Policy
Privacy

3sHealth is committed to protecting and respecting the privacy of personal information under its control. The purpose of this policy is to confirm 3sHealth's commitment to privacy and to establish new policies and procedures as required to comply with applicable privacy laws.

It is important to note that this Policy is not intended to be a complete statement of all aspects of privacy within 3sHealth. Instead, it is intended to establish a high-level policy that will guide and assist 3sHealth in complying with privacy law requirements in a timely and cost-effective manner. As such, this Policy may, from time to time, be supplemented by additional policies, standards, guidelines and procedures that address specific privacy related risks or issues relating to 3sHealth. Examples of situations where specific policies may be implemented:

- where further detail is required to meet the requirements, guidelines and overall objectives of this Policy; and
- where a new program or service offering is introduced at 3sHealth that has unique privacy related issues or requirements.

Any questions or clarification required should be referred to the 3sHealth privacy officer.

This Policy applies to all directors, officers, management and employees of 3sHealth and all contractors providing services to 3sHealth (collectively, "**3sHealth Representatives**").

Non-compliance with this Policy by any 3sHealth Representative may lead to disciplinary action including suspension, dismissal or termination of contract.

The primary objective of this Policy is to help ensure that 3sHealth meets its obligations under applicable privacy laws.

It is important to recognize, however, that the privacy laws may change from time to time. Where such changes occur, this Policy will be amended accordingly.

Procedure

1. Implementation

This Policy Framework will be implemented in accordance with the following process:

- Introduction – This version of the Policy Framework will be formally introduced and implemented by 3sHealth effective April 18, 2012.
- Annual Reviews – 3sHealth will conduct annual reviews of this Policy to ensure compliance with the existing Policy and determine whether any changes to this Policy are necessary to deal with new legal requirements and/or new business processes.

2. Implementation of Privacy Principles

2.1 Accountability

2.1.1 The Manager of Technical Support Services will assume the position of Privacy Officer for 3sHealth. The Privacy Officer will assume general responsibility for all personal information under the control of 3sHealth and will be generally accountable for 3sHealth's compliance with applicable privacy laws. However, this does not in any way relieve other 3sHealth Representatives of their respective individual responsibilities under this Policy.

2.1.2 If a communication is received from the public inquiring as to who within 3sHealth is responsible for privacy matters, the inquiring person shall be informed that the Privacy Officer is responsible for privacy (see Section 2.9 for further detail).

2.1.3 3sHealth's obligations with respect to personal information extends to personal information that 3sHealth provides, or allows access, to 3sHealth Representatives that are third party contractors. In any situation where personal information under 3sHealth's control will be disclosed to or accessed by a third party contractor, an appropriate written confidentiality agreement must be put in place with the third party contractor.

2.2 Identifying Purposes

2.2.1 3sHealth primarily collects personal information for the purpose of providing services to its members. A list of each of these services is below and is considered an "Authorized Purpose".

- Administering benefits, including health and dental benefits, disability income plan benefits and life insurance plans for member organizations.
- Providing payroll services including disclosures to Canada Revenue Agency as required by law.
- Providing consulting services with a 3rd party company on behalf of a member organization (i.e. DIP – return to work program.).
- Providing communication to member organizations.

2.2.2 3sHealth Representatives shall not use personal information for any other purpose without the prior approval of the Privacy Officer. In such situations, the Privacy Officer shall determine whether any additional consents are needed from the individual(s) to whom the personal information relates. Only the Privacy Officer will have authority to determine whether a purpose is otherwise "required or authorized by law".

2.2.3 3sHealth Representatives should familiarize themselves with the Authorized Purposes. Further, 3sHealth Representatives should be able to explain to any individual from whom they are collecting (or have collected) personal information the purposes for which that information is being collected and how it will be used or disclosed.

2.3 Consent

2.3.1 3sHealth has reviewed the types of personal information it collects to ensure that each type of personal information is reasonably necessary to fulfill specified and legitimate purposes (i.e. the Authorized Purposes).

2.3.2 3sHealth will obtain an individual's consent to collect, use or disclose personal information (except where, as noted below, 3sHealth is authorized to do so without consent).

2.3.3 Consent can be provided in writing, electronically, through an authorized representative or it can be implied where: (i) the information is voluntarily provided to 3sHealth for an Authorized Purpose; or (ii) the purpose for collecting, using or disclosing the personal information would be considered obvious and the client, customer, or member voluntarily provides personal information for that purpose.

2.3.4 3sHealth reserves the right to refuse to accept resumes or employment applications and to refuse to provide service to any person who refuses to provide consent in relation to an Authorized Purpose.

2.4 Limiting Collection

2.4.1 3sHealth has identified the following general categories of personal information that it collects in the regular course of its business:

- Basic Personal Identifiers (such as name, address, telephone number, etc.)
- Unique Personal Identifiers (such as social insurance number; employee number, WCB claim number)
- Financial/Banking Information (such as account number; name of institution; garnishee information, insurance coverage)
- Employment Information (such as department, job title, work phone number, work e-mail address, union affiliation, hours of work)
- Complaint Information (such as disciplinary action, investigations or formal disputes)
- Family Information (such as marital status, information about spouse, children, maintenance enforcement, trusteeship)
- Personal Health Information (such as information about sickness, mental health or disability)

2.4.2 3sHealth has reviewed the specific data elements collected under each of these general categories and determined that each is reasonably necessary in connection with their respective Authorized Purposes.

2.4.3 3sHealth Representatives shall not collect data outside of these general categories without the prior approval of the Privacy Officer.

2.5 Limiting Use, Disclosure and Retention

2.5.1 As described above, 3sHealth Representatives are only permitted to use personal information for an Authorized Purpose. If personal information is used for any other purpose (as may be approved by the Privacy Officer), it must be recorded as a note on the applicable client file.

2.5.2 Disclosures of personal information by 3sHealth Representatives which do not require the prior approval of the Privacy Officer are limited to the following:

- disclosures which are made for an Authorized Purpose;
- disclosures which are made on a need to know basis; **and**
- disclosures which are made in accordance with any specific disclosure policies which have been approved by 3sHealth and are in force.

2.5.3 In some situations, use or disclosure of personal information for a purpose other than an Authorized Purpose may be required by law. Such legal requirements will override this Policy. However, only the Privacy Officer is authorized to determine when such legal requirements apply.

2.5.4 3sHealth Representatives must be aware that documents and records containing personal information need to be disposed of or destroyed in a secure manner. 3sHealth Representatives shall follow approved practices when disposing or destroying documents or records containing personal information.

2.6 Accuracy

2.6.1 3sHealth Representatives shall use reasonable efforts to update personal information when possible. However, this should only be done where it is necessary to update the information for the on-going administration of the file.

2.6.2 3sHealth Representatives should not rely on stale dated information as a basis for refusing to offer a product or service to a particular individual, except where reasonably necessary to protect the interests of the organization.

2.7 Safeguards

2.7.1 3sHealth will maintain reasonable policies, procedures and practices to help ensure the security and confidentiality of personal information.

2.7.2 Such policies, procedures and practices include (without limitation) the following:

(a) **Need to Know Access:** 3sHealth Representatives are only permitted to access personal information as necessary to fulfil legitimate job or service functions.

(b) **Transmittal of Information:** 3sHealth Representatives shall use reasonable care to ensure that the method of transmitting personal information (whether by telephone, mail, fax, e-mail or otherwise) is sufficiently secure taking into account the sensitivity of the information.

(c) **Locked Filing Cabinets:** When not in use, 3sHealth Representatives shall ensure that client files are stored in the appropriate filing cabinets. Such filing cabinets shall be locked outside of regular business hours.

(d) **Passwords/Access Cards:** 3sHealth Representatives shall protect the security of their computer passwords, building access cards and any other security codes or devices issued to them. 3sHealth Representatives shall not share such codes or devices with any person.

(e) **Security Incidents:** 3sHealth Representatives who become aware of any security related incident, or suspect the occurrence of any security related incident must report the matter to appropriate management. 3sHealth Representatives shall co-operate in the investigation of any such incidents.

(f) **Computer Workstations/Laptops:** 3sHealth IS shall activate hard-disk encryption on all laptop computers. 3sHealth Representatives must set a password protected keyboard/screen lock that is automatically activated by a period of inactivity. 3sHealth Representatives should use all reasonable efforts to prevent unauthorized persons from viewing computer screens. 3sHealth Representatives should not leave laptops unattended unless necessary and, when necessary, should use a locking device to secure laptops or otherwise take steps to prevent theft of the laptop. Please refer to the IS policies on 3sHealth StaffNet regarding Computer Use and Data Use.

(g) **3sHealth Representative Security:**

- 3sHealth and all 3sHealth Representatives will take reasonable steps to ensure that only 3sHealth Representatives who have a need to know are authorized to have access to sensitive IT systems, information or assets.
- A record will be maintained and be readily available documenting the issuance and retrieval of security related items such as User ID's, passwords, keys, codes, combinations and badges.
- 3sHealth will, where appropriate, obtain confidentiality agreements from 3sHealth Representatives.
- On termination or transfer of 3sHealth Representatives, or when a particular 3sHealth Representative's duties no longer require access to data, 3sHealth will immediately:
  - revoke access privileges (e.g. User IDs and passwords) to system and data resources and secure areas;
  - retrieve sensitive information including access control items (e.g. keys and badges); and
  - retrieve all hardware, software and documentation issued or loaned to the 3sHealth Representative.

2.7.3 3sHealth Representatives are responsible for complying with the above security policies and any other security policies and procedures introduced from time to time.

2.8 Openness

2.8.1 Inquiries from the public as to 3sHealth's privacy policies and practices shall be promptly referred to the 3sHealth Privacy Officer for handling.

2.8.2 Upon request, the public shall be provided with the following privacy related information:

- The name, title and address of the Privacy Officer.
- 3sHealth's processes for allowing an individual to access the information it may hold about the individual (see Section 2.9).
- The type of personal information held by 3sHealth and a general account of its use.

2.9 Individual Access

2.9.1 All requests from individuals for access to their personal information must be reviewed and administered in accordance with this policy.

2.9.2 3sHealth will provide access to personal information, and will amend inaccurate or incomplete personal information, subject to any applicable exceptions or exemptions under applicable laws.

2.9.3 All requests submitted by an individual must be written and submitted via paper or electronically. Requests by an individual for access to his/her personal information shall be immediately forwarded to the Privacy Officer. The Privacy Officer is responsible for handling and responding to such requests in accordance with applicable laws.

2.9.4 Written requests for access to personal information shall be made using the form attached to this Policy as Appendix "A". Individuals wishing to request access to their personal information shall be provided with a copy of this form and told to submit the completed form to the Privacy Officer.

2.9.5 3sHealth will use reasonable efforts to assist an individual who requires assistance in order to request access to his/her personal information.

2.9.6 3sHealth will respond to a written request for access to personal information within 30 days of receipt of the request. This means requests in the possession of 3sHealth Representatives must be forwarded to the Privacy Officer as soon as possible. Generally, this means a request must be forwarded to the Privacy Officer on the same day as the request is received. If the Privacy Officer is unavailable, the matter should be immediately forwarded to other senior management who may refer to outside legal counsel.

2.9.7 3sHealth reserves the right to extend the time period for responding to an access. Only the Privacy Officer, or in the absence of the Privacy Officer, senior management after consultation with outside legal counsel, is permitted to extend such time frame.

2.9.8 It is the general policy of 3sHealth to charge any reasonable costs relating to a request for access to personal information to the individual making the request. However, when it is anticipated that the costs of responding to a request will exceed $100, the Privacy Officer shall provide notice of such cost to the individual making the request prior to proceeding with the request.

2.9.9 If a request for access to personal information is refused, the individual shall be informed in writing by the Privacy Officer of the refusal and the grounds for the refusal.

2.10 Challenging Compliance

2.10.1 An individual may file a complaint with the Privacy Officer if he/she feels his/her rights have been violated. All complaints received by 3sHealth Representatives shall be immediately forwarded to the Privacy Officer for investigation and handling.

2.10.2 The Privacy Officer will investigate all complaints received, and if necessary, appropriate steps will be taken to correct and resolve the complaint. If an individual is not satisfied with the outcome of the investigation, they have the right to pursue the issue with the Saskatchewan Information and Privacy Commissioner.

2.10.3 Individuals who wish to file a complaint must complete the form attached as Appendix “B” to this Policy. Individuals wishing to file a complaint shall be provided with a copy of this form and told to submit the completed form to the Privacy Officer.

2.10.4 Once a complaint has been received by the Privacy Officer, the receipt of the complaint will be acknowledged, and the validity of the complaint will be examined. If the complaint is determined to be valid, the Privacy Officer will ensure that appropriate action is taken. If the case is denied, an explanation will be provided. The Privacy Officer will provide a response in either case.