Agencies in Manitoba to record the placement of students that are placed by schools from outside of the province, and will allow Placing Agencies to record placement of their students outside of the province.

HSPnet was introduced in British Columbia in 2003 by the BC Academic Health Council (BCAHC) for use by its member agencies and other organizations (Placing and Receiving Agencies) that coordinate clinical placements for health sciences students. HSPnet is being made available to other Canadian jurisdictions (such as Manitoba Health, the Saskatchewan Academic Health Sciences Network, and the Council of Ontario Universities) under a Development Partnership model as described in the document entitled *HSPnet Partnership Structures, Roles & Responsibilities.* Under the Partnership, each jurisdiction is authorized to access the HSPnet application (in order to access an HSPnet instance established for their province alone) and associated tools and documentation at no licensing charge, in exchange for sharing the ongoing costs of operating and enhancing the system for the benefit of all users. A National HSPnet Steering Committee guides the strategic direction and sustainability of the Partnership and the shared operating infrastructure that supports all provincial instances.

Attachment (X) Appendix 1: *HSPnet Partnership Structures, Roles & Responsibilities*

Describe the mandate and functions of the organization and program area or initiative being assessed for privacy compliance (be sure to identify specific legislative authorities if applicable):

HSPnet is an initiative to address the growing shortage of skilled healthcare workers. HSPnet will introduce a province-wide system for coordinating and improving student placements for health sciences disciplines in Manitoba. The web-enabled application will support and streamline processes for:

- Initiating, tracking and processing (accepting or declining) placement requests among Placing Agencies and Receiving Agencies
- Reporting and analysis of placement activities (within and across programs, agencies, and disciplines) to support workforce development planning and initiatives to increase placement capacity;
- Facilitating evaluation of placement outcomes to ensure the best educational experience for health sciences students.

The HSPnet system enables schools to maintain information about students (with their consent) and enrollment levels, practicum course requirements, and available placement sites, in order to generate Placement Requests for delivery electronically via HSPnet (to Receiving sites also using the system) or manually via fax or email (to non-user sites). Receiving sites can then accept or decline electronically or via return fax/email, and can assign a local supervisor for the student as required. Each agency can only view their own placement data, and individual users are limited to data as appropriate for their organizational role and access rights. Identifiable student information is typically released by schools to Receiving sites only after the placement is confirmed, or if released earlier on a need-to-know basis only and for purposes consistent with the student's consent. All disclosures of personal information are tracked for audit purposes.

Each jurisdiction determines the specific legislative authorities that apply to the activities supported by HSPnet and the collection, use and disclosure of the information in that jurisdiction. HSPnet is designed as a principles-based system intending to meet the highest standard and thus the privacy legislation that applies in each province.

Provide details of any privacy impact assessments or other forms of *personal information* or *personal health information* assessments already conducted on this program or initiative:

Although a Privacy Impact Assessment (PIA) was not mandatory in BC at the time of HSPnet development, a formal PIA for HSPnet-BC was submitted in November, 2003 to four privacy offices (the BC Privacy Commissioner plus Privacy offices in three BC Ministries including the Ministry of Health, the Ministry of Management Services which is responsible for the BC privacy legislation, and the BC Office of the Privacy Commissioner). No privacy risks or system deficiencies were identified and feedback from the privacy offices was positive. The assessment from the OIPC ended with the following statement: "I am impressed with the privacy protections offered by the new system and the sensitivity displayed by the authors of the system."

In addition, Privacy Impact Assessments have been drafted for submission in the five other provinces in the process of HSPnet adoption. The national HSPnet Steering Committee has adopted a Policy that a formal PIA process will be undertaken in each province as a best practice, regardless of whether of a PIA is mandatory or not.

ELEMENT 1

IDENTIFYING PURPOSES AND LIMITING COLLECTION OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

This Element of the "Checklist" is designed to determine if the collection of *personal* and *personal health information* you undertake is authorized by FIPPA or PHIA and if the information you collect is limited to the purposes identified by the organization. The Element requires that you:

Identify the Purpose for which the information is collected at or before the time it is collected (FIPPA s.36(1)), or before it is collected or as soon as practicable afterward. (PHIA s.15(1))

Limit Collection of the information to that which is necessary for the purposes identified by the organization. (FIPPA s.36(2), PHIA s.13(1) and (2))

Collect information directly from the individual unless indirect collection is authorized according to the legislation. (FIPPA s.37(1), PHIA s.14(1) and (2))

Inform (notify) the individual, when collecting directly, of the purpose, legal authority (when FIPPA is involved), and provide contact information of an official who can answer queries about collection. (FIPPA s.37(2), PHIA 15(1))

Privacy Compliance "Checklist"

1. There is a detailed description of the type of *personal information*, *personal health information* or personal data elements collected for this program or initiative.

Yes X **No** □

Explanation:

The document entitled *HSPnet Data Uses Table* provides a detailed description of the personal data elements including personal information (PI) and personal health information (PHI) stored in HSPnet. It also details the specific data uses, levels of identification, and disclosure recipients. Note that collection of student PHI is optional and is limited to data on Tuberculosis testing results and immunity/immunization status for vaccine-preventable diseases. PHI is not collected for the purpose of delivering health care services to the student; it is used only as a status indicator of a student's compliance with the safety and/or infection control prerequisites of Receiving sites.

The student consent form for HSPnet references a handout entitled *Identified Purposes and Handling of Personal Information and Personal Health Information in HSPnet*. A copy of this handout, which describes the types and uses of their personal information, is provided to all students at the time of obtaining their consent. The handout is also available on the HSPnet website (*www.hspbc.net*) under Privacy and Security.

Attachment (X) or Action Plan ( ):[2]

Appendix 2: *HSPnet Data Uses Table*

Appendix 3: Student Handout: *Identified Purposes & Handling of Personal Information and Personal Health Information in HSPnet*

[2] Please mark with an "X" in parentheses if included with this assessment.

2. The purpose for collecting this *personal information* is authorized according to FIPPA. It is:
   a. authorized by an enactment of Manitoba or Canada, or
   b. directly related to and is necessary for a program or activity of the *public body*, or
   c. necessary for law enforcement or crime prevention.

   NOTE: please specify whether (a), (b), or (c) above applies, and if it is (a), identify the enactment(s) and applicable section(s).

Yes X **No □**

Explanation:
2b) is relevant. The identified purpose for collecting data via HSPnet is to support identification and coordination of appropriate placements for students as required by the curriculum of their educational program and/or discipline-specific certification body. This purpose is described in Policy No. 3.2: Identified Purposes and Ensuring Consent for Collection, Use and Disclosure.

This purpose supports processes limited to:

- Locating and confirming suitable placement opportunities for a student;
- Ensuring that information is available for an effective and safe placement (such as documentation for prerequisite skills and certifications, patient confidentiality orientation, or student identification);
- Tracking the placement throughout its duration for the purpose of locating and/or contacting the student within the receiving agency (in case of emergency or to alert the student of job action or facility problems), or for contacting the supervisor to discuss placement status, student progress against learning objectives, etc.

Attachment (X) or Action Plan ( ):
Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.2

3. *Personal health information* is not collected unless it is:
   a. for a lawful purpose connected with a function or activities of the trustee; and,
   b. is necessary for that purpose.

Yes X **No □**

Explanation:
As explained in HSPnet Policy 3.0, the national HSPnet Partnership members endorse the 10 Principles of the Canadian Standards Association (CSA) Model Code. One of these principles is limiting collection of personal information to that which is necessary for the specific purposes as identified before or at the time of collection.

Policy 3.1 specifies that information collected shall be limited to that defined within the *Identified Purposes* document.

An HSPnet-xx Data Stewardship Committee in each jurisdiction is responsible for reviewing the *Identified Purposes* and *HSPnet Data Uses Table* documents on an annual basis, and must approve any revisions to those documents and thus to the data collected that would result in a material change, as would be perceived by a “reasonable person”, to the type and/or uses/disclosures of personal information via HSPnet.

Attachment (X) or Action Plan ( ):
Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policies 3.0 and 3.1

4. *Personal* or *personal health information* is collected only directly from the subject individual or his or her authorized representative.

Yes □ **No X**

Explanation:

In general, PI and PHI are collected by Placing Agencies from their registered students, as provided at the time of their enrollment/registration into the educational program and updated throughout their program, and/or during their educational program as required to prepare for an upcoming placement.

Attachment ( ) or Action Plan ( ):

5. If *personal information* or *personal health information* is collected indirectly (i.e. from a third party), the *indirect collection* is authorized under Section 37(1) of FIPPA or Section 14 of PHIA.

Yes X **No** □

Explanation:

PHI and PHI may be collected indirectly through data uploads obtained from Student Information Systems that are maintained by the student's educational program, containing information collected directly from students as noted above. Data uploads to HSPnet from Student Information Systems are subject to the same consent and other requirements of HSPnet Policies on Privacy, Security, and Data Access, and are carried out within the specific requirements of the HSPnet Data Sharing Agreement

PI and PHI may also be collected from external agencies for entry into HSPnet, but only at the specific authorization of the student. For example, a student may authorize a Criminal Records Check and the disclosure of its results to their educational program. Educational program staff may then enter those results into HSPnet for the sole purpose of tracking the student's eligibility for placement against the Receiving site's published requirements for accepting students.

Attachment ( ) or Action Plan ( ):

Appendix 5: *HSPnet Data Sharing Agreement* (Version 2.2)

6. Individuals are informed (notified) of the purpose, authority (where FIPPA is involved) for *collection*, and how to contact an officer or employee who can answer their questions about the *collection*.

Yes X **No** □

Explanation:

The student consent form directs students to the HSPnet website which lists the relevant legislation for their province under which their information is being collected. The accompanying *Identified Purposes* handout summarizes HSPnet Policies on Privacy, Security and Data Access; provides instructions for accessing the full set of HSPnet Policies on the public website, and provides contact information for the HSPnet Privacy Officer (as appointed by the BCAHC) and the local Privacy Officer for the student's jurisdiction. The HSPnet Privacy Officer may handle questions and concerns independently if appropriate and adequate to satisfy the request, and/or would direct the individual to the Privacy Officer for their jurisdiction. The HSPnet Privacy Officer will also ensure that each jurisdiction publishes the name and contact information of their local Privacy Officer on the HSPnet website and in publications relating to the collection, use and disclosure of personal information in HSPnet. The role descriptions of the HSPnet Privacy Officer and the local Privacy Officer in each jurisdiction are summarized in Appendix 1.

Attachment (X) or Action Plan ( ):

Appendix 1: *HSPnet Partnership Structures, Roles & Responsibilities*

ELEMENT 2

LIMITING USE, DISCLOSURE, AND RETENTION OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

This Element is designed to determine if *personal* and *personal health information* is used or disclosed only for the purposes for which it was collected (or as otherwise authorized under Part 3 of FIPPA or of PHIA), and is retained only in accordance with a written retention and disposal policy that conforms with legal requirements.

If information is used or disclosed for another purpose, then either the *consent* of the individual is required or a law must require or permit that *use* or *disclosure*.

This Element also encompasses certain uses and disclosures of *personal information*, not otherwise authorized under FIPPA, that may or must be submitted to the Privacy Assessment Review Committee (PARC) process under Sections 46 and 47. It further deals with the disclosure of *personal health information* for health research under PHIA Section 24. The Introduction to the "Guide" provides additional important detail not repeated here and should be consulted to understand the questions more fully.

Note that *personal* and *personal health information* "sharing" and "exchange" are not concepts defined in FIPPA and PHIA. If the *disclosure* of such information forms part of an *Information Sharing Agreement*, the agreement must comply with the provisions of the Acts.

Users of the "Checklist" should note that Part 3 of FIPPA does NOT apply to *personal health information*. Also, when considering "Checklist" item A1 immediately following, FIPPA s.43(c) should be consulted for further guidance about the limits on permitted *use* of *personal information* and PHIA s.21 for details about restrictions on the *use* of *personal health information*.

Privacy Compliance "Checklist":

A. Limiting *Use*

1. *Personal information* or *personal health information* is used only for the purpose for which it was obtained, or for a *use* consistent with that purpose under FIPPA, or directly related to that purpose under PHIA.

Yes X **No** □

Explanation:

The HSPnet Data Table details the explicit uses of PI and PHI, and these uses are then summarized in the *Identified Purposes* handout for students, referenced in Element 1.

As stated in Policy 3.1 of the HSPnet Policies on Privacy, Security and Data Access, student PI and PHI in HSPnet are used only with student consent and only by authorized staff within a student's educational program for activities consistent with the *Identified Purposes.* All users of HSPnet are trained as to the *Identified Purposes* and must agree to a set of User Responsibilities relating to use of student information at the time of accessing HSPnet for the first time and again every 90 days prior to changing their expired password.

Attachment ( ) or Action Plan ( ):[3]

[3] Please mark with an "X" in parentheses if included with this assessment.

2. *Consent* is obtained from the individual before using *personal information* for a purpose NOT consistent with the original purpose for which it was collected or, in the case of *personal health information*, for a purpose NOT directly related to the original purpose for which it was collected.

Yes X **No** □

Explanation:

Active consent by students, as documented by a signed consent form, is the basis for use and disclosure of personal information via HSPnet in all provinces. This approach was chosen as a best practice to ensure a high standard of privacy protection and to allow the system to be implemented effectively across jurisdictions with differing privacy legislation.

Policy 3.2(10) of HSPnet Policies on Privacy, Security and Data Access states that "Informed consent for any new purposes beyond the *Identified Purposes* will be obtained from a student before collecting their personal information or prior to using their personal information if the new purpose applies to data already stored within HSPnet."

Attachment (X) or Action Plan ( ):

Appendix 6: *Consent Form for Use and Disclosure of Student Information*

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.2

3. There is a list of the staff positions or categories that use this *collection* of *personal* or *personal health information*.

Yes X **No** □

Explanation:

Staff categories that use student PI and PHI include Placing Agency staff in the roles of Placing Coordinator or Instructor, and Receiving Agency staff in the roles of Receiving Coordinator, Destination (unit) Coordinator, and Supervisor/Preceptor. Staff categories and their use of student PI and PHI are detailed in the *HSPnet Data Uses Table.*

Each authorized user is provided access to HSPnet as determined by the intersection of three data access dimensions: User Role, User Level and Access Rights.

- User Role determines which functions and screens can be accessed by a user. For example, senior managers may be provided with access to Report screens only (which produce aggregate or non-identifiable data), whereas Placing and Receiving Coordinators can access data on individual placements within their program areas and the students assigned to them.
- User Level determines whether a user has read-only rights (such as an Instructor), create/edit rights which are required by Placing Coordinators, or Local Administrator rights which are granted to a limited number of users within each site/program for the purpose of creating and maintaining User ID's within their site/program.
- Access Rights determine the school department and educational program(s) that may be accessed by Placing Agency staff, or the site, service and destination(s) that may be accessed by Receiving Agency staff when viewing incoming requests.

Attachment ( ) or Action Plan ( ):

4. Physical, administrative, and technical controls limit access to identifiable *personal* and *personal health information* to those who have a "need to know".

Yes X **No □**

Explanation:

All access to identifiable data is determined by the need to know. Identifiable student information is made available only when it is required as permitted in the *Identified Purposes*. Where data is required to manage programs and calculate statistics, such uses do not require identifiable data and such users do not see identifiable data.

HSPnet Policy 3.2 states that student information will be collected, used and disclosed via HSPnet on a need to know basis only and for activities consistent with the *Identified Purposes*. Policy 3.4 and its associated procedures identify the processes through which physical, administrative, and technical controls are used to enforce this "need to know" access. These controls include technical and procedural safeguards, user training and subsequent communications, and quarterly audits and monitoring.

Only HSPnet System Administrators (staff or contractors of the BCAHC as HSPnet Service Provider to each province) can create or edit User ID's at the Local Administrator level. Only Local Administrators, who agree to an expanded set of User Responsibilities when accessing HSPnet for the first time (and thereafter every 90 days upon password expiry), can create or edit User ID's within their site/program.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.2 and Policy 3.4

5. The least amount of *personal* and *personal health information* is used to meet the stated purpose.

Yes X **No □**

Explanation:

The HSPnet data set, as defined in the *HSPnet Data Uses Table,* is limited to data required to meet the *Identified Purposes* of HSPnet. The *HSPnet Data Uses Table* is reviewed and approved each year by the Data Stewardship Committee in each province, or upon material changes to the data set and/or its proposed uses.

System design elements, in the form of field definitions and business rules, determine when data is used by for each user as determined by their role, and new or revised fields and rules are released by the HSPnet Development Team within the constraints of the *HSPnet Data Uses Table*. In addition to such design elements, audits are undertaken on a regular basis, as defined by Policy 3.4, to ensure that design changes and/or user practices are not resulting in data collection, use or disclosure that is inconsistent with the *HSPnet Data Uses Table.*

Attachment ( ) or Action Plan ( ):

6. *Personal* or *personal health information* is used with the highest degree of *anonymity* to meet the stated purpose.

Yes X **No □**

Explanation:

The *HSPnet Data Uses Table* describes the data identification levels (identifiable, de-identified, and anonymous) by which PI and PHI are used within HSPnet. Within a student's educational program, their information is usually identifiable when displayed as part of their own placement record. However, when a placement is generated before student assignments are known or made, the placement is displayed as an anonymous student with no identifiers available.

Similarly, reports generated from HSPnet do not include any student identifiers unless the report is generated for a specific purpose consistent with the *Identified Purposes* of identifying and coordinating a student's placement. Reports generated in this manner include a clear statement defining the permitted uses of the data and include specific examples for which the data may NOT be used (e.g. research, contacting students for recruitment).

Attachment (X) or Action Plan ( ):

Appendix 7: Sample Report – Student Listing with Statement of Permitted Uses

B. Limiting *Disclosure*:

1. Individual *consent* is obtained before disclosing *personal* or *personal health information* to another government department or agency, *local public body*, *trustee* or other third party.

Yes X **No** □

Explanation:

The student's consent provides specific and time-limited instructions to their educational program on the use and disclosure of their PI and PHI as defined in the *Identified Purposes* handout. Note that collection of student PHI is limited to immunity/immunization status for vaccine-preventable diseases and Tuberculosis testing only, and is not collected for the purpose of delivering health care services to the student. PHI is collected only as a status indicator of a student's compliance with the safety and/or infection control prerequisites of the Receiving site, and is never disclosed via HSPnet to the Receiving site or to other users external to the student's educational program.

Attachment ( ) or Action Plan ( ):

2. If *consent* is not obtained, the *disclosure* is authorized according to a specific provision of Section 44(1) of FIPPA or Section 22(2) of PHIA.

Yes □ **No** □

Explanation:

Policy 3.2 requires each Placing Agency using HSPnet to establish a consent process whereby a signed consent form is collected from all new students registering in an educational program and prior to entry of their information into HSPnet. In recognition of the challenges of implementing a procedure to obtain signed consent for previously registered students during HSPnet implementation, a *Policy Application Guide* recommends options for entering student information into HSPnet in parallel with efforts to obtain a signed consent form *so long as another acceptable consent or notification process is already in place for those students*.

Attachment (X) or Action Plan ( ):

Appendix 9: *Policy 3.2 - Policy Application Guide*

3. When *disclosure* is required and authorized, the amount and type of information disclosed is limited on a "need to know" basis.

Yes X **No** □

Explanation:

As explained in Element 2A.4, HSPnet Policy requires that student information be disclosed via HSPnet on a need to know basis only and for activities consistent with the *Identified Purposes*. HSPnet Policy and associated procedures identify the processes through which physical, administrative, and technical controls are used to enforce this “need to know” access.

It is important to note that disclosure of personal information may occur on a regular basis but each disclosure is related to a *specific* placement request and is directed only to authorized individual(s) at the requested Placement Site. Within each Site, access is granted based on the user’s organizational role and need to know. For example, a user responsible for coordinating nursing placements across a site may be granted access rights to all Services and Units, whereas a Unit manager may be granted access to only the Unit(s) within her portfolio.

Attachment ( ) or Action Plan ( ):

4. *Disclosure* is made at the highest degree of *anonymity* possible while still meeting the purpose of the recipient.

Yes X **No □**

Explanation:

HSPnet business rules enforce anonymity in transactions until the placement is confirmed by the school. At the school's discretion, identifiable student information name may be released during the consideration process if the Placement Site has a need to know (i.e. in order to arrange an interview prior to accepting the student or to identify a student that has already contacted the site to arrange his or her own placement). The anonymity level of each disclosure is tracked within the History table of each placement request, including any early releases of identifable student information.

Business rules also determine what data is released at various points in the placement cycle, consistent with the *Identified Purposes* and as appropriate for the user's organizational role and associated need to know. For example, users at a student’s Receiving Agency are not given access to student name until the placement is confirmed (or earlier if released by the school on a need to know basis). If a placement is declined, the Receiving site maintains ongoing access to the statistical portion of the record (i.e. that a request was received but declined) but never gains access to the student that was intended for the placement.

Attachment ( ) or Action Plan ( ):

5. Staff maintains a *disclosure* log or audit trail of:
   a. what information has been disclosed,
   b. to whom it has been disclosed, and
   c. the purpose and authority for the *disclosure*.

Yes X **No □**

Explanation:

All disclosures of identifiable student information are tracked within the History table of each placement request, including detailed data on disclosure date, status change or manual release process that resulted in the disclosure, and the disclosing user name.

Attachment ( ) or Action Plan ( ):

C. Uses and Disclosures of Personal Information Not Otherwise Authorized under Division 3 of FIPPA

1. **For a *public body*** other than a *local public body* under Section 46 of FIPPA:

   The proposal or request has been referred to the Privacy Assessment Review Committee[4] (PARC) for its advice

   a. if the proposed *use* or *disclosure* is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or

   b. if the request is for disclosure on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information*.

Yes □ **No** X

Explanation:

Personal information is used and disclosed as authorized by consent and within the consistent purpose requirement.

Attachment ( ) or Action Plan ( ):

2. **For a *local public body*** under Section 46 of FIPPA:

   The proposal or request has been either assessed internally by the *local public body* or referred to the Privacy Assessment Review Committee (PARC) for its advice

   a. if the proposed use or disclosure is not otherwise authorized under
      Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or

   b. if the request is for disclosure on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information.*

Yes □ **No** X

Explanation:

Personal information is collected, used and disclosed as authorized by the student's consent and within the consistent purpose requirement.

Attachment ( ) or Action Plan ( ):

3. For *uses* or *disclosures* by *public bodies* contemplated under Section 46 of FIPPA, the Head of the *public body* or *local public body* has considered advice received through the statutory privacy assessment review process and approved conditions that must be met under Section 46(6), including a written agreement with the recipient of the *personal information.*

Yes □ **No** □

Explanation

Not applicable

[4] The Privacy Assessment Review Committee (PARC) is established under FIPPA s.77. The committee reviews requests for uses or disclosures of *personal information* that involve *data matching* or *data linking*, bulk disclosures and research requests. PARC provides advice to the Head of the public body under sections 46 and 47 of FIPPA.

Attachment ( ) or Action Plan ( ):

D. Disclosure of *Personal Information* for a Research Purpose under FIPPA

1. The Head of the *public* or *local public body* has considered any privacy assessment advice requested under Section 47(2) of FIPPA and approved conditions that must be met under Section 47(4), including a written agreement with the recipient of the *personal information.*

Yes □ **No** □

Explanation:

Not applicable. There is no disclosure of personal information for any research purpose. Personal information is used for specific and limited primary purposes.

HSPnet Policy 3.6 outlines Access to HSPnet Data for all purposes, including future research. As required by this policy, each province's Data Stewardship Committee will oversee an Approvals Process for access to their jurisdiction's HSPnet data according to the defined Data Access Approval Guidelines. These guidelines outline the level of requester (e.g. HSPnet users, User agencies, or External organizations); nature of the request; and corresponding approval process. The Guidelines permit research involving de-identified data only, and then only with the approval of the Data Stewardship Committee.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.6

E. Disclosure of *Personal Health Information* for a Research Purpose under PHIA

1. The *personal health information* required for the health research project is recorded information about an identifiable individual that relates to
   a. the individual's health, health history (including genetic information about the individual), or
   b. the provision of health care to the individual, or
   c. the payment of health care provided to the individual, and includes
   d. the Personal Health Identification Number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and
   e. any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.

Yes□ **No**□

Explanation:

Not applicable. There is no disclosure of personal health information for any research purpose at this time. Personal information is used for specific, and limited, primary purposes only.

See Element 2-D-1.

Attachment ( ) or Action Plan ( ):

2. The health research project has been approved according to the requirements of PHIA Section 24 by
   a. the Health Information Privacy Committee[5] (HIPC) if the *personal health information* is maintained by the government or a government agency, and
   b. an institutional research review committee if the *personal health information* is maintained by a *trustee* other than the government or a government agency.

Yes □ **No** □

Explanation:

This element is not applicable to HSPnet at this time. If health research involving PHI in HSPnet is to be considered in future, an update to the Privacy Impact Assessment will be undertaken at that time to consider all aspects of the proposed data use change.

Attachment ( ) or Action Plan ( ):

3. The researcher and the *trustee* have entered into an agreement under PHIA Section 24(4), and any regulations, in which the researcher agrees
   a. not to publish the *personal health information* in an identifying form,
   b. to use the *personal health information* only for the purposes of the approved research project,
   c. to ensure that reasonable safeguards are in place to protect the security and confidentiality of the *personal health information*, and
   d. to ensure that the information will be destroyed or de-identified at the earliest opportunity consistent with the purposes of the project.

Yes □ **No** □

Explanation:

This element is not applicable to HSPnet at this time. If health research involving PHI in HSPnet is to be considered in future, a Privacy Impact Assessment will be undertaken at that time.

Attachment ( ) or Action Plan ( ):

F. Limiting Retention:

1. There is a written records/data retention policy that meets all relevant legislative requirements.

Yes X **No** □

Explanation:

HSPnet Policy 3.4 requires that the HSPnet Director ensure that a system for records retention, disposal and archival is maintained, with processes and timelines consistent with the *Identified Purposes* handout and consistent with the Student Consent form. The processes and timelines will be reviewed annually by the HSPnet Steering Committee.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.4

[5] The Health Information Privacy Committee is established under Section 59 by the Minister of Health to approve research projects under Section 24 of PHIA and to perform any other functions assigned to it by the Minister.

2. *Personal* or *personal health information* used to make a decision that directly affects an individual is retained for a reasonable period of time to allow the individual to obtain access to it.

Yes X **No** □

Explanation:

The Student Consent Form provides a student's authorization to use and disclose their information for the program duration or six years whichever is less; consent is void upon graduation or withdrawal from their educational program or withdrawal of their consent. If a student continues in their educational program beyond the six year limit, the student will be required to sign another consent form.

Upon completion of a student's educational program, no new disclosures of their identifiable information will occur via HSPnet. However, a student may request access to their PI or PHI for up to two years following their graduation or withdrawal from their program through contact with their jurisdiction's Privacy Officer or the HSPnet Privacy Officer.

As outlined in Policy 3.2(12) the data archival system will include a provision for retention of student PI and PHI in an identifiable format for specific purposes limited only to responding to subpoena or other legally authorized access or to students' requests as noted above. Otherwise data will be accessible only in a de-identified format for reporting and statistical analysis purposes.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.2(12)

ELEMENT 3

ENSURING ACCURACY OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

These questions are designed to determine whether *personal* or *personal health information* collected is as accurate, complete, up-to-date, and not misleading as is necessary for the purposes for which it is to be used. (FIPPA s.38, PHIA s.16)

1. There are procedures in place to verify *personal* or *personal health information* and to manage requests for corrections that comply with FIPPA Sections 38 and 39 or with PHIA Sections 16 and 12.

Yes X **No □**

Explanation:
HSPnet Policy 3.3 outlines specific procedures and mechanisms to ensure that all reasonable efforts are made to guarantee the accuracy and completeness of PI and PHI in HSPnet. Such procedures and mechanisms include but are not limited to mandatory fields, data entry confirmation prompts and error messages, duplicate entry of critical data, and data formatting rules.

HSPnet reports of summary student profiles, class lists, and placement schedules will be used as appropriate by practicum coordinators and instructors to monitor data accuracy and completeness.

HSPnet Policy 3.5 provides a mechanism whereby students may request changes to their information held in HSPnet.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.3 and Policy 3.5

2. The authority to modify or correct *personal* or *personal health information* is clearly established to ensure that those without this authority may not or are unable to alter these records.

Yes □ **No □**

Explanation:
Policy No. 3.4 specifically addresses the authority levels and safeguards to ensure that limited numbers of users, with appropriate organizational responsibility, have create/edit rights for student information. All changes to student information are tracked within a History table for each student, and this history is readily visible to authorized users in order to ensure regular monitoring and early identification of inappropriate access and/or revision.

Attachment (X) or Action Pl ( )

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.4

3. An audit trail is maintained to document when and by whom a file or record was compiled or updated.

Yes X	**No □**
Explanation: Key changes to HSPnet placement records are recorded in History tables for each placement for the purposes of (1) providing an online transaction history and (2) to support periodic audits to identify potential problems with the user interface or training, to investigate reported or suspected security problems, or to detect unreported security problems. With regard to student information, all data creation/revision is tracked in a History table specific to each student. The history table identifies the field(s) affected, pre- and post-change data values, creation/revision date, and user ID that made the change.	
Attachment ( ) or Action Plan ( ):	

ELEMENT 4

SAFEGUARDING PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

Organizations are required to protect *personal* and *personal health information* by making reasonable security arrangements against risks such as unauthorized access, *use*, *disclosure*, or destruction. These security requirements apply to records in hard-copy form as well as to records that are kept electronically, such as a database. While the general security requirements for hard copy and electronic records are the same, the implementation of safeguards will differ. Therefore, the questions have been organized to address the general and then the specific, implementation requirements. (FIPPA, s.41; PHIA Part 3, Division 2 and Regulation 245/97)

The basic security requirements or safeguards for *personal health information* are laid out in more specific detail in PHIA Sections 18, 19, and the Regulations than for *personal information* under FIPPA (Section 41). Nevertheless, the intent is the same under both statutes: to ensure reasonable security arrangements are in place for personal data regardless of the physical form or characteristics of the information medium. Both Acts have specific regulation-making power for security matters, but only PHIA has specific regulations at this time (Spring 2003).

A Privacy Compliance "Checklist"

1. Security measures are in place for *personal* and *personal health information* regardless of media format (i.e. paper, photographic, electronic, etc.).

Yes X **No** □

Explanation

HSPnet Policy No. 3.4 defines the procedures to ensure that the BCAHC maintains a high level of physical and logical security of HSPnet data. Specifically:

- The BCAHC will maintain a comprehensive Service Level Agreement (SLA) to ensure its server host provider follows industry standards and/or best practices to safeguard the physical security of the server and network. These standards will include provisions for protection from viruses and other threats, firewall management, and data encryption.
- The BCAHC Privacy officer will monitor the activities of the server host and network provider and take immediate corrective actions if the minimum standards are not met.

External audits of the server host provider's physical and logical security process were conducted in May and October 2005, and no significant concerns were identified. *(Results of the security audit can be made available on a limited basis to Provincial Privacy Offices but must be restricted due to security risks).* All recommendations from those audits have been implemented as determined by a physical inspection conducted in November 2005, and ongoing monitoring of all audit indicators is required by HSPnet Policy 3.4 and reported to the National Steering Committee.

Attachment ( ) or Action Plan ( ):[6]

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.4

2. Written information security policies include a definition of roles and responsibilities, and sanctions for breaches of policy.

Yes X **No** □

[6] Please mark with an "X" in parentheses if included with this assessment.

Explanation:

Policy No. 3.4 outlines specific roles and responsibilities related to security measures for a) the BCAHC, (b) the HSPnet Director, b) Local administrators and other HSPnet users, d) HSPnet Steering Committee and e) local Data Stewardship Committees. Processes for monitoring policy compliance and sanctions for policy breaches are also defined, in the form of an escalation procedure leading to disabling of the user ID for the offending user(s) and/or all users within the user(s)' agency.

Attachment ( ) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.4

3. Staff receives ongoing training about security policies and procedures, and is made aware of the importance of security and *confidentiality* on an ongoing basis.

Yes X **No** □

Explanation:

All new users receive HSPnet training from an HSPnet trainer, a local Trainer from their own organization (trained by HSPNet to deliver local training), or via e-Learning tools. The curriculum for all user levels includes an orientation to HSPnet Policies on Privacy, Security and Data Access and to their application and monitoring within HSPnet. A subset of these Policies are presented to new users as "User Responsibilities in HSPnet" upon their first login and thereafter every 90 days when resetting their expired password. Ongoing training and reminders occur through a combination of procedural safeguards that enforce privacy requirements (e.g. screen prompts and online instructions), links from the HSPnet application to privacy content within Chapter 2 of the HSPnet User Guide, periodic user alerts on the HSPnet login page and individual user's Welcome screen, and targeted messages to specific user categories or even to individual users as required.

BCAHC staff and contractors that have access to HSPnet data are trained at a more detailed level by the HSPnet Privacy Officer on the privacy and security framework, and upon completion of their training these individuals sign an "Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers" that guides the activities of system administrators, developers, and Help Desk staff.

The National HSPnet Steering Committee, and/or local HSPnet Data Stewardship Committees, may recommend additional training or remedial action upon review of quarterly monitoring reports as required by HSPnet Policies.

Attachment (X) or Action Plan ( ):

Appendix 8: *Course Outlines – HSPnet Training*

Appendix 9: *Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers*

4. Security breaches and violations are documented, responded to, and corrective measures taken according to established processes.

Yes X **No** □

Explanation:

Policy 3.4 requires that any breaches of security or data loss are reported by the HSPnet Director to the BCAHC CEO, to designated representatives of any affected jurisdiction(s), and to members of the National HSPnet Steering Committee. Escalation procedures for minor privacy errors (i.e. inclusion of student name in a Comments field) are documented and occurrences and outcomes of escalation are reviewed at the National Steering Committee and by each province's Data Stewardship Committee.

Attachment ( ) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.4

5. Access to *personal* or *personal health information* is regularly monitored and audited.

Yes X **No** □

Explanation:

The HSPnet Director is responsible for ensuring that monitoring is carried out on a quarterly basis or more frequently as required by HSPnet Policies on Privacy, Security and Data Access. The National Steering Committee and local Data Stewardship Committees review the results of quarterly monitoring activities at each (semi-annual) meeting, along with recommendations of the HSPnet Director and/or results of any interim remedial actions taken in advance of their meeting. The national and local committees can also recommend additional actions and/or changes to Policy including monitoring processes and/or frequency at any time, and an annual review of the monitoring and escalation processes and monitoring schedules is a mandatory requirement of the Policy regardless of any breaches or other problems.

Attachment (X) or Action Plan ( ):

Appendix 10: *Sample Monitoring Report*

6. *Personal* and *personal health information* are stored or maintained in a physically secure location.

Yes □ **No** □

Explanation:

Physical access to HSPnet equipment and storage media is limited to authorized staff and contractors of the British Columbia Institute of Technology (BCIT) as contracted host provider to the BCAHC. Physical and logical security for BCIT-managed equipment and network services is guided by a Service Level Agreement between BCIT and the BCAHC, and compliance is monitored annually through a physical inspection by the HSPnet Director and/or an external expert. Administrator access to the servers is limited to authorized members of the HSPnet team, who are required to sign the "Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers" as referenced in Element 4A.3.

Attachment ( ) or Action Plan ( ):

7. *Personal* and *personal health information* in all media are disposed of securely to prevent unauthorized access.

Yes □ **No** □

Explanation:

No disposal of media has yet been required. The HSPnet director is responsible for maintenance of a data retention, archival and disposal system that will address the specifics of any future requirements in this regard.

Attachment ( ) or Action Plan ( ):

8. Physical removal of *personal* and *personal health information* of any medium from a secure designated area is always undertaken in a manner and in accordance with procedures that continue to ensure the security of the information at all times.

Yes X **No □**

Explanation:

Offsite backup media for HSPnet data is removed and stored offsite in a secure manner consistent with BCIT procedures used to protect backup media for all BCIT information systems for student, financial and human resource management. The BCIT manages all centralized electronic media and data according to the requirements and standards of the external BC Government Auditor requirements. Off site storage is managed completely by BCIT staff; data is spooled to tape backups and is relocated to another building on our campus (approx 0.6 KM away from our data centre. The tapes are transported both ways by BCIT staff and are stored in a secured, fire resistant safe.

Attachment ( ) or Action Plan ( ):

B Electronic Systems Security:

1. Users are assigned unique user identifications and passwords for access to personal data, and passwords are changed regularly.

Yes X **No □**

Explanation:

HSPnet Policy No. 3.4: describes the minimum user authentication requirements of HSPnet. The application automatically forwards a random, confidential, complex password to the user's email account upon creation of a new User ID. New users are required to select a new password upon login for the first time before proceeding to the application. Passwords are of a format complex enough to prevent guessing or other routine efforts to use another individual's user ID. User passwords expire every 90 days.

The National HSPnet Steering Committee is accountable to each partner jurisdiction for annual review and approval of common security standards relating to password expiry and system inactivity timeout. These standards are reviewed against industry standards and against results of monitoring (i.e. frequency of user lockout, repeated requests of forgotten password assistance, or potential indicators of unauthorized access) prior to adjusting the Policy. Local Data Stewardship Committees are also required to review the Policy and standards on an annual basis, and may forward recommendations to the National HSPnet Steering Committee for adoption as a national standard or Policy change, or to request introduction of jurisdiction-specific standards.

Attachment ( ) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.4

2. Network and application security status is assigned on a "need to know" basis according to the particular requirements of specific roles within the organization.

Yes X **No** □

Explanation:

HSPnet Policy No. 3.4 describes the procedures and roles through which network and application security status is assigned. The HSPnet Director is responsible for issuing, monitoring and revoking network or application access for all BCAHC staff and contractors, including users with System Administrator access. Only System Administrators can create new user ID's with Local Administrator access, and only Local Administrators in turn can grant or modify access rights for users as appropriate for their role as defined by the *HSPnet Data Uses Table*. When creating or modifying a user's access rights, Local Administrators are presented with summarized information regarding their responsibilities for granting access on a need to know basis only.

Attachment ( ) or Action Plan ( ):

3. Access privileges are revoked promptly when required (e.g. when an employee leaves or moves).

Yes X **No** □

Explanation:

All users agree to notify their local HSPnet Administrator to changes in their role or organizational jurisdiction, so the HSPnet Administrator can modify or terminate their access based on need to know. In addition, the HSPnet automatically inactivates users ID's that have been inactive for six months (the National HSPnet Steering Committee reviews this schedule on an annual basis as required by Policy 3.4). As student placements are a highly cyclical process, the last Steering Committee review determined that an inactivity threshold of less than six months would be impractical. The HSPnet Director runs quarterly reports of inactivated user ID's and forwards this report to the responsible Local Administrator for each site or program, as a double check regarding changes to user role.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.4

4. Systems contain audit trails for tracking data access and audit logs provide information about abnormal or unusual access.

Yes X **No** □

Explanation:

The HSPnet Director runs a quarterly report of record changes made by a user who was not authorized to access that record at the time of the revision. To date no such problems with abnormal or unusual access have been found via this audit process or as reported by users. This report will also be run on demand if any reason to suspect inappropriate activity is discovered.

Attachment ( ) or Action Plan ( ):

5. Access logs and audit trails are reviewed on a regular basis.

Yes X **No** □

Explanation:

Audit reports are run on a quarterly basis, as required by HSPnet Policy 3.4. The National Steering Committee reviews the audit schedule on an annual basis.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.4

6. *Personal* and *personal health information* is transmitted by secure means to minimize opportunities for unauthorized or accidental interception by third parties.

Yes X **No** □

Explanation:

All HSPnet page and data transmissions occur via SSL encryption (128-bit)

Attachment ( ) or Action Plan ( ):

7. Virus protection is implemented and an effective firewall is in place where necessary, for all information systems that contain *personal* or *personal health information*.

Yes X **No** □

Explanation:

BCIT, as server host provider, provides protection from external threats as per their SLA with the BCAHC. BCIT installs industry-standard anti-virus tools on all servers involved with HSPnet as managed for all jurisdictions. The HSPnet Director is responsible for ensuring that virus scanning patterns and other dynamic content are kept up to date, and a schedule is in place for regular checking of virus update status.

Attachment ( ) or Action Plan ( ):

8. External providers of information management or technology services are covered by written agreements dealing with risks including unauthorized access, *use*, *disclosure*, retention, and destruction or alteration as required under FIPPA Section 44(2) and PHIA Section 25(3).

Yes X **No** □

Explanation:

The SLA between the BCAHC and BCIT, and the HSPnet Confidentiality Agreement and Code of Conduct, document the responsibilities and obligations of external providers in protecting data privacy, security and integrity.

BCIT processes for managing privacy and security risks include:

o Ensuring there is adequate physical security to the data centre (swipe card door locks, two levels, with discrete access to the computer room ONLY for authorized staff with a direct need for access. Logs of swipe card access are stored and are searchable for forensic audit.

o Electronic access to all data stores is managed by 2 level secured logon (one to the network, and another to the data service). Only staff with a direct need as a result of their technical role have access; logs are maintained and available for forensic audit.

The HSPnet Data Sharing Agreement details the specific requirements in each jurisdiction as agreements are reviewed and refined in each jurisdiction, this may result in a need for additional language in the BCIT SLA and/or the HSPnet agreement with BCAHC staff and contractors.

Attachment ( ) or Action Plan ( ):

ELEMENT 5

ENSURING INDIVIDUAL ACCESS TO PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

An individual, or his/her *authorized representative*, is entitled to have access to information about the *personal* and *personal health information* an organization holds about him/her. (FIPPA Part 2, PHIA Part 2) An organization should be prepared to explain how *personal* and *personal health information* are used and disclosed. (FIPPA Part 3, ; PHIA Part 3)

Privacy Compliance "Checklist"

1. A process to respond to access requests under the Act(s) is in place.

Yes X **No** □

Explanation:

HSPnet Policy 3.5 outlines the process by which a student, or his/her designate as authorized in writing by the student, may request access to information about their PI or PHI held or disclosed via HSPnet. Access must be requested in writing to the HSPnet Privacy Officer. The process is also communicated to students through the *Intended Purposes* handout, and is published on the public website.

Attachment ( ) or Action Plan ( ):[7]

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.5

2. Individuals are informed that the organization holds *personal* or *personal health information* about them and that access to that data is provided, except in limited circumstances as defined in legislation.

Yes X **No** □

Explanation:

The HSPnet Student Consent Form and accompanying *Intended Purposes* handout serve to inform students that their PI and PHI will be used and may be disclosed via HSPnet, upon their consent.

Instructors of educational programs are provided with a companion document entitled *Guide for Instructors of HSPnet Programs* to assist them in answering student questions about the use and disclosure of their information via HSPnet.

Attachment (X) or Action Plan ( ):

Appendix 11: *Guide for Instructors of HSPnet Programs*

[7] Please mark with an "X" in parentheses if included with this assessment.

3. Requests for access are responded to within the legal time limits at minimal or no cost, or in compliance with legislation.[8]

Yes X **No □**

Explanation:

As noted in Policy 3.5 and in the *Identified Purposes* handout, a student or his/her designate may ask for a copy of their personal information in HSPnet by submitting a written request to the BCAHC Privacy Officer. The Privacy Officer will provide the student, within two weeks of the request, a list of specific information contained in HSPnet and, if requested, a list of uses/disclosures of that information. There are no costs at this time to the student or designate for such requests.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.5

4. The requested information is provided in an understandable format and the organization is prepared to explain any terms or abbreviations.

Yes X **No □**

Explanation:

Policy 3.5 requires that the Privacy Officer provide a written description of the information provided to the student or his/her designate to ensure their understanding of the content.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.5

5. A refusal to grant access to all or part of an individual's information includes the specific provision for refusal under the legislation and clear reasons for the refusal.

Yes X **No □**

Explanation:

HSPnet Policy 3.5 provides requires that a decision to refuse a student's request be relayed in writing to the student along with clear provisions and reasons.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.5

[8] FIPPA Regulation 64/98 sets the chargeable fees under this Act. PHIA s.10 states that a trustee may charge a reasonable fee for permitting examination of *personal health information* and providing a copy, but the fee must not exceed the amount provided for in the regulations. PHIA did not have a fee regulation as of Autumn 2003.

ELEMENT 6

CHALLENGING COMPLIANCE

People have the right to question public bodies and trustees about their compliance with the information privacy protection provisions under FIPPA and PHIA. It is extremely important that the public's right to make complaints about alleged infractions of the legislation is made known on a timely basis to individuals. The right to challenge compliance is one of the fundamental tenets of internationally accepted principles of fair information practices.

Privacy Compliance "Checklist"

1 There are communication policies and procedures in place that ensure individuals are routinely informed that they may make a complaint to the organization and are informed about their statutory right to make a complaint to the Manitoba Ombudsman respecting their *personal* and *personal health information* rights.

Yes X **No □**

Explanation:

HSPnet Policy 3.5 requires that HSPnet Policies on Privacy, Security & Data Access be made available on the HSPnet website or upon request by a student to the HSPnet Privacy Officer. This policy, and *Identified Purposes* handout provided to students, also states that a student may register a complaint or challenge regarding the handling of personal information in HSPnet in writing to the BCAHC Privacy Officer, who will investigate the complaint/ challenge through the involved Participating Agency.

The *Consent Form for Use and Disclosure of Student Information* and *Identified Purposes* handout directs students to the HSPnet website for up-to-date contact information for the Privacy Officer, and in Manitoba the website includes a specific reference to their ability to make a complaint to the Manitoba Ombudsman.

Attachment ( ) or Action Plan ( ):[9]

[9] Please mark with an "X" in parentheses if included with this assessment.

ELEMENT 7

ACCOUNTABILITY AND OPENNESS OF POLICIES AND PRACTICES

An organization is responsible for *personal* or *personal health information* in its custody or under its control, and specific individuals are designated by law, regulation or policy to be accountable for the organization's compliance with established privacy principles. (FIPPA Sections 80, 81, Regulation 64/98 Sections 1, 2; PHIA Sections 57, 58)

Under FIPPA Section 75, a *public body* must make certain basic information relating to the management of *personal information* available to the public.

Privacy Compliance "Checklist"

1. It is understood and known in the organization that the Head of a provincial government department or agency, or the Head of a *local public body*, or a *trustee* is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded.

Yes X **No □**

Explanation:

The HSPnet Data Sharing Agreement acknowledges the respective responsibilities of the Head and trustees for compliance with access and privacy legislation, and formally records any delegation of these powers and duties and any obligations in place as a result of this delegation.

Attachment (X) or Action Plan ( ):

Appendix 5: *HSPnet Data Sharing Agreement*

2. An employee (or employees) within the organization is formally delegated responsibility for the daily administration of privacy compliance ("access and privacy coordinator" under FIPPA, "privacy officer" under PHIA). The identity of the individual(s) is known throughout the organization.

Yes X **No □**

Explanation:

The HSPnet public website lists the identity and contact information for the national HSPnet Privacy Officer and for each jurisdiction-specific Privacy Officer. In addition, all key documents relating to privacy and security of personal information notes the existence of HSPnet and local privacy officers and directs the reader to the public website for access to their contact information.

Attachment ( ) or Action Plan ( ):

3. There are written organizational policies and procedures that define the responsibility for protecting *personal* and *personal health information*.

Yes X **No** □

Explanation:

Embedded in HSPnet Policies, and as referenced throughout the PIA, are descriptions of the organizational responsibilities and physical, administrative and technical procedures responsibility for protecting PI and PHI.

Attachment ( ) or Action Plan ( ):

4. Appropriate staff is provided with on-going training to implement privacy policies and procedures.

Yes X **No** □

Explanation:

HSPnet Policy 3.1 assigns responsibility to the BCAHC CEO for ensuring that all BCAHC staff and contractors, acting in roles that involve access to PI and PHI within the HSPnet database, receiving appropriate training on HSPnet Policies on Privacy, Security and Data Access.

Attachment (X) or Action Plan ( ):

5. Other parties, such as *information managers* and agents, who may have authorized access to *personal* or *personal health information* under Parts 3 of FIPPA or PHIA are aware of, and comply with, organizational privacy policies and relevant procedures.

Yes X **No** □

Explanation:

In general, information managers and agents do not have authorized access to PI or PHI in HSPnet. In the event that such an individual requires access, they would receive the same training as is provided to BCAHC staff and contractors.

Attachment ( ) or Action Plan ( ):

6. Individuals can obtain information about privacy policies and procedures with reasonable ease.

Yes X **No □**

Explanation:

HSPnet privacy Policies and procedures are referenced in all key HSPnet documents regarding privacy, are summarized as appropriate in the *Identified Purposes* handout for students and during staff and user training or upon reset of user passwords, and are published in full on the public website.

Attachment ( ) or Action Plan ( ):

7. Under FIPPA, *Personal Information Banks* have been identified, described, are up-to-date, and publicly available as required. [Note that PHIA does not have a corresponding provision in relation to production of a directory including a description of personal information banks.]

Yes X **No □**

Explanation:

Student information is organized within an HSPnet sub-database specific to each educational institution. Student name and student number are recommended to uniquely identify students within an educational institution; student number is never released outside of the student's educational program and is not used to link and/or uniquely identify students across multiple educational institutions (i.e. if a student has been registered in two different educational institutions. Student information banks are identified, described, and updated by a student's educational program as needed to maintain data quality for the *Identified Purposes*. It is the responsibility of each public body using HSPnet to ensure that they list HSPnet as a bank in which it holds personal data.

Attachment ( ) or Action Plan ( ):

8. Under FIPPA and in the case of a *public body* that is not a *local public body*, (1) a record is kept of uses and disclosures not included in the publicly available "Access and Privacy Directory", (2) this record is attached or linked to the *personal information* involved, and (3) a process is in place to have this information included in the "Access and Privacy Directory". [Note that PHIA does not have a directly corresponding provision.]

Yes X **No □**

Explanation:

A Placement Request history table records revisions to HSPnet placement transactions (including disclosure of PI of students that may be assigned to that Placement if confirmed), and a separate history table is maintained of all revisions and disclosures of student information.

Attachment ( ) or Action Plan ( ):

9. A procedure exists for responding to questions or concerns about privacy practices.

Yes X **No** □
Explanation: Policy No. 3.5 describes the procedures that direct responses to questions or concerns about privacy practices.
Attachment ( ) or Action Plan ( ): Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* - Policy 3.5

ELEMENT 8

ASSESSING PRIVACY RISKS IN ELECTRONIC SERVICE DELIVERY (ESD)

Ideally, privacy implications should be considered at the earliest stages of electronic service delivery (ESD) systems design. To avoid potentially costly modifications, fair information practices must be considered in the concept and system definition phases, and continue during the decision-making about use of the data through to final systems design and approval. A privacy impact assessment by the client organization is often an indispensable front-end part of the process, but it is important to recognize that the assessment needs to evolve with the system and be an integral reference point for subsequent maintenance and upgrades.

Privacy assessments should also be considered for existing systems, particularly when they are subject to major maintenance work or are being upgraded.

The principles reflected in Elements 1-7 of this Privacy Compliance Checklist may form the privacy-planning framework for policy choices and ESD technical design. PHIA and FIPPA do not in themselves restrict organizations to specific technologies or modes of delivery, but the organizations are expected to follow and be able to demonstrate informed decision-making where ESD systems will process *personal* and *personal health information*.

The questions in Element 8 will help determine whether privacy risks associated with electronic service delivery have been considered. They are intended to support the analysis of both simple and complex electronic service delivery options. These options include delivery of services through the public service administration, through private sector channels, or through public-private partnerships.

NOTE: *Explanations and/or Action Plans should be provided for all questions contained in this Element, regardless of a "yes" or "no" response.*

Privacy Compliance "Checklist"

1. Are diagrams available to illustrate the flow of *personal* and *personal health information* for this project?

Yes X **No □**

Explanation:
Privacy implications were a component of the HSPnet design process from the earliest stages of system development, in April 2002, through consultation with an independent privacy expert. Prior to any system design or development, a privacy model was designed, reviewed widely across project participants and through the public project website, and published in key design documents and in the Privacy Impact Assessment for BC.

Attachment (X) or Action Plan ( ):[10]
Appendix 12: *HSPnet Data Workflow and Privacy Model*

[10] Please mark with an "X" in parentheses if included with this assessment.

2. Has responsibility for control and custody for all *personal* or *personal health information* processed by the ESD system been identified and assigned?

Yes X **No □**

Explanation:

The HSPnet Parnership framework, HSPnet Policies, and the HSPnet Data Sharing Agreement identify and assign responsibilities for control and custody of all PH and PHI in HSPnet.

Attachment ( ) or Action Plan ( ):

Appendix 1: *HSPnet Partnership Structures, Roles and Responsibilities*

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access*

Appendix 8: *HSPnet Data Sharing Agreement*

3. If the ESD system will process transactions for more than one program, agency or department, have constraints been placed on data integration?

Yes X **No □**

Explanation:

HSPnet transactions are strictly segregated through Access Rights to ensure that each user can see only those transactions and information (and any PI or PHI that may be included) on a need to know basis and as appropriate for their role within their program, agency or department. No individuals except BCAHC staff and contractors in user support or system development/support roles, who are bound by a signed agreement on Confidentiality and Rules of Conduct, have access to identifiable PI or PHI across organizational boundaries. Policy 3.6 requires that only a jurisdiction-specific Data Stewardship Committee may approve requests for data (including or excluding personal identifiers) that cross organizational boundaries, and even then only as consistent with the *Identified Purposes* and HSPnet Policies.

Attachment ( ) or Action Plan ( ):

4. If this ESD project involves the use of common identifiers or a common identification infrastructure, have privacy-enhancing measures been considered to limit risks to privacy?

Yes □ **No □**

Explanation:

Not applicable. No common identifiers are used within HSPnet, only organization-specific identifiers that exist to uniquely identify a student for activities consistent with the Identified Purposes.

Attachment ( ) or Action Plan ( ):

5. Will this ESD initiative require *data linking* (data profiling) *or data matching*?

Yes □ **No X**

Explanation:

No data linking or data matching (across organizational boundaries) is undertaken within each jurisdiction's instance of HSPnet, nor is data linking or matching undertaken across provincial instances.

Attachment ( ) or Action Plan ( ):

6. Is there a means of obtaining, authenticating, registering and maintaining individual *consent* electronically, where required?

Yes □ **No X**

Explanation:

Student consent is obtained in writing during their registration into an educational program or during the program if necessary. Electronic consent processes are not in place at this time.

Attachment ( ) or Action Plan ( ):

7. Have privacy-enhancing technologies and/or techniques been considered for this ESD project?

Yes X **No** □

Explanation:

HSPnet employs use of anonymity in transactions until the placement is confirmed by the educational program, or student name may be disclosed at the educational program's discretion during the request consideration process if the Receiving Agency demonstrates a need to know. An educational program user's decision to disclose student information before confirmation is tracked in a history table, and quarterly audits of early releases are performed and reported to the National HSPnet Steering Committee and to local Data Stewardship Committees.

Complex screen rules determine what data is released at various points in the placement cycle, as appropriate for the user's organizational role and associated need to know. All HSPnet data transmissions are secured via industry-standard tools that provide 128-bit encryption. System requirements for user access to HSPnet include a minimum specified version of Internet Explorer, capable of accommodating 128-bit encryption.

In general, privacy is protected in HSPnet through application design (in the form of user authentication processes, system timeouts, and data encryption) as based on policies that permit minimal collection of PI and PHI and that permit use and disclosure in a phased manner throughout the placement process, based on a user's need to know.

A combination of user training and procedural/technical safeguards are used to further mitigate privacy risks, as outlined in HSPnet Policy 3.4.

Attachment (X) or Action Plan ( ):

Appendix 4: *HSPnet Policies on Privacy, Security and Data Access* – Policy 3.4

8. Have all the risks to privacy for this ESD initiative been identified and documented?

Yes X **No** □

Explanation:

The planning process that led to development of the original PIA in BC identified and documented five potential areas for privacy risk:

- Gaps in HSPnet Policies or procedures;
- Inappropriate or ineffective processes to inform students and obtain their consent;
- Design deficiencies that fail to address requirements of HSPnet Policies and procedures;
- User error (unintentional use/disclosure of information that exceeds the *Identified Purposes*, use/disclosure to authorized individuals in a manner inconsistent with *Identified Purposes*, or use/disclosure to unauthorized individuals); and
- Intentional privacy breaches (unauthorized system access, unauthorized direct access to the database or bypassing of the application layer).

All were considered when designing privacy enhancing process and technology, and monitoring activities are in place to ensure ongoing mitigation of these risks.

Attachment ( ) or Action Plan ( ):

9. Have all risks to privacy for this ESD project been minimized or averted?

Yes X **No** □

Explanation:

The PIA process in BC, and subsequent system design of HSPnet, addressed the five privacy risk factors identified above through design of a privacy framework based on the 10 Principles of the CSA Model Code. HSPnet Policies on Privacy, Security and Data Access address all five risks within the framework of the 10 Principles, and all subsequent documents and processes (role descriptions and accountability structures, agreements, consent forms and handouts, monitoring processes, etc.) are driven from the HSPnet Policies.

A feasibility study for introducing HSPnet across Western Canada as conducted in Spring 2005, involving a review of several feasibility dimensions including system scalability and technical issues, user functionality requirements, and legislated privacy requirements and best practices of the four provincial jurisdictions. An external privacy consultant reviewed the HSPnet Policies, data workflows and privacy framework, and assessed them against the legislative requirements in each province. The consultant's findings were that the HSPnet Policy requirement for active student consent provides a high standard of privacy protection, and that *HSPnet Policies on Privacy, Security and Data Access* represent best practices that can be applied to meet provincial requirements. Her analysis concluded that "… given the current practice of obtaining "active consent" from students, no major differences exist in the privacy legislation of any Western province that would create barriers to the implementation of HSPnet."

Attachment ( ) or Action Plan ( ):

10. Has a comprehensive risk analysis been undertaken to identify and implement appropriate ongoing monitoring and regular auditing requirements to protect *personal* and *personal health information*, including that of end-users, for all aspects of the ESD system?

Yes X **No** □

Explanation:

The original privacy risk analysis is updated and applied on an annual basis during review of HSPnet Policies on Privacy, Security, and Data Access. All proposed changes to Policies are reviewed to ensure there are no unintended or negative impacts on the five privacy risks identified.

The National HSPnet Steering Committee met in March 2006 to undertake a strategic planning exercise. The resulting strategic plan will drive development of a comprehensive Management Framework (draft to be reviewed at the October 2006 meeting) encompassing all performance evaluation and quality dimensions for the Partnership including privacy protection, system performance, user and stakeholder satisfaction, and cost-effectiveness. Each performance and quality dimension will include an external assessment component, which will dovetail existing external reviews (e.g. recent assessment of the SLA and associated processes with BCIT) and may lead to additional external assessments including those for privacy and security, and a usability review.

Attachment ( ) or Action Plan ( ):

11. Have key stakeholders been consulted about the privacy implications of this project?

Yes X **No** □

Explanation:

In addition to the Western Canada Feasibility study, which involved province-wide user consultation workshops in each province, implementation planning for HSPnet in Manitoba has involved informal and user consultation processes including HSPnet information sessions and system demonstrations, a facilitated implementation planning workshop, publication of draft versions of this PIA on the HSPnet-MB News (public) website, and formal distribution of the document to participating educational institutions for consultation with their organizational privacy offices.

Attachment ( ) or Action Plan ( ):

12. Where risks to privacy are not completely mitigated, is there a strategy for responding to public concerns over privacy protection?

Yes X **No** □

Explanation:

All identified privacy risks have been documented, as well as ongoing activities directed at mitigating these risks and monitoring effectiveness of mitigating activities over time. Strategies for responding to public concerns over privacy protection include a transparent approach to communicating with students, staff, industry stakeholders, other provinces, and the public. In general, all project documentation relating to privacy and security, excluding those that may divulge specific security measures that would increase privacy risks, are published on the public website. Students and the public are invited to communicate with the HSPnet Privacy Officer or local Privacy Officers in order to ask questions or to voice concerns.

Attachment ( ) or Action Plan ( ):

13. Have constraints been placed on ESD service providers regarding the *collection*, *use* and *disclosure* of information subject to FIPPA or PHIA?

Yes X	**No □**

Explanation:

Restrictions on service providers are in place regarding the collection, use and disclosure of all identifiable information of individuals, including that which falls under FIPPA or PHIA. Such restrictions are defined through HSPnet Policies, Service Level Agreements, Agreements on Confidentiality and Code of Conduct for staff and contractors, and through regular audits and monitoring of data accesses and uses.

Attachment ( ) or Action Plan ( ):

14. Do all contracts related to the implementation of this ESD project contain data protection provisions?

Yes X	**No □**

Explanation:

All contracts between the BCAHC and contractors and external service providers contain provisions for the privacy and security of all HSPnet data and intellectual property.

Attachment ( ) or Action Plan ( ):