	POLICY Number: 7311-75-003 Title: PRIVACY AND CONFIDENTIALITY
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Enterprise Risk Management Cross Index: 7311-25-001, 7311-25-003 Date Approved: June 3, 2015 Date Revised: March 16, 2017 Date Effective: March 16, 2017 Date Reaffirmed: Scope: SHR and Affiliates

DEFINITIONS

All Staff means SHR employees, practitioner staff, professional staff, affiliate employees, authority members, students and volunteers.

Business Information means confidential or internal information collected for SHR business purposes, including, but not limited to, disciplinary information, draft documents, legal advice, quality assurance reviews, disciplinary information, vendor proposals, and evaluations.

Confidentiality means a duty to keep information safe from unauthorized access, use or disclosure.

Current care means personal health information regarding a current hospital stay or information regarding recent care received.

Express consent means direct, explicit agreement given either verbally or in writing.

Implied consent means that the patient indicates willingness as a result of his or her behavior or conduct. Implied consent can be revoked under *The Health Information Protection Act* (HIPA) by an individual.

Personal health information (PHI) means, with respect to an individual, whether living or deceased[1]:

(i) information with respect to the physical or mental health of the individual;
(ii) information with respect to any health service provided to the individual;
(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
(iv) information that is collected incidentally to the provision of health services to the individual;
(v) registration information (e.g. demographic information).

[1] HIPA 2(m)

Personal Information (PI) means personal information about an identifiable individual, including employees, that is recorded in any form. Disclosure of PI requires written consent.[2]

Patient means a patient/client/resident.

Privacy means the right of individuals to determine for themselves when, how and to what extent information about themselves is communicated to others.

Record means a record of personal health information (PHI), business information or personal information in any form and includes information that is written, photographed, recorded, digitalized or stored in any manner.

Secondary use means using personal health information for a purpose other than the original purpose it was collected for (e.g. evaluation, research, quality of care committee).[3]

Trustee means an organization or individual listed in *The Health Information Protection Act* as having custody or control of personal health information. SHR is defined as the trustee in the context of this policy.

1. PURPOSE

The purpose of this policy is to outline fiduciary responsibilities to ensure our patient's personal health information (PHI) and Saskatoon Health Region (SHR) business information is protected during collection, use, disclosure, storage, and destruction. Information will be protected in accordance with *The Health Information Protection Act* (HIPA), *The Local Authority Freedom of Information and Protection Privacy Act* (LA FOIP) and other relevant legislation.

2. PRINCIPLES

Accountability - SHR is responsible for PHI and PI under its control. SHR has designated a Privacy Officer who is accountable for compliance with the following principles.

2.1 Identifying Purposes - The purposes for which PHI and PI is collected shall be identified by SHR at or before the time the information is collected.

2.2 Fiduciary - Fiduciary duties arise from the legal or ethical relationship of confidence or trust between two or more parties. Healthcare providers have fiduciary, legislated and/or professional responsibilities to maintain and protect patient confidentiality.

2.3 Consent – Implied or expressed consent is required for the collection, use, or disclosure of PHI, subject to the exceptions contained in HIPA. Consent should be given voluntarily and be informed when possible.

2.4 Limiting Collection - The collection of PHI and PI shall be limited to that which is necessary for the purpose for which it is being collected.

2.5 Limiting Use, Disclosure, and Retention – PHI and PI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent

[2] LAFOIP, Regulation 11
[3] HIPA s.27(4)(g)

of the individual or as required by law. PHI and PI shall be retained only as long as necessary to meet the original purposes, or as permitted by SHR Policy, legislation or common law.

2.6 **Accuracy –** PHI and PI shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

2.7 **Safeguards –** PHI and PI shall be protected by reasonable safeguards against risks such as loss, theft, and unauthorized access. Safeguards refer to a combination or policies, procedures, practices and technologies. Safeguards appropriate to the sensitivity of the information are to be used, regardless of form in which the information is stored (e.g. paper, electronic).

2.8 **Openness -** SHR shall make specific information about its policies and practices relating to the management of PHI and PI readily available.

2.9 **Individual Access -** Upon request, an individual shall be informed of the existence, use, and disclosure of his/her PHI and/or PI and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate (see SHR Policy: Amendment to Personal Health Information).

2.10 **Challenging Compliance -** An individual shall be able to address concerns related to compliance with any of the above principles to the SHR Privacy and Access Department.

2.11 If a patient records video, audio or takes photographs, this is not considered PHI or PI (e.g. it is not PHI as defined by HIPA and not PI as defined by LA FOIP), therefore SHR does not have control or ownership of it. Thus, healthcare providers should not have an expectation of privacy in the delivery of care.

3. POLICY

3.1 All staff are responsible for protecting PHI and SHR business information obtained or accessed during the course of his/her work within the Region.

3.1.1 All obligations to protect PHI and SHR business information continue indefinitely, even after discontinuation of employment/association/ privileges with SHR.

3.2 The access, collection, use, or disclosure of PHI is acceptable only on a need to know basis for the provision or support of health services for a client staff are providing care to (e.g. staff are not permitted to access their own PHI or anyone regardless of relationship unless they are providing care – see procedure 2.5.1).

3.2.1 In all cases of access, collection, use or disclosure of PHI should be limited to the least amount of information required to serve the purpose.

3.2.2 Secondary use (use of information for other than the original purpose) without patient consent must be:

- in accordance with HIPA or other applicable legislation; and
- approved by management and/or the Privacy and Access Department, or;
- authorized by other regional SHR policies *The Health Information, Protection Act, The Health Information Protection Regulations, The Local Authority Freedom of Information and Protection of Privacy Act and Regulations, Saskatchewan.*

3.2.3 Employees, physicians, volunteers and students **shall not** use their position at SHR in order to collect or access personal health information that is not required for employment related purposes.

3.3 All staff are required to review this policy and sign *the Saskatoon Health Region Confidentiality Agreement* (Appendix A) prior to or at the commencement of their employment/privileges/association with SHR.

3.3.1 Staff may also be required to sign Confidentiality Acknowledgement(s) specific to Electronic Health Record (EHR) applications.

3.3.2 SHR audits EHR applications for compliance with this policy.

3.4 Records containing PHI and/or business information shall only be destroyed in a confidential manner (e.g. use of approved confidential shred bins). See SHR policies: *Retention of Personal Health Information* and *Information Classification, Labelling and Handling*.

3.5 PHI and/or business information, which has not been de-identified, must not be discussed where other individuals are present and may overhear the information (e.g. cafeterias/elevators), unless unavoidable during the course of care or job duties (e.g. shared patient rooms/open office environments).

4. ROLES AND RESPONSIBILITIES

4.1 All Staff

4.1.1 Be familiar with and abide by this policy.

4.1.2 Sign the *Saskatoon Health Region Confidentiality Agreement* upon commencement of employment/privileges/association.

4.1.3 Report all breaches of this policy to management and/or Privacy and Access Department (see SHR Policy: *Speaking UP: Protection of Persons Reporting Wrongdoing*).

4.1.4 Provide adequate safeguards to all PHI and/SHR business information.

4.1.5 Maintain the confidentiality of all PHI and SHR business information, whether the information is accessed through normal duties or inadvertently during the course of duties.

4.2 Managers/Supervisors

4.2.1 Ensure staff are provided adequate training relating to confidentiality.

4.2.2 Determine appropriate access for staff related to electronic applications.

4.2.3 Cooperate with and assist the Privacy and Access Department during privacy incident reviews.

4.2.4 Determine appropriate action in cases of privacy violations (see Appendix B).

4.3 Directors

4.3.1 Review and respond to requests for confidential information.

4.3.2 Advise requestor of Access to Information process[4] where information will not be released informally.

4.4 Privacy and Access Department

4.4.1 Provide advice to staff on all matters relating to confidentiality.

4.4.2 Respond, review, and make recommendations relating to incidents of non-compliance of this policy.

[4] https://www.saskatoonhealthregion.ca/patients/Pages/Privacy-and-Health-Records.aspx

4.4.3 Review, manage and respond to Access to Information requests.
4.4.4 Audit EHR applications for compliance with this policy.

4.5 Ethics Services

4.5.1 Provide advice to staff on ethical matters related to disclosure, breach of confidentiality and issues related to any ethical duty to warn (e.g. warning another individual about a duty to report).

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring and implementation is the responsibility of the Privacy Officer(s). Amendment is the responsibility of the Director, Enterprise Risk Management.

6. NON-COMPLIANCE/BREACH

Non-compliance with this policy may result in disciplinary action up to and including termination of employment and/or privileges.

Appendix B outlines recommended actions for privacy violations.

A privacy breach may be reported to the Information Privacy Commissioner (IPC). The IPC and the Ministry of Justice may charge an individual with an offence under HIPA. Any person who knowingly contravenes HIPA may be subject to a fine of not more than $50,000 and/or not more than one year of imprisonment.[5]

7. REFERENCES

The Health Information Protection Act, Saskatchewan
The Local Authority Freedom of Information and Protection of Privacy Act, Saskatchewan

[5] HIPA Section 64(1)

PROCEDURE Number: 7311-75-003 Title: PRIVACY AND CONFIDENTIALITY	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Enterprise Risk Management Cross Index: Date Approved: June 3, 2015 Date Revised: March 17, 2017 Date Effective: March 17, 2017 Date Reaffirmed: Cross Index: Scope: SHR and Affiliates

1. PURPOSE

The purpose of this procedure is to establish the processes for ensuring compliance with HIPA, LA FOIP and other applicable legislation.

2. PROCEDURE

2.1 Confidentiality Agreements

2.1.1 All employees must complete online privacy training and review and sign the SHR Confidentiality Agreement prior to or at commencement of employment.

- Potential employees must provide confirmation of completed online privacy training to managers prior to a job offer.
- For employees, Confidentiality Agreements will be signed during Welcome Onboarding Week (WOW) and prior to commencement of job duties in the region.
- People Practice and Quality will store and manage SHR employee Confidentiality Agreements.
- For Affiliate Employees, Confidentially Agreements are signed at commencement of employment and retained by the Administrator (or designate).
- People Practice and Quality will store and manage employee signed Confidentiality Agreements.

2.1.2 Physicians will be provided a copy of the SHR Confidentiality Agreement by Practitioner Staff Affairs upon a physicians' request to have practicing privileges within an SHR facility.

- Physicians must provide a signed copy of the Confidentiality Agreement to Practitioner Staff Affairs as part of the application process for appointment and privileges.
- Practitioner Staff Affairs will store and manage physician signed Confidentiality Agreements.

2.1.3 Volunteer Services in Saskatoon, or Department Managers in rural facilities, will provide a copy of the SHR Confidentiality Agreement to all prospective volunteers.

- Volunteers must provide a signed copy of the Confidentiality Agreement to Volunteers Services/Rural Manager prior to commencement of volunteer duties.
- Volunteer Services/Rural Manager will store and manage volunteer signed Confidentiality Agreements.

2.1.4 For Vendor Confidentiality Agreements, see SHR Policy *Vendor Visitation and Conduct*.

2.2 Storage and Disposal of Personal Health Information, Personal Information and Business Information

2.2.1 All records containing PHI and/or business information are to be handled in accordance with SHR Policy: *Information Classification, Labelling, Handling and Storage*.

2.2.2 Documents containing PHI and/or business information shall be cleared from computer printers, photocopiers, scanners, and fax machines as soon as reasonably possible.

2.2.3 Desks and workstations shall be secured and/or cleared of PHI and PI when such information is not in use.

2.2.4 Identifiable patient information and/or business information should be discreetly hidden from view and kept private, including electronic screens/display boards, printed material such as patient lists and Operating Room slates and whiteboards.

2.3 Faxing/Emailing

2.3.1 Faxing of information must take place in accordance with SHR Facsimile (FAX) Policy.

2.3.2 Email must be used in accordance with SHR Policies: *Emailing Personal Health Information and Email Acceptable Use*.

2.4 Disclosure of PHI

General

2.4.1 Staff are not permitted to access records/electronic health records to access PHI of themselves, their family or friends (even with consent). Staff must abide by SHR policy: *Access to Personal Health Information*.

2.4.1.1 If the patient requests that their PHI not be shared/disclosed[6], identify those individuals on the *Consent Directive for Non-Disclosure of Personal Health Information Form* (see Appendix C).

2.4.1.2 Information relating to a patient's current care may be (use discretion) disclosed without consent to the patient's next of kin or a person they have a close personal relationship with as long as the patient has not indicated otherwise.

2.4.1.3 Information may not be disclosed by phone unless patient consent is received or at the discretion of the health provider. Use the least amount of information possible to satisfy the situation.

[6] HIPA 27(2)(c) (i) (ii)

Media

2.4.2 No PHI shall be disclosed to media without written consent of the patient (with capacity) or proxy or substitute decision maker (when the patient lacks capacity).

2.4.2.1 Forward all media calls to the Communications Department.

Authorities

2.4.3 SHR staff may disclose PHI to authorities without consent where SHR staff believe, on reasonable grounds, that the disclosure will avoid or minimize a danger to the health or safety of any person.[7]

2.4.3.1 This disclosure is usually seen as a 'duty to warn' based on professional code of ethics. The following conditions must be met for disclosure, to be ethically and legally justifiable.

- Must be a reasonable expectation of probable harm that is imminent;
- Harm must constitute damage or detriment and not mere inconvenience; and
- Must be a causal connection between disclosure and the anticipated harm.

2.4.4 Prior to such disclosure, Privacy must be consulted unless disclosure is authorized or obligated by the respective SHR staff professional association.

2.5 Provision of job duties relating to personally known individuals

2.5.1 In circumstances when a staff member's job duties (e.g. filing, providing treatment) requires him/her to access personal health information or provide services to a family member, staff must transfer duties to another who can assume the responsibilities, due to conflict of interest.

2.5.2 In circumstances where the individual is personally known (but not a family member), staff may assume the responsibilities when possible and when requested by the patient.

2.5.3 In all circumstances, staff must not share any information regarding the care of the individual (including the fact the individual was a patient) with family members, co-workers, or acquaintances without expressed consent to do so. Information can only be shared with those that have a need to know in order to provide/support the provision of care.

2.6 Overhead Paging

2.6.1 Paging of patients or families by their name is not permitted. Units requiring a method of communication must devise an alternate method of contact (e.g. cell phones, pagers).

- In cases of medical emergencies and where alternate methods of contact are not successful, patients/families may be paged to contact an extension number rather than return to a unit or room (e.g. Jane Smith, please call extension 1111).

2.7 Requests for SHR Business Information

2.7.1 All requests for business information must be forwarded to the relevant Director or designate. Director or designate will consult with relevant stakeholders prior to release.

2.7.2 In cases where information will not be released, the requestor must be advised of their right to request the information through the Access to

[7] HIPA s.27(4)(a)

Information process or directed to Privacy and Access for additional information.

3. PROCEDURE MANAGEMENT

The management of this procedure including procedures education, monitoring, implementation is the responsibility of Privacy Officer(s). Amendment is the responsibility of Director, Enterprise Risk Management.

4. NON-COMPLIANCE/BREACH

Non-compliance with this procedure may result in disciplinary action up to and including termination of employment and/or privileges.

Appendix B outlines recommended actions for privacy violations.

A privacy breach may be reported to the Information Privacy Commissioner (IPC). The IPC and the Ministry of Justice may charge an individual with an offence under HIPA. Any person who knowingly contravenes HIPA may be subject to a fine of not more than $50,000 and/or not more than one year of imprisonment.[8]

5. REFERENCES

SHR Policy *Emailing Personal Health Information*
SHR Policy *Information Classification, Labelling and Handling*
SHR Policy *Email Acceptable Use*
SHR Policy *Vendor Visitation and Conduct*
The Health Information Protection Act, Saskatchewan
The Local Authority Freedom of Information and Protection of Privacy Act, Saskatchewan

[8] HIPA Section 64(1)

Scan and email a signed copy of this form to:

ITS Security:
itssecurity@saskatoonhealthregion.ca, and

Human Resources:
PSPCentralFiling@saskatoonhealthregion.ca

- ☐ Employee
- ☐ Volunteer
- ☐ Student
- ☐ Contractor
- ☐ Affiliate

WHEREAS:

A. As an individual providing services (whether as employee, volunteer, student, or otherwise) to the Saskatoon Health Region, I understand that I may have access to confidential information that includes, but is not limited to, information relating to:

   - Patients (such as health records, conversations, admittance information, patient financial information, etc.);
   - Other Saskatoon Health Region employees or volunteers (such as employment records, disciplinary actions, etc.);
   - Saskatoon Health Region business information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.); and
   - Information about Saskatoon Health Region's business partners and service providers.

B. Confidential information is protected by legislation such as *The Health Information Protection Act, The Local Authority Freedom of Information and Protection of Privacy Act and The Mental Health Act*, as well as by strict Saskatoon Health Region policies.

As a condition of and in consideration of my access to confidential information, I agree that I am accountable and responsible to maintain confidential information in confidence and agree to uphold the following obligations:

BASIC CONFIDENTIALITY OBLIGATIONS

1. I will use confidential information only as needed to perform my legitimate duties with the Saskatoon Health Region. This means, among other things, that:
   (a) I will only access confidential information for which I have a need to know in connection with the services I am providing to the Saskatoon Health Region;
   (b) I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any confidential information except as properly authorized within the scope of my duties with the Saskatoon Health Region; and
   (c) I will not misuse confidential information or carelessly care for confidential information.
2. I will safeguard and will not disclose or share my passwords, User ID's, clearance badges, access cards, keys or other codes or devices assigned to me (or created by me) that allow me to access confidential information. I accept responsibility for all activities undertaken using such codes and devices.
3. I will retain Confidential Information in a manner appropriate for the form of confidential information (e.g. paper, electronic, thumb drive/memory stick, CD, DVD, remote access, etc.) including, but not limited to the following:
   (a) Automatic shutdown, locking, or timeout procedures for computer terminals not in use
   (b) A personal security pass code for each authorized individual
   (c) Locked and controlled access to areas housing Confidential Information
   (d) Secure directories on computers storing electronic files containing Confidential Information
   (e) Confidential Information not to be available, accessible to unauthorized persons
   (f) Confidential Information stored on thumb drive/memory stick, CD or DVD's must be password protected or encrypted where possible.
4. I agree that my privileges hereunder are subject to periodic review and, if deemed, appropriate by the Saskatoon Health Region, revision.
5. I agree that I have no right or ownership interest in any confidential information.
6. I agree to return all Confidential Information back to Saskatoon Health Region at the end of the contract. I will appropriately delete any electronic files that may have been created as a result of my accessing or using Saskatoon Health Region Confidential Information on my electronic devices.
7. I understand that my failure to comply with this Agreement may result in disciplinary action (including, without limitation, my loss of employment or affiliation with Saskatoon Health Region) and/or legal action being taken against me.
8. I agree to review and comply with all applicable legislation and Saskatoon Health Region policies respecting privacy and security, as amended from time to time.

USER ACCOUNT & DATA ACCESS RULES & REGULATIONS

9. If given an SHR User Account:
   (a) I agree to utilize the information provided on the Saskatoon Health Region computer system for the sole purpose of performing my legitimate duties with the Saskatoon Health Region.
   (b) In accordance with the obligations contained in section 2:
      (i) I agree I am responsible and accountable for all activities conducted on the computer network under my Saskatoon Health Region User Account.

(ii) I will not divulge or share my Saskatoon Health Region User Account or password to others as it is strictly prohibited.

(iii) I agree that my password will comply with the prescribed Saskatoon Health Region Password Policy, will not be documented, and must be changed as the system demands or if it is compromised.

(iv) I will ensure that my access to shared data (if I am granted permissions to any) is to be kept confidential and I will not share or distribute this data with those who are not authorized.

(c) I am responsible for immediately reporting all unauthorized use, sabotage, modification, or theft of Saskatoon Health Region Information Technology (IT) assets or information to the IT Services department.

(d) I agree to abide by the Saskatoon Health Region Internet Acceptable User Policy and the Saskatoon Health Region Email Acceptable Use Policy.

(e) I understand that I am prohibited from accessing or distributing objectionable material, including but not limited to:

- Obscene and pornographic material;
- hate propaganda or discriminatory material;
- defamatory and libelous material; and
- sexually harassing material.

(f) I acknowledge and accept that:

(i) Saskatoon Health Region system administrators reserve the right to actively monitor Saskatoon Health Region systems/applications (including Saskatoon Health Region email accounts and personal/shared network drives) in order to protect and maintain the integrity of Saskatoon Health Region system resources and to ensure Saskatoon Health Region User compliance with Saskatoon Health Region policy and procedures.

(ii) Any infringement on these rules and regulations or Saskatoon Health Region policy will be addressed by the User's manager/supervisor and may result in the suspension of the associated Saskatoon Health Region User Account and system access privileges.

REMOTE ACCESS

10. If I have been authorized by the Saskatoon Health Region to access the Saskatoon Health Region's computer systems from a remote location (such as my home), I further agree to the following:

(a) I will only remotely access the Saskatoon Health Region's computer systems in accordance with Saskatoon Health Region policies (including any specific remote access policies), as such policies may be amended from time to time.

(b) Without limiting the general effect of the foregoing paragraph, I understand that the hardware and other network access requirements related to my particular situation (taking into account, among other things, the types of applications I am permitted to access) will be evaluated and set by SHR IT staff. I agree to comply with such requirements, as they may be amended from time to time.

(c) I will take all reasonable steps to prevent unauthorized access to:

(i) the computer or other device by which I remotely access the Saskatoon Health Region's computer systems; and

(ii) any and all paper documents or electronic documents (such as disks, memory devices) containing any confidential information that I may generate, create and/or print-off.

(d) I will only remotely access the Saskatoon Health Region's computer systems as necessary for purposes authorized within the scope of my duties with Saskatoon Health Region.

(e) I will thoroughly delete any confidential information from the computer or other device by which I remotely access the Saskatoon Health Region's computer systems as soon as the information is no longer needed for the purposes for which it was accessed.

(f) If I generate, create or print-off any paper documents or electronic documents containing any confidential information, I agree to thoroughly destroy or erase such documents when they are no longer needed.

(g) Without limiting the general nature of preceding sentence, I agree that I will not dispose of any paper documents containing confidential information into the trash without first securely shredding the documents.

(h) I specifically acknowledge that remote access is a privilege that may be revoked by the Saskatoon Health Region in its sole discretion at any time and for any reason.

11. For greater certainty, the obligations contained in section 9 are supplemental to (and do not replace) the obligations contained in sections 1 through 6 (inclusive).

GENERAL

12. The obligations contained in this Agreement are intended to be complementary to any similar obligations I may have agreed to in other Saskatoon Health Region agreements or policies or as may be imposed by law or applicable professional ethical obligations. To the extent of any inconsistency between such obligations, the obligations imposing the highest confidentiality standard shall govern.

13. I agree that my obligations under this Agreement will continue after any termination of my employment or affiliation with the Saskatoon Health Region.

AGREED TO BY:

Employee/Volunteer/Student/Contractor/Affiliate Signature	Date
Printed Name	Position

Appendix B
Privacy Violations - Recommended Actions

Violation Level	Examples of Violations	Recommended Actions[9]
Level 1 - Unintentional Carelessness in handling personal health information or maintaining adequate security levels	• Disclosing personal health information without verifying identity of requestor • Leaving personal health information unattended or in public area • Failing to log off or lock computer that holds personal health information • Inadvertently sending personal health information via fax to incorrect fax number	• Discussion of applicable SHR policies and procedures • Privacy training and/or letter of expectation • Sign or re-sign confidentiality agreement
Level 2 – Intentional, non-malicious/multiple level 1 Breaching policies or legislation surrounding the access, collection, use and disclosure of personal health information	• Accessing personal health information without professional need to know • Discussion of personal health information with someone who does not have a legitimate need to know without consent • Allowing another individual to use your SHR computer account • Repeated Level 1 violations	• Discussion of applicable SHR policies and procedures • Privacy training • Sign or re-sign confidentiality agreement • Discipline, up to and including suspension • Notification of the de identified physician or employee's disciplinary action to the affected individual(s) and reported in the Privacy and Access Department Annual Report • May notify The Information and Privacy Commissioner (IPC) • May report to professional body (if applicable)

[9] All mitigating and aggravating circumstances related to employee will be considered prior to decision.

<u>Level 3 – Intentional and malicious/multiple levels 1 & 2</u> Knowingly breaching policies or legislation surrounding the access, collection, use and disclosure of personal health information for personal benefit* or to harm** another person(s)	• Accessing personal health information without professional need to know for personal gain or to cause harm to another • Using another employees computer account for personal gain or to cause harm to another • Intentionally altering data or removing personal health information from SHR • Repeated Level 1 or 2 violations	• Suspension or termination of employment (employee ineligible for future rehire), as determined by management • Revocation of Medical Staff privileges • Revocation of access to region applications • Notification of the de identified physician or employee's disciplinary action to the affected individual(s) and reported in the Privacy and Access Department Annual Report • Automatic reporting to professional body (if applicable) • Automatic reporting to IPC • May report to Ministry of Justice for consideration of charges and/or fines under *HIPA*

*Personal Benefit: accessing, collecting, using, or disclosing information with a motive that primarily benefits the individual. This includes but is not limited to favours, economic gain, and use for social and personal interests.

**Harm: negative impact to another individual(s) physically, emotionally, socially, or financially.

Appendix C

Consent Directive for Non-Disclosure of Personal Health Information

I, _____ on _____ direct the
(Name of client/patient/resident) (Date)

Saskatoon Health Region to not disclose my personal health information to: _____

_____.

The Saskatoon Health Region will place this form on the left hand side of my health record. I understand that:

- I have a responsibility to verbally inform health professionals of my wishes each time I am transferred to a new facility within the Saskatoon Health Region.
- There may be circumstances where the Saskatoon Health Region will be authorized or required by law to disclose my personal health information.
- I understand this consent will remain in place until I provide a signed and witnessed revocation.

_____ _____
(Name of client/patient/resident) (Signature of client/patient/resident)

_____ _____
(Health Card Number) (Date of Birth)

_____ _____
(Printed name of witness) (Witness signature)

Revocation:

_____ _____
(Name of client/patient/resident) (Signature of client/patient/resident)

_____ _____
(Printed name of witness) (Signature of witness)

_____
(Date)