



Privacy and Security Resource Materials
For Saskatchewan EMR Physicians

**Sample Privacy and Security
Policy and Procedures Manual
For Sole Practitioners**

Dr. Avery Rahal

**Privacy and Security
Policy and Procedures Manual**

January 2014

Text in bold is required under *The Health Information Protection Act*

Disclaimer

The information in this sample policy and procedures manual does not constitute legal advice. It is general information intended to assist physicians in understanding their obligations and general duties under *The Health Information Protection Act* of Saskatchewan and the expectations of the College of Physicians and Surgeons of Saskatchewan. The information is provided as guidance for medical practices in Saskatchewan developing privacy and security policies and procedures.

Dr. Avery Rahal – Statement of Accountability

Note: This is the trustee’s commitment to adhere to these policies and procedures and is the equivalent of a confidentiality agreement.

Dr. Avery Rahal, a sole practitioner and trustee under *The Health Information Protection Act*, operates a family practice in New Harbour, Saskatchewan. The practice includes a nurse practitioner and two office administrators.

Dr. Rahal, as a trustee, is accountable for the actions of his employees and third parties who use personal health information on his behalf. These written policies and procedures are to be adhered to by anyone who works at the medical practice, or has access to the personal health information Dr. Rahal is accountable for. Third parties who collect, use, or disclose personal health information on behalf of Dr. Rahal must also adhere to these policies and procedures. Information Management Service Providers must meet or exceed the standards of these policies.

In 2011, Dr. Rahal implemented an electronic medical record system (EMR) in the practice. The sharing of personal health information within the clinic is carried-out with patients’ expressed or implied consent. Dr. Rahal in the past has established arrangements with other health professionals to work as part of the practice’s care team within the clinic, including a physiotherapist, and a dietitian. It is expected that the arrangements with these and other health professional will continue and personal health information will be shared with them on a need to know basis when they are supporting or providing direct care to a patient.

All access, use and disclosure of personal health information about patients is restricted to those who are authorized by Dr. Rahal and have a need-to-know the information to carry out their duties.

I, Avery Rahal, accept the responsibility to protect the personal health information in my custody or control and to only collect, use or disclose the information needed for the benefit of my patients.

Signature

Avery Rahal

Date

Revised – September 2019

1



Tel: 306.657.4557
Toll Free: 1.800.667.3781
Fax: 306.974.0326
Email: emr@sma.sk.ca

www.sma.sk.ca/emr



Table of Contents

Dr. Avery Rahal – Statement of Accountability	1
Privacy and Security Statements.....	3
<u>Accountabilities</u>	
Responsibilities of the Privacy Officer and the Office Manager.....	5
Obligations of Health Professionals, Employees, Medical Students and Residents.....	6
Privacy and Security Awareness, Education and Training.....	8
Accuracy and Integrity.....	9
Identified Purpose and Openness	11
Challenging Compliance	12
Ceasing to be a Physician at This Location	13
<u>Patient Access, Amendment and Designates</u>	
Patient Access to Own Record.....	14
Amending Patient Record upon Request.....	18
Authorized Representatives Who Make Decisions On Behalf of Patients	20
<u>Collection, Use, Disclosure and Consent</u>	
Collection	22
Use	24
Disclosure	28
Managing Patient Consent and Masking in the EMR.....	33
<u>Safeguards</u>	
Agreements.....	36
Management of Breaches	38
Business Continuity and Disaster Recovery Plan.....	43
Retention, Storage and Destruction of Paper Records	44
Scanning and Destruction of Paper Records.....	46
Backups and Storage.....	47
User Account Management.....	49
Auditing.....	51
Destruction of Office Equipment and Medical Devices	53
General Security Software.....	54
Security of the Office.....	55
Glossary.....	53
Acronyms.....	59



Privacy and Security Statements

Note: This is a compilation of the policy statements in the manual. This is the privacy and security framework for the clinic. It should be posted in a spot visible to all employees and others who work at the clinic.

Dr. Rahal is the Privacy Officer for the clinic. The Office Manager has been appointed the Assistant Privacy Officer by Dr. Rahal. The Office Manager will manage the day-to-day compliance of these policies and procedures and is the point of contact for patients and other employees and health professionals for privacy-related questions and issues. All employees and health professionals are made aware of the roles of the Privacy Officer and the Office Manager through conversations, posters and other materials.

Dr. Rahal maintains policies and procedures to promote knowledge and awareness of the rights of patients including the right to access their own personal health information and to request amendment of their personal health information in the case of errors and omissions. Policies and procedures have also been established to maintain administrative, technical, and physical safeguards to protect personal health information. These policies and procedures are reviewed annually and amended as required.

All employees and health professionals at the medical practice are obligated to protect personal health information in accordance with HIPA and this Policy Manual which includes signing a confidentiality agreement annually.

Dr. Rahal creates a culture of privacy by awareness activities, educational opportunities, and privacy and security training to ensure compliance with HIPA by employees and health professionals.

Dr. Rahal takes reasonable steps to ensure the personal health information collected, used and disclosed is accurate and complete and its integrity is preserved.

Dr. Rahal provides patients with information on the purpose for the collection, use and disclosure of their personal health information and is open with patients about the clinic's privacy and information practices.

Dr. Rahal provides a confidential process for patients to lodge a complaint regarding the clinic's adherence to its policies and procedures, or to notify the clinic of a potential or suspected breach of personal health information.

Dr. Rahal will ensure the proper transfer of patient records to a designated archive or a trustee at another medical practice.

Dr. Rahal provides patients with access to their own personal health information upon request. Requests may be made verbally or in writing.

Dr. Rahal responds to all requests from patients to amend their personal health information. Factual personal health information that is incorrect will be corrected when reasonably possible. Professional opinions will be amended at the clinic's discretion. If an amendment is not made a notation must be added to the record.

Dr. Rahal recognizes the right of a patient to designate someone to make decisions on their behalf regarding the collection, use and disclosure of their personal health information. Others

Revised – September 2019

3



Tel: 306.657.4557
Toll Free: 1.800.667.3781
Fax: 306.974.0326
Email: emr@sma.sk.ca

www.sma.sk.ca/emr



may make decisions about a patient's personal health information when authorized to do so in HIPA or other law.

Dr. Rahal collects only the personal health information that is reasonably necessary to provide care and treatment to benefit patients.

Dr. Rahal uses the minimum amount of personal health information collected for the care and treatment of patients based on the implied consent of the patient.

Dr. Rahal discloses personal health information as part of providing care to patients. If personal health information is disclosed for other purposes it will be with the consent of the patient or the disclosure is authorized without consent by law.

Dr. Rahal will take all reasonable steps to comply with a patient's request to limit the collection, use and disclosure of their personal health information.

Dr. Rahal uses written agreements to establish responsibilities and mitigate risk when third parties have or may have access to personal health information on behalf of the practice.

Dr. Rahal considers a privacy breach as a collection, use or disclosure of personal health information in contravention of *The Health Information Protection Act* and these policies. Dr. Rahal responds promptly to potential, suspected and confirmed privacy and security breaches and will engage the necessary expertise in managing breaches.

Dr. Rahal maintains up-to-date business continuity and disaster recovery plans that provide guidance on how to manage an interruption in business due to unplanned events.

Dr. Rahal retains paper records, which have not been scanned into the EMR, for 10 years after the last entry into the patient record (either the paper record or the EMR). If the patient is under the age of 18, both the paper and electronic record will be retained for 10 years after the last entry into either patient record or for 10 years after the patient reaches age 18, whichever is the longer. Dr. Rahal stores and destroys all records securely.

The accuracy of scanned records is confirmed before the paper document(s) are destroyed.

Dr. Rahal maintains a program to backup all EMR and other electronic administrative records and to store the backups securely.

Each person with access to the EMR and the office computers will have their own user name and password.

Dr. Rahal monitors all activity in the EMR by employees and health professionals. Audit reports regarding patient records are made available to patients upon request.

Dr. Rahal ensures that all personal health information is removed from the office equipment and medical devices before the devices are recycled or destroyed.

Dr. Rahal maintains security software licenses that provide regular updates to the firewall, anti-virus, malware and the virtual private network software.

Dr. Rahal ensures that the medical practice's physical office space is secure.

Revised – September 2019

4



Tel: 306.657.4557
Toll Free: 1.800.667.3781
Fax: 306.974.0326
Email: emr@sma.sk.ca

www.sma.sk.ca/emr



Responsibilities of the Privacy Officer and the Office Manager	
Legislative Reference: HIPA s.58(3), 23(2)	CPSS Reference: Bylaw 23.2(c)(i)
Policy Author:	Effective and Revision Dates:

Policy

Dr. Rahal is the Privacy Officer for the clinic. The Office Manager has been appointed the Assistant Privacy Officer by Dr. Rahal. The Office Manager will manage the day-to-day compliance of these policies and procedures and is the point of contact for patients, employees and health professionals for privacy-related questions and issues. All employees and health professionals are made aware of the roles of the Privacy Officer and the Office Manager through conversations, posters and other materials.

Dr. Rahal maintains policies and procedures to promote knowledge and awareness of the rights of patients including the right to access their own personal health information and to request amendment of their personal health information in the case of errors and omissions. Policies and procedures have also been established to maintain administrative, technical, and physical safeguards to protect personal health information. These policies and procedures are reviewed annually and amended as required.

Procedures

Note: This policy does not require procedures. There does need to be a clear understanding of who in the clinic has the responsibilities listed in “Role of the Privacy Officer and Medical Office Administrator” in **The Privacy and Security Reference Manual for Saskatchewan Physicians**,. These may be listed here or with the relevant policies and procedures as has been done in this sample manual.



Obligations of Health Professionals, Employees, Medical Students and Residents	
Legislative Reference: HIPA s9,16,35, 61	CPSS Reference: Bylaw 23.1(c)(ii)(iii)
Policy Author:	Effective and Revision Dates:
Templates: Confidentiality Agreement	

Policy Statement

All health professionals, employees, medical students and residents at the medical practice are obligated to protect personal health information in accordance with HIPA and this Policy Manual which includes signing a confidentiality agreement annually.

Procedures

1. All health professionals, employees, medical students and residents at the medical practice
 - 1.1. Receive an electronic copy of this Policy Manual to read and use.
 - 1.2. Ensure they understand all policies and procedures and ask for clarification when they do not understand.
 - 1.3. Participate in all education and training offered by Dr. Rahal.
 - 1.4. Are responsible and accountable for ensuring the protection and security of personal health information they collect, use, and disclose and assist others to do the same.
 - 1.5. Are responsible and accountable for assisting patients in any request for their personal health information, requests for amendments to their personal health information, and inquires on the privacy practices of Dr. Rahal.
 - 1.6. Sign an agreement that will be held in each employee's personnel file or with correspondence related to the person's engagement.
 - 1.7. As a condition of engagement with Dr. Rahal all health professionals shall sign a confidentiality agreement.
 - 1.7.1. The signed agreement will be held in each employee's personnel file or with correspondence related to the person's engagement.
2. Those who do not comply with these procedures will be considered in breach of HIPA and the policies and procedures of medical practice and will be subject to



disciplinary action by Dr. Rahal, the health professional's regulatory body, or the courts as authorized by HIPA.



Privacy and Security Awareness, Education and Training	
Legislative Reference: HIPA s. 16	CPSS Reference:
Policy Author:	Effective and Revision Date:
Template: Confidentiality Agreement	

Policy Statement

Dr. Rahal creates a culture of privacy by awareness activities, educational opportunities, and privacy and security training **to ensure compliance with HIPA by health professionals, employees, medical students and residents.**

Procedures

1. The Privacy and Security Statements will be posted in a place visible to all employees and health professionals working at the medical practice.
2. The Office Manager is responsible for developing and maintaining an educational program about these policies and procedures.
3. Training is provided to health professionals, employees, medical students, residents and third parties who require training on privacy and security procedures such as faxing, emailing, scanning, storage, backups, destruction and other activities as identified.
4. The Office Manager provides orientation to new health professionals, employees, medical students and residents on their first day. This orientation includes a thorough discussion of the privacy and security policies and procedures.
 - 4.1. New health professionals, employees, medical students and residents are given a copy of the Policy Manual.
 - 4.2. New health professionals, employees, medical students and residents sign the confidentiality agreement before they are provided with access to personal health information.
 - 4.3. New health professionals, employees, medical students and residents and IT support personnel sign the acceptable use agreement before they are given a username and password for the EMR.



Accuracy and Integrity	
Legislative Reference: HIPA 25(3)	CPSS Reference: Bylaw 23.1(a)(b)(c) Bylaw 23.2(c)\(x)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal takes reasonable steps to ensure the personal health information collected, used and disclosed is accurate and complete and its integrity is preserved.

Procedures

1. Records are updated during the patient's appointment/contact or as soon as possible afterwards.
2. The patient's EMR record includes:
 - 2.1. The date that the Dr. Rahal or other health provider at the clinic sees the patient.
 - 2.2. A record of the assessment of the patient which includes the history obtained, particulars of the physical examination, the investigations ordered and where possible, the diagnosis; and a record of the disposition of the patient including the treatment provided or prescriptions written by Dr. Rahal, professional advice given and particulars of any referral that may have been made. Prescribing information includes the name of medication, strength, dosage and any other directions for use.
3. The patient record should include every report received respecting a patient from another trustee or other health professional.
4. The records are to be kept in a systematic manner.
5. Dr. Rahal takes steps to improve the accuracy of the information the clinic collects, which includes:
 - 5.1. That it be written in clear language with only common abbreviations used.
 - 5.2. The EMR records the date, time, and the name of the author.
 - 5.3. Additions and corrections are made in a manner that allows the original information to still be read.
 - 5.4. Ensuring scanned documents and photocopies are complete and readable.

Revised – September 2019



- 5.5. Staff is trained on how to keep accurate records.
6. Dr. Rahal takes steps to protect the integrity of the personal health information which include:
 - 6.1. Accurate recording of the personal health information.
 - 6.1.1. Updating records when notified of corrections
 - 6.1.2. Notifying other trustees when an amendment or notation is made in the record
 - 6.2. Accurate scanning and photocopying of personal health information.
 - 6.3. Perform daily backups.
 - 6.4. Ensure secure and environmentally safe storage.
 - 6.5. Audit of accesses to personal health information.
 - 6.6. Use up-to-date security software.
 - 6.7. Limit access to those who need to know the information.



Identified Purpose and Openness	
Legislative Reference: HIPA s 9, 10 & 16	CPSS Reference:
Policy Author:	Effective and Revision Dates:
Templates: Poster, Ministry of Health HIPA brochure	

Policy Statement

Dr. Rahal provides patients with information on the purpose for the collection, use and disclosure of their personal health information and is open with patients about the clinic’s privacy and information practices.

Procedures

1. The Office Manager ensures that **information is posted about the clinic’s privacy practices** at reception and in each examination room.
2. The poster will contain at a minimum
 - 2.1. The name and contact information for the Privacy Officer or the Office Manager.
 - 2.2. Information about Dr. Rahal’s information handling practices.
 - 2.3. The anticipated uses and disclosures of personal health information.
 - 2.4. How patients can manage their consent directives.
 - 2.5. How patients can ask for access to their personal health information and how to request an amendment to errors and omissions.
 - 2.6. How patients can make a complaint to the Office of the Information and Privacy Commissioner of Saskatchewan.
3. Copies of the Ministry of Health pamphlet about HIPA will be available in the waiting room. The pamphlet can be downloaded and printed from the Ministry of Health website (under Related Items):
<https://www.saskatchewan.ca/residents/health/accessing-health-care-services/your-personal-health-information-and-privacy>
4. Anyone authorized to collect personal health information at the clinic will answer all questions about the anticipated collection, uses and disclosures of the personal health information.



Challenging Compliance	
Legislative Reference: PIPEDA, Schedule 1	CPSS Reference:
Policy Author:	Effective and Revision Dates:

Policy Statement:

Dr. Rahal provides a confidential process for patients to lodge a complaint regarding the clinic's adherence to its policies and procedures, or to notify the clinic of a potential or suspected breach of personal health information.

Procedures:

1. A patient may submit a complaint to Dr. Rahal or an employee in writing or verbally.
2. Dr. Rahal will be notified of the complaint as soon as possible, or at least before the end of the clinic office hours.
 - 2.1. If the complaint is a suspected privacy or security breach, Dr. Rahal will activate the breach management plan.
 - 2.2. All discussions and actions related to the complaint will be documented.
3. The response to the patient may be provided verbally.
4. A periodic analysis is made of all complaints to determine if there are systemic issues that should be addressed through updates in policies, changes in education, awareness, training or other action.
5. A patient making a complaint or is dissatisfied with the response to a complaint will be provided with information on how to contact the Office of the Information and Privacy Commissioner of Saskatchewan.



Ceasing to be a Physician at This Location

Legislative Reference: HIPA s.22	CPSS Reference: Bylaw 23.1(g)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal will ensure the proper transfer of patient records to a designated archive or a trustee at another medical practice.

Procedures

1. Dr. Rahal will make reasonable efforts to notify all patients at least 60 days prior to when he/she ceases to be the trustee of their records.
2. Dr. Rahal will follow the guidelines of the College of Physicians and Surgeons of Saskatchewan Medical Records Bylaw 23.1.

A member who ceases to practice shall:

(i) transfer the records to a member with the same address and telephone number; or

(ii) transfer the records to:

1. another member practicing in the locality; or
2. a medical records department of a health care facility; or
3. a secure storage area with a person designated to allow physicians and patients reasonable access to the records.

3. Dr. Rahal will notify patients of the transfer through a newspaper advertisement, a poster at the clinic, or other reasonable method of notification.
4. Dr. Rahal will not transfer records outside of Canada.



Patient Access to Own Record	
Legislative Reference: HIPA s 12, 31-39,d 42	CPSS Reference: Bylaw 23.2 (c)(v)
Policy Author:	Effective and Revision Dates:
Templates: Access to Personal Health Information Form, Letter explaining refusal or partial refusal of access to personal health information, Letter of extension of the time to respond to a request.	

Policy Statement

Dr. Rahal provides patients with access to their own personal health information upon request. Requests may be made verbally or in writing.

Procedures

1. CPSS Bylaw 23.1 states
 - a) All members of the CPSS shall keep, as a minimum requirement, the following records in connection with their practice:
 - i) In respect of each patient a legibly written or typewritten record setting out the name, address, birthdate and Provincial Health Care Number of the patient;
 - ii) In respect of each patient contact, a legibly written or typewritten record setting out:
 - (1) the date that the member sees the patient;
 - (2) a record of the assessment of the patient which includes the history obtained, particulars of the physical examination, the investigations ordered and where possible, the diagnosis; and
 - (3) a record of the disposition of the patient including the treatment provided or prescriptions written by the member, professional advice given and particulars of any referral that may have been made. Prescribing information should include the name of medication, strength, dosage and any other directions for use.
 - b) The patient record should include every report received respecting a patient from another member or other health professional.

Informal Requests

2. Dr. Rahal will provide patients, at the time of their appointment, with copies of information discussed at the appointment, upon request.

Formal Requests

3. Patient requests for access to their own medical records may be made to the Office Manager.
 - 3.1. Patients wishing to make written requests are encouraged to use the clinic's application form.



- 3.2. The Office Manager will document a verbal request using the clinic form when the request cannot be meet immediately.
- 3.3. The Office Manager will help patients complete the request when necessary.
- 3.4. The Office Manager will confirm the identity of the requestor by viewing photo identification. This may not be necessary if the patient is known to the clinic.
4. A patient may view his or her own original chart in the presence of Dr. Rahal or the Office Manager.
5. Dr. Rahal charges the fees established by the Saskatchewan Medical Association as of April 2019

Transferring patient paper records

- 511A Photocopying/printing of records, base fee\$30.00*
- 512A plus per page\$0.30*

Transferring patient electronic records

- 513, Base fee.....\$40.00*
- 810A Physician time taken in reviewing the request/information and/or reviewing the chart if necessary, per 15 minutes or major portion thereof.....\$80.00

*Physicians may choose to waive all or part of the fee if it is fair to excuse payment.

Note: 810A should not be billed when patient has requested entire copy of the chart, unless there are circumstances, as set out in section 38(1) of the HIPA, in which a patient may be denied access to all or part of their medical record.

- 5.1. The Office Manager will provide the patient with an estimate of the cost for a copy of the record before preparing the copy
 - 5.1.1. The Office Manager will consider the patient's ability to pay when considering the fee to be charged. The patient may also request a fee waiver.
 - 5.1.2. The cost estimate will include, where applicable, the flat fee, the cost per page for copying, and the physician's time to review the chart.
 - 5.1.3. Dr. Rahal can approve a waiver of fees.
 - 5.1.4. The CPSS advices that it is customary not to charge a patient for a copy of the record if the patient's physician has moved or the patient is otherwise required to transfer care to another physician.



6. **At the patient's request all terms, codes, and abbreviations will be explained. If Dr. Rahal is unable to provide an explanation the patient will be referred to someone who can.**
7. **If Dr. Rahal does not have the information requested and is aware of another trustee who has the information, the patient's request will be sent to the other trustee.**
 - 7.1. **When Dr. Rahal transfers a request, the patient will be notified as soon as reasonably possible.**
8. **Patients are provided with access to, or a copy of, their own personal health information as quickly as possible within 30 calendar days after the completed request has been received by the Office Manager.**
9. **Dr. Rahal may take up to an additional 30 calendar days to provide access when**
 - 9.1. **It causes unreasonable interference with the practice's operations when the information is held in several different records or there is a large number of records to review.**
 - 9.2. **Consultations are necessary to comply with the request and these cannot be completed within the time period.**
10. **When the clinic exceeds the original 30 calendar days Dr. Rahal will send a letter to the patient, prior to the 30th day, explaining the delay.**
11. **Dr. Rahal may refuse access to the personal health information when:**
 - 11.1. **In the opinion of Dr. Rahal providing the information could reasonably be expected to endanger the mental or physical health or safety of the patient or another person (HIPA s 38(1)(c)(a)).**
 - 11.2. **Providing access reveals personal health information about a person who has not expressly consented to the disclosure to the patient (HIPA s 38(1)(b)).**
 - 11.3. **Providing access reveals the identity of another person who supplied the information in confidence and who expects confidentiality. This does not include information that would reveal the identity of another trustee (HIPA s 38(1)(c)).**
 - 11.4. **If the personal health information was collected and used for one of the following reasons the patient will be referred to the trustees who provided the information**
 - **peer review by health professionals (HIPA s38(1)(d))**
 - **review by a standards or quality of care committee studying or evaluating health services (HIPA s38(1)(d))**



- **the health professional regulatory body for discipline or quality of care purposes (HIPA s38(1)(d)).**
12. **When the record contains information that should not be given to the patient, that information should be severed from the record and the remaining information provided to the patient.**
- 12.1. Information is severed by printing the page with the information to be provided to the patient. The information to be severed is struck out with a black marker. In the margin write the section of HIPA that authorizes the severing of the information. The marked page is photocopied to ensure the severed information is not visible through the mark.
13. The Office Manager prepares all letters to patients explaining the refusal of access or the severed information and the relevant section of HIPA. All letters to patients explaining the amendment or notation and advises the patient that he/she can ask the Information and Privacy Commissioner to review the decision of the medical practice. The letter is signed by Dr. Rahal.



Amending Patient Record upon Request	
Legislative Reference: HIPA s. 13, 40	CPSS Reference:
Policy Author:	Effective and Revision Dates:
Templates: Request for Amendment Form, Letter confirming amendment, Letter notifying of Notation, Letter regarding amendment or notation to another trustee	

Policy Statement

Dr. Rahal responds to all requests from patients to amend their personal health information. Factual personal health information that is incorrect will be corrected when reasonably possible. Professional opinions will be amended at the clinic's discretion. **If an amendment is not made a notation must be added to the record.**

Procedures

1. **All requests must be in writing**
2. The Office Manager will assist the patient in completing the application form.
3. Amendments are made to factual information.
4. A patient request to correct a professional opinion or diagnostic test is made at the clinic's discretion. **If the amendment is not made a notation must be made in the record.**

Receiving the Request

5. All applications from a patient for amendment are dated and signed by the Office Manager the day the completed application is received by the practice.
 - 5.1. **Amendments or notations are made as soon as possible and in any event not more than 30 calendar days after receiving the completed request.**
 - 5.2. The Office Manager must be satisfied of the identity of the person making the application. For most patients this will have occurred at the time the patient requested the chart or they are known to the clinic.
6. **Amendments are made by recording the correct or omitted information in the record and if incorrect information must be struck out this will be in a manner that still allows the incorrect information to be read.**



- 6.1. When it is not possible to record the amended information in the record a note will be added to the record that directs anyone accessing the record to the location of the correct information.
7. Dr. Rahal will not make an amendment but will make a notation where:
 - 7.1. The record was not originally created by Dr. Rahal and Dr. Rahal does not have sufficient knowledge, expertise, or authority to correct the record.
 - 7.2. The information the patient is requesting be changed consists of professional opinion or diagnosis that Dr. Rahal made in good faith about the patient.
8. **Dr. Rahal provides written notification to the patient making the request that the amendment was made or not made, in which case a notation was added to the record.**
 - 8.1. **The letter explains when and how the amendment or notation was made.**
9. **Where practical, written notice is also sent to any other trustee or person, who was sent the information in the previous 12 months before the request for amendment or notation was received.**
 - 9.1. **Where the physician believes that the amendment will not have an impact on the patient's ongoing health care or other benefits, such notice is not required**
10. When Dr. Rahal does not make the amendment, the Office Manager will provide the patient with information on how an appeal can be made to the Office of the Information and Privacy Commissioner of Saskatchewan.



Authorized Representatives Who Make Decisions On Behalf of Patients	
Legislative Reference: HIPA s 15, 56	CPSS Reference: Bylaw 23.2 (c)(vi)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal recognizes **the right of a patient to designate someone to make decisions on their behalf regarding the collection, use and disclosure of their personal health information. Others may make decisions about a patient's personal health information when authorized to do so in HIPA or other law.**

Procedures

1. It is recommended that patients wanting to designate someone to make decisions about their personal health information on behalf of them do so in writing.
 - 1.1. All written appointments of a designate are scanned and stored in the patient's record.
2. A verbal request by the patient to designate someone to make decisions about their personal health information will be accepted by Dr. Rahal if the patient and the designate are known to Dr. Rahal.

People and Organizations Authorized to Exercise the Rights of Patients

3. Any person or organization who seeks personal health information about a patient without consent will be requested to show Dr. Rahal the authorization to receive the personal health information. HIPA gives this authority to the following individuals and organizations.
 - 3.1. **To the patient's personal representative when the patient is deceased and it is in relation to administration of the patient's estate.**
 - 3.2. **To a patient's personal guardian when the request is within the guardian's powers and duties.**
 - 3.3. **When the patient does not have the capacity to give consent:**
 - 3.3.1. **To a person designated when the patient is receiving services under *The Residential Services Act* or *The Rehabilitation Act*.**
 - 3.3.2. **To a person entitled to make decisions under *The Health Care Directives and Substitute Health Care Decisions Act*.**



By, or on Behalf of, a Minor

4. **A minor may make decisions regarding the collection, use or disclosure of personal health information where in the opinion of Dr. Rahal the minor understands the nature and consequences of the decision.**
 - 4.1. The decision made by the minor may be on his or her behalf, or on behalf of another person when appropriately authorized.

5. **When a patient is less than 18 the minor's legal guardian may make decisions about the personal health information when Dr. Rahal does not consider it would be an unreasonable invasion of the privacy of the patient.**
 - 5.1. If there is any uncertainty as to whether the minor would consent Dr. Rahal could conclude that it would be an invasion of privacy.



Collection	
Legislative Reference: HIPA s. 6, 19, 20, 23, 24, 25, 27, 28, 29	CPSS Reference: Bylaw 23.2(c)(vii)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal collects only the personal health information that is reasonably necessary to provide care and treatment to benefit his patients.

Procedures

1. Anyone collecting, using, and disclosing the personal health information on the basis of implied consent must be able to form the opinion that the patient will also consent to the use or disclosure if asked.
2. The patient is believed to have provided consent to the collection if there is a poster at the registration desk and the patient provides the requested information.
3. **The medical practice collects the personal health information directly from the patient unless the patient consents to collection from another source or the collection is authorized by law.**
4. **A patient may revoke his or her consent for the collection of personal health information and the medical practice will take reasonable steps to comply with the revocation promptly.**
 - 4.1. **A revocation is not retroactive.**
5. **Personal health information will be collected indirectly when**
 - 5.1. **The patient consents to collection from another source.**
 - 5.2. **The patient is unable to provide the information.**
 - 5.3. **The physician believes that direct collection would prejudice the mental or physical health or the safety of the patient or anyone else.**
 - 5.4. **The information has been collected and it is necessary for determining or verifying the eligibility to participate in a program, receive a product, or process an application.**
 - 5.5. **The information is available to the public.**



- 5.6. **Dr. Rahal collects the personal health information from another trustee in accordance with HIPA.**
- 5.7. **The information collected is about family members for the purpose of assembling a family health history.**
6. **Dr. Rahal may collect personal health information for another purpose as long as it is consistent with patient care and the patient has given consent.**
7. **Dr. Rahal takes reasonable steps to ensure that the information collected is accurate and complete.**
8. Only the minimum amount of information required is collected. This includes
 - Identification and contact information
 - name
 - date of birth
 - address
 - phone/fax/email
 - emergency contact information
 - record of patient appointment times
 - Billing information including
 - provincial health insurance plan number
 - private medical insurance details
 - Health information
 - medical history
 - presenting symptoms
 - physical examination findings
 - relevant medical history of family members
 - test requisitions and results including electrophysiological measurements, etc. and any reports and interpretations
 - reports from specialists or other health providers
 - diagnosis and treatment notes (including prescriptions)
 - allergies
 - information to be provided to third parties at the patient's request (workers compensation, reports for legal proceedings, insurance claims)



Use	
Legislative Reference: HIPA s26	CPSS Reference: Bylaw 23.2(c)(viii)
Policy Author:	Effective and Revision Dates:

The policies and procedures on Use and Disclosure may be combined.

Policy Statement

Dr. Rahal uses the minimum amount of personal health information necessary for the care and treatment of his patients based on the implied consent of the patient.

Procedures

1. **Dr. Rahal uses personal health information, based on implied consent for**
 - 1.1. **The care and treatment of patients.**
 - 1.2. **The purpose the information was collected.**
 - 1.3. **A purpose consistent with patient care including arranging, assessing the need, providing, continuing to support health or services for the patient.**
 - 1.4. **Discussing with the patient's next of kin, or someone the patient has a close personal relationship, the current health services being provided to the patient and the patient has not expressed a contrary intention to a disclosure of this type. .**
2. The clinic uses the least amount of personal health information necessary for the purpose.
3. All uses are consistent with the ethical practices of the medical profession.
5. Personal health information may be used without consent only as allowed in *HIPA*.
6. **A patient may revoke his or her consent for the use of personal health information and the medical practice will take reasonable steps to comply with the revocation promptly.**
 - 6.1. **A revocation is not retroactive**
7. Authorization to use personal health information is restricted to those who need it to meet the requirements of their role.
 - 7.1. Full access is provided all health providers at the clinic unless a patient restricts access to only Dr. Rahal.

Revised – September 2019

24



7.2. All employees and health professionals have access restricted through job descriptions, letters of engagement, and through technical features available in the EMR, including role-based access and masking.

8. Personal health information collected from patients is used by Dr. Rahal for Provision and continuity of care

- identify and contact patients
- historical record
- health promotion and prevention
- referral to specialists or other treating physicians
- requesting laboratory investigations
- requesting diagnostic tests
- generating prescriptions
- referral to other health care providers
- referral to home care agencies
- home care supervision

Billing

- billing provincial health plan
- billing third parties

9. Other uses authorized by HIPA

Note: Include the uses that are most likely to happen in the clinic and include a reference to HIPA and the Reference Manual for other uses.

Health or Social Services

- **Registering a patient in connection with another trustee (Regional Health Authority or affiliate, Ministry of Health or Cancer Agency for**
 - health care purposes
 - verifying eligibility for a program or service
 - verifying accuracy of registration information
- **Provision of health or social services for the patient.**
- **Payment for a health service.**
- **For the purposes of *The Health Care Directives and Substitute Health Care Decision Makers Act*.**
- **Avoiding or minimizing a danger to the health and safety of any person**

Criteria that can be used to make this decision include:

- There must be a reasonable expectation of probable harm;
- The harm must constitute damage or detriment and not more inconvenience; and
- There must be a causal connection between disclosure and the anticipated harm



- Generally, this means the trustee must make an assessment of the risk and determine whether there are reasonable grounds for concluding there is a danger to the health or safety of any person. That assessment must be specific to the circumstances of the case under consideration. This would involve the responsible trustee exercising the kind of professional judgment and experience common to Saskatchewan health care professionals.

Deceased Patients

- **In order to provide the individual's personal representative with information relating to the administration of the patient's estate and in accordance with established policies and procedures of the physician and the ethical practices of the medical profession.**
- **In order to provide the immediate family or to someone with whom the patient had a close personal relationship, information limited to the circumstances surrounding the death or services recently provided to the deceased.**

Programs

- **Planning, delivering, evaluating or monitoring a program of Dr. Rahal.**
- **A standards or quality of care committee established by one or more trustees to study or evaluate health services and the committee only uses it for those purposes, does not further disclose the information and takes reasonable steps to preserve the confidentiality of the information.**
- **Monitoring, preventing or revealing a fraudulent, abusive or dangerous use of publicly funded health services.**

Successors

- **Providing the information to another trustee who is a successor of Dr. Rahal and Dr. Rahal has made a reasonable attempt to notify patients**
 - **In preparation for disclosure to another trustee or a designated archive.**

Legal Investigations

- **For a health professional body to carry out its duties under the Act regulating the profession.**
- **Complying with a subpoena or warrant issued by a court, person or body that has the authority to compel the production of the information.**
- **Complying with the rules of court related to providing the court with the information.**
- **For the physician's legal counsel for the purpose of providing legal services to the physician.**



- **For the chief coroner or other appointed coroner with respect to an investigation or inquest.**
- **For the police when an authorized request has been made related to enforcing *The Criminal Code* or *The Controlled Drugs and Substance Act* or carrying out a lawful investigation under either of those Acts**

Research and Secondary Uses

- **Research under the conditions where express consent is not required pursuant to Section 29 of HIPA**

Other

- **De-identifying the information**
- **Any purpose permitted pursuant to any Act or regulation**

10. **Dr. Rahal will not use or obtain access to personal health information about one of the clinic employees for any purpose related to that person's employment without consent of the employee.**



Disclosure	
Legislative Reference: HIPA s. 27,28, 29, Reg. 5.1	CPSS Reference: Bylaw 23.2 (c)(ix)
Policy Author:	Effective and Revision Dates

Policy Statement

Dr. Rahal discloses personal health information as part of providing care to patients. If personal health information is disclosed for other purposes it will be with the consent of the patient or the disclosure is authorized without consent by law.

Procedures

1. Whenever possible, disclosures are noted in the patient charts. Sometimes this note is inferred by the completion of a prescription, requisition or other action.
 - 1.1. **Dr. Rahal will make reasonable efforts to inform patients of any disclosure of their personal health information.**
2. **A patient may revoke his or her consent for the disclosure of personal health information and the medical practice will take reasonable steps to comply with the revocation promptly.**
 - 2.1. **A revocation is not retroactive.**
3. **Dr. Rahal discloses personal health information to another trustee who is a health professional in accordance with the ethical practices of the trustee's profession.**
4. **When relying on the deemed consent of the patient, Dr. Rahal only discloses personal health information to trustees who are not health professionals when the trustee has established policies and procedures to restrict the access to the information to those who need it to carry out the purpose for which the information was collected.**
5. Dr. Rahal will ask any person or organization requesting personal health information the authority for the request to collect the personal health information, including with the patient's consent.
6. **When Dr. Rahal is aware, or should reasonably be aware, that the personal health information was collected or disclosed in contravention of HIPA, Dr. Rahal will not further disclose the personal health information without the consent of the patient.**



Express Consent

7. **Whenever reasonably possible Dr. Rahal will use the express consent of the patient when personal health information is disclosed.**
 - 7.1. **Express consent is used for disclosures to non-trustees, such as schools, employers and insurance companies.**

Implied Consent

8. When personal health information is disclosed as part of the patient's care to a health professional or another trustee, Dr. Rahal relies on implied consent from the patient. Disclosures with implied consent may be for
 - 8.1. **The care and treatment of the patient.**
 - 8.2. **The purpose the information was collected or a purpose consistent with that purpose.**
 - 8.3. **Arranging, assessing the need, providing, and continuing to support a service requested or required by the patient.**
 - 8.4. **Discussing with the patient's next of kin or someone the patient has a close personal relationship, the current health services being provided to the patient and the patient has not expressed that their personal health information not be disclosed to this person.**

Deemed Consent

9. When personal health information is disclosed as part of the patient's care to a health professional or another trustee, Dr. Rahal relies on implied consent from the patient. There may be occasions when deemed consent is used. Disclosures with deemed consent may be for
 - 9.1. **The care and treatment of the patient.**
 - 9.2. **The purpose the information was collected or a purpose consistent with that purpose.**
 - 9.3. **Arranging, assessing the need, providing, and continuing to support a service requested or required by the patient.**
 - 9.4. **Discussing with the patient's next of kin or someone the patient has a close personal relationship, the current health services being provided to the patient and the patient has not expressed that their personal health information not be disclosed to this person.**
 - Providing notice to the patient on anticipated uses and disclosures;
 - Providing information upon request to patients of all disclosures without consent of their personal health information;



- Reasonable safeguards are in place as stated in the clinic Policy Manual;
- Reasonable effort has been made to collect, use and disclose accurate information about the patient;
- The clinic adheres to the principle that all collection, use and disclosure of personal health information is based on “need-to-know” only; and
- The minimal amount of personal health information necessary is collected, used and disclosed.

Disclosure without Consent

10. Dr. Rahal may disclose personal health information without the consent of the patient for

Health or Social Services

- **Registering a patient in connection with another trustee (Regional Health Authority or affiliate, Ministry of Health or Cancer Agency for**
 - health care purposes
 - verifying eligibility for a program or service
 - verifying accuracy of registration information
- **Provision of social services for the patient.**
- **Provision of health or social services for the patient.**
- **Payment for a health service.**
- **For the purposes of *The Health Care Directives and Substitute Health Care Decision Makers Act*.**
- **Avoiding or minimizing a danger to the health and safety of any person.**

Criteria that can be used to make this decision include:

- There must be a reasonable expectation of probable harm;
- The harm must constitute damage or detriment and not more inconvenience; and
- There must be a causal connection between disclosure and the anticipated harm.
- Generally, this means the trustee must make an assessment of the risk and determine whether there are reasonable grounds for concluding there is a danger to the health or safety of any person. That assessment must be specific to the circumstances of the case under consideration. This would involve the responsible trustee exercising the kind of professional judgment and experience common to Saskatchewan health care professionals.



Deceased Patients

- **In order to provide the individual's personal representative with information relating to the administration of the patient's estate and in accordance with established policies and procedures of the physician and the ethical practices of the medical profession.**
- **Providing the immediate family or to someone with whom the patient had a close personal relationship, information limited to the circumstances surrounding death or services recently provided to the deceased.**

Programs

- **Planning, delivering, evaluating or monitoring a program of Dr. Rahal.**
- **A standards or quality of care committee established by one or more trustees to study or evaluate health services and the committee only uses it for those purposes, does not further disclose the information and takes reasonable steps to preserve the confidentiality of the information.**
- **Monitoring, preventing or revealing a fraudulent, abusive or dangerous use of publicly funded health services.**

Successors

- **Providing the information to another trustee who is a successor of Dr. Rahal and Dr. Rahal has made a reasonable attempt to notify patients.**
 - **In preparation for disclosure to another trustee or a designated archive.**

Legal Investigations

- **For a health professional body to carry out its duties under the Act regulating the profession.**
- **Complying with a subpoena or warrant issued by a court, person or body that has the authority to compel the production of the information.**
- **Complying with the rules of court related to providing the court with the information.**
- **To the physician's legal counsel for the purpose of providing legal services to the physician.**
- **To the chief coroner or other appointed coroner with respect to an investigation or inquest.**
- **To the police when an authorized request has been made related to enforcing *The Criminal Code* or *The Controlled Drugs and Substance Act* or carrying out a lawful investigation under either**



of those Acts and the information is limited to what is authorized in HIPA Regulation 5(1)(1).

Research and Secondary Uses

- **Research under the conditions where express consent is not required pursuant to Section 29 of HIPA.**

Other

- **De-identifying the information.**
- **Any purpose permitted pursuant to any Act or regulation.**



Managing Patient Consent and Masking in the EMR	
Legislative Reference: HIPA s 5-7,27	CPSS Reference: Bylaw 23.2(c)(xii)
Policy Author:	Effective and Revision Dates:
Templates: Consent Directive and Masking Form, Access to Personal Health Information Request Form	

Policy

Dr. Rahal will **take all reasonable steps to comply with a patient's request to limit the collection, use and disclosure of their personal health information.**

Procedure

Accepting Consent Directives

1. When personal health information is collected solely for health care purposes Dr. Rahal relies on implied consent from the patient.
2. A request to limit, restrict, or revoke consent will be accepted at any time.
 - 2.1. The clinic privacy poster will include information on a patient's right to limit access to their personal health information, including masking it.
3. Dr. Rahal will use the masking functionality in the EMR to restrict the use and disclosure of the patient's personal health information in accordance with the patient's consent directive.

Explaining Collection, Uses and Disclosures Mandated by Law

4. Anyone collecting, using, or disclosing personal health information will explain the authority for the action if a patient wants to limit consent for that activity.

Explaining the Benefits and Risks of Masking and Limiting Disclosure and Use

5. When the authority for the collection, use or disclosure allows for the patient to limit, restrict, or revoke consent the consent directive is met to the best of the clinic's ability.
6. Anyone collecting the personal health information will explain the benefits and risks of the consent directive if there are any. This may include
 - 6.1. Essential information is not available in a timely manner.
 - 6.2. Not all members of the care team will have access to the correct information to provide appropriate care.



- 6.3. Staff will be unable to check whether the patient's results, specialist reports, etc. are available before booking an appointment for the patient with Dr. Rahal. Staff will not be able to assist the physician in making specialist referrals, sending requisitions for diagnostic services, procedures, or prepare billing work for the physician.
- 6.4. In extreme cases, when a patient refuses to allow an override of the mask, care may be denied because of lack of information and the patient will have to wait until Dr. Rahal is available.

Alternatives to Masking

7. Dr. Rahal will advise the patient of alternatives to masking.
 - 7.1. The Office Manager can provide printed audit reports to the patient.
 - 7.2. Dr. Rahal can receive an automatic alert from the EMR each time the patient's record is accessed.
 - 7.3. Dr. Rahal will also consider alternative solutions suggested by the patient that will not be in contravention of any law or ethical practice by a physician.

Process for a Patient to Give a Consent Directive

8. When the patient informs Dr. Rahal that they wish to limit the access, collection, use or disclosure of their personal health information.
 - 8.1. A Masking Request Form is completed, scanned and held as part of the EMR record.
 - 8.2. A simple restriction on a use or disclosure is noted in the patient's record and the record is flagged.
 - 8.3. Patients wanting an audit of their record should complete the Access to Personal Health Information Request Form.

Unmasking a Record/Overriding a Consent Directive

9. Only Dr. Rahal and the Office Manager have the authority to unmask a record in the EMR or in any other way override a patient's consent.
 - 9.1. When a record is unmasked the reason must be indicated. The reasons include:
 - Patient Consent
 - Provider Consent because of safety concerns related to the patient
 - Access is required to complete, verify or document a previously provided health service requested or required by the patient
 - Access is required for billing
 - Access for use or disclosure is required by law
 - 9.2. The person authorized to unmask the record in the EMR should also indicate the time period the record is to remain unmasked. The users



should select the minimum time necessary to fulfill the identified purpose for the unmasking.



Agreements	
Legislative Reference: HIPA s. 18	CPSS Reference: Bylaw 23.2(c)(xii)(xii)
Policy Author:	Effective and Revision Dates:

Policy

Dr. Rahal uses written agreements to establish responsibilities and mitigate risk when third parties have or may have access to personal health information on behalf of the practice.

Procedures

Information Management Service Providers (IMSP) Agreements

1. Agreements with IMSPs cover
 - Name of the parties
 - Authority to enter into the agreement
 - Duration of agreement
 - Description of services to be provided
 - Description of the personal health information that is the subject of the agreement
 - Responsibilities of both parties
 - Privacy and security requirements
 - Deliverables, if any
 - Price/Fees
 - Terms
 - Indemnification
 - Termination
2. Dr. Rahal currently uses IMSP agreements with companies and individuals that process, store, archive or destroy personal health information on behalf of the clinic or provide information technology services. This includes
 - River Information Management and Storage
 - Oak Computing Services
 - Windy Road Transcriptionists
 - ABC EMR Vendor
 - Transcriptionist
 - Telephone answering service

Other Agreements with Third Parties

3. Dr. Rahal also enters into agreements with other companies and individuals who are using personal health information on behalf of the clinic, or who may



- inadvertently see personal health information while performing a service. This includes
- Landlord
 - Security company
 - Cleaning company
4. Contracts and agreements are used by Dr. Rahal when the disclosure of personal health information is ongoing, such as when a third party provides a service on behalf of the clinic.
 5. In accordance with HIPA, Dr. Rahal requires an agreement to be signed by any researcher receiving personal health information from the clinic.



Management of Breaches	
Legislative Reference: HIPA s16	CPSS Reference:
Policy Author:	Effective and Revision Dates:
Templates: Privacy and Security Breach Reporting Form, Breach notification letter	

Policy Statement

Dr. Rahal considers a privacy breach as a collection, use or disclosure of personal health information in contravention of *The Health Information Protection Act* and these policies. Dr. Rahal responds promptly to potential, suspected and confirmed privacy and security breaches and will engage the necessary expertise in managing breaches.

Definitions

Types of Breaches, a breach may be any or all of these:

Confidentiality: personal health information becomes known or is at risk of becoming known by a person who does not have a need to know the information and/or is not authorized to see the information.

Integrity: personal health information has been modified or in some other way has been interfered with such that Dr. Rahal or patient does not consider the information reliable.

Availability: personal health information has been stolen, lost, moved, destroyed, blocked from view or in some manner is not available to the trustee or the patient.

Procedures

1. The first person aware of the suspected breach will take actions to stop or contain, the breach if it is ongoing,
 - 1.1. Anyone aware of a suspected breach shall notify the Office Manager or Dr. Rahal.
2. Dr. Rahal and the Office Manager will work to ensure
 - 2.1. Unauthorized copies of the personal health information are retrieved, or notification of the destruction of the information is received. The notification of destruction includes the type of information that was involved in the suspected breach and how it was destroyed.



- 2.2. Disconnection of the EMR, and other information systems, from the Internet and the Network if they have been compromised. Oak Computing Services is contacted to assist in containing the suspected breach and investigation.
- 2.3. Deactivate the user account if an authorized user is accessing personal health information inappropriately.

Investigation and Analysis

3. Dr. Rahal leads an internal investigation into the suspected breach which includes
 - 3.1. Establishing an investigation team with the necessary expertise which may include experts in information technology, eHealth Saskatchewan, and other trustees who may have their own accountability for the information.
 - 3.2. Understanding the circumstances of the breach and determining if it was a breach of personal health information.
 - 3.3. Examining physical and technical security and business process for a role in the breach.
 - 3.4. Identifying anyone who may have had unauthorized access to the personal health information through the examination of the audit logs of the EMR.
 - 3.5. The Office Manager thoroughly documents the breach using the form developed by the Saskatchewan EMR Program.
 - 3.6. Determine if an actual breach occurred.
 - 3.7. Document recommendations and develop strategies to minimize any potential future risks at the medical practice.

Notification of Others

4. Key stakeholders are contacted as appropriate for the breach
 - 4.1. If the breach involves information from the EHR (PACS, SLRR, PIP) the Privacy Officer at eHealth Saskatchewan is contacted at 1-888-316-7446.
 - 4.2. If the breach involves information received from another trustee, that trustee is contacted.
 - 4.3. If the breach involves information from a person who is not a trustee, that person is contacted.
 - 4.4. The Office of the Information and Privacy Commissioner of Saskatchewan may be contacted for assistance and advice on managing the breach or on the notification of patients.

Telephone: (306) 787-8350



Toll Free in Saskatchewan: 1-877-748-2298

- 4.5. The Office of the Information and Privacy Commissioner of Saskatchewan should be contacted if the breach will cause significant harm to the patients whose information was breached, involves a large number of patients, or is systemic in nature and the Commissioner may want to notify other trustees of the potential for a similar breach.
- 4.6. The Privacy Officer at the Saskatchewan Medical Association may be contacted for assistance and advice on managing the breach or notification of patients.
Phone: (306) 657-4581
Toll Free in Saskatchewan: 1-800-667-3781
- 4.7. Contact the police if there is possible criminal activity.
- 4.8. The EMR vendor is contacted if the breach is related to the EMR.
- 4.9. Contact the Research Ethics Board (REB) if the breach involves personal health information used in a clinical trial or other research approved by the REB.
- 4.10. Contact legal counsel and insurers if deemed appropriate.

Notification of Patients

5. Patients are notified as soon as possible after the breach and the potential harm to the patient is understood.
 - 5.1. Patients are notified when there is a real risk of significant harm to
 - the provision of health care or other benefits to the patient and/or
 - the mental, physical, economic or social well-being of the patient.
 - 5.2. Notification of patients is made by telephone, mail or at the next appointment, depending on the seriousness of the breach.
 - 5.3. A notification to a patient about a breach includes
 - the date of breach,
 - details of the extent of the breach and the type of personal health information involved,
 - the potential risks to the patient,
 - the steps that have been taken to address the breach both in the immediate and long term,
 - how the patient can contact the Office of the Information and Privacy Commissioner of Saskatchewan,



- how the patient can contact Health Registration at the Ministry of Health should they want to check for any misuse of their health services number.
6. Dr. Rahal may contact the Office of the Information and Privacy Commissioner of Saskatchewan to assist in determining the most appropriate method of notifying patients.
 - 6.1. The Office of the Information and Privacy Commissioner of Saskatchewan may recommend indirect notification of patients through the news media, a website or a poster in the clinic when direct notification is not possible or inappropriate in the situation.
 7. The Privacy Officer at the Saskatchewan Medical Association may be contacted for assistance and advice on notification of patients.

Phone: (306) 657-4581
Toll Free in Saskatchewan: 1-800-667-3781

Prevention

8. Document recommendations and develop strategies to minimize future risks at the medical practice.
9. The Office Manager ensures that the containment and notification recommendations of this policy have been met.
10. Dr. Rahal ensures the disciplinary policy is followed if an employee is involved.
 - 10.1. If a health professional is involved Dr. Rahal will contact the appropriate regulatory body.
11. If the breach occurred at an IMSP the contract will be reviewed.
12. The Office Manager reviews these policies and procedures after the completion of the investigation and makes any necessary changes based on the lessons learned.
13. The Office Manager arranges for additional training based on lessons learned.
14. Dr. Rahal cooperates with any and all investigations by the Office of the Information and Privacy Commissioner of Saskatchewan into a breach of privacy at the clinic.
15. Dr. Rahal cooperates with any and all investigations by eHealth Saskatchewan into a breach of privacy involving the EHR.

Penalties

16. When a privacy breach has been substantiated the Privacy Officer determines if it was willful or unintentional.



16.1. Users who unintentionally collect, use, access or disclose personal health information without authorization are subject to all or any of the following:

- further privacy training
- loss of privileges to use the EMR
- suspension without pay for one day
- dismissal

16.2. Users who willfully collect, use, access or disclose personal health information without authorization are subject to all or any of the following

- further privacy training
- loss of privileges to use the EMR
- suspension without pay for up to five days
- dismissal



Business Continuity and Disaster Recovery Plan	
Legislative Reference: HIPA s 16	CPSS Reference:
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal maintains up-to-date business continuity and disaster recovery plans that provide guidance on how to manage an interruption in business due to unplanned events.

Procedures

1. The business continuity plan includes
 - 1.1. Emergency contact numbers
 - 1.2. Employees contact numbers
 - 1.3. Vendor and other third party contact numbers with account numbers for the medical practice
 - 1.4. Recommended alternative sites for patients to receive care
 - 1.5. A plan on how to notify patients if their appointment is cancelled or they should go to an alternate location.
2. The disaster recovery plan includes
 - 2.1. A list of all IT and telecommunications systems with contact information for assistance
 - 2.2. A checklist of actions that should be taken in an emergency to protect systems
 - 2.3. A step-by-step process for resuming the normal operations of the EMR
 - 2.4. The location of backups and how to access them if necessary.
 - 2.4.1. At least one person is trained in recovering a backup and who's responsibilities will include semi-annual testing of a backup to ensure reliability
3. The business continuity and disaster recovery plan will be reviewed annually and updated as necessary.



Retention, Storage and Destruction of Paper Records	
Legislative Reference: HIPA s. 16, 17	CPSS Reference: Bylaw 23.1(f), 23,2(c) (x)(xi)(xii)
Policy Author:	Effective and Revision Dates:
Template: Record of Destruction	

Policy Statement

Dr. Rahal retains paper records, which have not been scanned into the EMR, for 10 years after the last entry into the patient record, whether it is the paper record or the EMR. If the patient is under the age of 18, both the paper and electronic record will be retained for 10 years after the last entry into the patient record or for 10 years after the patient reaches age 18, whichever is the longer. Dr. Rahal stores and destroys all records securely.

Procedures

1. Once a year the Office Manager removes the records of patients who have been inactive for five years. Paper records are placed in banker boxes.
 - 1.1. The Office Manager prepares a list of all records selected for archiving; the number of the banker box the record is stored and signs the list.
 - 1.2. The list contains
 - patient name and health services number
 - physician name
 - last year an entry was made in the record.
 - 1.3. The list is confirmed for accuracy by one other person who also signs the list.
 - 1.4. Dr. Rahal reviews the list of records for archiving and signs the list.
 - 1.5. The banker boxes are sealed and initialed by the Office Manager.
2. The Office Manager arranges for River Information Management and Storage to pick up the banker boxes and place them in storage.
3. Annually, the Office Manager prepares a list of paper records that can be destroyed according to the policy statement.
 - 3.1. The Office Manager ensures that the patient has not returned to the practice under a different name or health services number.



- 3.2. The Office Manager reviews the list of records that belong to patients that have not been active in the clinic in over six years with Dr. Rahal.
- 3.3. The list of records to be destroyed is signed by Dr. Rahal.
4. The Office Manager contacts River Information Management and Storage to confirm the records that are to be destroyed. A copy of the signed list of records is sent by bonded courier or encrypted email to the company.
 - 4.1. After the company has confirmed by email they have the records on the list they proceed with destroying the records by shredding.
 - 4.2. After the shredding of the records River Information Management and Storage sends a letter signed by the manager of the shredding operation and at least one other employee involved in the shredding of the records confirming the destruction.
5. A record of destruction is kept by the Office Manager with
 - description of information destroyed
 - date the information was destroyed
 - how the information was destroyed
 - why the information was destroyed
 - who destroyed the information.

Information Management Service Provider (IMSP) Agreement

6. Dr. Rahal has signed an IMSP agreement for secure storage and destruction of paper and electronic records with
 - Oak Computing Services
 - River Information Management and Storage.
7. The IMSP agreement includes
 - 7.1. All IMSP employees are bonded and sign confidentiality agreements with the supplier.
 - 7.2. The IMSP premises are monitored 24 hours a day, seven days a week.
 - 7.3. There are environmental controls against damage to the records from water, fire and insects.
 - 7.4. Dr. Rahal or a representative may visit the premises annually to review security practices.
 - 7.5. The IMSP is knowledgeable about HIPA and adheres to its requirements.



Scanning and Destruction of Paper Records	
Legislative Reference: HIPA s16 and 17(2)	CPSS Reference: Bylaw 23.2(c)(x)
Policy Author:	Effective and Revision Date:

Policy

The accuracy of scanned records is confirmed before the paper document(s) are destroyed.

Procedures

1. The Office Manager will train the office assistant on the procedure for scanning documents of personal health information.
2. All scanned documents are saved as PDF, a read only format.
3. The person scanning the document shall review the scanned document to ensure it is readable and copied completely.
4. The scanned document is named and filed according to clinic procedures.
5. The paper documents are placed in the designated secure receptacle which is locked by the Office Manager.
6. Once a month the Office Manager will randomly select documents from the receptacle and perform a complete quality assurance test to ensure the scanned document is accurate, complete, retrievable, readable and useable.
7. When the quality assurance procedure has been completed all documents in the secure receptacle are securely shredded.



Backups and Storage

Legislative Reference: HIPA s16 and 17(2)	CPSS Reference: Bylaw 23.2(c)(xi)
Policy Author:	Effective and Revision Dates:

Policy Statement:

Dr. Rahal maintains a program to backup all EMR and other electronic administrative records and to store the backups securely.

Procedures

1. The Office Manager carries out the duties related to backups.

Clinics will probably only use only one type of backup.

Vendor Backups

2. The EMR Vendor is contracted by Dr. Rahal to manage all backups through remote VPN access.

Offsite Backups

3. Dr. Rahal has a contracted Oak Computing Services to perform daily remote backups.
4. The Office Manager ensures there is a successful backup each day.
5. Oak Computing accesses the clinic EMR through an encrypted virtual private network (VPN).

Onsite Backups

1. The schedule for automatic encrypted backups.
 - 1.1. Regular encrypted backups are performed daily and taken off-site.
 - 1.2. Weekly encrypted backups are performed and taken off-site weekly.
 - 1.3. Annual encrypted backups are performed and taken off-site.
 - 1.4. Backup devices are reused on rotation schedule which provides data recovery access for up to 13 months, which is adequate from a disaster recovery/availability:
 - daily incremental backups – use a 7 day rotation of backup devices

Revised – September 2019

47



Tel: 306.657.4557
Toll Free: 1.800.667.3781
Fax: 306.974.0326
Email: emr@sma.sk.ca

www.sma.sk.ca/emr



- weekly complete backups – use a 5 week rotation of backup devices
 - annual complete backup – stored securely in an offsite safe and kept for two years.
2. The Office Manager initials the Daily Backup Record each day after confirming the previous day's backup was completed.
 - 2.1. The Office Manager sends the encrypted weekly backup devices to Oak Computing Services by bonded courier.
 - 2.2. Each month, Oak Computing Services returns the backup devices for reuse.
 3. Dr. Rahal will at least semi-annual test the reliability of the backed-up information
 - 3.1. Testing the backups will be done by a qualified IT specialist and using a second server.

Administrative Records

4. Electronic administrative records that are inactive for five years are copied onto an encrypted hard drive storage device by the Office Manager.
 - 4.1. Each year when new files are added the Office Manager confirms that previously stored records are accessible and readable.
 - 4.2. Administrative records that remain inactive for an additional two years are deleted from the storage device.

Recovering Information from Backup Devices

5. If the information on the EMR becomes corrupt, the hard drive crashes or the server is stolen; Oak Computing Services is contacted to recover the information on the backup and to transfer it to an operating server. This may require the involvement of the EMR vendor if the EMR software is corrupt or the server is stolen.

Information Management Service Provider (IMSP) Agreements

6. Dr. Rahal maintains up to date IMSP agreements with Oak Computing Services and River Information Management and Storage in relation to the management and secure storage of backup devices. These agreements include the following requirements.
 - 6.1. Ensure that facilities are controlled for temperature, fire, and other environmental factors that may damage the tapes.
 - 6.2. Ensure that personal health information is encrypted whenever the backups are being transported and stored.
 - 6.3. Ensure that personal health information stored in any format is retrievable, readable and useable by Dr. Rahal.



User Account Management	
Legislative Reference: HIPA s 16	CPSS Reference: Bylaw 23.2(c)(xii)
Policy Author:	Effective and Revision Dates:
Templates: Acceptable Use Agreement	

Policy Statement

Each person with access to the EMR and the office computers will have their own user name and password.

Procedures

1. The Office Manager manages the creation and deletion of user accounts and has the administrative rights to change the privileges for each user.
2. Before each user is assigned access to the EMR or other information system they are required to sign an Acceptable Use Agreement.
3. A user name and password is the equivalent of a signature for ensuring users only access the personal health information they need to know to perform their role.
4. Each user will be authorized to view, use, collect, disclose, create, amend and mask the personal health information according to the requirements of that person's position.
5. A user's account is suspended should any concerns arise about the use of the account. If the issue is resolved, the account will be re-activated.

Passwords

6. Users select their own passwords which are a minimum of eight characters and are a combination of numbers, letters, symbols, and upper and lower case.
7. Passwords should be changed every three months.
8. Passwords should never be shared with anyone else.

Penalties

9. Accessing the EMR or other information systems without appropriate authorization is seen as a privacy breach.



10. When accesses are deemed inappropriate or a privacy breach has been substantiated the Privacy Officer determines if it was willful or unintentional.

9.1 Users who unintentionally access personal health information are subject to all or any of the following:

- further privacy training
- loss of privileges to use the EMR
- suspension without pay for one day
- dismissal

9.2 Users who willfully access personal health information are subject to all or any of the following

- further privacy training
- loss of privileges to use the EMR
- suspension without pay for up to five days
- dismissal



Auditing	
Legislative Reference: HIPA 16(b)(iii)	CPSS Reference: Bylaw 23.1(e)(v)
Policy Author:	Effective and Revision Dates:
Template: Access to Personal Health Information Form	

Policy Statement

Dr. Rahal monitors all activity in the EMR by employees and health professionals. Audit reports regarding patient records are made available to patients upon request.

Procedures

1. Dr. Rahal maintains an EMR that has the ability to audit users of the system.
 - 1.1. All employees and health professionals are aware of the auditing of all of their activities in the EMR.
 - 1.2. All employees are aware that Dr. Rahal is notified automatically on all accesses and attempted accesses to masked information, all overrides of masking, and all accesses to flagged patient records.
 - 1.3. The Office Manager is authorized to run regular audit reports to be reviewed by the Dr. Rahal.
2. Audit reports will be created if there is a suspected breach, for random reviews of user activities or at the request of a patient.

Information Captured in Audit Logs

3. The audit logs capture information required by CPSS, information useful to patients and information necessary to monitor user activity of the EMR. The information captured in the audit logs
 - Name of the patient
 - Name of user
 - Date and time of access
 - Information that was accessed
 - Action performed related to personal health information – create, add, modify, delete, view, or disclose
 - Who the information was disclosed to
 - Preserves the original content of the recorded information when changed or updated
 - Accesses to masked information



- Overrides of masked information
- Failed attempts to access masked information
- Changes in consent directives
- Successful and failed login attempts.

Patient Requests and Complaints

4. Patients requesting an audit report of users should complete the Access to Record Request Form.
5. The Office Manager prepares all audit reports requested by patients and Dr. Rahal reviews and signs the report before it is given to the patient.

Monitoring Program

6. Dr. Rahal reviews a random selection of audit reports once per week.
 - 6.1. At least one report reviewed is by user for a minimum one week period.
 - 6.2. At least one report reviewed is by patient over a minimum one week period.
7. Dr. Rahal receives all alerts sent automatically by the EMR and reviews for inappropriate access.
8. When accesses are deemed inappropriate or a privacy breach has been substantiated Dr. Rahal determines if it was willful or unintentional.
 - 8.1. Users who unintentionally access personal health information inappropriately are subject to all or any of
 - further privacy training
 - loss of privileges to use the EMR
 - suspension without pay for one day
 - dismissal
 - 8.2. Users who willfully access personal health information inappropriately are subject to all or any of
 - further privacy training
 - loss of privileges to use the EMR
 - suspension without pay for up to five days
 - dismissal
9. Patients are notified of the breach in accordance with the Management of Breaches Policy.



Destruction of Office Equipment and Medical Devices Retaining Personal Health Information	
Legislative Reference: HIPA s 17(2)(b)	CPSS Reference: Bylaw 23.2(c)(xi)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal ensures that all personal health information is removed from the office equipment and medical devices before the devices are recycled or destroyed.

Procedures

1. Neither the office equipment nor medical devices will be disposed of in the regular garbage or recycling.
2. The Office Manager maintains a list of office equipment and medical devices that could possibly retain personal health information. The list of such devices as of October 2011 is:
 - 1 client-server
 - 1 laptop computer
 - 2 desktop computers
 - 1 fax machine
 - 1 photocopier
 - 25 backup tapes
 - 2 USB memory keys
 - 1 iPad
 - 1 cell phone
 - 1 scanner
3. A record of destruction is kept by the Office Manager with the following information
 - Description of information potentially on the device
 - When the device was destroyed
 - How the device was destroyed
 - Why the device was destroyed
 - Who destroyed or recycled the device
4. Any device retaining the primary source of the personal health information is examined by the Office Manager to ensure the information has been properly transferred to the replacement device. The old device is not destroyed until the Office Manager has confirmed the accuracy and integrity of the transferred information.
 - 4.1. This procedure applies to:
 - client server
 - laptop and desktop computers
 - photocopiers and scanners
5. Oak Computing Services is contracted to destroy all devices securely.



General Security Software	
Legislative Reference: HIPA s 16	CPSS Reference: Bylaw 23.2(c)(xi)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal maintains security software licenses that provide regular updates to the firewall, anti-virus, malware and the virtual private network software.

Procedures

1. The Office Manager maintains a license for security services from SaskTel which includes firewall protection, encryption for emails, and scanning emails for viruses.
2. All servers, computers, USB keys and mobile devices purchased by the clinic will include encryption capabilities.
3. The Office Manager maintains other security software update licenses as appropriate.
4. The Office Manager reviews the security updates from the EMR vendor monthly to ensure updates have been received and installed.
5. Dr. Rahal use a VPN to connect to the EMR server remotely.



Security of the Office	
Legislative Reference: HIPA s 16	CPSS Reference: Bylaw 23.2(c)(xii)
Policy Author:	Effective and Revision Dates:

Policy Statement

Dr. Rahal ensures that the medical practice's physical office space is secure.

Procedures

1. Dr. Rahal has signed a lease with the landlord that stipulates the hours the exterior doors are locked.
 - 1.1. Access to the building after hours is monitored by a swipe card entry system that records the ID number of the person entering the premises and records the time the person enters and leaves the building.
 - 1.2. The landlord has provided an alarm system for the office.
 - 1.3. Dr. Rahal has a contract with Night and Day Security to monitor the alarm system.
2. The Office Manager manages the office keys and the opening and closing of the office each day.
 - 2.1. All physicians are provided with a key to the office door and to their own office and examination rooms.
3. Monitors, printers, and fax machines are placed where patients, unauthorized staff and others cannot see the personal health information on them.
 - 3.1. The server is in an environmentally safe area and secured to the floor or wall, or place in a locked cupboard.
4. Portable equipment such as laptops, external hard drives, USB keys, CDs should be stored in a secure location and use a lockable box to store and transport small storage media devices.
 - 4.1. Portable equipment is never left unattended when taken outside the office, such as in cars or the hospital cafeteria.
 - 4.2. All portable equipment has strong encryption capabilities and all personal health information on portable equipment is encrypted.
 - 4.3. Physicians, employees and third parties are required to lock screen or log off whenever they leave their workstation unattended. Use CTRL, ATL, DELETE.
5. All computers are password protected.

Revised – September 2019

55



Tel: 306.657.4557
Toll Free: 1.800.667.3781
Fax: 306.974.0326
Email: emr@sma.sk.ca

www.sma.sk.ca/emr



Glossary

Definitions in bold are from *The Health Information Protection Act (HIPA)*

“**Access**” means to obtain or retrieve information

- **Access** may be used in relation to the patient’s right to review and/or obtain a copy of his or her medical record
- **Access** may be used in relation to the act of viewing information in the EMR

“**Breach**” means an unauthorized collection, use or disclosure of personal health information.

“**Collect**” (or collection) **means to gather, obtain access to, acquire, receive, or obtain personal health information from any source by any means.**

“**Confidentiality**” means the obligation of the person or organization collecting or using the information to not reveal it to anyone who is not authorized to know it.

“**Consent**”

Trustees must determine, in accordance with the Canadian Medical Association Code of Ethics, CPSS professional standards and the circumstances and urgency of the health service, which consent option is most appropriate.

- **Express consent** means the individual has indicated in writing or verbally an agreement with the collection, use or disclosure of the information. This is the highest standard for consent.
- **Implied consent** means that the individual’s consent to the collection, use or disclosure of their personal health information is implied based on the circumstances. The individual may withhold or withdraw consent for the collection, use or disclosure. For example, where a patient presents for service it is reasonable to imply the individual’s consent to the collection, use and disclosure of their personal health information to provide the service, even though they have not expressly said so.
- **Deemed consent** means that the individual’s personal health information is used or disclosed without the individual’s consent, provided that it is used or disclosed for a purpose prescribed under section 27(2) of HIPA (i.e. for the purpose of providing or supporting a healthcare service to the individual) and the conditions set out in HIPA are met
- NOTE: Deemed consent is not the preferred model of consent as the individual is not involved in a consent process. Whenever possible, implied or express consent should be used



“Control” means the power or authority to manage, restrict, regulate or administer the collection, use, or disclosure of the record¹.

“Custody” means the physical and/or legal responsibility for the collection, use, disclosure of the personal health information

“De-identified personal health information” means personal health information from which any information that may reasonably be expected to identify an individual has been removed. This includes information that has been aggregated or transformed so that it cannot reasonably be re-identified.

“Designated archive” means an archive designated in the regulations of HIPA.

“Disclose” (or disclosure) means to transfer or release information to another person or organization separate entity outside of the trustee’s authority.

“Electronic Health Record” (EHR) means a secure and private lifetime record of an individual’s key health history and care within the health system. The record is available electronically to authorized healthcare providers and the individual in support of high quality care.

“Electronic Medical Record” (EMR) means a computer-based patient record system. It is sometimes extended to include other functions, such as order entry for medications and tests. For the purposes of this document, EMR is the system used in medical practices.

“Health services number” means a unique number assigned to an individual who is or was registered as a beneficiary to receive insured services within the meaning of *The Saskatchewan Medical Care Insurance Act*.

“Information and Privacy Commissioner of Saskatchewan” (OIPC) means an independent officer of the Saskatchewan Legislative Assembly who oversees three different Saskatchewan privacy and/or access statutes.

“Information management service provider” (IMSP) means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf

“Integrity” means the assurance that personal health information has not been modified, or in some other way interfered with such that the physician or patient does not consider the information reliable. This includes throughout the storage, use, transfer and retrieval of the personal health information.

“Personal health information” means, with respect to an individual, whether living or deceased:

- Information with respect to the physical or mental health of the individual

¹ A Contractor’s Guide to Access and Privacy in Saskatchewan, Office of the Information and Privacy Commissioner, <http://www.oipc.sk.ca/webdocs/ContractorsGuide.pdf>
Revised – September 2019



- **Information with respect to any health service provided to the individual**
- **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**
- **Information that is collected**
 - **in the course of providing health services to the individual; or**
 - **incidentally to the provision of health services to the individual;**
- **Registration information**

“Physician-trustee” means a physician who is a trustee under HIPA and not an employee of a trustee.

“Primary purpose” means the purpose for which personal health information was originally collected, and includes any purpose that is consistent with that purpose.

“Privacy” means a broad concept which involves the right of the individual to exercise a measure of control over his or her personal health information. It involves the decision of the individual about what personal health information will be disclosed to a trustee and for what purposes. It captures both security and confidentiality which are subsets of privacy.

“Privacy Officer” means a person designated to make decisions or form opinions required under HIPA.

“Regional Health Authority” means a health organization established pursuant to section 14, 24 or 25 of *The Regional Health Services Act* (Saskatchewan).

“Record” means a record of information in any form and includes information that is written, photographed, recorded, digitized, or stored in any manner, but does not include computer programs or other mechanisms that produce records.

“Registration information” means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual’s health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations.

“Secondary purpose” means the use or disclosure of information for a purpose other than that for which it was originally collected, which is a program activity or service related to patient care. An example is the collection, use, and disclosure of personal health information for billing purposes.

“Security” means the procedures and systems used to restrict access, and to protect and maintain the integrity of the personal health information.

“Third Parties” means individuals and organizations who provide a service to the practice that does, or has a significant chance of, seeing or using personal health information, but who are not trustees, employees, health professionals, medical students, residents.

“Trustee” means any of the following that have custody or control of personal health information as defined in HIPA s.2 (t):

- a government institution



- a regional health authority or a health care organization
- a licensee as defined in *The Personal Care Homes Act*
- a person who operates a facility as defined in *The Mental Health Services Act*
- a licensee as defined in *The Health Facilities Licensing Act*
- an operator as defined in *The Ambulance Act*
- a licensee as defined in *The Medical Laboratory Licensing Act, 1994*
- a proprietor as defined in *The Pharmacy Act, 1996*
- a community clinic
 - as defined in section 263 of *The Co-operatives Act, 1996*
 - within the meaning of section 9 of *The Mutual Medical and Hospital Benefit Associations Act* or
 - incorporated or continued pursuant to *The Non-profit Corporations Act, 1995*
- the Saskatchewan Cancer Foundation
- a person, other than an employee of a trustee, who is
 - a health professional licensed or registered pursuant to an Act for which the minister is responsible or
 - a member of a class of persons designated as health professionals in the regulations
- a health professional body that regulates members of a health profession pursuant to an Act
- a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee
- any other prescribed person, body or class of persons or bodies

“Use” includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

Acronyms

CPSS – College of Physicians and Surgeons of Saskatchewan

EHR – Electronic Health Record

EMR – Electronic Medical Record

HIPA – The Health Information Protection Act

IMSP – Information Management Services Provider

OIPC – Office of the Information and Privacy Commissioner of Saskatchewan

PIP – Pharmaceutical Information Program

PIPEDA – Personal Information Protection and Electronic Documents Act

REB – Research Ethics Board

Revised – September 2019

59



Tel: 306.657.4557
Toll Free: 1.800.667.3781
Fax: 306.974.0326
Email: emr@sma.sk.ca

www.sma.sk.ca/emr

