MEMORIAL UNIVERSITY

Information Access and Privacy Protection

HSPnet Newfoundland and Labrador

Privacy Impact Assessment

Health Sciences Placement Network:
Newfoundland and Labrador User Community

Developed by IAPP Office and School of Nursing
Memorial University of Newfoundland
In collaboration with BC Academic Health Council
12 September 2013

INTRODUCTION

Memorial University's Privacy Policy guides the University's compliance with the *Access to Information and Protection of Privacy Act,* S.N.L. 2002, Chapter A-1.1, as amended (*"ATIPP Act"* or *"the ATIPPA"* or *"the Act"*), and other relevant privacy legislation. The Policy incorporates the principles of the Canadian Standards Association's Model Privacy Code, which itself forms part of Canada's *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5).

The Privacy Policy requires that all new programs and projects at the University that involve personal information be reviewed *prior* to implementation for compliance with privacy law and the policy.

> *8. To monitor compliance with the Privacy Policy, all projects involving personal information must be reviewed using the Privacy Compliance Checklist, in accordance with the PROCEDURE FOR CHECKING PRIVACY COMPLIANCE. This may determine that a Privacy Impact Assessment is required. This compliance requirement does NOT apply to research projects involving human participants which have received ethics approval from a duly-constituted research ethics board, including a research ethics body under the Health Research Ethics Authority Act.*
> From Privacy Policy
> Available at: http://www.mun.ca/policy/site/policy.php?id=145

The School of Nursing contacted the IAPP Office in June 2012 and requested its assistance in a privacy compliance review of the School's participation in the Health Sciences Placement Network (HSP*net*), a national program that manages practice education in the health sciences. The PIA was prepared by HSP*net's* national director and privacy officer and conforms to similar PIAs completed for school participants in seven provinces.

Note: All references in this report to sections of legislation refer to the *Access to Information and Protection of Privacy Act,* S.N.L. 2002, Chapter A-1.1, as amended, unless otherwise specified.

THE PROJECT

Project Information

This Privacy Impact Assessment (PIA) is submitted by Memorial University of Newfoundland as lead agency in the Newfoundland and Labrador User Community (NLUC) of HSP*net*-NL. The user community is comprised of Regional Health Authorities, health service providers, and postsecondary institutions (PSI) that use HSP*net* for the coordination and improvement of health sciences practice education. Although this PIA covers all current and future users of HSPnet in Newfoundland and Labrador, the PSI involved in the initial HSPnet implementation are; Memorial University of Newfoundland, the Centre for Nursing Studies, and Western Regional School of Nursing.

Background about HSPnet

The Health Sciences Placement Network, or HSP*net,* was launched in April 2003 by the BC Academic Health Council (BCAHC) as an initiative to address the growing shortage of skilled healthcare workers in BC. HSPnet, a web-based data system, was designed as a tool for managing practice education in the health sciences. The success of HSPnet in BC resulted in the system being adopted and implemented in six other Canadian provinces over 9 years: Alberta, Saskatchewan, Manitoba, Ontario, Quebec and Nova Scotia.

HSPnet will introduce a province-wide system for coordinating and improving student placements for health sciences disciplines in Newfoundland & Labrador. 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 enrolment 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.

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."

The National HSPnet Alliance and Service Providers

The current stakeholders are involved in the success of HSPnet are; the BC Academic Health Council, owners of the HSPnet initiative, Roberts Hendrickson Consulting Inc. (the HSPnet Team) contracted to manage the service component of HSPnet, the BC Institute of Technology (BCIT) the server host provider responsible for the management and protection of the HSPnet servers, and the National HSPnet Alliance Steering Committee (NHASC) who provides national leadership for HSPnet and determines policies and processes to harmonize HSPnet operations across jurisdictions.

The National HSPnet Policies were developed to govern the use of HSPnet by licensee and sub-licensee organizations, to ensure:

- Compliance with provincial and federal legislation on privacy and security of personal information;
- Consistency of policy and procedures across user organizations and Lead Agencies; and
- Effectiveness of infrastructure operations.

The BCAHC and the National HSPnet Alliance members endorse the 10 Principles of the Canadian Standards Association (CSA) Model Code, now included in the federal *Personal Information Protection and Electronic Documents Act*. These principles are recognized as the foundation for privacy protection legislation and are reflected in BC's *Freedom of Information and Protection of Privacy Act* and in other provincial legislation.

The National HSPnet Alliance Steering Committee has adopted a policy that a formal PIA process will be undertaken in each province as a best practice, regardless of whether a PIA is mandatory or not.

ANALYSIS AND RECOMMENDATIONS

Collection of Personal Information

1. Authorization for Program to Proceed

What the Act/Policy require:

When a public body collects personal information in order to operate a program or activity, the program or activity must be approved at an appropriate level. See s.32(c), ss. 33(2)(b), and also ss. 38(1)(a). Approval for a program may derive from Senate or the Board of Regents, or another person with authority to give such an approval.

The* HSP*net* *Program:

The Dean of the School of Nursing authorized the Schools' participation in the HSP*net* program.

2. Minimization of Collection

What the Act/Policy require:

A public body must limit its collection of personal information to only the information that is necessary to carry out the program or activity.

The* HSP*net* *Program:

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 includes details on the specific data uses, levels of identification, and disclosure recipients.

The National HSPnet Policy 3.2(1)b. states that:

> *Student gender may be entered into* HSP*net by an educational program if placements are made in Destinations that respect patient/client preference for the gender of their provider (e.g. homecare visits) and therefore require the Program to disclose Student gender so they can assign students. Student gender would be disclosed only to Destinations that specify this requirement in their online Destination Profile*

Notes: see Appendix 1 - *HSPnet Data Uses*

3. Authorization to Collect Personal Information

What the Act/Policy require:

Under s.32, a public body is permitted to collect personal information only if:

(a) the collection of that information is expressly authorized by or under an Act;
(b) that information is collected for the purposes of law enforcement; or
(c) that information relates directly to and is necessary for an operating program or activity of the public body

The majority of projects and programs at the University rely on (c): the information relates directly to and is necessary for an operating program or activity.

The* HSP*net* *Program:
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). 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.

Notes:
Appendix 4 – *Consent Form for Use and Disclosure of Personal Information* (or at the link: http://hspcanada.net/privacy/resources.asp) and Appendix 5 – *Identified Purposes and Handling of Personal Information and Personal Health Information* (or at the link: http://hspcanada.net/docs/policies_consent/identified_purposes_summary_all.pdf)

4. Method of Collection

What the Act/Policy require:
Personal information must be collected directly from the person the information is about, except in prescribed circumstances (see s.33).

Section 33 sets out in what circumstances indirect collection is permitted. Such circumstances include a law enforcement matter, existing or anticipated judicial or quasi-judicial proceedings, and where another method of collection is authorized by the individual concerned, or authorized by an act or regulation, among others. Indirect collection of personal information is not permitted unless the requirements of s.33 are satisfied.

The* HSP*net* *Program:
The National 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*.

In general, PI and PHI are collected by Placing Agencies from their registered students, as provided at the time of their enrolment/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, PI 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.

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.

Notes: Appendix 4 – *Consent Form for Use and Disclosure of Personal Information* (or at the link: http://hspcanada.net/privacy/resources.asp) and Appendix 5 – *Identified Purposes and Handling of Personal Information and Personal Health Information* (or at the link: http://hspcanada.net/docs/policies_consent/identified_purposes_summary_all.pdf)

5. Privacy notice/consent

What the Act/Policy require:

While consent is an authority for collection of personal information in certain privacy laws (eg, PIPEDA), under the *ATIPP Act* consent alone does not permit a public body to collect personal information. All collections of personal information must be for one of three purposes (set out above under #3). At all times when a public body collects personal information directly from an individual, it is required to notify the individual – at the time of collection – of three things:

- The purpose for collection of the information
- The legal authority for the collection of the information
- The contact information of a person who can answer questions about the collection and the use of the information

All forms (electronic and paper) in which individuals are asked to provide personal information must, under the *ATIPP Act* and University policy, include a privacy notice setting out the information above. The IAPP Office web site, under "For Employees: Privacy Rules! Privacy Tools!" located at http://www.mun.ca/iapp/resources/, contains sample privacy notices. The IAPP Office will provide advice on developing privacy notices.

The* HSP*net Program:

The National HSPnet 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;

Also under Policy 3.2, students may withhold consent to collect, use or disclose their personal information via HSPnet, and will be advised of the potential delays or other impacts of withholding that consent. As well students may revoke their consent by submitting a written request to their educational program coordinator. Revocation of consent will not be effective for uses or disclosures already made as permitted by the prior consent.

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.

Notes: see Appendix 6: *Policy 3.2 – Policy Application Guide (or at the link: http://hspcanada.net/docs/policies_consent/policy32_%20app_guide_package.pdf)*
Appendix 5 – *Identified Purposes and Handling of Personal Information and Personal Health Information* (or at the link: http://hspcanada.net/docs/policies_consent/identified_purposes_summary_all.pdf)

Use of Personal Information

6. Consistent purposes

What the Act/Policy require:

The *ATIPPA* requires that personal information collected by a public body be used only for purposes consistent with the original purpose for collection and that it is not to be used for another purpose unless it is permitted to do so under s.38. Section 38 (in conjunction with s.39) sets out the only uses a public body is authorized to make of personal information. One of the authorizations in s.38 is written authorization from the individual. Others include compliance with an Act, a subpoena, law enforcement, and contacting next of kin where an individual is injured, ill or deceased. The IAPP Office or Office of General Counsel should be consulted for assistance in interpreting section 38.

The* HSP*net Program:

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 3.2(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.*

Also under Policy 3.2 (i), it is noted that if a student's identifiable information contained in HSPnet is to be used for any new or previously unidentified purpose, including but not limited to research or quality assurance activities, the student(s) affected will be contacted by a

representative of their educational program for the purpose of updating their informed consent to include the new or previously unidentified purposes.

Notes:
Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

7. Minimization of use

What the Act/Policy require:
Public bodies must minimize their access and use of personal information to the minimum amount of information necessary to accomplish the purpose for which it is used – see s. 38(2). This means, for example, that an employee with access to a database is permitted to access only that information needed for her/him to perform job responsibilities, even though the database may contain other types of personal information which is used by another employee for *their* job responsibilities. In other words, access to personal information out of curiosity or for any purpose inconsistent with the purpose of collection, or as otherwise authorized in the *ATIPPA*, is not permitted.

The* HSP*net Program:
The *HSPnet Data Uses Table*, referenced in this document, 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.

The national HSPnet Policy 3.4 (h) states:

> Local Administrators will assign a **unique User ID to each individual user**; there will be no shared User ID's among HSPnet users. Local Administrators will ensure that each user has a secure email address entered into HSPnet for the purpose of communication with other HSPnet users and for receipt of system messages from HSPnet.

Policy 3.4 identifies the escalation procedures for policy and privacy breaches, review results of periodic audits of data entered into HSPnet fields, in order to detect intentional or unintentional release of private information that is not otherwise authorized.

Notes:
Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

8. Authority to disclose

What the Act/Policy require:

Just as a public body must have authority under the *Act* to collect personal information, and to use personal information, so must it have authority before it is permitted to disclose personal information. The university is prohibited from disclosing personal information to an outside person or entity unless authority for the disclosure is found in ss. 39(1).

The* HSP*net* *Program:

The National HSPnet policy 3.2 (8) states that

> A student has the right to request that the use and/or disclosure of their personal information in HSPnet be restricted. Such requests must be made in writing to their educational program coordinator. If restriction of use of their personal information as requested precludes the use of HSPnet, they will be informed of the potential delays or other impacts of requesting that restriction.

Notes:

Appendix 6: *Policy 3.2 – Policy Application Guide (or at the link: http://hspcanada.net/docs/policies_consent/policy32_%20app_guide_package.pdf)*
Appendix 5 – *Identified Purposes and Handling of Personal Information and Personal Health Information* (or at the link: http://hspcanada.net/docs/policies_consent/identified_purposes_summary_all.pdf)

9. Minimization of disclosure and method of disclosure

What the Act/Policy require:

A public body must minimize its disclosure of personal information to the minimum amount of information necessary for the disclosure.

The* HSP*net* *Program:

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. The HSPnet dataset, as defined in the *HSPnet Data Uses Table*, is limited to data required to meet the Identified Purposes of HSPnet.

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.

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.

Notes:
Appendix 6: *Policy 3.2 – Policy Application Guide (or at the link: http://hspcanada.net/docs/policies_consent/policy32_%20app_guide_package.pdf)*
Appendix 5 – *Identified Purposes and Handling of Personal Information and Personal Health Information* (or at the link: http://hspcanada.net/docs/policies_consent/identified_purposes_summary_all.pdf

Security of Personal Information

10. Security of information

What the Act/Policy require:

The *ATIPP Act*, in s.36 requires public bodies to protect personal information by making reasonable security arrangements. The University's Privacy Policy requires that:

> ***7. F. Security:*** *The University ensures that personal information in its custody is secured in a manner appropriate to the sensitivity and purpose of the information. The University ensures that records containing personal information are protected from unauthorized collection, access, use, disclosure and disposal by putting in place reasonable administrative, physical and technical security measures. All employees ensure that personal information which they handle as part of their job is secure from unauthorized access, that collection, use and disclosure of personal information is minimized and that records are managed in accordance with an established records retention and disposal system.*

From Privacy Policy
Available at: http://www.mun.ca/policy/site/policy.php?id=145

The university's Electronic Data Security policy contains specific requirements for the security of information stored electronically. According to the Policy, "[s]tandards for approved security software and configurations shall be set by the Department of Computing and Communications, and periodically revised in response to best practices and emerging technologies."

Security in the Department of Computing and Communications (C&C) requires that the Electronic Data Security policy be followed and, specifically, that:

- The machines that will be used by authorized employees in the School of Nursing to access HSP*net* must have approved McAfee anti-virus software installed as required by policy;
- The connection to HSP*net* must be SSL encrypted

In addition to technical security measures that may be required by C&C, administrative and physical measures are required to protect personal information from such risks as unauthorized access, collection, use, disclosure, modification or disposal.

***The* HSP*net* Program:**

BC Institute of Technology (BCIT), as server host provider, provides protection from external threats as per their Service Level Agreement with the BC Academic Health Council (BCAHC). BCIT installs industry-standard anti-virus tools on all servers involved with HSPnet as managed for all jurisdictions.

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. Offsite storage is managed completely by BCIT staff; data is spooled to tape backups and is relocated to another building on their campus (approx 0.6 KM away from the BCIT data centre). The tapes are transported both ways by BCIT staff and are stored in a secured, fire resistant safe.

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

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 audits of early releases are performed and reported to the National HSPnet Alliance 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.

Notes:
Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

11. Retention of personal information

What the Act/Policy require:

The *ATIPP Act* requires that personal information used to make a decision affecting an individual be retained for at least one year following the last use of the information (s.37). The purpose of this provision is to allow sufficient opportunity for an individual to seek and obtain access to her/his own personal information. The legislation and the university's Privacy Policy do not directly address maximum retention periods. However, a fundamental principle of privacy protection is not retaining personal information if no legitimate need for it exists. Retention of personal information may be addressed in legislation or regulation, contractual obligations, policy or best practices for a particular type of activity, etc.

Following an approved records retention and disposal schedule is strongly advised, to ensure that personal information is not retained longer than necessary.

Since data collected and stored electronically may not pose significant "space" problems, keeping data indefinitely may be an attractive proposition. However, personal data retained must be protected against unauthorized access, protected against unauthorized use, and be available for access by the individual the information is about. For example, personal information that has not been used for ten years but continues to reside in the system must be made available to the person the information is about if the person seeks access to it.

The* HSP*net Program:

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 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 includes 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. The archival of HSPnet data separates "live" placement request data from older placement request data in HSPnet which results in improving the system performance.

Notes:
Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

Accuracy of Personal Information

12. Accuracy

What the Act/Policy require:
The *ATIPP Act* specifies that public bodies are required to ensure that personal information used to make a decision affecting an individual is accurate and complete (s.34). The requirement for accuracy is directly related to individuals' right to request correction of their own personal information (see 13) below.

The* HSP*net Program:
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.

The policy also states that User Agencies are responsible for ensuring the accuracy of information uploaded into HSPnet. 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.

Notes:
Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

Individuals' Right to Access and to Request Correction of their Personal Information

13. Access to personal information

What the Act/Policy require:
The *ATIPP Act* and university policy (the Privacy and the Information Request policies) give individuals a right of access to personal information about themselves, subject to limited exceptions (s.3). Routine (informal) access is encouraged, with the caveat that in doing so the university does not violate another person's privacy (see the Information Request policy specifically). Any concerns by the Department in responding to a request for access to personal information held in HSPnet can be addressed with the IAPP Office. Individuals have a right to file a formal request for access under the *ATIPP Act*; such requests are made through the IAPP Office.

The Purpose section of the *ATIPP Act* states:

> *3. (1) The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by*

(b) giving individuals a right of access to, and a right to request correction of, personal information about themselves;

A person's right of access to personal information about her/him that the university has in its custody and/or control is an important right under access and privacy law.

The* HSP*net* *Program:

The HSPnet Policy 3.5 (b) states:

> A student can request a copy of their personal information in HSPnet by presenting a written request to the placement coordinator of their educational program along with two pieces of identification, one of which must be their current student identification card with student number and photograph. The placement coordinator 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/disclosure of that information plus an explanation of the list provided. The placement coordinator will copy the HSPnet-NL privacy officer (Clinical Program Administrator, School of Nursing, Memorial University) on the responses to the student.

Notes: see Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

14. Right to request correction of personal information

What the Act/Policy require:

Individuals have the right to request correction of a record of information if they believe it contains an error. Often, this is achieved informally. Individuals also have a right under the *ATIPP Act* to formally request a correction of personal information in a record held by a public body. Such a formal request for correction is made through the IAPP Office and decisions are subject to review by the province's Information and Privacy Commissioner, an officer of the House of Assembly. If no correction is made following a request, the public body is required to annotate the file accordingly.

When a public body corrects an error in a record in response to a request by an individual, the public body must (under s. 35) notify a public body or a third party to whom the information had been disclosed in the previous 12 months.

The* HSP*net* *Program:

The 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

Notes: see Appendix 2 – *HSPnet Policies on Privacy, Security and Data Access* (or at the link: http://hspcanada.net/docs/Policies_Consent/HSPnet_Policies.pdf)

Contractual Relationship

15. Third party access

What the Act/Policy require:

To comply with the *Act*'s requirements regarding security of personal information, the Procedure for Administering Privacy Policy within a Unit states:

> *Ensure that all contracted individuals and entities, including consultants and external service providers, whose work will involve access to personal information sign the Privacy Schedule. The IAPP Advisory Committee has approved the standard Memorial University Privacy Schedule. In certain situations, alternative privacy provisions may be made with the approval, in writing, of the University Privacy Officer and General Counsel. The standard Privacy Schedule is available from the University Privacy Officer and at www.mun.ca/iapp/resources.*

The* HSP*net Program:

BCAHC staff and contractors (supporting the BCAHC's role as service provider to HSPnet-AC) 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.

The Service Level Agreement (SLA) between the BCAHC and BCIT, and the HSPnet *Confidentiality Agreement and Code of Conduct* 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.

Notes: see Appendix 3 - *Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers*

LIST OF APPENDICES

Appendix 1: HSPnet Data Uses Table

Appendix 2: 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 3: Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers

Appendix 4: Consent Form for Use and Disclosure of Personal Information

Appendix 5: Identified Purposes and Handling of Personal Information and Personal Health Information in HSPnet

Appendix 6: Policy 3.2 – Policy Application Guide

APPENDIX 1 (PIA-NL)

HSP*net* Data Uses

Updated: March 31, 2012

Health Sciences Placement Network
Réseau de gestion des stages en sciences de la santé

Background

The purpose for collecting, using and disclosing personal information via HSPnet is stated within the HSPnet Policies on Privacy, Security and Data Access, and in the student handout entitled *Identified Purposes and Handling of Personal Information in HSPnet*.

The purpose of this document is to provide detailed information on the individual data elements that are collected, used and disclosed via HSPnet and the user role(s) involved in these processes.

Levels of Data Identification

HSPnet data involving personal information can be categorized as either:

- Identifiable (i.e. would or could lead a user to identify the individual concerned),
- De-identified (identifying information has been removed or suppressed), or
- Anonymous (no identifiable information is included and/or the information collected could not lead a user to identify the individual).

Data Purposes:

Data Identification Level	Data Purpose	
	Identifying and Coordinating Student Placements	**Program / Site Evaluation**
Identifiable *(Released with Consent)*	• To confirm an accepted placement request and exchange information necessary to manage the placement (release of student name by Placing Agency to Receiving Agency, release of supervisor name by Receiving Agency to Placing Agency) • To support consideration of a pending placement request for a known student (student name is released in these situations on a need-to-know basis and on occasion only, such as when student name is needed to identify an individual that has already contacted a unit to request their own placement).	None at this time
De-identified	• To support consideration of a pending placement request for a known student (student name is generally withheld during the consideration process, and is released prior to confirmation only by exception as noted above).	• To review placement activities (number of students, hours) by educational program or for a site or unit/destination
Anonymous	• To support consideration of a pending placement request when student assignment is occur later (the specific student to be placed is not known at this time).	

Student Data Uses – Detailed Description

Key: **PR –** Placement Request

Agency Type: **PA** ï Placing Agency **RA** ï Receiving Agency
PA Staff: **PC** ï Placing Coordinator **IN** ï Instructor (PA)
RA Staff: **RC** ï Receiving Coordinator **DC** ï Destination Coordinator **SU** - Supervisor

Data Details	Source [1]	Data Uses [2]	Level of Identification	Disclosure Recipient
Identifiers • First • Last • Middle (optional) • Student Number	Placing Agency	By PA staff (PC, I) to identify and track students	De-identified	Disclosed to RC for the Site and DC for the student's placement location, during the PR consideration process (before PR is confirmed).
			Identifiable	Same as above ï Name only is disclosed if the placement is confirmed, or on occasion prior to confirmation if RA has a need to identify student in order to consider the PR.[3] *NOTE – Student number is not disclosed to anyone external to PA*
Gender	Placing Agency	By PA staff (PC, I) to assist with assignment of students	Identifiable	Disclosed only to the RA when justified as per the policies (e.g. in homecare, to accommodate patient/client preference for gender of their care provider)
Contact Information • Mailing address • Email address • Phone(s), fax	Student, via the PA information system for students	By PA staff to contact student regarding PR schedule, prerequisites, placement outcomes	Identifiable	Contact information (excluding email address) is not disclosed to anyone external to the student's educational program). If students have access to HSPnet, their screen provides an option to release their email address to contacts at the receiving site for placement-related purposes
PR History • PA Program and Course • Placement location • IN and/or SU assigned	HSPnet PR data (displays listing of confirmed PRs to which a student was assigned)	By PA staff to track student progress within Program, or to determine upcoming PR needs	Non-identifiable	*This information is not disclosed to anyone external to the student's educational program*
			Identifiable	*This information is not disclosed to anyone external to the student's educational program*
PR Prerequisites – e.g. • Criminal Records Check status • Immunization/TB test status • CPR status • N95 Mask size	Placing Agency	By PA staff to track student's compliance with RA prerequisites for students	Identifiable	*This information is not disclosed to anyone external to the student's educational program*
Student Preferences (or Instructor Recommendations)	Student, or IN may determine student readiness for a placement area	By PA staff to track student/ instructor preferences for upcoming and past PRs	Identifiable	*This information is not disclosed to anyone external to the student's educational program*
Photograph	PA systems for issuing photo ID cards	By PA staff to confirm student identity	Identifiable	*This information is not disclosed to anyone external to the student's educational program*

[1] In all cases unless noted otherwise, this information is collected directly from the Source noted

[2] In all cases unless noted otherwise, the authority for use and disclosure is the student's signed consent form

[3] Disclosed prior to confirmation at the discretion of the PC of the educational program, and tracked in the PR History table by date and user that released student name early.

Staff [4] Data Uses – Detailed Description

Key: **PR –** Placement Request

Agency Type: **PA** ï Placing Agency **RA** ï Receiving Agency
PA Staff: **PC** ï Placing Coordinator **IN** ï Instructor (PA) **StdA** ï Student Administrator
RA Staff: **RC** ï Receiving Coordinator **DC** ï Destination Coordinator **StaffA** ï Staff Administrator **SU** - Supervisor

Data Details	Source	Data Uses [5]	Level of Identification	Disclosure Recipient
Identifiers • First • Last • Middle (optional) • Employee number	Staff member, or indirectly from Human Resources database or listing	By PA staff for tracking, and assigning IN staff; by RA staff for tracking and assigning SU staff	Identifiable	• RA staff can view IN name and contact information immediately upon assignment to a course and/or PR of any status. • PA staff can view SU name and contact information only if PR is accepted or confirmed. • In addition to these PR-specific disclosures, all HSPnet users can perform a directory search of all PA and RA staff. *NOTE: Employee number is used only by authorized users (PC, StaffA) in the employee's department*
Contact Information • Mailing address • Email address • Phone(s) • Fax	Staff member, or indirectly from Human Resources database or listing	By PA staff for contacting their own IN staff about students and placements; by RA staff for contacting SU staff about students and placements	Identifiable	
PR History • PA Program and Course • Placement location • Student name • IN and/or SU assigned (if applic.)	HSPnet PR data (displays listing of confirmed PRs to which a staff member was assigned)	By PA staff to identify past assignments of students and placement locations for IN staff; by RA staff to identify past assignment of students to SU staff	Identifiable	*This information is used only by authorized users (RC, StaffA) of the employee's department and is not disclosed to external parties except for purposes such as preceptor recognition by the educational program, and only for placements assigned to students of that program*
PR Prerequisites (IN only) – e.g. • Criminal Records Check status • Immunization/TB test status • CPR status • N95 Mask size	Staff member (IN only)	Track the instructor's compliance with RA prerequisites for supervisors provided by the educational program	Identifiable	*This information is used only by authorized users (PC, CL) in the instructor's department and is not disclosed to external parties*

[4] "Staff" data includes PA staff in the roles of Placing Coordinator or Instructor, and RA staff in the roles of Receiving Coordinator, Destination Coordinator, and Supervisor

[5] Staff contact information (excluding employee number) is considered the business information of the employer and is disclosed only for purposes consistent with the staff member's employment role as it relates to student placements. PR Prerequisite information is collected by schools as authorized by consent by the staff member, and this information is never disclosed to anyone external to the staff member's employer.

APPENDIX 2 (PIA-NL)

Health Sciences Placement Network
Réseau de gestion des stages en sciences de la santé

National HSP*net* Policies

Approved by the

National HSPnet Alliance Steering Committee

Updated: February 5, 2013

Preamble

HSPnet is an initiative of the BC Academic Health Council (BCAHC), a not-for-profit organization that developed HSPnet for use in BC and subsequently established the National HSPnet Alliance to allow other provinces to access the system. Through the Alliance, a Lead Agency in each province or jurisdiction enters into an agreement with the BCAHC to license HSPnet on behalf of user agencies (sub-licensees) within the Lead Agency's province or jurisdiction.

The shared infrastructure of the National HSPnet Alliance (encompassing system/network management, user training and support, documentation, enhancements, evaluation, and policy) is governed by the National HSPnet Steering Committee. This Committee is responsible for ensuring the success of the shared infrastructure through financial sustainability and achievement of mutual goals.

The National HSPnet Policies were developed to govern the use of HSPnet by licensee and sub-licensee organizations, to ensure:

- Compliance with provincial and federal legislation on privacy and security of personal information;
- Consistency of policy and procedures across user organizations and Lead Agencies; and
- Effectiveness of infrastructure operations.

TABLE OF CONTENTS

Section 1: Eligibility for HSP*net* Access

Policy No. 1.0: HSPnet Access - General

Section 2: HSPnet Funding & Sustainability

Policy No. 2.1: Cost Recoveries and Subscription Fees

Section 3: Privacy, Security and Data Access

Policy No. 3.0: Privacy and Security - General

Section 3: Privacy, Security and Data Access

Policy No. 3.1: Accountability

Section 3: Privacy, Security and Data Access

Policy No. 3.2: Identified Purposes and Ensuring Consent for Data Collection, Use and Disclosure of Personal Information

Section 3: Privacy, Security and Data Access

Policy No. 3.3: Accuracy of HSPnet Data

Section 3: Privacy, Security and Data Access

Policy No. 3.4: Safeguards for HSPnet Data

Section 3: Privacy, Security and Data Access

Policy No. 3.5: Openness, Individual Access and Challenging Compliance of HSPnet Data

Section 3: Privacy, Security and Data Access

Policy No. 3.6: Access to HSPnet Data

Section 4: HSPnet Governance and Management

Section 5: HSPnet Systems Development

Section 6: Training and Support

Policy No. 6.1: HSPnet Training

Section 7: Language Duality

Policy No. 7.0: General

Record of changes to Policies and Procedures:

Date	Policy	Description of Change
Mar 30/09	2.1	Replaced reference to ñPartnershipò with ñAllianceò
Mar 30/09	3.0	Replaced 2 references to ñPartnersò with ñAlliance membersò and ñAllianceò
Mar 30/09	3.2	Policy 1.b ï added policy to allow Destinations to request release of Student gender on a need-to-know basis. Procedures (e), (f) and (g) ï added procedures to support release of Student gender
Mar 30/09	3.4	Procedure (h) ï added requirement for Local Administrators to ensure that a dedicated, and not shared, email address is entered for each user account,
Sep 30/09	3.2	Procedure (f) ï added requirement for organizational policy to support request for student gender; added limitation for only Receiving Coordinators to modify this field.
Mar 31/10	3.4	Procedure (o) ï added a clause to permit immediate disabling of user ID(s), at the HSPnetôDirectorôs discretion, in a serious situation.
Jul 27/11	All	Policies were reviewed and approved by all NHASC members.
	2.1	Change from HSPnet-XX Coordinator to HSPnet-XX Lead Agency or HSPnet-XX Provincial Coordinator **Intent:** many provinces do not have HSPnet Coordinators. This clarifies roles
	3.0	Change from CEO to Executive Director **Intent:** Clarification
	3.1	Change from CEO to Executive Director / Change from Privacy Officer to National Privacy Officer **Intent:** Clarification between provincial
	3.3, 3.4, 3.5	Minor changes in roles and titles **Intent:** Clarification
	3.6	Remove Item #2 re: Data Sharing Agreement - **Intent:** This policy item is embedded in the new Collaborative Agreement between Lead Agencies and the BCAHC. A separate document will not be developed.
	3.4	(n) change the auditing period from six month to three months after a breach of policy
Aug 1/11	All	Approved as distributed
May/12	5.0	User Reference Group
Dec 4/12	3.0	(2.) Only completed PIAs will be posted on the public website
	3.4	(i) updated policy to allow users to use shared/generic emails addresses as long as they enter a secure email.
	3.6	(3.) Added a policy whereby Lead Agency representatives will be granted access to specific provincial data in support of their mandate for HSPnet in their province. (d) added a procedure for cross-agency access
Jan 4/13	3.0.2	Changed the requirement for each Alliance jurisdiction to submit a PIA from a mandatory requirement (ñwillò) to a best practice (ñshouldò)
	3.1.a	Amended ñé establishes an ongoing HSPnet-XX Data Stewardship Committeeò to ñé establishes an ongoing national HSPnet Data Stewardship Committeeò
	3.4	Procedures (j), (k) and (o) ï transfer responsibility for annual review to the national Data Stewardship Committee
		Procedures (l) and (m) ï merged as a single reference to ñdata quality, privacy and securityò
Feb 5/13	3.4	Clarified the requirement for secure email to be a requirement for direct communication from other users, and delivery of passwords
		Procedure (p) ï updated reference to the automatic inactivation of idle user accounts, on a quarterly basis
	3.6	Additional Documents: added a reference to the procedure for Lead Agency access to provincial data

Section 1: Eligibility for HSP*net* Access

Policy No. 1.0: HSP*net* Access - General

Purpose

To ensure that HSPnet access is made available to all Agencies that could benefit from its use while contributing to the system-wide benefits for all HSPnet users.

Principle

Once admitted to a health professional education program, students deserve a quality learning experience *(*from *"BCAHC Post-Summit Action for Student Placements – January 14, 2005")*

Policy

1. The BCAHC will maintain a definition of eligibility for HSPnet access that will maximize the system-wide benefits for all Participating Agencies.

2. All agencies that use HSPnet will agree to comply with the National HSPnet Policies.

Definitions

Eligible Agency ï An Agency is eligible for access, via an authorized User ID, to a provincial instance of HSPnet (HSPnet-XX) if the Agency:

- Registers students in health sciences educational programs and places those students in clinical practica or fieldwork opportunities within that province; OR

- Acts as a Receiving site in that province for students registered in health sciences educational programs by accepting those students into clinical practica or fieldwork opportunities.

Procedures

a. The National HSPnet Alliance Steering Committee will review the above definition of an Eligible Agency on an annual basis.

b. The BCAHC will ensure that all Lead Agencies joining the national HSPnet Alliance include a requirement by sub-licensee agencies to comply with the National HSPnet Policies.

Section 2: HSPnet Funding & Sustainability

Policy No. 2.1: Cost Recoveries and Subscription Fees

Purpose

To facilitate (optional) processes in each province that enable user agencies to contribute to the ongoing costs of HSPnet implementation, operations and enhancement.

Principle

Agencies that use HSPnet may contribute towards the costs of operating and enhancing the system.

Policy

1. Each province or jurisdiction represented in the National HSPnet Alliance may choose to develop one or more mechanisms to recover ongoing costs of HSPnet operation and enhancement from Agencies that use HSPnet in that province.

2. If a jurisdictionôs cost recovering mechanisms include a subscription fee for some or all members, then that province may adopt the following Procedures to manage the subscription application and renewal process.

Definitions

User Agency ï An Agency eligible for access under Policy 1.0 to use HSPnet.

Subscriber Agency ï A User Agency that holds a subscription under this Policy to use HSPnet.

Procedures

a. User Agencies wishing to access HSPnet on a subscription basis (Subscriber Agencies) will contribute to their jurisdictionôs one-time implementation costs, ongoing support, and access to HSPnet fixes and enhancements through payment of an annual subscription fee, to be payable in each HSPnet budget year (April 1 to March 31).

b. Any jurisdiction wishing to collect Subscription Fees will:

   - Require their HSPnet-XX Lead Agency or HSPnet Provincial Coordinator to develop and maintain a process for Subscription applications and renewals;
   - Require the HSPnet-XX Management Committee to develop a Subscription Fee Schedule for their jurisdiction, and to review and update that Schedule on an annual basis.

c. The HSPnet-XX Lead Agency or HSPnet Provincial Coordinator will provide new Subscriber Agencies in their jurisdiction with an HSPnet Subscription Application/Renewal Form, based on information about the Subscriber Agencyôs educational programs, intakes (cohorts), and student enrolment.

d. Subscriber Agencies will return their signed Subscription Application/Renewal Forms to the HSPnet-XX Lead Agency or HSPnet Provincial Coordinator, who will then invoice the Subscriber Agency for the coming year and follow up regarding payment to the jurisdiction. The invoice amount may be pro-rated for partial year access.

e. The HSPnet-XX Lead Agency or HSPnet Provincial Coordinator will forward a copy of the signed Subscription Application/Renewal Form to the BC Academic Health Council and HSPnet Director, who will then schedule implementation training for the new Subscriber Agency. On mutual agreement, the HSPnet Director, Subscriber Agency, and HSPnet Subscription Coordinator may

agree to schedule implementation training prior to receipt of the subscription payment so long as the Subscription Application/Renewal Form has been signed and returned.

f. The HSPnet Subscription Coordinator will establish an escalation procedure for following up on delinquent payments from Subscriber Agencies (new applicants or renewals), up to and including advising the National HSPnet Director to de-activate all user IDôs in a Subscriber Agency that has not paid the current yearôs subscription fees.

Related Documents

- HSP*net-BC Subscription Application / Renewal form*

Section 3: Privacy, Security and Data Access

Policy No. 3.0: Privacy and Security - General

Purpose

To ensure the protection of personal information in HSPnet under the management of the BCAHC.

Principles

The BCAHC and the National HSPnet Alliance members endorse the 10 Principles of the Canadian Standards Association (CSA) Model Code, now included in the federal *Personal Information Protection and Electronic Documents Act*. These principles are recognized as the foundation for privacy protection legislation and are reflected in BC's *Freedom of Information and Protection of Privacy Act* and in other provincial legislation. The 10 principles that underlie the HSPnet privacy and security program are:

- ***Accountability -*** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
- ***Identifying purposes*** - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
- ***Consent -*** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
- ***Limiting Collection -*** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
- ***Limiting Use Disclosure and Retention*** - Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
- ***Accuracy*** - Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.
- ***Safeguards -*** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- ***Openness -*** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- ***Individual Access -*** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information.
- ***Challenging Compliance -*** An individual shall be able to address a challenge concerning compliance with the above principles to the designate individual or individuals accountable for the organization's compliance.

Policy

1. The BCAHC Executive Director will ensure that a comprehensive privacy and security program is maintained for HSPnet, in order to meet the requirements of provincial and federal legislation in each province where HSPnet is used.

APPENDIX 2 (PIA-NL)

2. As a best practice, each Alliance jurisdiction should conduct a Privacy Impact Assessment (PIA) to ensure HSPnet meets or exceeds the legislated privacy requirements of the jurisdictionôs province(s). The completed PIA will be submitted by the jurisdictionôs Lead Agency on behalf of participating agencies, in the format required for the jurisdictionôs province(s) if specified, to the required privacy office(s) if specified or on a voluntary basis to one or more privacy offices as recommended by the Lead Agency. Completed PIAs will be posted on the HSPnet website for each jurisdiction.

Section 3: Privacy, Security and Data Access

Policy No. 3.1: Accountability

Purpose

To establish accountability for personal information in HSPnet under the management of the BCAHC.

Principles (based on the 10 Principles of the CSA Model Code)

- Accountability is organizational in focus and will apply to all systems and programs and all data for which BCAHC acts as a steward.
- The BCAHC is responsible for personal information under its control and shall designate an individual or individuals who are accountable for compliance with legislation and professional standards governing the protection of personal information.

Policy

1. The National HSPnet Alliance Steering Committee will be responsible to the organizations represented by its members for the development and effectiveness of National HSPnet Policies, including policies to support the privacy and security of personal information in HSPnet.

2. The BCAHC Executive Director is accountable to the National Steering Committee and provincial Lead Agencies for the conduct of HSPnet Service Providers, including compliance with the National HSPnet Policies.

3. The BCAHC Executive Director will ensure that all of its staff and contractors who have access to HSPnet data are guided by clear rules of conduct and confidentiality.

4. Provincial Lead Agencies are responsible for compliance with the National HSPnet Policies by user agencies within their jurisdiction.

5. The BCAHC Executive Director will ensure that policies relating to privacy and security of personal information in HSPnet are maintained in the event that the BCAHC transfers management of HSPnet to an external organization on either a temporary basis (e.g. outsourcing contract) or permanent basis (legal transfer).

Definitions

Data Steward ï an individual or body responsible for managing and protecting data on behalf of others. Stewardship encompasses responsibilities for development and oversight of policies and processes for data creation or acquisition, sharing and access, reliability, security, and disposition.

Service Provider ï an employee or contractor in physical or logical possession of information that is protected by a Data Steward. Typically, Service Providers provide day-to-day management of the databases, applications, and/or hardware that support the collection, use and disclosure of information. Given their potential access to personal information, Service Providers should operate under clear rules of conduct and confidentiality.

Procedures

a. Provincial lead agencies may act as Data Steward or may establish a provincial Data Stewardship Committee accountable to the National HSPnet Alliance Steering Committee and to agencies using HSPnet-XX (ñParticipating Agencieso) in their province. National HSPnet Alliance Steering Committee will ensure that each province using HSPnet establishes an ongoing national HSPnet Data Stewardship Committee.

b. The national HSPnet Data Stewardship Committee will conduct an annual review to assess the effectiveness of its role as Data Steward, and will report the results of this review to the National HSPnet Steering Committee. The review will include a process to facilitate input from HSPnet-XX users into the development, application, and ongoing review of the National HSPnet Policies Privacy, Security & Data Access.

c. The BCAHC Executive Director will ensure that all new BCAHC staff and contractors with access to personal information in HSPnet receive appropriate training and sign a document entitled *Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers* prior to gaining access to HSPnet. The signed document will be maintained on file at the BCHAC offices.

d. The BCAHC Executive Director will appoint a National HSPnet Privacy Officer to be responsible for overseeing processes to protect personal information in HSPnet, and to act as a resource to the Privacy Officer in each jurisdiction.

- The National HSPnet Privacy Officer will develop, maintain, and coordinate application of the national HSPnet policies in each province.

- The National HSPnet Privacy Officer will ensure that each province using HSPnet publishes the contact information of the BCAHC National Privacy Officer and the HSPnet-XX Privacy Officer (title and office phone, email and mailing addresses) on the HSPnet-XX website and in publications relating to the collection, use or disclosure of personal information in HSPnet.

- The National Privacy Officer will train BCAHC staff and contractors involved with HSPnet on the National HSPnet Policies.

e. The Lead Agency in each jurisdiction will appoint a provincial Privacy Officer to be responsible for overseeing processes to protect personal information in their jurisdiction.

Related Documents

- *Role Description – HSPnet-XX Privacy Officer*
- *Terms of Reference – National Data Stewardship Committee*
- *Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers*

Section 3: Privacy, Security and Data Access

Policy No. 3.2: Identified Purposes and Ensuring Consent for Data Collection, Use and Disclosure of Personal Information

Background

Students may choose to authorize their educational institution to use and/or disclose their personal information via HSPnet for the purpose of locating and coordinating student placements within participating agencies.

Purpose

To identify the purposes of personal information in HSPnet and to ensure that informed consent is obtained prior to collecting personal information for the identified purposes.

Principles (based on the 10 Principles of the CSA Model Code)

- The purposes for which personal information is collected shall be identified by an organization at or before the time the information is collected.
- The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information.
- The collection of personal information shall be limited to that which is necessary for the purposes identified by an organization. Information shall be collected by fair and lawful means.
- Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Definitions

Students ï An individual registered in an educational program. A studentôs name, contact information and practice education profile are considered to be ***Personal Information***.

Staff ï An individual employed or contracted by an educational institution or receiving site that is involved in practice education activities. Staff name, business contact information, and practice education profile are considered to be the ***Business Information*** of the employing/contracting organization and are not considered to be personal information.

Policies

1. Personal information will be collected, used and disclosed via HSPnet on a need-to-know basis only and for purposes consistent with identifying and coordinating appropriate placements for students (the identified purposes for collecting data via HSPnet, or ñIdentified Purposesò). In general, ñneed-to-knowò will commence after the placement is confirmed, in order to initiate communications with the student and to coordinate their placement.

    a. Student identity may be released prior to confirming a placement in situations where communications must start before the placement can be accepted (i.e. for a placement interview) or when considering where a student should can be placed (i.e. if the student is employed by the placing site).

    b. Student gender may be entered into HSPnet by an educational program *if placements are made in Destinations that respect patient/client preference for the gender of their provider (e.g. homecare visits) and therefore require the Program to disclose Student gender so they can assign students.* Student gender would be disclosed only to Destinations that specify this requirement in their online Destination Profile.

2. The Identified Purposes will be explained to students at the time of entering their personal information into HSPnet, or within a reasonable period of time after entry into HSPnet if the entering agency is relying on a previous consent or notification process relating to use/disclosure of their personal information for the purpose of coordinating a placement experience.

3. 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.

4. Personal information will be obtained directly from the student or from information provided with the student's consent and for the Identified Purposes, and will not be used or disclosed after fulfillment of the Identified Purposes.

5. Informed consent, based on receipt and acknowledgement of the Identified Purposes, will be obtained from a student before entering their personal information into HSPnet.

    a. During initial implementation of HSPnet, the agency entering the student information may elect to rely on a previous process whereby students have been notified and/or given consent to use/disclose their personal information for the purpose of coordinating a placement experience.

    b. Any agency relying on a previous process for notification and/or consent will make reasonable efforts, during the months following HSPnet implementation, to obtain formal consent based on the Identified Purposes and handling of their personal information via HSPnet.

6. A student may withhold consent to collect, use or disclose their personal information via HSPnet, and will be advised of the potential delays or other impacts of withholding that consent.

7. A student may revoke their consent by submitting a written request to their educational program coordinator. Revocation of consent will not be effective for uses or disclosures already made as permitted by the prior consent.

8. A student has the right to request that the use and/or disclosure of their personal information in HSPnet be restricted. Such requests must be made in writing to their educational program coordinator. If restriction of use of their personal information as requested precludes the use of HSPnet, they will be informed of the potential delays or other impacts of requesting that restriction.

9. 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.

10. Personal information will be used or disclosed via HSPnet only during the period covered by the student's consent, which will expire automatically upon graduation or after six years (whichever is less), plus 180 days. After that time, personal information will no longer be used or disclosed via HSPnet.

11. Personal information may be stored in HSPnet archives beyond the consent period, in accordance with Data Retention and Archival schedule approved by the National 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.

Procedures

a. The BCAHC will develop and maintain a document entitled *Identified Purposes and Handling of Personal Information in HSPnet*. The document will summarize the amount, type and purposes of personal information to be used or disclosed via HSPnet, and will be provided to all students at the time of obtaining their informed consent and prior to entry of their personal information into HSPnet.

b. Students providing personal information for use in HSPnet will indicate their informed consent by signing a *Consent Form for Use and Disclosure of Personal Information* (ñConsent Formò) for each educational program that uses HSPnet, prior to their personal information being entered into HSPnet.

c. Signed Consent Forms will be maintained on file by the educational program of the Participating Agency that enters the student information into HSPnet for a minimum of seven years or longer if required by the Participating Agencyôs record retention policies.

d. HSPnet users will ensure that an up-to-date Consent Form is on file before entering a studentôs identifiable information into HSPnet. If student information is entered into HSPnet during the implementation period based on a previous consent or notification process, HSPnet users will make reasonable efforts to obtain a signed Consent Form for all students whose personal information is being entered into HSPnet.

e. Educational Programs will be permitted to enter Student gender in HSPnet only if they setup their Program to use this data field. If gender is entered, it will be disclosed via HSPnet only to Destinations that specify this requirement.

f. Receiving Destinations that require Student gender in order to assign students based on patient/client preference must specify this requirement in their online Destination Profile. This requirement should be based in organizational policy as appropriate, and can be entered into HSPnet only by a user with the role of Receiving Coordinator (Local Administrator access level) on behalf of the Destination Coordinator.

g. On an annual basis, the National HSPnet Director will report to the jurisdictionôs Data Stewardship Committee on the name and discipline of all educational Programs setup to use/disclose Student gender, and the Agency/Site/Service of all Destinations specifying a requirement for disclosure of Student gender.

h. HSPnet users will only enter identifiable student information into the fields specified for this purpose (student last name, student first name) and will not enter names or other information that may identify a student into fields designated for Comments, Alerts, or other purposes.

i. If a studentôs identifiable information contained in HSPnet is to be used for any new or previously unidentified purpose, including but not limited to research or quality assurance activities, the student(s) affected will be contacted by a representative of their educational program for the purpose of updating their informed consent to include the new or previously unidentified purposes.

Related Documents

- *Consent Form for Use and Disclosure of Personal Information*
- *Identified Purposes and Handling of Personal Information in HSPnet*
- *BCAHC Policy 3.4: Safeguards*

Section 3: Privacy, Security and Data Access

Policy No. 3.3: Accuracy of HSPnet Data

Purpose

To ensure that all reasonable efforts are made to guarantee the accuracy and completion of personal information in HSPnet.

Principle (based on the 10 Principles of the CSA Model Code)

Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

Policies

1. Participating Agencies will ensure that students have mechanisms to notify their educational institution of changes to their personal information.

2. The BCAHC and Participating Agencies will make reasonable efforts to ensure that personal information provided by a student is entered into HSPnet without errors or omissions.

Procedures

a. The BCAHC will build, test and implement mechanisms in HSPnet that facilitate the accurate entry of information by including tools such as:

   - Mandatory fields
   - Data entry confirmation prompts
   - Duplicate entry
   - Formatting rules

b. The National HSPnet Director will monitor reported problems relating to data and accuracy completeness and will alert the National HSPnet Alliance Steering Committee as to the nature and cause of the data quality issue plus recommendations or actions taken. Such actions may include training, user communications, and improvement of HSPnet functionality.

c. User Agencies may contact the HSPnet Help Desk to arrange for a direct upload of student or staff data from their school information system or other databases into the HSPnet database. The BCAHC will maintain detailed instructions and data specifications to guide uploads from external data sources, and will ensure that the data to be uploaded is consistent with the purposes for collecting student information as defined by the Identified Purposes.

d. User Agencies will be responsible for ensuring the accuracy of information uploaded into HSPnet.

e. The HSPnet Team Leader will ensure that data uploads into HSPnet are checked for generic data errors, such as extra spaces or punctuation, that would impact data quality in HSPnet.

Section 3: Privacy, Security and Data Access
Policy No. 3.4: Safeguards for HSPnet Data

Purpose

To ensure personal information is protected by appropriate security safeguards.

Principles (based on the 10 Principles of the CSA Model Code)

- Safeguards are necessary to protect the data's confidentiality, integrity and availability.
- Safeguards must include: 1) preventive, 2) detective, and 3) corrective controls.
- Effective controls consist of four elements: 1) the control itself, 2) an agreement to employ the control, 3) a compliance mechanism to ensure that the agreement is being upheld, i.e., that the control is being used effectively and 4) consequences for breach of the agreement.
- Security controls apply to all individuals - staff, students, contractors, affiliates and partners. Security controls must be applied to all elements of information management: information, infrastructure, applications, and business process and should include physical measures, organizational measures and technological measures.
- Access control is required to prevent unauthorized persons from accessing data and to prevent authorized persons from accessing data for unauthorized purposes. Data accessed for an authorized purpose must not be used for an additional purpose.

Policies

1. The BCAHC will follow industry standards and/or best practices on safeguards to protect the confidentiality, integrity and availability of data in HSPnet.

2. The BCAHC will enforce compliance with standards wherever possible through automated tools and scheduled activities that detect possible problems with safeguards and facilitate development and introduction of remedies.

3. The BCAHC will incorporate initial and ongoing education about National HSPnet Policies into all training materials and processes, and into regular user communications.

Procedures

a. 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, data encryption, and reporting of security breaches or data loss to the National HSPnet Director by the end of the work day during which the breach or loss occurred.

b. The BCAHC will monitor the activities of the server host and network provider and take immediate corrective actions if the minimum standards of the Service Level Agreement (SLA) are not met.

c. The National HSPnet Director will report any security breaches or data loss by the end of the work day during which the breach or loss occurred, to the BCAHC Executive Director, HSPnet Coordinator and/or Lead Agency representative of the affected jurisdiction, and National HSPnet Alliance Steering Committee members as deemed appropriate.

d. The BCAHC will issue a User ID with Local Administrator rights to one or more authorized individuals within each Participating Agency, and will provide Local Administrators with comprehensive training and documented instructions on their responsibilities as Local Administrator.

e. Local Administrators will be responsible for creating, managing, and deleting User IDôs for authorized individuals within their organization. They will not be permitted to create additional User IDôs with Local Administrator rights.

f. Local Administrators will grant or modify access rights for a user as appropriate for that individualôs organizational responsibility for placing students as defined by the Identified Purposes. Local Administrators will grant access on a need-to-know basis only, and will limit each userôs access to placement information that is within their organizational responsibility.

g. The BCAHC will ensure that HSPnet tools for managing user access provide adequate granularity and specificity to allow users to perform their work while protecting personal information from intended or inadvertent browsing or tampering.

h. Local Administrators will assign a unique User ID to each individual user; there will be no shared User IDôs among HSPnet users. Local Administrators will ensure that each user has a secure email address entered into HSPnet for the purpose of direct communication from other HSPnet users and for receipt of system messages from HSPnet including delivery of passwords.

i. HSPnet users will notify their Local Administrator of any changes to their organizational role that may impact their need for access to identifiable student information in general or for a specific educational program, discipline, or receiving destination. For example, if a user is no longer responsible for a unit or program area, the Local Administrator will be notified to remove that unit or program area from the userôs access.

j. The HSPnet application will automatically forward a random, confidential, complex password to the userôs email account upon creation of a new User ID. New users will be required to select a new password upon login for the first time. Passwords will be of a format complex enough to prevent guessing or other routine efforts to use another individualôs User ID. The password format and rules will be reviewed annually against industry standards by the Technical Advisory Committee.

k. The HSPnet application will automatically require users to change their password according to a set schedule to be determined and reviewed annually by the Technical Advisory Committee.

l. The national HSPnet Data Stewardship Committee will review the results of semi-annual data audits related to data quality, privacy and security in order to detect intentional or unintentional release of private information and inappropriate access to data.

m. The National HSPnet Director will address any breaches of Policy by:

- On a first offence, alert the offending user as to their Policy breach, direct them to the Policy regarding next steps upon escalation, and audit 100% of transactions for that agency for three months;
- On a second offence of one or any users in a single agency, alert the Dean/Director or Department Head for the user(s), direct them to the Policy regarding further escalation, and audit 100% of transactions for that agency for three months;
- On a third offence of one or any users in a single agency, alert the BCAHC Executive Director for action up to and including disabling the access rights of the offending user(s)ô and/or all usersôaccess rights; if access is permitted to continue, audit 100% of transactions for that agency for three months.

n. Notwithstanding the escalation process outlined in Procedure 3.4.n above, the National HSPnet Director may disable access rights for one or more offending user(s) immediately at his/her discretion, even for a user's first offence, in serious situations including but not limited to:

- An offence that represents an immediate and/or significant risk to student privacy;
- An offence where the user's action appears to be intentional or malicious in nature.
- An offence that significantly and negatively impacts data quality in HSPnet

o. The HSPnet application will automatically time-out if left inactive for a set period of time. The time-out period will be reviewed annually by the Technical Advisory Committee.

p. Unused User ID's, which have been inactive for a period of six months, will be inactivated automatically on a quarterly basis via an HSPnet utility.

q. The National HSPnet Director will 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 national Data Stewardship Committee and recommendations sent to the National HSPnet Alliance Steering Committee.

Section 3: Privacy, Security and Data Access

Policy No. 3.5: Openness, Individual Access and Challenging Compliance of HSPnet Data

Purpose

To ensure openness and accessibility for students whose personal information is contained in HSPnet.

Principles (based on the 10 Principles of the CSA Model Code)

- An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information.
- An individual shall be able to address a challenge concerning compliance with the above principles to the designate individual or individuals accountable for the organization's compliance. Safeguards must include: 1) preventive, 2) detective, and 3) corrective controls.

Policies

1. National HSPnet Policies will be made available and open with respect to management of personal information. These policies will describe the mechanism whereby a student can access their own information as well as a complete description of the type of personal information collected and the Identified Purposes for the information.

2. The BCAHC will provide the opportunity for students to access data collected in their name. Only the student or their designated representative has a right to access such personal information and no student will be entitled to personal information on another individual.

Procedures

a. National HSPnet Policies will be made available on the HSPnet website at www.hspcanada.net, or upon request by a student to the BCAHC National Privacy Officer.

b. A student can request a copy of their personal information in HSPnet by presenting a written request to the placement coordinator of their educational program along with two pieces of identification, one of which must be their current student identification card with student number and photograph. The placement coordinator 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/disclosure of that information plus an explanation of the list provided. The placement coordinator will copy the provincial privacy officer on the responses to the student.

c. Any decision to refuse all or part of a studentôs request for access to information will be relayed in writing to the requestor and will include (1) the specific provision for refusal under the jurisdictionôs legislation and (2) clear reasons for the refusal.

d. 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 studentôs record that their request for a change was refused.

e. A student may register a complaint or challenge regarding the handling of personal information in HSPnet in writing to their provincial Privacy Officer, who will investigate the complaint/challenge through the involved Participating Agencies. If the student is unsatisfied with the response from the provincial Privacy Officer, this student may register a complaint to the National Privacy Officer.

f. The National Privacy Officer and Participating Agencies will take appropriate measures, including as necessary the adjustment of National HSPnet Policies. The National Privacy Officer will relay the measures taken or proposed, back to the student within one month of their original complaint or challenge.

Related Documents

- *Identified Purposes and Handling of Personal Information in HSPnet*
- *Policy 3.1 - Accountability*
- *Role Description – Privacy Officer*

APPENDIX 2 (PIA-NL)

Section 3: Privacy, Security and Data Access

Policy No. 3.6: Access to HSPnet Data

Purpose

To ensure appropriate access to HSPnet data by HSPnet users and external requesters.

Principles (based on the 10 Principles of the CSA Model Code)

- An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the CSA Model Code principles.

Definitions

HSPnet user ï An individual with an active HSP*net* user ID who may access data as determined by his Access Rights (set by a Local Administrator) and as appropriate for his organizational role.

Participating Agency ï An agency with one or more staff members who are HSPnet users.

External Requester ï An individual or agency that makes a request for HSPnet data but does not have any HSPnet users on staff.

Policies

1. The Data Stewardship Committee for each province will establish a process to guide consideration of requests for access to data at all levels, and will conduct an annual evaluation of the effectiveness of that process.

2. A Data Sharing Agreement between the BCAHC and each Lead Agency, on behalf of user agencies in each jurisdiction, will be established to document the respective rights and responsibilities of parties in contributing, protecting, and enabling access to HSPnet data.

3. The National HSPnet Alliance will grant Lead Agency representatives, or designates, access to provincial HSPnet data. Access will be limited to data required to support their mandate as HSPnet-xx Lead Agency for managing the HSPnet budget and internal cost recovery, user communications, and participating in practice education initiatives (eg: capacity management, improving data quality and network processes).

Procedures

a. HSPnet-XX Data Stewardship Committees will oversee an Approvals Process for access to HSPnet data according to the Data Access Approval Guidelines on the following page. HSPnet-XX Data Stewardship Committees will conduct an annual review of the outcome of requests considered through the Approvals Process, and if necessary advise the National HSPnet Alliance Steering Committee on the need to revise this Policy and/or the Approvals Process.

b. One or more HSPnet users may request a data extract or development of a Custom Report by forwarding a completed HSPnet Data Access Request Form (http://www.hspcanada.net/resources/forms.asp) to the HSPnet Help Desk. The HSPnet Help Desk will review the request against the Data Access Approval guidelines and deliver the completed report if authorized by the guidelines, or will seek approval from the National HSPnet Director or from that user's HSPnet-XX Data Stewardship Committee (or from all committees if the data request crosses provincial boundaries). The Data Stewardship Committee may consider such data access requests

from the user's jurisdiction by using the Data Access Request Template for Data Stewardship Committees (http://www.hspcanada.net/privacy/resources.asp).

c. If a Custom Report has ongoing value to other HSPnet users, the National HSPnet Director may publish the report as a new pre-defined report to the Reports Menu, in accordance with the Data Access Approval Guidelines.

d. Cross-agency access may be permitted when partnering agencies have entered into a formal agreement compliant with the jurisdiction's privacy legislation, the provincial Privacy Impact Assessment and the National HSPnet Policies.

e. Jurisdictions will ensure Student data sharing Agreements are in place that will address situations where two or more educational Programs may operate under a collaboration or affiliation arrangement whereby students transfer from one Placing Agency to another during completion of their Program. The Student Consent form for Students enrolled in such collaborative or "transfer" programs will include reference to a potential need to transfer a copy of their personal information from the "starting" Placing Agency to their "finishing" Placing Agency involved in the collaborative Program.

f. On an annual basis, the National HSPnet Alliance will review and update a list of standard extracts available to the Lead Agencies and consistent with their provincial mandate.

Related Documents

- *Terms of Reference – HSPnet Data Stewardship Committee*
- *Provincial Collaborative Agreement (Province & BCAHC)*
- *Procedure: HSPnet-XX Lead Agency Access to provincial data*

APPENDIX 2 (PIA-NL)

Data Access Approval Guidelines

Level of Requester	Type of Request and *Example(s)*	Approval Process
Non-Identifiable Data (student personal information removed)		
HSP*net* users	**Placement Data** ▪ *List of students on my unit next month* ▪ *Placement hours per student in my allowed educational programs*	▪ Pre-defined reports and customizable report wizards will be made available within the HSP*net* Reports menu, available to authorized HSP*net* users as permitted by their Access Rights. ▪ Requests for data that is not available from a pre-defined report or wizard may be submitted via the Custom Report Queue in HSPnet. The requested data will be released by the HSPnet Team if the data is within the requesting user's Access Rights and is consistent with the permitted uses of data (e.g. a list of supervisors for purposes of preceptor recognition).
	Cross-Department Data ▪ *Comparison of placement hours across multiple departments or programs not within my access rights*	Data requests to be approved by National HSPnet Director if the data requested is within the scope of the requester's role in their agency
User Agencies *(individuals who are not an active HSPnet user but who are authorized representatives of an agency that uses HSPnet)*	**Agency-Specific Data** ▪ *# of Placements in all departments in my agency*	Data requests to be approved by National HSPnet Director if the data requested is within the scope of the requester's role in their agency
	Cross-Agency Data: agency non-specific ▪ *List of all LPN nursing placements in BC*	Data requests to be approved by the National HSPnet Director if the data requested is specifically related to the requester's role in their agency and the data will provide information that would otherwise be publicly available
	Cross-Agency Data: agency-specific *Placements involving multiple schools as members of a committee or collaborative (e.g. Nursing Interschool in BC, Ottawa region's Clinical Resource Committee)* *Pediatric placements across multiple Placing or Receiving agencies*	Data requests to be approved by: ▪ the jurisdiction's Data Stewardship Committee; OR ▪ the National HSPnet Director if all agencies contributing data give permission to generate the combined report on a one-time or ongoing basis
Non-Identifiable Data (student personal information removed)		
External Organizations *(non-users of HSPnet*	**Aggregate Data:** Government and Policy organizations may be granted access to aggregate (de-identified) data as available within the Policy Access Level (PAL) module of HSPnet.[1]	PAL user ID's to be approved by the jurisdiction's Data Stewardship Committee.
	Non-aggregated Data: Limited to agency program- or site-identified data; no personal identifiers	Data requests to be approved by: ▪ the jurisdiction's Data Stewardship Committee; OR ▪ the National HSPnet Director if all agencies contributing data give permission to generate the combined report on a one-time or ongoing basis
Identifiable Data (student personal information included)		
All Requesters	**All Requests**	Data requests to be approved by the jurisdiction's Data Stewardship Committee

[1] PAL access allows generation of aggregate data on placement activities and related information, based on data for which all personal identifiers (student/staff) and agency identifiers (Placing or Receiving Agency, program, site) have been removed.

APPENDIX 2 (PIA-NL)

Section 4: HSPnet Governance and Management

Under Development:

- **Development and Change Control**
- **Release Management and Control**
- **HSPnet System Maintenance**
- **System Performance Standards and Monitoring**

Section 5: HSPnet Systems Development

Policy No.5.0: User Reference Group for HSPnet Enhancements

Purpose

The User Reference Group is a voluntary consultative resource to the HSPnet development team in the development, assessment and evaluation of enhancements. Communications and consultation is required before introducing enhancements, new data fields ad associated enforcement rules, and reporting on new fields.

Principles

- ***HSPnet functionality***: should not unproductively duplicate other systems. Request would have to have rationale and self-assessment against principles ï expand to include analysis against these principles once finalized. Encompass impacts within the overall HSPnet risk management plan ï issues of privacy, data quality, system performance, etc. Enhancements are in alignment with the National HSPnet Alliance strategic plan.

- ***Financial Impacts:*** research and document the one-time and ongoing cost impacts

- ***Compliance with national policies***: Research privacy and legislative considerations where needed. Consider non-HSPnet policy issues and requirements, before and after implementation

- ***Ongoing evaluation*** of impacts (post-implementation and periodic review) ï define evaluation indicators and tools (e.g. surveys)

- ***Equity:*** design enhancements to be generic so as to benefit a high number of users and/or multiple disciplines. Consideration for both PA and RA and other scenarios - Impacts of enhancements and associated business rules should be considered and mutually agreed upon

Definitions

Enhancement: may be an improvement or expansion of an existing functions, addition of new data fields, addition of rules that enforce use or fields or features or of new modules.

- ***Class 1 Enhancement****: Minor fixes or changes to maintain or improve HSPnet functionality which does not require consultation from users.*
- ***Class 2 Enhancement****: Planned enhancements, identified on an ongoing basis by HSPnet users or other stakeholders*
- ***Class 3 Enhancement****: Specially funded enhancement projects by provincial lead agencies outside the national budget.*

User Reference Group: a volunteer group of HSPnet users, who, on occasion, are consulted for input and assessment of enhancement idea.

APPENDIX 2 (PIA-NL)

Procedures

HSPnet-XX Management Committees and Data Stewardship committees to propose individuals to participate on the User Reference Group. Participants would be chosen based on a high level of use and understanding of HSPnet functions, able to objectively assess and make recommendations on proposed enhancements.

The selected participants would be part of an informal user reference group (URG) composed of a varied users (placing and receiving)

Requirements / Principles from URG:

- Assist the HSPnet team in defining specifications and determining user impact of enhancement
- Consultation and participation from URG members is voluntary
- Requests for input to be sent to URG members via email.

Related Documents

Enhancement Request Form

Section 6: Training and Support

Policy No. 6.1: HSP*net* Training

Purpose

To ensure cost-effective access to high quality training for HSPnet users.

Principles

All users of HSPnet should receive a standardized minimum of training before being granted an HSPnet user ID, including:

- Privacy and security of personal information (as required to meet local legislative requirements and commitments of the Privacy Impact Assessment in all provinces)
- HSPnet navigation (characteristics of web-enabled applications, saving changes, etc.)
- Access to online help and User Support

HSPnet Training should be designed and delivered to meet the varying needs of different user levels

HSPnet Training should be delivered by the most cost-effective mechanisms that ensure:

- User satisfaction and self-assessment of competency to continue independently
- User proficiency levels that minimize ongoing use of Help Desk
- Opportunities for user feedback during training, thereby ensuring that HSPnet functionality continues to evolve and meet user needs

User Agencies are responsible for effective utilization of Training resources through:

- Timely advance registration and provision of adequate information to setup trainees prior to training;
- Compliance with policies and procedures regarding attendance and cancellation and completion of pre-training requirements;
- Trainee compliance with rules of conduct during HSPnet training (respect for fellow trainees, completion of pre-training requirements, etc.)
- Timely payment of training fees that may be established by the Management Committee for each jurisdiction, such as fees for late cancellation or ñextraò training outside of the approved annual budget.

Policy

1. The HSPnet team will maintain a Training Plan that is appropriate for each user level, encompassing:
   - Effective processes including registration mechanisms, trainee communications, and distribution of pre-training instructions and materials.
   - Detailed training curricula (learning objectives, resources, activities)
   - Training materials including course outlines, worksheets, quick reference guides, and handouts
   - e-Learning resources to provide standardized background content, ongoing access to refresher opportunities, and in some cases an alternative to classroom based learning.
2. The HSPnet team will evaluate and report on the effectiveness of Training activities on an annual basis, including (but not limited to) measures of user/trainee satisfaction, user proficiency, ongoing use of Help Desk resources, and User Agency compliance with policies and procedures.

Procedures

a. The National HSPnet Director will ensure that a Training Plan is updated annually and published, along with associated documents and materials, on the public website.

b. The National HSPnet Director will report on an annual evaluation of Training utilization and effectiveness to the National Steering Committee and to each provincial Management Committee.

c. The National HSPnet Director will report annually regarding User Agency compliance with this Policy including attendance rates and late cancellation or no-show rates and associated impacts.

d. The Management Committee for each jurisdiction will have the option to set an HSPnet-XX Fee Schedule to recover costs for training activities outside of the annual approved budget. Such fees would reflect the fact that the National HSPnet Alliance operates on a cost recovery basis, and fees may therefore be necessary to cover costs such as:

    - ñExtraòtraining for any User Agency wishing to fund additional training due to high staff turnover, customization to support unique organizational processes, etc.;
    - Charges for late cancellation and ñno showòregistrants (to be defined by National HSPnet Director and reviewed annually);
    - Training binders and other materials;
    - Partial or full recovery of training costs to offset the jurisdictionôs annual operating budget.

Related Documents

- *HSPnet-XX Fee Schedule*

Section 7: Language Duality

Policy No. 7.0: General

Purpose

To ensure equitable access to HSPnet functionality and support for users in both official languages of Canada.

Principles

- All users of HSPnet should have access to training and support in the language of their preference (French or English).
- HSPnet should function effectively and at an equivalent level for anglophone, francophone and bilingual users.

Policy

1. The HSPnet team will strive over time to recruit bilingual staff/contractors and to develop bilingualism in all team members.

2. The National HSPnet Alliance will establish an HSPnet Language Duality Subcommittee to advise the Alliance on ongoing practices and needs to ensure that HSPnet meets its language duality commitments.

3. The National HSPnet Director will ensure that all formally published documents are made available in both official languages on the public website and for user distribution.

4. Time-limited or project-specific documents (e.g. an enhancement funded and led by one organization or a province) may be published on the public website in the preferred language of the lead jurisdiction if project funding is not available to support translation to both languages during project planning and development stages.

Procedures

a. The BCAHC will ensure that the Training Plan addresses the needs of all HSPnet users in an equitable fashion, including evaluation of training utilization and effectiveness.

b. The BCAHC will maintain a Help Desk staffing and development plan to deliver an equitable standard of response to all users in their preferred language.

c. For project-specific or time-limited documents, the National HSPnet Director will publish a summary statement of the project or initiative in both official languages for the benefit of all HSPnet users and interested audiences.

- Any organization or jurisdiction wishing to ensure that their users can follow and/or participate in a project in their preferred language may volunteer resources (translation services or funding) to facilitate translation of key documents throughout the project. For example, a bilingual member of a project team may offer to translate Meeting Notes and Requirements Specifications into the other language.
- Upon project completion any documents with ongoing value, including final versions of key project documents and all instructions for implementing and using the new enhancement, would be translated and published in both official languages.

Health Sciences Placement Network
Réseau de gestion des stages en sciences de la santé

APPENDIX 3 (PIA-NL)

Agreement on Confidentiality and Rules of Conduct for HSPnet Service Providers

Name: _____

I, _____, acknowledge that I am an employee, contractor, or subcontractor of the BC Academic Health Council (BCAHC) or other organization contracted to provide services to HSPnet users, and therefore acting in the capacity of "HSPnet Service Provider." In this capacity I have been granted access to the HSPnet application and databases ("HSPnet Access"), for the purpose of enabling me to perform the following activities (check all that apply):

- ❑ View identifiable personal information of students, and/or business information of employees or contractors from Participating Agencies (HSPnet users and agency contacts);
- ❑ View and/or modify setup information of Participating Agencies including HSPnet user contact information and access rights, plus other setup information including but not limited to Agencies, Departments, Programs and Courses, Sites, Services, and Destinations;
- ❑ View and/or modify HSPnet intellectual property in the form of the application and/or databases, including but not limited to hardware and software configurations and settings, programming code of the application, database structures and content, data queries and reports, HSPnet screen and forms designs, business rules, and system documentation.
- ❑ View and/or modify HSPnet intellectual property in the form of documentation, including but not limited to the public HSPnet website(s), user guide, handouts, forms, and training materials.

In accepting the role of HSPnet Service Provider:

1. I acknowledge that all HSPnet intellectual property is and will remain the property of the BCAHC. I will not reproduce, adapt for another project or purpose, or otherwise disclose it to any external party without the written permission of the BC Academic Health Council.

2. I agree to view identifiable information on individuals only as required to meet my responsibilities as HSPnet Service Provider. I acknowledge that viewing data that is not required to meet my responsibilities is considered to be unauthorized browsing and is strictly prohibited.

3. I am in receipt of the HSPnet Policies on Privacy, Security & Data Access ("the Policies") and agree to meet my responsibilities as described in the Policies and in my job description and/or services contract as HSPnet Service Provider. I acknowledge that the Policies may change over time and that the BCAHC will notify me of changes that materially impact my role.

4. I will not copy, discuss, or otherwise disclose information on individuals or Agencies entered into HSPnet that was obtained as a result of my access to HSPnet, except in the performance of my duties as HSPnet Service Provider and only to authorized HSPnet users who are specifically permitted to access that information as outlined in the Policies, or as required by law.

5. I acknowledge that the obligation to maintain confidentiality as outlined above survives the termination of my role as HSPnet Service Provider, even after any HSPnet access has been revoked.

6. I will take all reasonable steps to maintain the integrity and value of the HSPnet intellectual property by documenting my activities involving any modification to the intellectual property as noted above.

_____ _____

Signature of HSPnet Service Provider Date

Copyright © 2010 Roberts Hendrickson Consulting Inc.

APPENDIX 4 (PIA-NL)

Health Sciences Placement Network
Réseau de gestion des stages en sciences de la santé

Consent Form for Use and Disclosure of Student Information

Student Name: _____ Student No: _____

1. Permission to Use and Disclose Your Student Related Personal Information and Personal Health Information

By signing this consent, you authorize your educational Program _____ to:

- Use and/or disclose your personal information (name and student profile information that is under the custody and control of your Program) to authorized staff of Receiving Agencies for the purpose of locating and coordinating an appropriate placement experience (e.g. clinical practica, fieldwork, or preceptorship) as required by your educational program;
- Use your student related personal information and personal health information relating to placement prerequisites, for the purpose of tracking your compliance against Receiving Agency safety and infection control prerequisites for accepting students. Placement prerequisites that may be tracked include personal information such as CPR certification or criminal records check status, and personal health information such as immunity/immunization status of vaccine-preventable diseases. Placement prerequisite information is used only by staff involved with your educational program, and is never disclosed to users external to your educational program.

2. Consent Period

This consent is effective immediately and shall remain valid for up to six years, or shall be voided upon your completion of the Program, your formal withdrawal from the Program, or upon written request as described below.

3. Your Rights With Respect to This Consent

3.1 Right to Refuse Consent - You have the right to refuse to sign this consent, and if you refuse your placement will be processed manually at the earliest convenience of the Program and Receiving Agency.

3.2 Right to Review Privacy & Security Policies - A copy of the document entitled *Identified Purposes and Handling of Personal Information in HSPnet*, which summarizes Privacy and Security policies relating to how we may use and disclose your personal information via HSPnet, is distributed with this Consent Form. You may wish to review the complete Privacy and Security Policies for HSPnet before signing this consent. The Privacy and Security Policies may be amended from time to time, and you may obtain an updated copy by contacting privacy@hspcanada.net.

3.3 Right to Request Restrictions on Use/Disclosure – You have the right to request that we restrict how we use and/or disclose your personal information or personal health information via HSPnet for the purpose of locating and coordinating a suitable placement experience. Such requests must be made in writing to the placement coordinator for your Program. If we agree to a restriction you have requested, we must restrict our use and/or disclosure of your personal information in the manner described in your request. If this restriction precludes our ability to coordinate your placement via HSPnet, then your placement will be processed manually at the earliest convenience of the placement coordinator and receiving agency.

3.4 Right to Revoke Consent - You have the right to revoke this consent at any time. Your revocation of this consent must be in writing to the placement coordinator for your Program. Note that your revocation of this consent, or the voiding of this consent upon your completion or withdrawal from the Program, would not be retroactive and would not affect uses or disclosures we have already made according to your prior consent.

3.5 Right to Receive a Copy of This Consent Form - You may request a copy of your signed consent form.

Collection of your personal information is done under the authority of the privacy legislation that applies to educational institutions in your province. For more information visit www.hspcanada.net/privacy/index.asp.

I hereby authorize my educational Program to use and/or disclose my personal information via HSPnet for the purpose of locating and coordinating appropriate student placement(s) as required by the curriculum.

_____ _____

Signature of Student Date

Health Sciences Placement Network
Réseau de gestion des stages en sciences de la santé

APPENDIX 5 (PIA-NL)

Identified Purposes and Handling of Personal Information and Personal Health Information in HSPnet

Updated: July 1, 2013

Background

The Health Sciences Placement Network (HSP*net*) is a secure web-enabled application that is used by several jurisdictions in Canada. The HSPnet database contains information about students in clinical placements within health agencies and other locations. Students authorize their educational program to use and disclose their personal information (name, student profile) and to use (but not disclose) their personal health information via HSPnet for the purpose of locating and coordinating placements as required for an educational program. This document provides a summary of the national HSPnet Policies on Privacy, Security and Data Access, relating to the protection of student information within HSPnet. The full Policies can be viewed on the HSPnet website at www.hspcanada.net.

Collection, Use, and Disclosure of Personal Information (PI) and Personal Health Information (PHI) in HSPnet

HSPnet policies ensure that PI and PHI in HSPnet:

- Are collected, used, and disclosed only for purposes consistent with identifying and coordinating a student's clinical placements;
- Cannot be used or disclosed without the consent of the student whose PI or PHI is to be collected; and
- Are used by or disclosed only to authorized individuals on a need-to-know basis, by/to staff involved in student placements within the student's educational program or placement site. PHI is never disclosed via HSPnet to users who are external to the student's educational program.

PI Collected *May include any or all of:*	**Uses of PI** *BY authorized users only within Student's Educational Program*	**Disclosure of PI** *TO authorized users only within the Placement Site being asked to accept the Student*
• Student names • Student home address, phone numbers or email addresses • Student number • Student photograph • Placement Preferences (1st, 2nd and 3rd choices if offered) • Student gender – limited to students placed in locations that accommodate patient/ client preference for the gender of their care provider gender (e.g. homecare visits).	• To contact students regarding placement needs or status, or regarding urgent issues such as labour disruption at the placement destination • To generate class placement lists, confirmation notices and schedules • To maintain a student history of placements	Student name is disclosed upon confirmation of an accepted placement, for the purpose of facilitating placement arrangements (orientation, preceptor assignment) and as a record of students received by the Site. Name may be disclosed, at the discretion of the educational program, prior to acceptance if the Receiving Site has a need to know (e.g. to arrange a student interview, if the student is an employee). The student's school-issued email address may be released for the limited purpose of delivering passwords to Site computer networks. No other student PI (besides name) is disclosed under any circumstances, excluding Student gender which may be disclosed on specific request by a placement site that requires this information to accommodate patient/client preference (e.g. placements in homecare agencies).
Student Prerequisites as required by Placement Sites (e.g. criminal records check, CPR or other certifications)	To track student compliance with each site's published requirements for criminal records check, CPR certification, etc.	*Not disclosed under any circumstances*
Student Profile of educational or work history relevant to placement requests	To facilitate a good fit between the student and Placement Site, learning experiences offered, and supervisor/preceptor to be assigned.	

PHI Collected *May include any or all of:*	**Uses of PHI** *BY authorized users only within Student's Educational Program*	**Disclosure of PHI**
Status of indicators for safety and/or infection control as required by Placement Sites prior to accepting students: • Information on a student's immunity or immunization status for vaccine-preventable diseases such as Varicella, Diptheria/Tetanus, Influenza, and Measles/Mumps or Rubella • Information on Tuberculosis status including TB test and/or chest X-ray results	To track status of a student's eligibility according to the requirements of Receiving Agency sites where students may be placed	*Not disclosed under any circumstances*

Safeguards

- The accuracy and completeness of personal information within HSPnet is maintained through the use of system tools such as mandatory fields and formatting rules, and through periodic reviews of data quality to identify the need for interventions such as user training or system modifications.
- HSPnet data is physically and logically secured in accordance with industry standards and best practices, including enforcement of strict rules for physical security and backups, password protection at all points of access, and use of anti-virus software, firewall protection, and data encryption.
- Periodic audits of HSPnet transactions are carried out to ensure there are no problems and/or gaps in the user interface that might permit inappropriate access to or update of data.
- Personal information on each student, along with their placement history, is retained for a housekeeping period of180 days after the student's completion of or withdrawal from the educational program, or after the consent expiry period of six years, whichever occurs first. A copy of their personal information is available to a student upon request to their jurisdiction's Privacy Officer or the national HSPnet Privacy Officer.

Openness, Access, and Challenging Compliance

- An individual can access their own information as well as a complete description of the type of PI or PHI used/disclosed and the purposes for using or disclosing the information. Such requests can be made in writing by the student to the national HSPnet Privacy Officer and/or to the local Privacy Officer within the student's jurisdiction (contact information for each province or jurisdiction is available on the HSPnet website at www.hspcanada.net/privacy/index.asp).
- An individual may request changes to their PI or PHI contained in HSPnet, or may register a complaint or challenge regarding the handling of their information in HSPnet, by submitting a request in writing to the national HSPnet Privacy Officer or local Privacy Officer within their jurisdiction.

Updated March 15, 2010

Policy Application Guide:

Policy 3.2 - Identified Purposes and Ensuring Consent for Data Collection, Use and Disclosure

Introduction

This guide includes the following information and documents:

Section	Document Name
Background and Recommended Policy Application	
Workflow Diagram	*Consent Implementation Options*

Background

HSPnet Policy 3.2 *Identified Purposes and Ensuring Consent for Data Collection, Use and Disclosure* sets a high standard for privacy protection by requiring active consent from students for the use and disclosure of their personal information. Compliance with this policy requires an educational Program to collect a signed consent form from students, through an informed consent process that is supported by a handout describing the use and handling of student information in HSP*net*.

This document outlines a process for implementing Policy 3.2, including both a ***long term*** approach (whereby all new students provide consent prior to their entry into HSP*net*) and an ***interim*** approach to support a Program's use of HSP*net* during the transition period of implementing a long term consent process.

Recommended Policy Application

1. During HSPnet implementation planning, educational Programs should develop a mechanism within their admission or registration process for distributing the HSP*net* consent form and handout to all new applicants or registrants. The **long term** objective of this mechanism should be to ensure that HSP*net* consent is obtained as an integral part of documentation collected for all new (first year) students, thereby over time replacing the need for interim mechanisms as outlined below.

2. As an **interim** approach during the transition period (before all new students can sign HSP*net* consent forms), a Program may elect to enter student information into HSPnet if they determine that existing consent/notification processes are adequate to cover uses/disclosures of student information via HSP*net* (i.e. for the purpose of locating and coordinating an appropriate practice education experience). Examples of existing consent/notification processes include:

- Other 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 personal information;
- Online processes for notifying students and/or obtaining consent.

3. Even if existing consent/notification processes are determined to be adequate during the transition period, the Program should notify previously admitted students about the use of HSP*net* for student placements and should make reasonable efforts to collect signed HSP*net* consent forms within the months immediately following HSP*net* implementation. Such efforts could include:

   - Distribution and collection of HSPnet forms/handouts during class (if instructors are involved in this process, they should receive the handout entitled *Guide for Instructors of Programs Using HSPnet* to support their role in answering student questions and/or directing them to other resources);
   - Distribution of the HSP*net* form/handout as an email attachment, with instructions for fax/mail return of signed forms to the educational program.

4. As outlined in Policy 3.2, educational Programs must document cases where a student refuses their consent and follow the procedure for removing the student's record from HSP*net* or limiting information that is disclosed.

For more information, contact your province's HSP*net* Privacy Officer (visit the website at www.hspcanada.net/privacy/index.asp) or contact privacy@hspcanada.net.