The Saskatchewan Privacy Impact Assessment

INTRODUCTION:

PROJECT INFORMATION

Date: March 31, 2007
Name of Organization and Program Area: Submitted by the Saskatchewan Academic Health Sciences Network (SAHSN), on behalf of the Saskatchewan User Community of HSPnet-SK (SKUC), comprised of regional health authorities, health service providers, and post-secondary educational institutions that use HSPnet-SK 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: Tammy Ives, Clinical Education Resource Officer Saskatchewan Academic Health Sciences Network
Telephone and FAX: Phone: (306) 966-1395 Fax: (306) 966-2898
Address: Room 427, RJD Williams Building 221 Cumberland Avenue North Saskatoon SK S7N 1M3
E-mail: tammy.ives@usask.ca

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

DESCRIPTION OF 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 Saskatchewan. Students to be placed are generally enrolled in schools within Saskatchewan, although HSPnet will allow Receiving Agencies in Saskatchewan 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 in other provinces.

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.

Attachments:

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

MANDATE AND FUNCTIONS OF INITIATIVE

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 Saskatchewan. 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.

PREVIOUS PRIVACY IMPACT ASSESSMENTS FOR THIS 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.

Worksheet for The Freedom of Information and Protection of Privacy Act (FOIP) Privacy Impact Assessment

I. Definition of personal information & authorization to collect, use, and disclose

Question	Yes	No
Is personal information being collected?	X	

Notes: Personal information (PI) is collected by Placing Agencies at the time of registration of students into an educational program, and throughout the student's educational program. A subset of this information, suitable for coordinating placements as required by the student's educational program, may be entered into HSPnet and used/disclosed as described in this document.

Placing Agencies may also collect (and enter into HSPnet) information that could be categorized as personal health information (PHI). 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.

Question	Yes	No
What personal information is being collected?	X	

Notes: The document entitled *HSPnet Data Uses Table* provides a detailed description of the personal data elements including PI and PHI stored in HSPnet. It also includes details on the specific data uses, levels of identification, and disclosure recipients.

Attachments:

Appendix 1*: HSPnet Data Uses Table*

Question	Yes	No
Is the organization recognized as a "government institution" (FOIP) and accountable under either legislation for the collection, use, and disclosure of personal information?		X

Notes:
Saskatchewan Academic Health Sciences Network, is an organization comprised of the University of Saskatchewan, Saskatoon Health Region, Regina Qu'Appelle Health Region, other provincial Health Regions, Saskatchewan Institute for Applied Science and Technology, University of Regina, and the Province of Saskatchewan. Individual partners maintain their primary responsibilities, but where joint collaboration can enhance optimal delivery of service to clients, the Saskatchewan Academic Health Sciences Network is expected to assist through collaborative practices and processes in the achievement of enhanced service, research, and teaching.

The Saskatchewan Academic Health Sciences Network will carry out its mandate of enhancing clinical services, conducting health research, and educating future health care professionals through the joint and collaborative relationship of its interdependent partners. The Network will ensure an effective, accountable, and visionary governance and management structure through which collaborative service, research, and teaching will be delivered.

SAHSN has entered into an HSPnet licensing agreement with the BCAHC on behalf of SKUC members. SAHSN will in turn enter into sub-licensing agreements with each Placing and Receiving agency using HSPnet-SK. One of the roles of the SAHSN Advisory Council for Clinical Placements will be to act as the HSPnet Management Team.

Attachments:

SAHSN Terms of Reference

II. Access of Individuals to Personal Information for Amendment and Review

Question	Yes	No
Are policies and procedures in place to accommodate individual requests for access to personal information?	X	

Notes: HSPnet operations in each province are governed by national *HSPnet Policies on Privacy, Security and Data Access.*

Policy 3.2 outlines the rules by which individuals access identifiable personal information in HSPnet. The rules limit access to personal information that is appropriate given the individual's organizational role, involvement in the student placement process, and associated "need to know."

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 screens that display individual placements within their program areas and the students/staff assigned to them.
- User Level determines whether a user has read-only rights (e.g. an Instructor), create/edit rights as required by Placing and Receiving Coordinators, or Local Administrator rights which are granted to a limited number of users within each agency/program for the purpose of setup table management and for creating and maintaining User ID's within their areas of responsibility.
- 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.

Policy 3.6 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.

Attachments:

Appendix 3: *HSPnet Policies on Privacy, Security and Data Access*

Question	Yes	No
Are there policies and procedures in place to, when appropriate, deny an individual request for access to personal health information?	X	

Notes: HSPnet Policies 3.2 and 3.6 define the limits of individual access, both for routine transaction-based activities and when seeking aggregate or summary data (reports). The HSPnet Director applies these policies and the Data Access Guidelines in Policy 3.6 to approve or decline requests for ongoing access (a new user ID) or for access to reports or data extracts. The Director has declined requests for access that are not consistent with the policies. Examples of declined requests include those for "convenience" access (e.g. for access by IT staff to issue computer ID's) or for uses that are not consistent with the *Identified Purposes* (e.g. to contact students post-placement for recruitment purposes).

Question	Yes	No
Are there procedures in place to correct an individual's personal information, if requested?	X	

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

> A student may request changes to their personal information contained in HSPnet by submitting a request in writing to the placement coordinator of their educational program. If the request cannot be accommodated, the educational program will provide a written explanation of the reasons that their request cannot be granted and a notation will be made on the student's record that their request for a change was refused.

Students are notified of these mechanisms on the *Identified Purposes* handout, which also references the full policies and information about contacting a Privacy Officer, as available on the public website.

Question	Yes	No
Are there policies and procedures in place to ensure that personal information is as accurate and complete as possible?	X	

Notes: 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 such as student profiles, class lists, and placement schedules are also useful for monitoring by practicum coordinators and instructors for data accuracy and completeness.

III. Limits on Collection, Use, and Disclosure

Question	Yes	No
Is personal information collected for a program, activity, or service that will be of benefit to the subject individual?	X	

Notes: 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*, and supports processes limited to:

- Identifying 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.

Question	Yes	No
Is personal information being collected directly from the individual? In the situation(s) where personal information is NOT collected directly from the individual, is it collected in a manner allowed by legislation?	X	

Notes: 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.

As outlined in Policy 3.3 and the *HSPnet Data Sharing Agreement* between the BCAHC and each agency using HSPnet, 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, and are carried out within the specific requirements of the *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.

Attachments:

Appendix 4: *HSPnet Data Sharing Agreement*

Question	Yes	No
Will individuals be informed as to the anticipated uses and/or disclosures of their personal information?	X	

Notes: HSPnet Policies require *active consent* from students based on information about the permitted use and disclosure of their personal information via HSPnet, as detailed in the student handout that

accompanies their consent form *Identified Purposes and Handling of Personal Information and Personal Health Information in HSPnet*.

Policy 3.2(3) of HSPnet Policies on Privacy, Security and Data Access states:

> All personal information to be used or disclosed via HSPnet will be described clearly by the *Identified Purposes* and the amount and type of information, and length of time that the personal information is retained, will be limited to that required to meet the Identified Purposes.

Attachments:

Appendix 5*: Consent Form for Use and Disclosure of Personal Information*

Appendix 6*: Identified Purposes and Handling of Personal Information and Personal Health Information in HSPnet*

Question	Yes	No
Is personal information being used for its originally prescribed purpose? If not, has consent been obtained to use the information in a different manner than originally intended?	**X**	

Notes: Policy 3.2(10) of HSPnet Policies on Privacy, Security and Data Access states:

> 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.

Question	Yes	No
Will consent be *obtained from* the individual before the disclosure of personal information?	**X**	

Notes: 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. However, in recognition of the challenges of implementing a procedure to obtain signed consent for previously registered students during HSPnet implementation, *Policy Application Guide* for Policy 3.2 recommends options for entering student information into HSPnet in parallel with efforts to obtain a signed consent form s*o long as another acceptable consent or notification process is already in place for those student*s, such as:

- Consent form whereby students authorize the educational institution and/or specific Program to release their information to placement sites (sometimes worded as “prospective employers”);
- General consent form of the institution or Program on release of student information for related educational purposes;
- Notification received by all students in the school calendar or other documentation, on the use/ disclosure of their information;

Attachments:

Appendix 7: *Policy 3.2 – Policy Application Guide*

Question	Yes	No
In the event that consent is not obtained for the disclosure of personal information, will disclosure(s) be made in accordance with situations approved by legislation?		

Notes: Not applicable. Consent is obtained as noted above prior to using or disclosing a student's identifiable information via HSPnet.

Question	Yes	No
Are there policies and procedures in place to accommodate the disclosure of personal information belonging to a person that is deceased?	X	

Notes: A deceased individual would be withdrawn from their educational program, which results in automatic withdrawal of the student's consent for continued use/disclosure of their personal information. Once a student's consent is withdrawn or expired, then ongoing use of their identifiable personal information is permitted only in limited situations as per Policy 3.2(12):

> Personal information may be stored in HSPnet archives beyond the consent period, in accordance with Data Retention and Archival schedule approved by the HSPnet Steering Committee, for the following specific and limited purposes:
>
> - Release to a student, upon written request accompanied by proof of identification, of a copy of their own placement history;
> - Compliance with a subpoena or other legally binding access to the information;
> - Quality assurance or research purposes that involve use of de-identifiable data only.

Worksheet for the Organizational Privacy Practices

2. Questions Dealing with Organizational Privacy Practices

Note: While not part of the worksheet template provided, the following questions relating to Organizational Privacy Practices and Program/Project Privacy Practices were copied from the website of the Office of the Saskatchewan Information and Privacy Commissioner into this document, in the same format as provided for FOIP questions in order to provide a consistent approach.

I. Organizational Governance

Question	Yes	No
Is there an organizational strategic plan or business plan that clearly addresses privacy protection?	X	

Notes: Privacy implications were a component of the HSPnet design process from the earliest stages of system development, during 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.

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."

The National HSPnet Steering Committee met in March 2006 to undertake a strategic planning exercise. The resulting strategic plan has driven development of a comprehensive Management Framework (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.

Question	Yes	No
Does a written privacy charter or policy exist?	X	

Notes: The National HSPnet Steering Committee maintains a comprehensive privacy and security program as encompassed by HSPnet Policies Section 3. The privacy and security program is based on the Privacy Model developed during HSPnet Design.

Attachments*:*

Appendix 8*: HSPnet Data Workflows and Privacy Model*

Question	Yes	No
Have privacy guidelines been developed for various aspects of the organization's operations?	X	

Notes: Ongoing maintenance and enhancement of HSPnet-SK is the responsibility of the BCAHC as service provider to provinces operating HSPnet. The BCAHC is directed in its activities by the national HSPnet Policies, which are the responsibility of the national HSPnet Steering Committee.

Attachments*:*

Appendix 9*: Terms of Reference - National HSPnet Steering Committee*

Question	Yes	No
Is there an appointed privacy director or champion within the organization?	**X**	

Notes: In its role as service provider to the national Partnership, the BCAHC has designated a national Privacy Officer for HSPnet to act as a central point of contact as needed, to support local privacy officers in each jurisdiction, to coordinate privacy officer orientation and communications across provinces, and to identifies trends or problems that may require review and/or action by the national HSPnet Steering Committee.

As identified in the "Partnership Roles" diagram in the Steering Committee Terms of Reference (Appendix 9), each province or jurisdiction appoints a local Privacy Officer for their HSPnet instance. The local Privacy Officer reports to the jurisdiction's Data Stewardship Committee, which is accountable to user agencies and responsible for ensuring that their jurisdiction's instance of HSPnet complies with applicable provincial legislation.

Attachments*:*

Appendix 10*: Role description for the HSPnet Privacy Officer*

Appendix 11: *Terms of Reference – Data Stewardship Committee*

Question	Yes	No
Does a management reporting process exist to ensure that management is informed of any privacy compliance issues?	**X**	

Notes: The national HSPnet Steering committee is accountable to each partner jurisidiction (in this case, to SAHSN and to the SKUC) for annual review and approval of the Policies including definition of key security standards such as those for password expiry and system inactivity timeout.

The national HSPnet Steering Committee is also responsible for oversight and evaluation of monitoring activities as required by the Policies. For example, the Steering Committee will define the nature and minimum frequency of audits as required by Policy 3.4 to identify instances of inappropriate access and unauthorized release of personal information.

Each province's local Data Stewardship Committee is responsible for application of the Policies and local processes as needed to ensure the integrity of user data, protection of privacy and security of personal information, and permitted uses of data to support business objectives. The Data Stewardship Committee for HSPnet-SK will report on local monitoring activities and the results of compliance and enforcement activities to the SKUC, and will provide an annual report of these activities to the national HSPnet Steering Committee for monitoring and oversight.

Question	Yes	No
Is senior management actively involved in the development, implementation and/or promotion of privacy measures within the organization?	**X**	

Notes: As oulined in Policy 3.0 the BCAHC, as service provider to the national HSPnet Partnership and to each provincial instance including HSPnet-SK, has assigned accountability to the CEO for maintaining a comprehensive privacy and security program for HSPnet as outlined in the Policies.

HSPnet Policies are governed by the national HSPnet Steering Committee, which is comprised of senior representatives from each jurisdiction represented in the HSPnet partnership. Each jurisdiction must identify a Lead Agency, in this case the SAHSN, to identify senior management representatives to the Steering Committee, to establish an HSPnet-SK Management Committee, and to establish an HSPnet-SK Data Stewardship Committee.

Question	Yes	No
Is it understood in the organization that the Head is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded?	**X**	

Notes: The HSPnet Data Sharing Agreement (Appendix 4), which will be signed by the BCAHC and each organization using HSPnet, 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.

Question	Yes	No
Are there written organizational policies and procedures that define the responsibility for protecting personal information/personal health information?	**X**	

Notes: 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.

II. Human Resource Practices

Question	Yes	No
Do employees with access to personal information/personal health information receive training related to privacy legislation as well as organizational privacy policies and practices?	**X**	

Notes: BCAHC staff and contractors (supporting the BCAHC's role as service provider to HSPnet-SK) who have access to HSPnet data are trained at a 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.

Attachments:

Appendix 12: *Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers*

Question	Yes	No
Is an employee within the organization formally designated responsibility for the daily administration of privacy compliance? Is the identity of the individual known throughout the organization?	**X**	

Notes: 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 note the existence of HSPnet and local privacy officers and direct the reader to the public website for access to their contact information.

Question	Yes	No
Is there a list of the staff positions or categories that use this personal information/personal health information?	X	

Notes: 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* (Appendix 1).

The HSPnet Director maintains a list of all staff and contractors that may access personal information in their role as service provider. This list is maintained on the HSPnet Administrative intranet site, which is accessed by the BCAHC CEO and Business Manager, HSPnet staff and contractors, and local Privacy Officers in each province.

Question	Yes	No
Do staff receive ongoing training about security policies and procedures, and are they made aware of the importance of security and confidentiality on an ongoing basis?	X	

Notes: 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.

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.

Attachments:

Appendix 13: *Course Outlines – HSPnet Training*

Question	Yes	No
Can individuals within the organization obtain information about privacy policies and procedures with reasonable ease	X	

Notes: 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 (which is linked directly to the HSPnet application and referenced specifically on certain Help screens and warnings/error messages).

III. Privacy Controls and Security

Question	Yes	No
Have security procedures for the collection, transmission, storage, and disposal of personal information/personal health information, and access to it, been documented?	X	

Notes: Data management and security procedures are documented in HSPnet Policy 3.4. In general, data security is protected through application design (in the form of user authentication processes, system timeouts, and data encryption) and through the policies and procedures of the server host provider (BC Institute of Technology), whose practices are defined within a Service Level Agreement with the BCAHC. The BCAHC is accountable for evaluating the security policies and procedures and physical arrangements at BCIT on an annual basis.

The relatively low volume of HSPnet data has not necessitated any archival or disposal to date. In anticipation of archival requirements within the coming three to five years, a data archiving and retrieval strategy is currently under development.

Question	Yes	No
Is there an audit trail maintained to document when and by whom a file or record was created, updated, or viewed?	X	

Notes: 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 also 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.

Question	Yes	No
Does staff maintain a disclosure log or audit trail of: i. What information has been disclosed ii. The recipient iii. Purpose and authority for the disclosure	X	

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

Question	Yes	No
Are access logs and audit trails reviewed on a regular basis?	X	

Notes: 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.

Question	Yes	No
Are there written information security policies including a definition of roles and responsibilities and sanctions for breaches of policy?	X	

Notes: 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.

Question	Yes	No
Are there security measures in place for personal information/ personal health information regardless of media format?	X	

Notes: 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 otherwise 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.

Question	Yes	No
Is access to personal information/personal health information regularly monitored and audited?	X	

Notes: 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.

Question	Yes	No
Are users assigned unique user identifications and passwords for access to personal information/personal health information and are passwords changed regularly?	X	

Notes: 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 other 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.

Question	Yes	No
Are access privileges revoked promptly when required (e.g. when an employee leaves or moves)?•	X	

Notes: As outlined in Policy 3.4, users are required to notify their local HSPnet Administrator to changes in their role that would necessitate changing their access rights or user level. In addition to this voluntary responsibility and the responsibility of Local Administrators to monitor and act upon inactive users or role changes, the HSPnet team automatically cancels users ID's that have been inactive for six months (as per the schedule reviewed annually by the National HSPnet Steering Committee). 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 at this time. 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.

Question	Yes	No
Are external providers of information management or technology services covered by written agreements dealing with risks including unauthorized access, use, disclosure, retention, and destruction or alteration as a best practice?	X	

Notes: The SLA between the BCAHC and BCIT, and the HSPnet Confidentiality Agreement and Code of Conduct (Appendix 12) with all staff and contractors, document the responsibilities and obligations of external providers in protecting data privacy, security and integrity.

BCIT processes for managing privacy and security risks include:

- Agreement on minimum physical security standards to the data centre, at this time including swipe card door locks and discrete access to the computer room for authorized staff with a direct need for access. Logs of swipe card access are stored and are searchable for forensic audit.
- Limited electronic access to all data stores through 2 level secured logon, for staff with a direct need only as a result of their technical role; logs are maintained and available for forensic audit.

The HSPnet Data Sharing Agreement details specific requirements in each jurisdiction and may result over time in the need for additional language in the BCIT SLA and/or the agreement with BCAHC staff and contractors.

Worksheet for the Program/Project Privacy Practices

3. Questions Dealing with Program/Project Privacy Practices

Question	Yes	No
Has a listing of all personal information/personal health information or data elements to be collected, used or disclosed in the project/program been prepared?	X	

Notes: The *HSPnet Data Uses Table* (Appendix 1) provides detailed documentation on the PI and PHI that are used and disclosed via HSPnet.

Question	Yes	No
Is there a detailed description of the type of personal information/ personal health information collected for this project/program?	X	

Notes: The *HSPnet Data Uses Table*, referenced above, provides a detailed description of the personal data elements including personal information (PI) and personal health information (PHI), and explains when this information may be anonymous, identifiable, and de-identified.

Question	Yes	No
Have diagrams been prepared depicting the flow of personal information for this project/program?	X	

Notes: A document entitled *HSPnet Data Workflow and Privacy Model* (Appendix 8) was prepared during the 2002 design stages of HSPnet, and is updated upon any material changes as a permanent record to depict the flows of personal information in HSPnet.

Question	Yes	No
Are there physical, administrative and technical controls that limit access to identifiable personal information/personal health information to those who have a need to know?	X	

Notes: All access to identifiable data is determined by organizational role and need to know. Where data is required to manage programs and calculate statistics such uses do not require identifiable data and hence such users do not see identifiable data.

As detailed in Policy 3.4, a combination of controls are used to mitigate privacy risks including limit of access to PI and PHI by those who have a need to know. 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.

Question	Yes	No
Have documents been prepared showing which persons, positions or employee categories will have access to which personal information/personal health information?	X	

Notes: See previous reference to *HSPnet Data Uses Table* (Appendix 1).

Question	Yes	No
Is the least amount of personal information/personal health information collected and used to meet the stated purpose?	X	

Notes: The HSPnet dataset, 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, and upon material changes to the dataset 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.

Question	Yes	No
Will personal information/personal health information collected or used in this project/program be disclosed to any persons who are not employees of the responsible organization?	X	

Notes: Personal information will be disclosed only with student consent to authorized users (staff or contractors) of the receiving site for the student, on a need to know basis as permitted by HSPnet Policies. No other disclosures of personal information are permitted via by system rules or by direct request to the BCAHC or it staff/contractors.

LIST OF APPENDICES

Appendix 1: HSPnet Data Uses Table

Appendix 2: SAHSN – Terms of Reference

Appendix 3*:* HSPnet Policies on Privacy, Security, and Data Access

Policy No. 3.0: Privacy and Security – General
Policy No. 3.1: Accountability
Policy No. 3.2: Identified Purposes and Ensuring Consent for Data Collection, Use and Disclosure
Policy No. 3.3: Accuracy of HSPnet Data
Policy No. 3.4: Safeguards for HSPnet Data
Policy No. 3.5: Openness, Individual Access and Challenging Compliance of HSPnet Data
Policy No. 3.6: Access to HSPnet Data

Appendix 4: Data Sharing Agreement

Appendix 5: Consent Form for Use and Disclosure of Personal Information

Appendix 6: Identified Purposes and Handling of Personal Information and Personal Health Information in HSPnet

Appendix 7: Policy 3.2 – Policy Application Guide

Appendix 8: HSPnet Data Workflow and Privacy Model

Appendix 9*:* Terms of Reference National HSPnet Steering Committee

Appendix 10: Job Description – HSPnet Privacy Officer

Appendix 11: Terms of Reference for the Data Stewardship Committee

Appendix 12: Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers

Appendix 13: Course Outlines – HSPnet Training

LIST OF ACRONYMS

HSPnet – the Health Sciences Placement Network – the application that is licensed by the BCAHC at no charge to Canadian provinces participating in the national partnership.

HSPnet-SK – the Health Sciences Placement Network of Saskatchewan – the copy or “instance” of HSPnet that is operated by the BCAHC on behalf of users in Saskatchewan

BCAHC – the BC Academic Health Council

SAHSN – the Saskatchewan Academic Health Sciences Network

SKUC – the Saskatchewan User Community – agencies authorized to use HSPnet-SK via a sublicensing agreement with SAHSN