THE SASKATCHEWAN EMR program

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

Privacy and Security Resource Materials for Saskatchewan EMR Physicians: Guidelines, Samples and Templates

Reference Manual

Guidelines on Requirements and Good Practices For Protecting Personal Health Information

January 2013

Disclaimer

The information in this reference 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. The information is provided as guidance for medical practices in Saskatchewan developing privacy and security policies and procedures.

Table of Contents

Appendices

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

"Agent" means a person that with the approval of the trustee acts for or on behalf of the trustee in respect to personal health information and only for the purpose of the trustee and not the agent's purpose whether or not the agent has the authority to bind the trustee, is paid by the trustee, or is remunerated by the trustee.

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

"Collect" 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, using or disclosing the information to not reveal it to anyone who is not authorized to know it.

"Consent"

Trustees must determine, in accordance with the HIPA, CPSS, Canadian Medical Association Code of Ethics, 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 their personal health 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 infer 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 record[1].

"Custody" means the physical and 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. Th**is 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 a 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

[1] A Contractor's Guide to Access and Privacy in Saskatchewan, Office of the Information and Privacy Commissioner, http://www.oipc.sk.ca/Old%20Website%20Content/webdocs/ContractorsGuide.pdf. Also see OIPC Report F-2008-002 (Ministry of Justice and Attorney General).

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**
- **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 HIPAs. 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 Ac*t 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

Principles in the Preamble to *The Health Information Protection Act*

An Act respecting the Collection, Storage, Use and Disclosure of Personal Health Information, Access to Personal Health Information and the Privacy of Individuals with respect to Personal Health Information and making consequential amendments to other Acts

That personal health information is private and shall be dealt with in a manner that respects the continuing interests of the individuals to whom it relates;

That individuals provide personal health information with the expectation of confidentiality and personal privacy;

That trustees of personal health information shall protect the confidentiality of the information and the privacy of the individuals to whom it relates;

That the primary purpose of the collection, use, and disclosure of personal health information is to benefit the individuals to whom it relates;

That, wherever possible, the collection, use, and disclosure of personal health information shall occur with the consent of the individuals to whom it relates;

That personal health information is essential to the provision of health services;

That, wherever possible, personal health information shall be collected directly from the individual to whom it relates;

That personal health information shall be collected on a need-to-know basis;

That individuals shall be able to obtain access to records of their personal health information;

That the security, accuracy, and integrity of personal health information shall be protected;

That trustees shall be accountable to individuals with respect to the collection, use, disclosure, and exercise of custody and control of personal health information;

That trustees shall be open about policies and practices with respect to the collection, use, and disclosure of personal health information;

Instructions

Using the Privacy and Security Reference Manual

It is recommended that anyone creating a privacy and security policy manual for a medical practice read **Creating a Policy Manual** first.

Throughout the **Reference Manual** the term "physician-trustee" is used. This term is a reminder that physicians who are trustees under HIPA have different legal accountability than physicians who are employees, medical students and residents, of another trustee, such as a regional health authority.

Physicians who are employees, medical students and residents, or on contract with a non-trustee may use this **Reference Manual** to establish privacy and security policies and procedures for their practice location if the non-trustee does not have such policies and procedures in place.

This **Reference Manual** provides guidelines for physicians to use in interpreting *The Health Information Protection Act* of Saskatchewan (HIPA). These guidelines do not constitute legal advice. It is divided into sections of related policy topics.

- There are several general responsibilities that a physician-trustee must meet and these are covered in the Accountability section. This section discusses the roles and responsibilities of a privacy officer and the obligations of employees, medical students and residents, and others who are subject to the policies and procedures and other requirements of HIPA.

- This is followed by the Patient Access, Amendment, and Authorized Representatives section. HIPA is very specific about patients' rights to have access to their own personal health information and to ask for amendments when there are errors or omissions. This section also includes information about patient designates and personal representatives.

- The third section is about the consent related to the collection, use and disclosure of a patient's personal health information. This does not include consent for treatment or service. There is an explanation of the different types of consent under HIPA and how to manage a patient's consent directive. There are several restrictions and authorizations in HIPA on the collection, use, and disclosure of personal health information.

- The Safeguards section contains overviews of some of the tools that physicians can use to mitigate risks, such as agreements, breach management, and business continuity and disaster recovery plans. While these are not specifically required in HIPA, they will help physicians meet some of their general duties to protect personal health information.

- This is followed by guidelines on other safeguards, including retention, storage, and destruction of records. This section provides advice applicable to both paper and electronic information.

NOTES:

When the word "must" is used in the **Privacy Resource Materials** it means it is a requirement under HIPA. "May" is used, as it is in HIPA, when a physician has discretion in how the HIPA requirement is met. "Should" and "recommended" generally refers to the expectations of the College of Physicians and Surgeons what are considered good practices.

For additional information, useful reference materials include:

- *The Health Information Protection Act,*
- The SMA's and CPSS' websites,
- Relevant CPSS Regulatory Bylaws,
- Relevant policies from any Regional Health Authority with which personal health information is shared,
- The Saskatchewan Ministry of Health website (http://www.health.gov.sk.ca/),
- The Saskatchewan Office of the Information and Privacy Commissioner website (http://www.oipc.sk.ca/).

Accountability

Text in bold is a legislative requirement

Trustees

(HIPA s. 2(t)

HIPA establishes the rules and responsibilities for physicians and other trustees in the protection of the privacy of patients and the security of their personal health information. All physicians implementing an EMR need to understand the concept of a trustee under HIPA, and how to determine if they are one.

Determining if a Physician is a Trustee under The Health Information Protection Act

For physicians to determine if they are a trustee, they should consider the following questions, 1) are they an employee, and 2.) do they have custody or control of the personal health information they collect?

Is the physician an employee of a Trustee? (see the definition of trustee in the Glossary) If so, the physician is not a trustee. If the physician is an employee of a non-trustee such as a private company the physician should consider whether he/she has custody or control of the personal health information.

If the physician is an employee of a trustee, the physician does not need to put in place a privacy program in accordance with the HIPA. They would however still need to be aware of and meet the obligations contained within HIPA. They would also be expected to be aware of and follow all of the trustees' privacy policies and procedures. The Bylaws of the College of Physicians and Surgeons of Saskatchewan College require if there is a privacy policy available at a practice location, the physicians who work at that practice location should read and be familiar with that privacy policy.

Does the physician have custody of personal health information? Custody refers to the guardianship or care of the personal health information beyond the period of providing care. If the physician were to leave the current location of practice could he/she take the records or a copy of them to a new practice location? If a physician enters into an agreement with another trustee to leave the records at the original practice it does not minimize the responsibilities of the physician as a trustee while still practicing at that location.

a) If the physician has custody or control of the personal health information then the physician is a trustee and must meet the requirements of HIPA.

b) If the physician does not have custody or control of the personal health information then the responsibility to ensure the privacy and security of the personal health information belongs to the trustee with custody or control, such as a regional health authority. This does not negate however the physician's obligations under HIPA with respect to the personal health information.

Does the physician have responsibility for, or control of, the personal health information that has been placed under the guardianship of someone who is not a trustee, such as an EMR vendor or storage facility?

- If yes, then the physician is a trustee and must meet the requirements of HIPA.
- If the physician does not have control of the personal health information, or custody of it, then the physician is not a trustee. Such would be the case when a physician transfers records to another trustee or a designated archive.

Determining Accountability in a Group Medical Practice

It is very common for a group of physicians to establish a group practice, whether it is a legal entity or a group of physicians in a shared space using some common services. In a group practice each physician is a trustee. In many of these practices all resources of the practice are shared, including employees and management of the EMR and, in some practices, the actual EMR records are shared.

Physician-trustees must determine if they have sole custody or control of their patients' records or if this responsibility is shared with the other physician-trustees in the practice. Two questions to consider are:

1. Does each physician have his/her own EMR or a separate patient list within a common EMR?
2. Do employees, medical students and residents, work for just one physician?

If the answers to these questions are yes then each physician-trustee is solely accountable for the personal health information under his/her custody or control and must meet his/her duties under HIPA.

Where several physician-trustees in one medical practice each have their own separate database within the EMR and accordingly, sole custody or control of their patient's personal health information there is an expectation that they develop common approaches to protecting the personal health information, including a single policy manual for the entire practice.

Where several physicians in one medical practice share a single, common database within the EMR, it is essential the physicians develop a common approach to protecting the personal health information and develop a single policy manual for the entire practice.

Responsibilities of Trustees

It is important to determine the trustee model at each clinic. The type of model will influence the privacy accountabilities for each trustee. The following describes the responsibilities of each model of trustee.

A sole practitioner

- A complete set of privacy policies
- No clinic exit agreement is required; however there should be a policy with procedures to follow when the physician ceases to practice at that location that is consistent with their legal responsibilities and the CPSS Bylaws and guidelines.
- No information sharing agreement internal to the clinic is required.
- Education of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.
- Confidentiality agreements signed with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.
- IMSP Agreements required with
    - EMR Vendor
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist

- Telephone answering service

- Agreements requiring a privacy clause or schedule
  - Landlord
  - Cleaners
  - Other third parties who may have access to personal health information

Physicians in a group practice

- Complete set of common privacy policies including a clinic-information sharing agreement or an understanding of how information is shared within the clinic and included at the beginning of the clinic policy manual and signed by all trustees at the clinic.

- Clinic exit agreement signed by all physicians and any other health professional who has patient records at the clinic. Example - physiotherapist. If this is addressed in another practice agreement the physicians may have the clinic exit agreement will not be necessary. The policy manual should identify the elements of the clinic exit agreement and what agreement the trustees sign to cover them.

- Education of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.

- Confidentiality agreements with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.

- IMSP Agreements required with
  - EMR Vendor
  - IT support company
  - Storage company
  - Shredding company
  - Transcriptionist
  - Telephone answering service

  - Agreements requiring a privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

A physician in a group medical corporation, partnership or other legally recognized entity

If the medical corporation is a sole practitioner he/she should implement to the responsibilities of the sole practitioner.

If the medical corporation is a group practice or a group of physicians who are each incorporated they should implement:

- A complete set of common privacy policies including a clinic-information sharing agreement or statement of how information is shared within the clinic and included at the beginning of the clinic policy manual and signed by all trustees at the clinic.

- Clinic exit agreement signed by all physicians and any other health professional who has patient records at the clinic. Example - physiotherapist. If this is addressed in another practice agreement the physicians may have the clinic exit agreement will not be necessary. The policy manual should identify the elements of the clinic exit agreement and what agreement the trustees sign to cover them.

- Education of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.

- Confidentiality agreements with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.

- IMSP Agreements required with
    - EMR Vendor
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service

    - Agreements requiring privacy clause or schedule
        - Landlord
        - Cleaners
        - Other third parties who may have access to personal health information

A contract physician

A physician who is on contract with another trustee, such as a regional health authority, may or may not be a trustee depending on the custody or control of the information. A physician, whose contract gives him/her responsibilities for the personal health information, including responsibilities when the physician ceases to practice on contract should be considered a trustee. He/she should have in place:

- Complete set of privacy policies with consideration of the policies and procedures of the trustee that holds the contract.

- Clinic exit agreement with the other trustee.

- Information sharing agreement with the trustee that holds the contract (e.g.: regional health authority).

- Education of employees, medical students and residents on the clinic policies and procedures, and their responsibilities.

- Confidentiality agreements with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.

- IMSP Agreements required with
    - EMR Vendor
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service
  - Agreements requiring privacy clause or schedule
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

A physician who does not have custody or control of the personal health information he/she collects, uses or discloses is not considered a trustee but is required by CPSS Bylaw 23.3 to read and be familiar with the privacy policy of the trustee of the location(s) where the physician practices.

A physician whose office is located on the premises of another trustee, such as a regional health authority, and from whom the physician avails many benefits such as IMSP services and provision of hardware:

- Complete set of privacy policies with consideration of the policies and procedures of the trustee that is the landlord.

- Information sharing agreement with the trustee who is the trustee-landlord.

- Education of employees, medical students and residents on the clinic policies and procedures and their responsibilities.

- Confidentiality agreements with employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.

- IMSP Agreements required if not covered by the trustee-landlord
    - EMR Vendor
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service

  - Agreements requiring privacy clause or schedule
    - Landlord
    - Cleaners

- Other third parties who may have access to personal health information may have access to personal health information

A physician who practices at more than one location, sometimes as a trustee and other times on contract or as a primary care physician

A physician can be a trustee at one location and a non-trustee at another location. At the locations where the physician is not a trustee he/she is responsible for reading, being familiar with, and complying with the policies and procedures of the trustee at that location.

A physician who is an employee at a medical clinic owned and operated by a non-trustee.

The physician is the trustee if a written agreement with the clinic allows the physician to take a copy of their records when he/she leaves the clinic, and the agreement gives the physician responsibility for the personal health information he/she collects, uses and discloses and for recognizing patients' rights in relation to their information.

If the employer (non - trustee) has custody or control of the records of personal health information, the management and protection of the records is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA). The policies and procedures in the Privacy Resource Materials can be followed to meet the requirements of PIPEDA **with the exception of deemed consent**, which is not authorized.

Note: What follows is best practice and recommended. The physician if not deemed as the trustee should work to ensure these best practices are implemented. If they are the trustee however, they would have responsibilities to ensure these recommended practices are implemented.

- A complete set of privacy policies must be in place. If the non-trustee has policies and procedures for the clinic the physician should approve them or make the necessary amendments.
- Clinic exit agreement signed with the non-trustee owner.
- Information sharing agreement with the non-trustee detailing the responsibilities of both parties.
- Physician has an obligation to ensure the non-trustee educates employees, medical students and residents, on the policies and procedures and their responsibilities.
- Physician has an obligation to ensure the non-trustee has signed confidentiality agreements with employees, medical students and residents, other health professionals working in the clinic, and third parties.
- Physician should strongly encourage the non-trustee to have:
  1) IMSP Agreements with:

- EMR Vendor
- IT support company
- Storage company
- Shredding company
- Transcriptionist
- Telephone answering service

2) Agreements requiring a privacy clause or schedule

- Landlord
- Cleaners
- Other third parties who may have access to personal health information

A physician - trustee working with a physician employed by another trustee, such as a regional health authority

The physician-trustee should enter into an agreement with the other trustee to clarify or establish who the trustee of the records is at the beginning of the relationship.

- If the physician is the trustee, he/she should develop a complete set of privacy policies with consideration of the policies and procedures of the other trustee.

- Clinic exit agreement signed by all physicians and any other health professional who has patient records at the clinic.

- Information sharing agreement with the trustee (ex: regional health authority) should state:
  - Who is responsible for the education of employees, medical students and residents, on policies and procedures and their responsibilities.
  - Who is responsible for ensuring confidentiality agreements are signed by the employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.

- IMSP Agreements required with
    - EMR Vendor
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service
  - Agreements requiring a privacy clause or schedule if not covered by the other trustee
    - Landlord
    - Cleaners
    - Other third parties who may have access to personal health information

Community Clinic

The matter of trusteeship, accountability and custody must be clearly documented and agreed to by all regulated health professionals at the Community Clinic who could be considered a trustee.

- A complete set of common privacy policies must be in place. If the clinic's trustee is a regional health authority the policies must take into consideration the region's policies and procedures.

- Clinic exit agreement signed with the trustee.

- If there is more than one trustee, an information sharing agreement is signed detailing the responsibilities of the trustees
    - The agreement should state who is responsible for the education of employees, medical students and residents, on policies and procedures and their responsibilities.
    - The agreement should state who is responsible for ensuring confidentiality agreements are signed by the employees, medical students and residents, other health professionals working in the clinic, and third parties who have access to personal health information.

- IMSP Agreements are in place with
    - EMR Vendor
    - IT support company
    - Storage company
    - Shredding company
    - Transcriptionist
    - Telephone answering service

    - Agreements requiring a privacy clause or schedule
        - Landlord
        - Cleaners
        - Other third parties who may have access to personal health information

Other Trustees

During the time a trustee has custody or control of personal health information he/she may collect personal health information from or disclose personal health information to other people or organizations. It is important to know if the other person or organization is a trustee under HIPA, as the responsibilities of collecting from or disclosing to a non-trustee are more stringent. There is more information about non-trustees in the guidelines for collection and disclosure.

The following are trustees under HIPA if they have custody or control of personal health information

- Ministry of Health and all government institutions,
- licensed health professionals and their professional regulating bodies,

- hospitals,
- pharmacies,
- laboratories,
- nursing homes and long-term care facilities,
- homes for the aged and homes for special care,
- community care clinics,
- ambulance services, and
- regional health authorities (health regions) or health care organizations.

Trustees in the Electronic Health Record as of October 1, 2012

As the Electronic Health Record (EHR) becomes operational in Saskatchewan and there is a seamless flow of personal health information between the EMR and the EHR, physicians should understand who the trustees of EHR systems are. As of October 1, 2012 the trustees of the EHR systems are

- Pharmaceutical Information Program (PIP) Trustee is the Ministry of Health
- Saskatchewan Laboratory Results Repository (SLRR) Source Trustees are the regional health authorities and the Ministry of Health
- Radiology Information System (RIS) and Picture Archiving and Communications System (PACS) Source Trustees are the regional health authorities.

Custody or Control

A physician has to have custody or control of personal health information to be a trustee under HIPA.

Indirectly Collected Personal Health Information

In general, having custody or control of personal health information does not apply only to personal health information the physician-trustee collected from the patient but also to personal health information that has de facto become part of the physician's information holdings.

When a physician-trustee receives reports, test results and other personal health information about a patient from another physician, trustee or person, that information is considered part of the patient's record. The physician-trustee is considered to be in custody or control of this indirectly collected personal health information and is responsible for the protection of this information, just as if it had been collected directly from the patient.

Personal Health Information in the Control of the Physician-Trustees

Control refers to having the power or authority to manage, restrict, regulate or administer the collection, use or disclosure of the record.

When a physician-trustee contracts with another organization to process, store, or destroy patient information the physician-trustee remains responsible for the privacy of that information.

Further, if the physician has asked a non-trustee to manage personal health information, it does not alleviate the physician from the responsibility of ensuring that the third party non-trustee continues to protect the personal health information.

When personal health information is disclosed by the physician-trustee to another trustee for the purpose of providing health care or another disclosure authorized by HIPA, the trustee receiving the personal health information will become responsible for the protection of the information once it is within its custody or control.

Personal Health Information as defined in HIPA

(HIPA s. 2(m), 3)

The Health Information Protection Act gives a clear definition of what is personal health information and in addition states what is not considered 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**
- **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**

HIPA does not apply to the following information

- **statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified**
- **personal health information about an individual who has been dead for more than 30 years or**
- **records that are more than 120 years old**

Other Relevant Legislation

(HIPA s4(4))

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is the federal legislation that applies to the collection, use and disclosure of personal information and personal health information by organizations that are involved in a "commercial activity". Independent medical clinics are considered a commercial activity. As a result, physician-trustees in Saskatchewan who are engaged in commercial activities are governed by both HIPA and PIPEDA.

The Privacy Commissioner of Canada and the Saskatchewan Office of the Information and Privacy Commissioner have agreed to a protocol providing that complaints received by the federal Privacy Commissioner under PIPEDA regarding HIPA trustees will be referred to Saskatchewan's Commissioner for investigation under HIPA as the primary instrument for compliance. As a result, while HIPA and PIPEDA will continue to apply generally, the primary means of enforcing individual privacy rights will focus on HIPA rather than PIPEDA.

This Reference Manual concentrates on the requirements under HIPA. For the most part, if physician-trustees meet the requirements of HIPA they will also be in compliance with PIPEDA. The most notable difference is that PIPEDA does not allow for the disclosure of personal health information based on deemed consent.

Saskatchewan Legislation

There are several other Acts which require physician-trustees to collect, use and disclose personal health information in a manner not addressed in HIPA.

Personal health information obtained for the purposes of the following Acts are not subject to Parts II (Rights of the Individual), IV (Limits on Collection, Use, and Disclosure) and V (Access of Individuals to Personal Health Information) of HIPA:

- *The Adoption Act* or *The Adoption Act, 1998*
- Part VIII of *The Automobile Accident Insurance Act*
- *The Child and Family Services Act*
- *The Mental Health Services Act*
- *The Public Disclosure Act*
- *The Public Health Act, 1994*
- *The Vital Statistics Act, 2009* or any former *Vital Statistics Act*
- *The Vital Statistics Administration Transfer Act*
- *The Workers' Compensation Act, 1979*
- *The Youth Drug Detoxification and Stabilization Act*; or
- Any prescribed Act or regulation or any prescribed provision of an Act or regulation.

If a physician-trustee collects, uses or discloses personal health information in accordance with any of these Acts, consideration should be given to including appropriate procedures in the medical practice's policies and procedures.

Part I (Preliminary Matters), Part III (Duty of Trustee to Protect Personal Health Information), Part VI (Review and Appeal), Part VII (Commissioner) and Part VIII (General) of HIPA **Jig,** apply to personal health information obtained under the authority of these Acts.

Role of the Privacy Officer and Medical Office Administrator

(HIPA ss. 16, 23(2) and 58.3, CPSS Bylaw 23.2(c)(i))

The term "privacy officer' is not used in HIPA but **the Act does require a trustee to designate a person to make decisions or form opinions required under HIPA**. The term privacy officer is the one most consistently used across Canada to refer to this person.

There are several factors to consider when designating a privacy officer at a medical practice.

- The College of Physicians and Surgeons of Saskatchewan recommends that the privacy officer be a physician.

- Physicians in a group practice can select one of the physician-trustees to act as the privacy officer for all of them.
    - The appointed person should be, or become, knowledgeable on HIPA and privacy best practices.

- If one physician is appointed as the privacy officer in a group practice, this does not negate the other physician-trustees in the practice from their legal obligations under HIPA.

- If one physician is appointed privacy officer, all physicians are expected to agree to the policies and procedures of the medical practice and be aware of how to comply with the procedures.

- A physician-trustee can appoint a non-physician to assist in the privacy activities of the practice. This person is normally the senior office administrator.

- Large clinics may appoint the senior administrative person to be the privacy officer because of the large number of administrative functions undertaken by this individual. The physician-trustees in the practice will still have legal obligations under HIPA and be responsible for decisions with respect to the personal health information they have custody and control of.

Typical Responsibilities

The privacy officer has many responsibilities under HIPA. Whether the physician-trustee takes on these responsibilities him/herself or shares them with the medical office administrator, it is recommended that these responsibilities be documented.

- Developing and maintaining practices that ensure compliance with clinic policies and that those policies are in compliance with law and professional standards of practice, including

  - Establishing policies and procedures to maintain administrative, technical, and physical safeguards for the protection of personal health information.
  - Developing and managing the process for patients:
    - requesting access to their own records, including fees
    - requesting an amendment to their records
    - inquiring about the clinic's policies and procedures.

- Trustees should consider that their responsibility to ensure compliance includes all health professionals, employees, medical students and residents, and third parties such as transcriptionists and telephone answering services.

- The usual way of ensuring compliance is to be sure health professionals, employees, medical students and residents are aware of the clinic's policies through awareness activities, education, and training, including orientation for all new employees, medical students and residents.

- Both CPSS and the Information and Privacy Commissioner of Saskatchewan recommend all health professionals, employees, medical students and residents sign a confidentiality or non-disclosure agreement annually.

- Maintaining up-to-date records of all information holdings of the medical practice, including paper records, electronic records, disease-specific registries, clinical trial records, records in storage and others.

- Maintaining a record of when and how personal health information is destroyed.

- Maintaining a breach management plan including procedures to notify patients of a breach or suspected breach of their personal health information.

- Ensuring reasonable safeguards are in place and enforced.

- Ensuring the privacy officer is knowledgeable and up to date on HIPA and good privacy practices for personal health information and can provide advice to physicians, employees, other health professionals, and third parties.

- Identifying when written agreements are necessary to ensure the continued privacy protection of personal health information that is provided to an information management service provider (IMSP) or disclosed to a third party.

- Maintaining a record of clinic exit agreements, information sharing agreements, vendor contracts, and other documentation required under HIPA or considered good privacy practices.

- Ensuring all research requests are assessed for any privacy risks, that the research proposal has been approved by a research ethics committee approved by the Saskatchewan Ministry of Health and that all other

requirements under section 29 of HIPA are met. This includes research projects conducted by private sector organizations, such as a clinical trial.

Obligations of Health Professionals, Employees, Medical Students and Residents

(HIPA s. 9, 16, 35, 61, CPSS Bylaw 23.2(c)(ii)(iii))

This guideline applies to health professionals, employees, medical students and residents who collect, use, and disclose personal health information on behalf of the physician-trustees. **Physician-trustees are required to ensure employees comply with HIPA and the physician-trustee's policies and procedures.**

Physicians can meet this responsibility by

- Developing a policy and procedures manual (policy manual);
- Ensuring all employees are educated to increase their understanding of HIPA and the policies and procedures;
- Ensuring employees who handle personal health information are trained on the specific procedures that apply to their work;
- Ensuring all employees has signed a confidentiality agreement.

Obligations of Health Professionals, Employees, Medical Students and Residents

Health professionals, employees, medical students and residents are responsible for

- Reading the policy manual and asking for clarifications on procedures they do not understand;
- Participating in all privacy and security education and training as requested by the physician-trustee;
- Ensuring the protection and security of personal information they collect, use, and disclose.

Health professionals, employees, medical students and residents who do not comply with this policy can be subject to employment discipline, contractual remedies or professional discipline.

Confidentiality Agreement

The CPSS recommends that physician-trustees have a confidentiality agreement that health professionals, employees, medical students and residents are required to sign. The confidentiality agreement is a commitment by health professionals, employees, medical students and residents to adhere to the policy manual and HIPA. It also helps them to maintain awareness of their obligations with respect to the protection of personal health information.

- The confidentiality agreement should be signed at regular intervals and as a condition of employment for all new employees, and engagement of health professionals, medical students and residents. CPSS and the Office of the Information and Privacy Commissioner recommend that confidentiality agreements be signed annually.

- New employees, health professionals, medical students and residents should sign the confidentiality agreement before they are provided with access to personal health information.

- Current health professionals (both those considered as trustees and those not), employees, medical students and residents should be asked to sign the confidentiality agreement when they are first provided with, and have read the medical practice's policy manual.

- Trustees should ensure that any third parties that they have contracted have a signed confidentiality agreement in place prior to any services being rendered.

- The confidentiality agreement signed by employees should be held in their personnel file.

- The confidentiality agreement signed by health professionals and third parties should be stored with other documents related to their engagement with the clinic.

- The confidentiality agreement should include a commitment or understanding that
    - Personal health information is only accessed, used, and disclosed by authorized employees and on a need to know basis;
    - All personal health information is covered, whether verbal or written;
    - Assistance will be provided to patients requesting access to their own personal health information, requesting an amendment to a record, or clarification of the medical practice's privacy and security practices. Employees will follow clinic procedures and third parties will follow contractual obligations;
    - All actual, suspected and potential privacy or security breaches will be reported immediately;
    - Failure to comply with the terms of the confidentiality agreement could lead to disciplinary action, up to and including termination, withdrawal of privileges, termination of contract, or professional sanctions;
    - The confidentiality agreement survives the individual's employment or association with the medical practice.

Acceptable Use Agreements

- Physicians and employees who are granted access to the EMR and the office computer should sign an acceptable use agreement before they are given a user account which could be a user name and password or some other method of user authentication such as a key card.

- The user account is equivalent to a signature and should not be shared or disclosed to any other physician, employee, health professional, third party, or anyone outside the clinic.

- The EMR should record all users' actions (searches, views, entries, edits, etc.) in an audit log. Regular reviews of the audit log should be conducted without notice.

Privacy and Security Awareness, Education, and Training

(HIPA s. 16)

An important part of a privacy and security program in a medical practice is making best efforts to ensure trustees, health professionals, employees, medical students and residents know the policies and procedures and understand their obligation to follow them. Knowledgeable trustees, health professionals, employees, medical students and residents are better at:

- Managing personal health information consistently and in compliance with HIPA;
- Responding positively and in an effective manner when patients make requests for access, amendment or masking of personal health information:
- Avoiding and identifying privacy and security breaches.

Awareness Activities

- Making available high-level information about the legal requirement to protect personal health information and about the medical practice's policies and procedures.

- Ongoing awareness activities contribute to a culture of privacy at the practice. Examples of awareness activities include:
  - Posting a news article about a privacy breach on a employees bulletin board;
  - Distributing buttons to employees that say, "We respect your privacy".

Employee, Health Professional, and Medical Students and Residents' Education Activities

- Providing education sessions or reading the medical practice's policy manual to gain knowledge about how they should protect personal health information.

- Responding to questions about how they should follow the procedures.

- Continuing education as new procedures are developed or existing ones revised.

- Providing information at employees meetings or at specially designated workshops.

- Inviting guest speakers to employees meetings, such as a privacy officer from a hospital, long-term care facility, or another medical practice with which personal health information is regularly shared.

Employee training

Some policies and procedures require more detailed instruction, such as new procedures for faxing. Training on specific activities should be conducted for those who need to know it for their job or as support for the person doing the work.

- Specific training should be given on the following:
  - Faxing and emailing,
  - Scanning,
  - Managing consent directives,
  - Managing patient requests for access to, or amendment of, their personal health information,
  - Responding to breaches of personal health information,
  - Storing paper records,
  - Destruction of records,
  - Acceptable uses of technology.

New Employees, Health Professionals, Medical Students and Residents

All new employees should receive privacy and security orientation before being given a username and password for the EMR. The new employee could be given the clinic's privacy and security policy manual to read before the start date. The orientation, which should be offered by the privacy officer or medical office administrator, will then involve reviewing and clarifying the policy manual and providing training on the procedures specific to the new employee's responsibilities.

New health professionals, employees, medical students and residents should receive privacy and security orientation before being asked to sign the confidentiality agreement and the acceptable use agreement if applicable.

Accuracy and Integrity of Personal Health Information

(HIPA s. 16, 25(3), CPSS Bylaw 23.1(a)(b)(d), 23.2(c)(x))

Physicians have a responsibility to their patients to take reasonable steps to ensure the personal health information in their custody or control is accurate and complete, and its integrity is preserved.

Bylaw 23.1 states that all members of the CPSS shall keep, as a minimum requirement, the following records in connection with their practice:

- 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;

- In respect of each patient contact, a legibly written or typewritten record setting out:
    - The date that the member sees the patient.
    - 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 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,
    - The patient record should include every report received respecting a patient from another member or other health professional,
    - The records are to be kept in a systematic manner,
    - The records must be completed in a timely manner.

Steps physicians can take to improve the accuracy of the information they collect include:

- Be written in clear language with only common abbreviations used,
- Document current information on the care and condition of the patient as soon as possible, ideally at the time of the appointment or later the same day,
- Record the date, time, and the name of the author,
- Make additions and corrections in a manner that allows the original information to still be read,
- Ensuring scanned documents and photocopies are complete and readable,
- Train employees on how to keep accurate records.

Physicians are also responsible for the integrity of their patients' records, where integrity is 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. The preservation of the records' content is maintained throughout storage, use, transfer and retrieval so that there is

confidence that the information has not been tampered with or modified other than as authorized.

Steps physicians can take to protect the integrity of the personal health information include:

- Accurate recording of the personal health information,
- Accurate scanning and photocopier of personal health information,
- Perform daily backups and periodically confirm the reliability of the backups,
- Secure and environmentally safe storage,
- Auditing of accesses to personal health information,
- Use of up-to-date security software.

Identifying Purposes and Openness

(HIPA s. 9, 10, 16, 24)

Physician-trustees have significant responsibility to be transparent on how they manage their patients' personal health information.

HIPA gives patients the right to be informed on the anticipated uses and disclosures of their personal health information at the time the information is collected. The Act also requires that patients be informed of their right of access to their personal health information and to request amendments where there are errors and omissions, and, , the right to consent to the collection, use, and disclosure of their personal health information, subject to some exceptions, in accordance with HIPA.

The general principle of openness is that it will be easy for patients to be aware of the privacy practices of any trustee collecting, using, and disclosing their personal health information and their rights under HIPA. This information will help patients achieve a greater degree of comfort that their privacy will be protected.

There are several ways a physician-trustee can meet the expectations of openness:

- Discussing the purpose for collecting the information
- Discussing the clinic's privacy practices,
- Displaying a poster in a spot that is easily seen by patients before or when their personal health information is being collected,
- Making a pamphlet available where personal health information is collected,
- Posting the information on the medical practice's website.

The information that should be made available includes:

- Contact information for the privacy officer and/or medical office administrator,
- A description of the physician-trustee's information practices, including the purposes for collection,
- A description of the anticipated uses and disclosures of the information,
- Contact information for the Office of the Information and Privacy Commissioner of Saskatchewan,
- An explanation of the patient's right to access and request amendment of their own personal health information.
- The patient's right to manage consent through masking or alternative methods agreed to by the patient and the physician.

To meet these requirements physicians-trustees can display the posters available from the Saskatchewan EMR Program or the SMA. This should be supplemented by making available to patients the Ministry of Health's pamphlet on HIPA which can be order by calling the Ministry at 1-306-787-2137 or emailing: HIPAFOIhelp@health.gov.sk.ca.

Challenging Compliance/Patient Complaint Process

(PIPEDA Schedule 1)

It is important that physicians' accountability to their patients extends to how they manage complaints from patients and challenges to how the clinic adheres to its written policies. This is **mandatory** activity **under the *Personal Information Protection and Electronic Documents Act*** and highly recommended by the Office of the Information and Privacy Commissioner of Saskatchewan.

- A clinic's complaints process will work best if it is known to all physicians, health professionals, employees, medical students and residents. This means a complaint can be received by anyone at the clinic. The person contacted by the patient about the issue should document and date the complaint.

- One person in the clinic should be assigned the responsibility for receiving and investigating complaints. This will probably be the privacy officer or the medical office administrator.

- The clinic policy should state that all complaints will be investigated.

- A patient should be informed at the time of the complaint that he or she can contact the Office of the Information and Privacy Commissioner of Saskatchewan and/or the professional regulatory body if the complaint is about a regulated health professional.

- A complaint investigation process should also include recommendations for how to avoid a similar type incident.

- Types of complaints include:
    - Reporting of an actual, suspected or potential breach,
    - Failing to comply with the clinic's policies and procedures.

Ceasing to Practice or Leaving a Medical Practice

(HIPA s. 22, Regulations Section 4 (1), CPSS Bylaw 23(1)(g))

Personal health information must continue to be protected after a physician-trustee ceases to practice or leaves a practice.

CPSS requires physicians to notify patients when ceasing to practice, or moving the location of their practice, by placing a notice within the clinic and a newspaper advertisement indicating when the transfer to the new trustee, or location, will take place and the contact information for the new trustee or location. If the new trustee is at the same medical practice no notice is required.

Ceasing to Practice as a Trustee

The most common examples of ceasing to be a trustee are retirement, relocating to another province or country, and transferring to a staff position. **A physician-trustee who ceases to practice, or ceases to practice as a trustee, must make arrangements to transfer the custody and control of patient records to another trustee or a designated archive. The designated archives are not required to accept personal health information from another trustee.**

CPSS Bylaw

The CPSS Medical Records Bylaw 23.1 states that

- A member who ceases to practice shall:
  - transfer the records to a member with the same address and telephone number; or
  - transfer the records to:
    - another member practicing in the locality; or
    - a medical records department of a health care facility; or
    - a secure storage area with a person designated to allow physicians and patients reasonable access to the records.

Physicians are also required to notify patients of the transfer through a newspaper advertisement, a poster at the clinic, or other reasonable method of notification.

Designated Archives

- **Affiliates (as defined in *The Regional Health Services Act*).** For example, affiliates include organizations such as All Nations Healing Hospital, Regina Pioneer Village Ltd. and Sherbrooke Community Centre. A complete list of designated affiliates in Saskatchewan can be found at: http://www.saho.org/portal.jsp?y3uQUnbK9L2RmSZs02CjVwr9HGVsNebc3OzcFXGKKWFGZaWhY+yDdA==
- **Ministry of Health**

- **Health professional bodies that regulate members of a health profession pursuant to an Act (such as the College of Physicians and Surgeons of Saskatchewan)**
- **Regional Health Authorities**
- **Saskatchewan Archives Board**
- **eHealth Saskatchewan (formerly the Saskatchewan Health Information Network)**
- **University of Saskatchewan Archives**
- **University of Regina Archives**

When a Physician-Trustee Dies

When a Physician-Trustee dies the personal representative of the physician is required to ensure the duties of HIPA continue to be met until the personal representative transfers custody and control of the records to another trustee or a designated archive.

Failure to Transfer Records to Another Trustee

When a former trustee fails to carry out the duties required under HIPA, the Minister of Health may appoint a person or body to act in place of the former trustee until custody and control of the personal health information is transferred to another trustee or a designated archive.

When a Physician-Trustee Leaves a Practice

If a physician-trustee leaves a medical practice to join another practice, proper notice should be given to the other physicians in the practice and a notice to patients should be posted in the clinic. The physicians should agree on how the exiting physician's patient records will be transferred to the other medical practice. These details should be included in documentation that all physicians in the medical practice agree to. It could be in the partners' agreement or a Clinic Exit Agreement.

The purpose of the agreement is to have a transition plan in place when a physician leaves a practice. The transition plan should include:

- Giving 30 or more days' notice,
- Managing the costs associated with the implementation and operation of the EMR,
- Managing the records in the EMR and any paper records associated with the leaving physician, specifically:
    - Retaining EMR records in a shared database at the originating clinic and the leaving physician can take a copy at a fair cost agreed to by all the physicians in the transition plan,
    - Transferring EMR records in a database only used by the leaving physician to the leaving physician, with cost assigned to the leaving physician,

- Cooperating with the leaving physician and the EMR vendor to facilitate a smooth transfer,
- Complying with any technical, security or other protocols in the medical practice's policy manual,
- Encouraging the EMR vendor to release the leaving physician from any contracts entered into between the medical practice and the EMR vendor.
- Physicians should not take records outside Canada.

For more information on transferring records please see the CPSS Guideline on the Transfer of Records in Appendix A or http://www.quadrant.net/cpss/resource/records.html.

PATIENT RIGHTS

Text in bold is required by HIPA

Patient Access to Their Own Information

(HIPA ss. 12, 31 – 39, 42, CPSS Bylaw 23.2(c)(v))

HIPA confirms patients' rights in legislation to have access to their own information and establishes further direction on the management of patients' access requests. Patients are entitled to examine and obtain a copy of all information in their medical record, with very limited exceptions. This includes information prepared by other physicians included in the record.

Review of Current Practices

Physician-trustees who currently have established procedures for providing patients access to, and copies of, their medical record, will probably be able to follow the same procedures.

Privacy officers should incorporate into the medical practice's procedures the legislated timelines within which patients must receive access to, or a copy of, their own information.

Access Request Form

Physician can still provide patients with copies of reports without following the formal process set out in HIPA if the information requested is provided at the time of the request.

Physician-trustees should have a standard application form for patients to use to request access to their own information. The form should include all information the physician needs to find the correct information and a place to record that proper identification of the patient has taken place.

All written requests should be dated clearly with the date the request is received and if the request form is incomplete the date it is completed.

A patient may request access to their records verbally. The staff should then fill in the form on the patient's behalf.

Copies of information given to patients should be clearly marked "patient copy".

Requirements under HIPA

A patient may make a request for access to personal health information either verbally or in writing.

The physician-trustee must confirm the identity of the patient making the request, or have reasonable grounds to believe the patient is who they say they are, as may be the case if the requestor is a regular patient.

A physician-trustee may charge a reasonable fee to recover costs for providing access to personal health information.

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) ofthe HIPA, in which a patient may be denied access to all or part of their medical record.

The cost estimate should include the flat fee, the cost per page for copying and the physician's time to review the record, if applicable. This estimate should be provided to the patient before preparing the copy. It is recommended that this be a detailed cost estimate if the fee will be greater than $20.00.

Consider the patient's ability to pay when establishing the fee to be charged, including a complete waiver of fees. The patient may also ask for a fee waiver.

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.

A written request must have enough detail to enable the physician-trustee to identify the personal health information requested.

A patient is not required to explain why the request is being made but the application form can include a request for this information as it will help in preparing the information for the patient.

When the request is written, the physician-trustee must respond to the request for access to the personal health information within 30 calendar days.

On request of the patient, the physician-trustee must:

- **Provide an explanation of any term, code or abbreviation used in the record; or**

- **If the physician is unable to explain any terms, codes or abbreviations, refer the patient to another trustee that is able to provide an explanation.**

IfAnother Trustee has Custody or Control of the Information

A physician who does not have custody or control of the personal health information requested by a patient, but is aware that it is in the custody or control of another trustee:

- **May transfer the written request for access to the other trustee.**
- **Must notify the patient of the transfer as soon as reasonably possible.**
- **The trustee to whom the written request for access was transferred must respond within 30 calendar days after the date of transfer of the request.**

Refusing Access

A physician-trustee may refuse to give the patient access to all or some of the requested personal health information if

- **In the opinion of the physician, knowledge of the information could reasonably be expected to endanger the mental or physical health or safety of the patient or another person (HIPAs38(1)(c)(a)).**
- **Providing access would reveal personal health information about another person who has not expressly consented to the disclosure of the information to the person requesting it (HIPA s38(1)(c)(b)).**
- **Providing access could reasonably be expected to reveal 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 s38(1)(c)(c)).**
- **When the record contains information which the physician-trustee has determined should not be released to the patient, that information must be severed from the record and the remaining information provided to the patient.**
- Information should be severed by printing or photocopying the page with the information to be severed. On the page strike out the information to be severed with a black marker. Photocopy the marked page to ensure the severed information is not visible through the mark [2]. Write the section of HIPA that authorizes the withholding of the information beside the severed information.

A physician-trustee may also refuse to give the patient access to all or some of the requested personal health information if

[2] See the guidelines from the Office of the Information and Privacy Commissioner on severing at http://www.oipc.sk.ca/Resources/BBL%20Severing%20presentation%20March25%202009%20for%20participants.pdf)

- **The information was collected in anticipation of, or for use in, a civil, criminal or quasi-judicial proceeding;**

- **Disclosure of the information could interfere with a lawful investigation or be injurious to the enforcement of an Act or regulation;**

- **It was collected and used solely for (HIPA s38(1)(c)(d))**
  - **Peer review by health professionals**
  - **Review by a standards or quality of care committee studying or evaluating health services**
  - **A health professional body for discipline or quality of care purposes**
  - **When access is denied for one of these reasons, the physician-trustee must refer the patient to the trustees from which the personal health information was originally collected.**

A written explanation of the refusal to provide all or some of the requested record must be given to the patient before the 30th calendar day after receipt of the request, and include the HIPA reference that allows for the refusal. The patient that made the request must also be informed of his or her right to request a review of the refusal by the privacy commissioner pursuant to Part VI of HIPA.

Timeline for Responding to an Access Request

A physician-trustee must respond to a written access request from a patient within 30 calendar days.

A failure to respond within 30 calendar days is considered a refusal to grant access unless the patient has been notified that there has been an extension of an additional 30 calendar days.

The extension of an additional 30 calendar days is allowed by HIPA when:

- **The request is for a large number of records.**

- **A large number of records need to be reviewed before responding.**

- **There is a large number of requests to be addressed within the same time period and meeting the 30 calendar days would unreasonably interfere with the operations of the medical practice.**

- **Consultations that are necessary to comply with the request cannot be completed within 30 calendar days.**

The patient must be notified in writing of the extension to the response period within 30 calendar days of the physician-trustee receiving the request.

It is recommended that the physician include information on how to contact the Office of the Information and Privacy Commissioner in the written response to the patient.

Patient May Appeal to the Information and Privacy Commissioner

If the patient has made a written request for access to his or her own personal health information and is not satisfied with the decision of the physician-trustee, the patient may apply to the Information and Privacy Commissioner for a review.

- **The application must be made within one year of the patient receiving notice of the physician-trustee's decision; or**

- **The application must be made within one year if there is no response from the physician-trustee after 30 calendar days from the initial request for access or 60 days if the physician trustee has provided notice of an extension.**

Physicians are expected to retain all information related to the request long enough for the patient to appeal a decision to the Office of the Information and Privacy Commissioner.

Patient Requests for Amendment of Their Record

(HIPA ss. 13, 40)

Physicians have, in most cases, followed patients' requests to correct or amend personal health information in their records. HIPA puts in law the physician-trustee responsibility to meet these patient requests.

Requests from Patients

Under HIPA patients have the right to request amendment of the personal health information in their own medical record when they believe that there is an error or omission in it.

- **The request for amendment must be in writing.**
- **The amendment must not destroy or obliterate existing information in the record, other than registration information.**
- The medical practice should provide the patient with a form that includes all the necessary details required by the practice to assess the request.
- All amendments should be dated and signed by the physician, or digitally dated and signed.

Responding to a Request for Amendment

The physician-trustee must respond in writing to the patient within 30 calendar days after the request for amendment is received to advise that either:

- **The amendment was made as requested or**
- **The amendment was not made but a notation has been made in the record.**
- The physician should include information on how to contact the Office of the Information and Privacy Commissioner in the written response to the patient.

Refusing a Request for Amendment

A physician-trustee may refuse to amend personal health information when the patient request relates to the physician's diagnosis or opinion.

- **Where a physician refuses to make a requested amendment, a notation must be made in the file indicating the information is under dispute by the patient.**

Providing Notice to Other Trustees

When a physician-trustee amends the patient's record or makes a notation that the information is under dispute, the physician-trustee must, when practical, give notice of the amendment or notation to any other trustee or person to whom the personal health information has been disclosed by the physician within the year previous to the request for amendment by the patient.

- **The physician-trustee does not have to send this notice of amendment or notation when there is no reasonable expectation that the amendment or notation will have an impact on the patient's ongoing health care or provision of services.**

- It is recommended that physicians provide notice to other trustees involved in the current care of the patient.

Receiving a Notice ofAmendment

A trustee that receives a notice of amendment or notation must make the same amendment or notation to any record in the trustee's custody or control that contains personal health information respecting the patient who requested the amendment.

Authorized Representatives and the Exercise of Rights by Others

(HIPA s. 15, 27 (4) (e) (i), 56, CPSS Bylaw 23.2(c)(vi))

Patient Designates

There are situations where a patient may have another person represent or make decisions on his or her behalf for care and treatment. HIPA provides the authority for a designate to make the same decisions for the patient regarding personal health information.

- **A patient may designate in writing another person to exercise on his/her behalf, any of the patient's rights or powers with respect to personal health information**.

Others Who May Exercise Rights

Where a person or organization seeks personal health information from a physician without patient consent, that person or organization should be able to refer the physician to the authority for the request.

The following people may also exercise the rights of the patient in regards to personal health information.

- **Where the patient is deceased, by the patient's personal representative if the exercise of the right or power relates to the administration of the patient's estate.**

- **Where a personal guardian has been appointed for the patient, by the guardian if the exercise of the right or power relates to the powers and duties of the guardian.**

- **Where the patient does not have the capacity to give consent:**
  - **By a person designated by the Minister of Community Resources and Employment if the patient is receiving services pursuant to *The Residential Services Act* or *The Rehabilitation Act*; or**
  - **By a person who, pursuant to *The Health Care Directives and Substitute Health Care Decision Makers Act*, is entitled to make a health care decision, as defined in that Act, on behalf of the patient.**

Decisions by, or on behalf of, a Minor

Any right or power conferred on an individual by HIPA may be exercised:

- **By an individual, including a patient, who is less than 18 years of age in situations where, in the opinion of the physician, the individual or patient understands the nature of the right or power and the consequences of exercising the right or power.**

- **Where the patient is less than 18 years of age, by the patient's legal custodian in situations where, in the opinion of the physician, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the patient.**

- The direction in HIPA allows physicians to disclose personal health information if they believe it would not constitute an unreasonable invasion of privacy. If there is any doubt or uncertainty as to whether the minor would consent, it is reasonable to conclude that it would be an invasion of privacy.

CONSENT, COLLECTION, USE, and DISCLOSURE

Text in bold is required by HIPA

Collection of Personal Health Information

(HIPA s. 6(2), 7, 19, 20, 23, 24, 25, 27, 28 and 29, CPSS Bylaw 23.2(c)(vii))

Whenever possible, the collection of personal health information shall occur with the consent of the patient to whom it relates.

- **Physicians must only collect personal health information that is reasonably necessary for the purpose for which it is being collected.**

- **The primary purpose for collecting personal health information is for the provision of health care, which includes any program, activity or service offered by the physician that can reasonably be expected to benefit the patient.**

- **A physician may collect personal health information under the authority of another Act, such *as The Mental Health Services Act* or *The Public Health Act, 1994*.**

- **When physicians collect personal health information they must take reasonable steps to ensure the information is accurate and complete.**

Types of Information Collected

- Identification and contact information, including
  - 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 including
  - Medical history
  - Presenting symptoms
  - Physical examination findings
  - Relevant medical history of family members
  - Test requisitions and results
  - 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)

Manner of Collection

Physicians must only collect personal health information that is reasonably necessary for the purpose for which it is being collected.

Physicians must collect the personal health information directly from the patient, except where:

- **The patient consents to the collection by a different method**
- **The patient is unable to provide the information**
- **The physician believes that collecting directly from the patient would prejudice the mental or physical health or safety of the patient or anyone else**
- **The information is collected, and is necessary for, determining or verifying the eligibility of the patient to participate in a program or receive a product from the physician.**
- **The information is available to the public**
- **The physician collects the personal health information from another trustee in accordance with HIPA**
- **The collection is from the patient about family members for the purpose of assembling a family health history; or**
- **Other circumstances that may be set out in the regulations to HIPA**

When a physician collects personal health information from another trustee and the information becomes part of the patient's record, this information is now considered to be in the custody or control of the collecting physician. The physician collecting the personal health information is accountable for the information in the patient's record.

Consent for Collection

Consent for the collection of personal health information is considered informed if the patient is provided with information to make a decision about the collection, which a reasonable person in the same circumstances would require.

Physicians may collect personal health information for any purpose with the consent of the patient.

A patient may revoke consent for the collection of personal health information.

- **A revocation is not retroactive.**

Collection for Other Purposes

Physicians may collect personal health information for another purpose as long as it is consistent with a purpose designated in HIPA. These purposes for collection include:

Health or Social Services

- **Arranging, assessing the need, providing, continuing to support health and social services for the patient**
- **Registering a patient in connection with**

  - **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**

Deceased Patients
- **In relation to the death of a patient, 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**

Programs
- **Planning, delivering, evaluating or monitoring a program of the physician**
- **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
- **In preparation for disclosure to another trustee or a designated archive who is a successor of the physician and the physician has made a reasonable attempt to notify patients**

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 the production of information**
- **For the physician's legal counsel for the purpose of providing legal services to the physician**

Research
- **Research approved according to Section 29 of HIPA**

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

Use of Personal Health Information

(HIPA s.23, 26, 27, 28, 29 and 30, CPSS Bylaw 23.2(c)(viii))

A use of personal health information occurs when a physician, or other health professional, employees, or medical students or residents use the information for a purpose within the clinic.

- **A physician must not use a patient's personal health information except with the consent of the patient or in limited circumstances authorized in HIPA.**
- Whenever possible, the physician should rely on express or implied consent when using personal health information.
- **A physician may not rely on implied or deemed consent unless the physician uses it in accordance with the ethical practices of the profession.**
- The physician must be able to form the opinion that the individual would consent to the use if asked.
- **A physician who is aware, or should reasonably be aware that the personal health information was collected or disclosed in contravention of HIPA must not use the personal health information without the consent of the patient.**
- Physicians should only use the minimal amount of personal health information that is necessary for the purpose for which it is collected**.**
- **A physician must, whenever practicable, use de-identified health information if it will serve the purpose.**

Typical Uses

- Identify and contact patients
- Provision and continuity of care
- 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
  - Provincial health plan
  - Third parties

  - Facilitating reimbursement of patient claims at patient's request
- Professional Requirements
- Risk or error management
- Quality assurance
- Maintenance of competence

Implied Consent

A physician may use personal health information, relying on implied consent for

- **A purpose that will primarily benefit the patient**
- **The purpose for which the information was collected by the physician or for a consistent purpose**
- **Arranging, assessing the need, providing, continuing or supporting the provision of a service requested or required by the patient**
- **Discussing with the patient's next of kin or someone the patient has a close personal relationship with, as it relates to health services currently being provided to the patient and the patient has not expressed that the information not be used for this purpose.**

In order to rely on implied consent, there must be:

- Some communication to ensure the individual understands the purposes for which their information is being collected, how their information may be used and to whom their information may be disclosed; and
- An opportunity for the individual to opt out of the collection, use and disclosure of their personal health information. In some instances the collection, use and disclosure of personal health information is a condition of service and the individual cannot opt out if they want to receive the service. Where condition of service applies, the physician-trustee should look for ways to provide the individual with a reasonable ability to control the collection, use and disclosure of their personal health information.

Uses Without Consent

A physician may use personal health information without the consent of the patient for the following purposes:

Health or Social Services

- **Registering a patient in connection with**
  - **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**

Deceased Patients

- **In relation to the death of a patient, 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**

Programs

- **Planning, delivering, evaluating or monitoring a program of the physician-trustee**
- **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

- **In preparation for disclosure to another trustee or a designated archive and the physician has made a reasonable attempt to notify patients**

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 the production of information.**
- **For the physician's legal counsel for the purpose of providing legal services to the physician**

Research

- **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**

Employees' Information

Physicians are not authorized to use or obtain access to personal health information of an employee or prospective employee for any purpose related to the individual's employment without consent.

Disclosure of Personal Health Information

(HIPA s. 10, 20, 21, 23, 24(1), 27, 28 and 29 and *Regulations s. 5.1 (1) and (2), CPSS Bylaw 23.2(c)(ix))*

A physician discloses personal health information when the information is transferred or released to another trustee, person or organization that is not required to follow the policies and procedures of the physician-trustee.

It is recommended that physicians rely on express or implied consent whenever possible.

- **A physician must not disclose personal health information except with the consent of the patient or in accordance with HIPA, in particular Sections, 27, 28 and 29.**

- **A physician must only disclose personal health information that is reasonably necessary for the purpose for which it was collected.**

- **Physicians who disclose personal health information without a patient's consent must take reasonable steps to be able to inform patients of disclosures of their personal health information made without consent. Physicians are required to be in a position to respond to a patient's request for such information.**

- **If a physician discloses personal health information to another trustee, the physician is still accountable for the personal health information remaining as part of the record.**

- **A physician must, whenever practicable, disclose only de-identified health information if it will serve the purpose.**

Disclosure to Non-Trustees

If a physician discloses personal health information to a person who is not a trustee, the physician must take reasonable steps to verify the identity of the person receiving the information.

The physician is responsible for ensuring the non-trustee knows that the information is disclosed without consent and must not be used for another purpose unless authorized by HIPA.

A trustee should still maintain a need to know approach to personal health information and not disclose personal health information to a non-trustee, including the non-trustee for whom the trustee is working for or with, unless:

- **the individual whose personal health information is at issue has given express consent;**

- **the disclosure is to a police officer after having been served with a production order or in accordance with HIPA Regulations, section 5.1 (1)**
- **the disclosure is permitted or required by another law; or**
- **a non-trustee data sharing agreement has been signed, each party has a clear policy on handling the information and complementary procedures have been established managing the disclosed personal health information.**

If the disclosure is a one-time release permitted by law through a production order or an investigation then the requesting paperwork or the action itself should be recorded in the subject individual's medical record.

- **This ensures that if, at any time in the future, there is an inquiry called by the health care professional's regulatory oversight body or the Office of the Information and Privacy Commissioner that the documentation supports the action of the trustee.**

Deemed Consent

Physicians who are not trustees or employees of trustees should be managing the privacy of personal health information in accordance with PIPEDA. These physicians may not disclose personal health information based on deemed consent.

There are limited situations in a physician's clinic when deemed consent is necessary. Physicians should rely on expressed or implied consent instead. When using deemed consent the physician should ensure the following duties under HIPA are met:

- 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.

Deemed consent is when the patient voluntarily provides information and the physician can infer from that the patient expects that the information will be disclosed for the same or directly related purpose. Deemed consent is appropriate when the purpose is requested or required by the patient.

- **A physician may disclose personal health information, based on deemed consent for:**
  - **The purpose it was collected and which will primarily benefit the patient and it is not reasonably possible to obtain consent**
  - **The purpose for which the information was collected by the physician or for a consistent purpose**

- **Arranging, assessing the need, providing, continuing or supporting the provision of a services requested or required by the patient**
- **Discussing with the patient's next of kin or someone the patient has a close personal relationship with as it relates to health services currently being provided to the patient and the patient has not expressed that the information not be disclosed for this purpose**

- **A physician may rely on deemed consent for disclosures to another trustee when the other trustee is a health professional who will use the personal health information in accordance with the ethical practices of the profession.**

- **A physician may rely on deemed consent for disclosures to another trustee who is not a health professional, such as a regional health authority and the Saskatchewan Cancer Agency, when the other trustee has written policies and procedures to restrict the disclosure of the personal health information to those who require the information to carry out the purposes of why the information was collected or for a purpose authorized by HIPA**

- A physician may not rely on deemed consent when disclosing to a non-trustee such as a school, an employer or an insurance company. The disclosure should be done with the expressed consent of the patient or the physician should ensure there is authorization in HIPA for disclosure without consent.
  - In these situations, the physician should take reasonable steps to ensure the recipient of the personal health information is aware that the information must not be used or disclosed for any other purpose unless authorized by HIPA.

Disclosures Without Consent

It is recommended that physicians obtain expressed consent whenever possible.

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 relation to the death of a patient, 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**
  - **To the immediate family or to someone with whom the patient had a close personal relationship, provided the information is limited to the circumstances surrounding death or services recently provided to the deceased**

Programs

- **Planning, delivering, evaluating or monitoring a program of the Ministry of Health, a regional health authority or the physician**
- **Planning, delivering, evaluating or monitoring a program of the physician-trustee**
- **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 the physician and the physician has made a reasonable attempt to notify patients**

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 the production of information**
- **For the physician's legal counsel for the purpose of providing legal services to the physician**
- **To the chief coroner or a coroner appointed under *The Coroners Act. 1999* with respect to an investigation or inquest.**

Research

- **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**

Where a person or organization seeks health information from a physician without patient consent, that person or organization should be able to refer the physician to the authority for the request.

A physician who is aware, or should reasonably be aware, that the personal health information was collected or disclosed in contravention of HIPA must not disclose the personal health information without the consent of the patient.

Disclosure to Police Officer

This guideline discusses the authority for a physician in a medical practice to disclose personal health information to a police officer. Physicians who also work in hospitals should check with the policies and procedures for that practice location. The trustee of the hospital may have differing procedures related to the disclosure to police officers.

Physicians may disclose a limited amount of personal health information, without the consent of the patient to a police officer. In order to be authorized to do that, a number of conditions must be met:

- **The information must be requested by a police officer. The physician-trustee should not provide the information without such a request;**
- **The request from the police officer must relate to enforcing *The Criminal Code* or *The Controlled Drugs and Substance Act* or carrying out a lawful investigation under either of those Acts;**

The personal health information that may be disclosed is limited to:

- **Registration information about the patient which is information that was collected for the purpose of registering the patient for a health service, including the Health Service Number**
- **The nature and severity of an injury that was suffered by the patient or another individual and is connected with the enforcement or lawful investigation of *The Criminal Code* or *The Controlled Drugs and Substances Act.***

Physicians may also disclose a limited amount of personal health information if:

- **The patient received, or was offered, health services as a direct result of an incident that has been made the subject of a lawful investigation under *The Criminal Code* or *The Controlled Drugs and Substances Act***
- **The personal health information that may be disclosed is limited to**
  - **The factual circumstances surrounding the incident for which the patient received or was offered health services**
  - **The factual circumstances surrounding the provision of or offer to provide, health services**

- **The factual circumstances do not include the health history of the patient before the incident**

Whenever possible a physician-trustee should obtain advice from CMPA or CPSS before releasing information to the police pursuant to the HIPA authority to disclose personal health information to the police.

Physicians' requirements to disclose information to police about gun shot and stab wounds vary depending on whether the physician is in a private medical practice or in a health care facility. *The Gunshot and Stab Wounds Mandatory Reporting Act* does not apply to physicians in their private practice. However, physicians may disclose this information in accordance with their ethics in order to prevent serious injury or harm.

Where a facility such as a hospital treats a patient for a gun shot or stab wound the chief executive officer of the regional health authority, or a person designated by the CEO is responsible to report that to the police.

Managing Patient Consent and Masking

(HIPA s 5-7, 27, CPSS Bylaw 23.2(c)(xii))

The *Overview of Consent Requirements in HIPA* prepared by the Ministry of Health and included in Appendix B or http://www.health.gov.sk.ca/hipaprovides an excellent review of the different consents authorized under the Act. There will be occasions when a patient gives only limited consent for the use and disclosure of his/her personal health information. It is a best practice for physicians to manage these limited consents according to the patient's direction whenever possible. When a patient revokes consent, physicians must take all reasonable steps to comply with the revocation promptly after receiving it.

The notice that the trustee uses when notifying patients of the clinic's information management practices and patient's rights, should include how the patient can manage his/her consent through masking or alternative methods agreed to by the patient and the physician. When a patient wants to limit consent the physician or qualified employees should provide the patient with the Consent Directive and Masking Form and have a conversation with the patient on the benefits and risks of limiting consent. This discussion should include who at the clinic will or will not be able to view the masked record and for what purposes.

The EMRs approved by the Saskatchewan EMR Program have the capability to mask personal health information from view by all or designated EMR users. Masking can be applied to the whole record except the patient registration, or selected elements of the record.

Implementing Consent Directives on Access or Use

All EMR vendors approved by the Saskatchewan EMR Program have the ability to mask all or some of a patient's personal health information in the EMR. The masking function helps physicians meet a request by a patient to restrict who can see his/her record in the EMR and what uses that personal health information can be subject to. It can also be used when a patient revokes consent to the further access and use of the information and the physician must take all reasonable steps to comply with the revocation.

If, through counselling, a patient agrees that masking might not be suitable at this time the patient and the physician can jointly monitor who accesses the patient's record. If the patient does not want personal health information used in research or quality assurance activities by the medical practice, the record should be noted with this request if possible.

The physician may be able to receive automatic alerts whenever someone has accessed the patient's record if that functionality is available in the practice's EMR. The patient could also receive a regular audit report of who has accessed the record. It might also be satisfactory to the patient to mask older information and leave current information available to authorized users of the EMR.

If the consent directive cannot be met through masking, auditing, or some other solution, the physician-trustee should document the process of trying to find a solution. The result could be that the patient's record is masked and the authorized

users of the patient's information will then have to override the masking with consent or without consent in appropriate circumstance.

Counselling a Patient on Consent Regarding Access or Use

Whenever a patient places a limit on who can access or on the uses of his/her personal health information it is important that the patient have a conversation with the person collecting or using the personal health information about the risks and benefits of the restriction.

The possible risks and benefits of a restriction on the access or use of personal health information by employees at the medical practice can include

- Not being able to access the necessary information during care outside the medical practice, such as a hospital.
- No access by another member of the patient's care team within the practice to use for the patient's care.
- Care might be delayed as employees will not be able to prepare for the appointment.
- In extreme cases, when a patient refuses to allow an override of the mask, a health care provider might deny care because of lack of information and the patient will have to wait until the primary physician is available.

The patient's choice of consent cannot be coerced.

Implementing Consent Directives on Disclosures

When a patient requests that personal health information not be disclosed, the physician-trustee should confirm what disclosures in particular the patient does not want. While HIPA does not include the authority for a patient to withhold consent where deemed or no consent is used, the physician-trustee should make a note of the consent directive in the patient chart.

Several disclosures are authorized without the consent of the patient as noted in HIPA s. 27 (4). However, many of these disclosures without consent are discretionary in nature. This allows the physician-trustee the opportunity to consider the consent directive of the patient and not disclose the personal health information. The physician is not bound by these consent directives. See the guideline on **Disclosures of Personal Health Information** for more information.

Overriding a Consent Directive

When a record is unmasked the EMR requires that a reason be indicated. The reasons can 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

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

SAFEGUARDS

Text in bold is required by HIPA

Organizational, Physical and Technical Safeguards

(HIPA s. 16, 17, 18)

For the most part, HIPA establishes a general duty for physician-trustees to implement safeguards. The Saskatchewan Information and Privacy Commissioner has recommended the use of the **COACH Guidelines for the Protection of Health Information** for more specific direction on safeguards. The COACH Guidelines are available from the eHealth Saskatchewan Service Desk at 1-888-316-7446.

Organizational safeguards, also known as administrative safeguards, are the policies and procedures related to the activities and processes of the organization as a whole, including health professionals, employees, medical students and residents, contractors and other third parties. Some examples are:

- Agreements,
- Breach Management Guidelines,
- Business Continuity/Disaster Recovery Policies,
- Retention, Storage, and Destruction Policies and Processes,
- Acceptable Use Guidelines,
- Email and faxing rules,
- Password rules,
- Retention schedules,
- Scanning rules.

Physical Safeguards are the policies and procedures related to the physical environment where personal health information is collected, used, and disclosed. Some examples are:

- Locked building and locked office,
- Physically secured server,
- Lockable and fireproof filing cabinets,
- Location of equipment.

Technical Safeguards are security features found on computers, mobile devices, and other office equipment. Some examples are:

- User account management,
- Auditing of EMR users,
- System auditing,
- Technical controls restricting viewing of information,
- Data backups,
- Encryption,
- Anti-virus protection,
- Firewalls,
- Local Area Networks (LAN),
- Secure Wireless Network,
- Secure Portable Devices.

Agreements

(HIPA s. 18, CPSS Bylaw 23.2(c)(xi)(xii))

The use of written agreements to document and formalize privacy and confidentiality obligations will assist physician-trustees with meeting their general duties under HIPA. Using written agreements also has other practical benefits.

- The use of written agreements within a physician practice is recommended as a good business practice and risk mitigation tool

- Good agreements will clearly state each party's responsibilities and liabilities and will provide documented evidence of the arrangements reached between the parties. When a dispute arises, the parties may not have the same recollection of the verbal arrangement. The use of a written agreement will reduce the risk of misunderstanding and disputes.

- Contracts and agreements are necessary when the disclosure is ongoing, usually in the course of services being provided by an external third party on behalf of the trustee.

- There are several types of agreement templates that are available in **Templates - Agreements** of the Privacy Resource Materials.

External Agreements

- *External Information Sharing Agreement* - These are used when personal health information is being disclosed by a physician to another trustee outside the regular referral process or to a non-trustee. These are required under HIPA when personal health information is disclosed for research purposes.

- *Information Management Service Provider Agreement* for Information Technology (IT) or Information Management Services (All Clinics) - Where IT or information management services are being provided to a clinic and the service provider has access to the clinic's EMR system or other electronic systems, additional considerations will apply. Please see the Ministry of Health and CMPA sites for more information on IMSP agreements.
  - http://www.health.gov.sk.ca/health-agreement-guideline-final
  - http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_data_sharing_principles-e.cfm
  - http://www.oipc.sk.ca/Reports/IR%20H-2011-001.pdf

- A checklist has been prepared that can be used when reviewing agreements from an IT or IM Service Providers that uses its own agreement. This can be found in **Template - Forms and Letters**.

- When the clinic is purchasing an EMR system and IT or IM Services from one of the approved Saskatchewan EMR Vendors, a standard agreement has

been pre-negotiated with the EMR Vendors. Please ensure this is the version of the agreement being signed.

- *Data Protection Schedule* – This schedule should be used as a supplement to a service agreement to protect the privacy and confidentiality of personal health information.

- *Third Party Confidentiality Agreement* – This agreement should be used as a supplement to a service provider's standard service agreement to address confidentiality and privacy concerns.

EMR Program Required Agreements

Physicians should use the implementation of their EMR as an opportunity to review the written agreements they have in place and improve their procedures going forward.

Internal Agreements

- *Clinic Exit Agreement* -The purpose of a clinic exit agreement is to outline each physician's responsibilities when a physician leaves the clinic after the implementation of an EMR system.

- *Clinic Information Sharing Agreement* - This agreement outlines each physician-trustee's roles and responsibilities for sharing/disclosing information with other physician-trustees in the clinic and their commitment to ensure the security and confidentiality of the personal health information.

- *Clinic Information Sharing and Clinic Exit Agreement (Small Clinic Form)* – This is a simplified version of the two agreements that can be used in smaller clinics (i.e. 2 or 3 physicians).

Purpose of the Clinic Exit Agreement

- The Saskatchewan EMR Program requires that physicians put a Clinic Exit Agreement in place when multiple physicians are jointly using (i.e. sharing) a single EMR system. A Clinic Exit Agreement is not required when there is a single physician-trustee who employs other physicians who do not have custody or control of the personal health information of their patients. It is important for the physicians to outline and document ahead of time what will happen when one of them leaves the clinic.

- Establish each physician's rights and obligations with respect to the implementation, cost and ongoing operation of the EMR.

- Determine the terms and conditions that will apply in the event one of the physicians leaves the clinic.

- Description of the structure of the EMR and its database(s).

- The appointment of a lead EMR physician and the physician's responsibilities.

- The documentation of a transition plan including the required notice period, what original or copies of records the leaving physician is responsible for, and cooperation with the EMR vendor to facilitate the transfer of records.

- Commitment to comply with agreed upon technical, security or other protocols for the transfer of records.

- How to deal with the orderly transition of the information.

Purpose of the Clinic Information Sharing Agreement

- Outlines physicians' roles and responsibilities for the sharing of personal health information between and amongst the signing physicians and their employees.

- Commitment to develop and use a common privacy and security policy and procedure manual.

Alternative to the Clinic Exit Agreement and the Clinic Information Sharing Agreements

- *Associates/Partnership/Management Agreement* - Physicians use many different business structures to support the management and operation of their clinics. The issues addressed in the Clinic Information Sharing Agreement and Clinic Exit Agreement could already be addressed in the clinic's partnership or management agreement. Each clinic will need to check with their legal counsel to determine the best way to meet the requirements.

Managing Agreements

It is recommended that physicians establish a system to keep a record of all written agreements to which they are signatories. This record or a copy of it should be held off-site as part of the physician's business continuity plan. This is an example of a record of agreements.

Vendor	Subject of Agreement	Parties to the Agreement	Effective Date	Expiry Date	Location of Agreement
ABC Medical Storage Inc.	IMSP - storage and destruction of paper records	John Smith, ABC Medical Storage , and Drs. Jones, and Winter.	July 1, 2009	June 30, 2014	Filing cabinet in Dr. Jones' office E-version: admin/ contracts/storage

Breach Management

(HIPA s. 16)

The breach management process can be followed in situations involving personal health information in electronic and paper form that is under the custody or control of the physician. Breaches involving personal health information within the Electronic Health Record, specifically SLRR, PIP or PACS should be immediately reported to eHealth Saskatchewan Service Desk at 1-888-316-7446 who will assist in the management of the breach in cooperation with the medical practice.

Understanding Breaches

Simply, a breach is an unauthorized collection, use or disclosure of personal health information.

There are three types of breaches:

Confidentiality: the ethical responsibility for the protection of personal health information once obtained against improper or unauthorized access use or disclosure. This is just one aspect of privacy and is not synonymous with privacy.[3]

Integrity: personal health information has been modified or in some other way has been interfered with such that a trustee 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.

What Does Contravention of HIPA Mean?

The Information and Privacy Commissioner of Saskatchewan has described a privacy breach as:

> A privacy breach happens when there is unauthorized collection, use or disclosure of personal health information. Such activity is 'unauthorized' if it occurs in contravention of … HIPA. An example … would be a health care professional accessing the EMR to check a patient's status when he or she has no professional need to know the information.
>
> Privacy breaches most commonly occur when personal health information about patients is stolen, lost, mistakenly or purposely used or disclosed without the requisite need to know. Examples include when a computer containing personal health information is stolen or when personal health information is mistakenly emailed or faxed to the wrong person.[4]

[3] http://www.oipc.sk.ca/Resources/HIPA%20Glossary%20-%20Blue%20Box.pdf

[4] http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Privacy%20Breach%20Guidelines%20-%20September%202010.pdfp. 4

Purpose of Breach Management Policy and Procedures

All physician-trustees enrolled in the EMR Program are required to write a breach management process to ensure they are able to respond quickly when they first become aware of any activity that is an actual or suspected breach involving personal health information. A written procedure ensures the physician and employees will be able to respond, investigate, analyze and remedy a situation quickly.

- A physician-trustee should also include in agreements with Information Management Service Providers and other third parties who have, or could have, access to personal health information, a requirement to report any actual or suspected breaches and to participate in the containment, investigation and analysis of the breaches. A copy of the physician-trustee's written policies and procedures should be appended to these agreements as well.

Considerations When Writing Breach Management Policy and Procedures

Definitions - definitions of the common terms specific to breach management will assist physicians and employees to better understand the policy and procedures.

Identification of how the physician becomes aware of an actual or suspected breach and how this influences the response to the breach including:

- Auditing users of the EMR - managing the response will primarily be internal, although patients might still need to be notified.

- From the Patient - when patients report an actual or suspected breach they might exert influence on timelines and other aspects of the investigation.

- From the Office of the Information and Privacy Commissioner - the OIPC might notify the physician of an actual or suspected breach and might become involved in the investigation if it considers that the physician needs assistance to conduct the investigation properly. The OIPC may also issue a public report regarding the breach.

- Media - the actual or suspected breach might be reported in the media before the physician is aware of it. In these situations all actions by the physician will be in the public eye and the OIPC might become involved immediately.

- Another trustee - other trustees could notify the physician of an actual or potential breach and, in some cases, it may result in or require a joint investigation.copy rfid card to iphone
- IT support or EMR vendor - their involvement with the investigation will be from the beginning. They might have even contained the breach before contacting the physician.how to get rfid

Breach Management Process

- The Office of the Information and Privacy Commissioner of Saskatchewan has issued guidelines on managing breaches: http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Privacy%20Breach%20Guidelines%20-%20September%202010.pdf)
- Breach management is generally recognized to have five activities. These are usually done in consecutive order with the exception of patient notification which could occur immediately depending on the actual or suspected breach and the personal health information involved. See **Patient Notification** for more information.
- It is important to respond to an actual or potential breach immediately to reducing harm to both the patient and the medical practice. Physicians and privacy officers should respond in accordance with their policy and procedures.
- During the process every effort should be made to maintain the privacy of the patient and the confidentiality of the personal health information. Not all people involved in the process need to be made aware of the patient(s) name or other personal health information.
- There will be many lessons learned during the breach management process. It is important to document as much as possible and double check facts during the investigation and analysis. During the prevention step, be sure to consider the lessons learned.

Contain the Breach - stop the breach from continuing. Examples of how to contain some types of breaches:

- If the breach is in the EMR, whether through an unauthorized access, a hacker, or a hijacking (viruses, worms, Trojans), disconnect the Internet and the LAN, but leave the server on, then contact IT support to determine how to contain the breach.
- If a person authorized to access personal health information is doing so inappropriately, immediately cancel their user account upon discovery of the actual or suspected breach.
- If personal health information is sent to or received by the wrong person and the person is known and/or trusted ask that the information be destroyed and that you receive confirmation of the destruction. This might be the case if a fax was sent to the wrong physician.
- If the person is unknown and trust is not established have a trusted person retrieve the personal health information. This might be the case if a fax was sent to a business unknown to the clinic.
- If records in storage, or being transferred to storage, are compromised, have a trusted person retrieve the records.
- If records are lost, start with **Investigate the Breach**.
  Rfid metal cards

- If records are stolen, contact the police.

Investigate the Breach – determine the cause and the events surrounding the breach.

- Document all aspects of the investigation, people involved, information involved, and timelines; this will be used in the analysis of the actual or suspected breach by the medical practice's investigation team. If the Office of the Information and Privacy Commissioner or the police become involved they will need this documentation.

- Interview the person who first reported the breach, the person who contained the breach and others involved, as appropriate.

Assess and Analyze the Breach and Associated Risks – understand what happened, if personal health information was involved and determine if patient notification is necessary.

- Additional people with specific expertise can be involved in assessing and analyzing. Too large an investigation team can hinder the timeliness of the investigation. Some people just need to be informed of the progress of the assessment and analysis, rather than being fully involved in the investigation. The more people involved increases the risk of a further breach of patient privacy among the investigation team.

- Did the actual or suspected breach involve personal health information? If the information was de-identified and the team believes that there is no expectation that the information can be re-identified then personal health information was not involved.

- Take advantage of the expertise of the Office of the Information and Privacy Commissioner on complex assessments and analysis.

Determining if Personal Health Information was Breached

- The breach investigation team should consider if personal health information was actually involved or whether the information had been modified to the extent that no individual could be identified. To determine if personal health information was breached consider the following:

    - Is the information publicly available? This is unlikely to be the case for personal health information.

    - Has the information been erased or modified by malware such that it could not be accessed by anyone but a reliable backup will restore all compromised information?

    - Was the information de-identified so that there is no reasonable expectation that it could be re-identified when linked with other information?

Joint investigations

- If the personal health information breached came from, or was sent to, another trustee or third party a joint investigation is often appropriate.

- Concerns with joint investigations are the differing procedures and the number of people who are involved. These cannot fully be anticipated in procedures but will need to be managed as the investigation continues.

Notification of Interested Parties and Patients - who needs to be notified and when.

- See the next guideline on **Patient Notification** for comments on when and how to notify patients.

- Who else needs to be notified, and when, depends upon the assessment of the severity, scope and nature of the personal health information that was compromised.

    - eHealth Saskatchewan - contact the eHealth Service Desk at 1-888-316-7446 if the breach involved information that was received from or was being disclosed/transferred through the EHR, including SLRR, PIP, and PACS. eHealth can be contacted to help in the containment of the personal health information. They will need to be involved in Steps 2 through 5. eHealth will assist in contacting the source trustees.

    - Other physicians in a joint practice - Other physicians in the same clinic should be involved either to aid in the containment or at the beginning of the investigation.

    - Other Trustees - contact the Privacy Officer for the other trustee(s). If the breach involved information that was received from or being disclosed/transferred to the other trustee they might need to be involved in the containment. Otherwise, they should be contacted as part of the evidence gathering in step 2.

    - Police - contact the police when the breach is caused by a theft or other criminal activity. They might want to be part of or lead the investigation of the incident. If the breach is a result of an external intruder into the EMR, inform the police and they will indicate if they want to be involved and when.

    - Saskatchewan Medical Association - the SMA can provide advice and identify the necessary expertise to help physicians in the breach management process.

    - Vendor - the EMR vendor might need to be contacted to assist in the containment of the breach if the breach involves the EMR. The vendor, whether the physician uses a client-server or an ASP model, should be involved in Steps 2 through 5 to provide advice and develop their own

lessons learned. The degree of the vendor's involvement depends on how the EMR was involved in the breach.

- Other third parties - the notification of other third parties will depend on the type of breach. Example: if the office was broken into the landlord should be contacted, or if it is information used in a clinic trial the researcher should be contacted.

- Research Ethics Board - if the breach was by a researcher in custody of the personal health information for research, notify the Research Ethics Board.

- Office of the Information and Privacy Commissioner - the OIPC can provide valuable advice and guidance to physicians involved in a breach. When deciding whether to contact the OIPC consider:
  - The sensitivity of the personal health information
  - Whether the disclosed personal health information could be used to commit identity theft
  - Whether there is a reasonable chance of harm from the breach
  - The number of people affected by the breach
  - Whether the personal health information was fully recovered without further disclosure, or if any further unauthorized use has been thwarted.

- Contacting the OIPC will not immediately open an investigation file; they will monitor the situation to ensure that the response of the physician-trustee is adequate. In those instances where the response is inadequate or not timely, the OIPC could open a formal investigation case file. Furthermore, if the OIPC does a formal investigation they may publish the report on their website.

Prevention - to provide recommendations and strategies to minimize future risk.

- After completing investigation and analyses, the physician-trustee should take the lessons learned from the investigation and make changes at the medical practice to minimize the risk of a breach in the future. The physician should consider:

- Reviewing the medical practice's policies and procedures;

- Reviewing written agreements to ensure they include necessary safeguards and a requirement to participate in the breach management process;

- Updating privacy awareness, education, and training activities at the medical practice and for vendors and other third parties;

- Ensuring physical safeguards are in place and working, including separate space for EMR equipment and paper records and locks are in place and working;safecard rfid blocking card

- Ensuring technical safeguards are in place, including, but not limited to:
  - The auditing function for the EMR has been set to meet the needs of the medical practice and is turned on;
  - Employees are aware of the auditing function;
  - Security recommended by IT support and/or vendor is considered and/or implemented;
  - All software for virus protection, virtual private network, and firewalls are updated on a regular schedule;
  - Evaluate the efficiency and effectiveness of the breach and incident management process and update accordingly.

- Violation of the Breach Management policy and procedures should be considered to be grounds for disciplinary action. Trustees should consider creating a progressive discipline policy that establishes penalties up to and including termination and/or reporting to the appropriate regulatory authority or body, depending on the seriousness of the violation

Patient Notification when a Breach Occurs

The **Breach Management** discussion provides guidance to physician-trustees on what to consider when drafting a breach management policy and procedures. One of the steps in the breach management process is the notification of patients. This topic provides guidance on the factors to consider when drafting a policy for patient notification. Breach Management and Patient Notification can be written as two policies or one.

Obligations to Notify Patients

There is no requirement in *The Health Information Protection Act* (HIPA) to notify patients when a breach occurs; however the Information and Privacy Commissioner expects trustees to notify individuals to avoid, mitigate or address harm to an individual whose personal health information has been collected, used or disclosed without appropriate authorization.

It is recommended that physicians enter into contractual arrangements with information management service providers (IMSP) that include how breaches and patient notifications are managed. The physician-trustee can also have information sharing agreements with other trustees and non-trustees for one-time or ongoing sharing of personal health information. These agreements should all include a requirement that only the trustee approves the notification of patients if a breach occurs involving that information.

Determining if the Patient(s) Should be Notified

The key consideration in deciding whether to notify affected patients is based on the harm or potential harm to the patient. Review the assessment of the breach to determine whether or not notification is required; document any analysis and decisions.

Considerations include:

- The severity, scope, and nature of the breach,
- The sensitivity of the information,
- The expectations of the patient when information was collected, i.e. did the medical practice provide information to patients that they would notify them if there was a breach,
- Where the personal health information was disclosed to a trustee or non-trustee;
- Probability and gravity of harm
  - Is there a chance of misuse, for example, a misdirected fax that went to the wrong physician and only viewed by an employee has a low risk of harm;

- Ease of exploitation for fraudulent or other harmful purpose;
- Risk to public health and safety;
- Identity theft;
- Loss of business or employment opportunities;
- Hurt, humiliation, damage to reputation or relationships.

- Also consider the potential harm to the medical practice, medical profession, or EHR system, including loss of trust, if the patient is not notified but becomes aware of the breach.

Preparing to Notify Patients

Patients should be notified as soon as possible once the breach is understood.

- Consider consulting legal counsel and/or the OIPC before notifying patients.
- If police are involved, confirm a notification timeline with them to avoid compromising their investigation.
- Designate one person to speak publicly on the matter, ensure this person has the most up-to-date information on the breach and can provide the official response.
- Prepare a statement for the medical practice's receptionist should patients call.
- Ensure the physician-trustee and/or privacy officer are prepared.
- If providing third party information in the notification, such as contact information for the Ministry of Health Privacy and Access Office or the OIPC, ensure they are contacted beforehand so they can prepare for inquiries from patients.

Notifying Patients

- Directly notify patients through a telephone call, letter or at the next visit to the medical practice if:
  - Identities of the patients are known,
  - Current contact information is available,
  - Patients need to have direct contact to get the necessary details to protect themselves.
- Notification should be adapted for patients who have difficulty understanding why they are being contacted.

Indirect Notification ofPatients

- Indirect notification could be through a medical practice's website, posted notices or through the media.rfid wooden card

- Indirect notification is appropriate in situations where:
  - direct notification could cause further harm to the patient,
  - contact information is not available or is out-of-date,
  - a very large number of people are affected by the breach

Physician-trustees should only use indirect notification of patients on the advice of the Office of the Information and Privacy Commissioner or the Saskatchewan Medical Association.

Details Included in Notification

The notification, whether direct or indirect, to a patient(s) about a breach should include:

- Date of breach,
- Details of the extent of the breach and the personal health information involved,
- Steps that have been taken to address the breach both in the immediate and long term,
- Potential risks to the patient,
- Contact name at the medical practice for the patient to get more information and,
- Contact information for the OIPC and other third parties patients might wish to contact, such as the Heath Registration Branch of the Ministry of Health to inquire about possible inappropriate use of the Health Services Number.

Notes for Physician enrolled in the Saskatchewan EMR Program

The Saskatchewan EMR Program requires physician-trustees, as a part of participation in the program, to have a complete breach management policy and procedures that includes patient notification.where can i get rfid.

Developing a Business Continuity and Disaster Recovery Plan

Business continuity and disaster recovery planning is a process that helps organizations prepare for disruptive events. A business continuity plan assesses all aspects of an organization's operation for critical activities that need to be restored quickly and the steps to achieve this. A disaster recovery plan focuses on the IT operations of the organization. A disaster recovery plan will identify proactive steps an organization should undertake to prevent, or to be prepared for, in the event of a disruption event.

Planning in advance will allow medical practices to respond quickly in an emergency to facilitate the return to delivering patient care with minimal loss of time and patient information whether the event is a power outage or a pandemic.

For a breach that involves the inability to access personal health information use the **Breach Management** guidelines in conjunction with the disaster recovery plan.

Business Continuity Plan

A business continuity plan for a medical practice should address the threats specific to that practice and provide practical strategies for business survival and resumption. To continue operations in the loss of access to the physical location of the medical practice, for example, one practice might need only employee and patient contact information and the name and location of an alternate location to see patients. Under the same circumstances another medical practice might plan to refer patients to another physician while continuing to handle phone calls at an alternate site. What really drives the form and content of a plan are the functions the medical practice needs to recover for minimum operations and how soon they need to be available.

Disaster Recovery Plan (important notes for physicians with EMRs)

IT disaster recovery plans provide step-by-step procedures for recovering disrupted systems and networks to help restore normal operations. The process of developing a disaster recovery plan will examine all IT systems including the EMR, Internet, LAN, access to other health information systems, telephone, fax, photocopier, and even electricity. Some or all of these systems might require outside expertise to restore operations. Work closely with the EMR vendor or IT support in designing the disaster recovery plan.

Determining What Is Critical

Begin with identifying what aspects of a practice are critical to survival. What employees, equipment, facilities, records, and other assets and the processes they support are essential to the operation of the medical practice? At the most basic level a medical practice will need employees, a place to see patients,

possibly some diagnostic equipment, and a list of patients with contact information.

The next step is to determine the maximum impairment the practice can withstand and still make alternative arrangements to see patients. For example, would the medical practice still see patients if there was no access to the EMR?

The final step in developing a plan is to determine how the practice will survive if an adverse event has a negative impact on a critical process or asset. How can the practice re-establish full patient care? Alternatives might include setting up a mutual employee back-up arrangement with another physician in the area, reducing office hours, documenting office procedures so that they can be done by any available employee, contracting with a temporary agency, or sending patients to the local hospital for a service that the medical practice temporarily cannot provide.

Elements ofa Disaster Recovery Plan

There are several things a physician-trustee should ensure are in place and activities that should be performed regularly to minimize the risk due to a disruptive event.

- Regular backup and/or protection of EMR records and other vital information. Encrypt and store backups off-site, ideally not in a location close to the medical practice. A power outage, flood, and other disasters can affect a large geographic area.

- Keep information system versions up-to-date. Have automatic updating of anti-virus software, malware, and other security features for information systems.

- Have IT support develop a checklist of things to monitor on your system to reduce the possibility of downtime.

- Have IT support develop a checklist as part of the disaster recovery plan to reduce the time it takes to become fully operational again.

Elements ofa Business Continuity Plan

Medical practice physicians and a senior administrative employee should form a crisis management team responsible for declaring a disaster, activating the plan, and directing and managing the office recovery operations, including:

- Setting priorities and objectives,
- Overseeing, directing, and managing all team members and the entire recovery process in all alternate locations,
- Directing, controlling, and ordering resources, and maintaining a manageable span of control,
- Approving expenses,
- Resolving conflict and making and implementing strategic and policy decisions,Hotel card.

- Designating a spokesperson for any inquiries from patients, the media or the OIPC.

Having this plan in place ahead of a disaster will assist in quick recovery.

- Financing is a key component of business continuity. Cost will be a factor in how quickly the medical practice is operational again and if only part of the practice will resume operations. Determine who or how these decisions will be made. Ensure that ability to do banking, including paying employees, is maintained.

- A list of key contacts should be easily retrievable. For a medical practice this might be employee phone numbers, third party IT support, EMR and other vendors, the landlord, local media contacts for public service announcements to notify patients that the medical practice is closed, suppliers, hospitals or other organizations to which the medical practice frequently refer patients, and insurers.

- Consider how patients can be contacted. Will someone keep a list of patients off site? Can the EMR backup serve this purpose? Will radio stations be used?

- Consider alternative locations for the practice if access to the clinic will not be possible for some time. Make arrangements with other medical practitioners in the area.

Notes for Physicians Enrolled in the Saskatchewan EMR Program

As part of participating in the Saskatchewan EMR Program, physician-trustees are required to develop a disaster recovery plan. This plan should be broad enough to cover reasonably anticipated events such as EMR downtown, power failures, system crashes, Internet failures, fires, and floods, to highly unlikely events such as an earthquake or all employees resign on the same day because they won the lottery.

References

Wisconsin Medical Society Risk Management Manual, 1997

Retention Periods for Personal Health Information

(HIPA s. 16, 17(2), CPSS Bylaw 23.1(f), 23,2(c) (x)(xi)(xii))

It is important that physicians establish and follow a written retention period for records of personal health information. As long as the record exists, or until the physician transfers the records to another trustee, the physician has responsibility for it. These responsibilities include secure storage and destruction, availability of the personal health information upon patient request for access, and ensuring the information remains retrievable, readable and useable for health care purposes even if it will not be used for that purpose again. Records can become unreadable when a physician upgrades the EMR system. Physicians could have to convert their records to the new software or retain older versions of the software that will read the records. This needs to be discussed with the EMR vendor before any upgrades.

There are several sources to consider when determining how long records should be retained.

- HIPA does not specify a period physicians should retain personal health information, but physician-trustees need to have a storage policy regarding irretrievability, readability, and usability of the records, and a secure destruction policy.

- CPSS requires records to be held for six years after the patient was last seen. Records of pediatric patients shall be retained until 2 years past the age of majority or 6 years after the date last seen, whichever may be the later date. (By-law #23.1 under the *Medical Profession Act*).

- CMPA advises its members that for medico-legal purposes a physician's medical records should be retained for at least 10 years from the date of last entry or, in the case of minors, 10 years from when the age of majority is reached or 10 years from the last entry, whichever is greater.

- Physicians involved in clinic research trials are generally required to keep the records related to the trial for 25 years. More information on retention as part of a clinical trial is available on the Health Canada website at http://www.hc-sc.gc.ca/dhp-mps/compli-conform/clini-pract-prat/docs/gui_68-eng.php.

- Physicians are also governed by PIPEDA in some of their activities. PIPEDA states, "Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made". "Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous."

Physicians should set a retention period that at a minimum complies with the CPSS By-Laws and allows for records to be held as long as necessary for patient care, and within the policy include an exception to allow for individual records to be held longer if determined necessary.

Physicians may be concerned about destroying records that are then required for a legal reason. Both the courts and the Privacy Commissioner of Canada have deferred to retention periods established by organizations thoughtfully and in good faith. A policy of permanent retention of records is generally not an acceptable retention period.

Patients could request that a record be destroyed earlier than the retention period. If a physician has established a written policy based on medical and legal factors the request does not need to be met.

Storage of Personal Health Information

(HIPA ss. 16, 17, CPSS Bylaw 23.2(c)(x))

Secure storage of records of personal health information is essential for all trustees. Physician-trustees are expected to meet the same level of protection as hospitals, although it is anticipated that they will use different safeguards. Secure storage integrates the three types of safeguards: organizational, physical, and technical.

Organizational safeguards for storage

- Ensure there is documentation on the medical practice's record holdings
  - Type of media: paper, film, optical media, micro media, magnetic tapes, storage media, office machines or audio recordings
  - Classifying type of personal health information considered extremely sensitive.
- Ensure consistent use of a record naming convention.
- Document a concise set of security rules on access restrictions, and security safeguards.
- Appoint someone for overall responsibility for storage of records.
- Ensure regular training of health professionals, employees, medical students and residents.
- Use security clearances and ID badges.
- Restrict access to personal health information to those who need to know.
- Regular reviews of the adherence to procedures for compliance with security policies.
- Ensure confidentiality agreements are signed.

Physical safeguards for storage

- Lock fireproof filing cabinets.
- Restrict office access and alarm systems.
- Protection from environmental factors.

Technical safeguards for electronic storage

- User authentication, including passwords and user IDs,
- Encryption,
- Firewalls and virus scanners.

Storage at the Medical Practice

- A good rule of thumb is to have three locks protecting personal health information.
  - These can be all physical for paper records, such as locked building, locked office and locked filing cabinets.

Active Paper Records

- Many medical practices have their active paper records conveniently located behind the reception desk in open shelving.
  - During the time the medical practice is open to patients the reception counter acts as a physical barrier.
  - If these shelving units cannot be locked at night the three locks principle cannot be met.
  - Practices should consider other ways of physically securing the records, such as a motion sensor that detects after hour intruders. If physicians purchase new storage units for active records they should consider fireproof filing cabinets.

Inactive Paper Records

- The same principle applies to records in long term storage before destruction: locked building, locked office, and locked storage room.

- The storage room should be single purpose, or if it is a room used for storage of supplies and other things it should be accessible by a password keypad (available at local hardware stores) or swipe card.

Electronic Records

- Store inactive records in the EMR Archive

Off-Site Storage

- If a physician-trustee arranges off-site storage that is still managed by the physician-trustee, be sure it has greater protection than onsite storage as there will not be the daily oversight by employees as there is at the medical practice's office.

- If the offsite storage is in the physician-trustee's home the space should be single purpose, protected from environmental factors and physically secure.

- Using an Information Management Service Provider (IMSP) for offsite storage is generally a safer way to store records long term.
  - A professional IMSP will have a secure location and will monitor the site.
  - The Saskatchewan EMR Program requires that medical practices using an EMR enter into an IMSP agreement which should detail the

expectations the physician has for secure storage, reliable access to the records, the right to audit the protection practices of the IMSP, and notification of all incidents and breaches.hilton hotel key card.

Scanning and Destruction of Original Paper Records

(HIPA s. 17)

With the adoption of the EMR, many physicians who have a vision of a paperless office find that even after scanning they are still responsible for the old paper records and new patient information received by mail and fax.

CMPA advises that these paper records do not have to be held for the full retention period if they have been scanned into the EMR and may be destroyed if the physician chooses[5]. The scanning process needs to create an unalterable digital image of the original paper record which, if done correctly, will be admissible in a legal proceeding in place of the original paper record. A popular format for a scanned document is Portable Document Format or PDF.

The physician-trustee is required to develop and document scanning, quality assurance and destruction procedures that are consistently followed in the medical practice.

- The types of procedures that should be in place include:
  - Assigning one person to be responsible for scanning, even if this person oversees someone else,
  - Regular employees training on the scanning procedures,
  - Document how the paper record is to be scanned to ensure the accuracy, completeness, retrievably, readability and usability of the information,
  - Scanned document must be saved in a read only format,
  - Document how quality assurance is tested,
  - When and how the paper original is destroyed,
  - If a partial paper chart is scanned and destroyed, a note in the paper record should indicate that personal health information was scanned into the EMR, the date of the scanning, and the date of the destruction after scanning,
  - If a full paper chart is scanned follow the documentation procedures for destroying records.

- Procedures to ensure scanned documents are complete, retrievable, readable, and useable could include:
  - Random checking of several originals against the scanned documents,
  - Retaining the original paper document for a short time period as a reference should someone become aware that the electronic version may not be a true copy.

- Ensure that adequate security measures, including both technology measures and policy measures, are built into the EMR, and computer security and user policies are implemented and enforced and can be relied upon when it is called to prove the integrity of the electronic record.

[5] https://www.cmpa-acpm.ca/cmpapd04/docs/resource_files/perspective/2010/02/com_p1002_9-_e.cfm

- If the scanner has reporting capabilities run a report regularly and save in the administrative files with other records of destroyed records.

- After following these procedures each original paper chart can be securely destroyed according to the medical practice's destruction policy.

Sample Verification of Scanned Record Text

There may be times when physician-trustees want a higher standard for assuring of the authenticity of the scanned record, this can be done by using a verification certification in addition to the standard procedure adopted by the clinic. The verification certificate states that each scanned document is a true and complete copy of the original paper medical record.

Text for an Entire Medical Record
I, [insert name], being a [insert employee or physician] of the [insert name of clinic] (the "Clinic") located at [insert address of the Clinic], hereby certify that I have scanned the entire original paper medical record (the "Record") for [insert name of patient] (the "Patient") into the Clinic's Electronic Medical Record System (the "EMR System") on [insert date].

To ensure the accuracy and integrity of the information that was scanned from the Record into the EMR System, I certify that I compared the information contained on the Record to the information scanned into the EMR System. To the best of my knowledge, this has created a true and exact copy of the Patient's Record in the Clinic's EMR System.

Or

Text for a Single Letter, Report, etc.
I, [insert name], being a [insert employee or physician] of the [insert name of clinic] (the "Clinic") located at [insert address of the Clinic], hereby certify that I have scanned the original paper [insert type of report, letter etc.] (the "Record") for [insert name of patient] (the "Patient") into the Clinic's Electronic Medical Record System (the "EMR System") on [insert date].

To ensure the accuracy and integrity of the information that was scanned from the Record into the EMR System, I certify that I compared the information contained on the Record to the information scanned into the EMR System. To the best of my knowledge, this has created a true and exact copy of the Patient's Record in the Clinic's EMR System.

Signature of Employee/Physician
Date

Signature of Witness
Printed Name of Witness

Destruction of Paper Records of Personal Health Information

(HIPA s 17)

Records should be stored securely and according to the policy of the medical practice.

Records need to be retained for the minimum time period established in the medical practice's retention policy.

Records must be stored in a format that is retrievable, readable, and useable for the purpose for which it was collected and for the full retention period set by the medical practice.

Scanned records should only be securely destroyed in accordance with the scanned records policy.

Before any records are destroyed it is recommended that the physician-trustee sign a confirmation of the records to be destroyed. This confirmation should include several details:

- Who will be performing the destruction?
- What method will be used to destroy the records?
- The date the records are scheduled for destruction.
- Location of records to be destroyed, i.e. in office or offsite storage.
- A list of the records with the patients' name, physician's name, and the last year an entry was made.

Paper records need to be destroyed to a degree that they cannot be recreated. Methods include:

- Crosscut shredding not strip shredding, crosscut shredding can then be recycled,
- Private companies can be hired to shred records this may be done either on site or off. One needs to ensure that the proper agreement is in place (see Agreement Templates - External),
- Burning to a white ash with no partially burned pieces remaining,
- Pulping or pulverizing.

Personal health information stored in other mediums such as X-rays, labeled prescription bottles, etc. need to be destroyed in a secure manner.

Acceptable methods of destroying confidential information recorded on microfilm, photographic negatives, motion picture films, or other photographic media include pulverization and chemical disintegration.

Containers used for prescriptions and bodily substance samples can have their labels removed and then the labels are securely destroyed, or the bottles with labels can be given to a private company to destroy.

Using a Private Company for Destruction of Records

A private company can be engaged to securely destroy (i.e. shred, burn, pulp) medical records.

- In such cases, the physician should enter into an IMSP agreement with the company. The IMSP agreement should include requirements that the company:
  - Have written privacy and security policies that are made available to the physician,
  - Provide a Certificate of Destruction for each time records are destroyed and a verification that includes the method of destruction used,
  - Have a confidentiality agreement with each employee,
  - Is willing to submit to independent audits by the physician or the physician's representative.

It is recommended that physician-trustees contract the destruction of records to a certified member of the National Association for Information Destruction (NAID) or a company that adheres to the principles of NAID. NAID's website is www.naidonline.org. As of October 2011, there were two companies NAID certified in Saskatchewan, Iron Mountain and Shred-IT International. The physician needs to ensure there is secure transfer of the records to the destruction site.

After Destruction

Upon completion of destruction whether by employees or a private company a confirmation of destruction should be signed by the person supervising the destruction. This can be managed by using a log in the clinic which is signed when records are destroyed.

Destruction of Non-Confidential Records

Records that contain non-confidential information can be discarded by any means consistent with the clinic's waste management practices and the waste removal requirements of the locality where the records will be discarded. Recycling is an acceptable method of destroying records that contain non-confidential information.

Reference

Ontario Information and Privacy Commissioner and National association for Information Destruction, Inc., Get Rid of it Securely to Keep it Private: Best Practices for the Secure Destruction of Personal Health Information http://www.ipc.on.ca/English/Resources/News-Releases/News-Releases-Summary/?id=899

Backups including Storage of Backup Tapes

(HIPA ss. 16, 17, CPSS Bylaw 23.2(c)(xi))

A significant advantage of electronic medical records over paper records is the ability to have a complete copy of the record in a backup that requires very little space for storage. Backups of the EMR are a relatively easy safeguard to implement and manage yet can have the greatest impact on ensuring business continuity for a medical practice.

When a clinic selects an EMR vendor a decision will also be made about how backups will be done. The three options are 1) backups by the vendor, 2) backups by local IT support, and 3) backups done in the clinic when a client server model is chosen.

Each medical practice should designate one person to be responsible for ensuring there is an effective backup program as part of the Disaster Recovery Plan. The responsibilities of this person are to establish a program, ensure that the program is followed including overseeing the role of the IMSPs. If the medical practice uses an ASP model for record management, the designated person is responsible for working with the EMR vendor to develop a program that includes notification to the designated person on issues related to the backup.

Backup Schedules and Retention

A significant part of the backup program is establishing a schedule for automatic backups of the EMR. Consideration also needs to be given to the backup of other files, both of personal health information and corporate information.

- Ensure remote backups are done at a minimum daily and this is included in the ISMP or vendor agreement.
- When backups are done by the clinic ensure there is a well-documented backup schedule, including:
  - Regular backups are performed daily and taken offsite in a secure manner
  - All backups must be encrypted
  - A process should be in place to confirm that backups were successful. Periodic testing of backups should be done with the help of IT support as it requires two servers.

Recovering a Backup on a Client Server

- If the medical practice suffers a loss of information then the backup will be used to restore the information. In most cases this requires the skills of an IT professional or the EMR vendor. It is important that the recovery of information using a backup be executed properly or the data could be corrupted or lost.

Storage Security

- The storage of backup tapes should meet all the protection expectations of personal health information. If the backup tapes are stored with an external company, attach the medical practice's backup policy to the IMSP agreement.
- Ensuring all backups are kept off site and if possible the site is greater than 10 kilometers from the medical practice.
- Ensuring that facilities are controlled for temperature, fire, floods, and other measures for environmental factors.
- Ensuring that personal health information is encrypted whenever the backups are being transferred and stored.
- Ensuring that personal health information stored in any format is retrievable, readable, and useable for the purpose for which it was collected for and for the full retention period.
- Ensure the personal health information can be accessed to respond to a access request from an individual.

Destruction of Devices
containing Personal Health Information
(HIPA ss. 16, 17)

Devices, such as servers, computers, laptops, fax machines, and photocopiers, retain personal health information on their hard drives even after the user has deleted the information using the application delete functionality.

To securely and permanently delete this information, the hard drive should be destroyed. A company certified by the National Association for Information Destruction (NAID) or a company that adheres to the principles of NAID should be used. NAID's website is www.naidonline.org. They will degauss the hard drives or use some other method of destroying the information permanently. As of October 2011 there were two companies NAID certified in Saskatchewan, Iron Mountain and Shred-IT International.

- Physicians should maintain an up to date list of all office and medical equipment that retains personal health information.

- Before a device that contains personal health information is destroyed the information should be backed-up or archived.

- The policy and procedures for retention and destruction of personal health information should be followed when destroying these devices.

User Account Management

(HIPA s. 16, CPSS Bylaw 23.2(c)(xii))

Physician-trustees need to ensure the proper ongoing management of the accounts of users of the EMR.

- One person should be assigned the responsibility for account management.

- The activities that could require changes in a user's account include:
  - Disable generic or shared user accounts,
  - Disable inactive accounts,
  - Changes in employment status. This is particularly important when someone is terminated and the EMR is an ASP model. The account should be terminated immediately as ASP can be accessed outside the office.

- Role-based access controls are highly recommended and is available in most EMR systems used today.

- Role-based access controls use technology to ensure that access to the patient record is based on the "need to know" principle.

Access Privileges

- The EMR system requires that each user has defined access privileges. The user account manager should ensure that each user's access is determined according to their need to know information to complete their work. Do not use a default setting of full access.

Passwords and Logins

- EMRs are required to be accessed by two-factor authentication - something the user has and something the user knows. This could be a user name and password, or a swipe card and PIN.

- Require the use of strong passwords and PINs that have a minimum of 8 characters and a mix of letters, numbers, symbols, and upper and lower case.

- Require automatic password protected screen savers that are activated after a maximum of 10 minutes and sooner in high traffic areas.

EHR Systems

- Trustees are also responsible for authorizing employees, other health professionals and medical students and residents to be given an account and password on some of the EHR systems, such as PIP. The trustee does this in his/her role as an Approver.

EMR and EHR Auditing

(HIPA s 16(b)(iii), CPSS Bylaw 23.1(e)(v))

The auditing function in the EMR is valuable for supporting the physician-trustee's responsibility to restrict access to personal health information to those who need to know, making available to patients a record of activity associated with their electronic record, and when investigating a breach.

As valuable as auditing user activity is, it will only detect when a breach has happened, it will not prevent an inappropriate use or disclosure. Educating EMR users on the auditing functionality might reduce the chance of them browsing records and other inappropriate uses.

The audit logs and audit reports from the EMR are personal health information about the patient. They should be retained as long as the personal health information it is associated with and in compliance with the clinic retention policy.

Responsibilities for Audit Logs

The physician-trustee is responsible for the proper management and use of the auditing information.

- These responsibilities include:
  - Ensuring at least one person within the medical practice is trained on how to use the auditing function,
  - Restricting access to the audit logs and reports to those who need to know,
  - Ensuring employees, other health professionals, and medical students and residents are aware that all actions within the EMR are audited,
  - Determining what information will be collected in the audit log,
  - Developing a standard report for audit logs, one by user and another by patient and an understanding of how to run ad hoc reports,
  - Establishing a regular schedule for reviewing audit logs,
  - Implementing an automatic alert if there is an override or an attempt to override the masking of a record, if it is a function available in the EMR,
  - Establishing procedures for storage, retention, and destruction of audit logs consistent with personal health information,
  - Ascertaining from the EMR vendor if system administrators can be audited,
  - Ascertaining from the EMR vendor if the audit function can run a report on the physicians and trustees that should be notified when an amendment is made to a patient's record,
  - Ascertaining from the EMR vendor if there is a VIP flag that can be used for patients' records that need closer monitoring. Can access to a VIP send an automatic alert?

Information in an Audit Log

Physician-trustees need to determine what information they would like collected in the audit log. The EMR vendor will confirm if the audit log can record the information. The recommended information is:

- Name and/or ID number of the patient,
- Name and/or ID number of user,
- Date and time of access,
- Name of the patient's primary physician at the practice,
- Information that was accessed,
- Access to masked information,
- Overrides of masked information,
- Failed attempts to access masked information,
- Changes in consent directives,
- Action performed related to personal health information - create, add, modify, delete, view, or disclose,
- Successful and failed login attempts,
- Preserves the original content of the recorded information when changed or updated,
- Account creation, modification, and deletion.

The Metadata in the audit logs is considered personal health information and should be retained as long as the personal health information it is about.

Monitoring Program

- Physician-trustees should develop procedures documenting the monitoring of EMR users.
- There should be a designated person responsible for the audit monitoring program.
  - The person responsible for authorizing ad hoc reports on user activities should not be the one who runs the reports. This separation of duties might not be possible in small practices.
  - The person who will receive automatic alerts of overriding of masking.
- What action will be taken if the audit report shows an EMR user has accessed a record without authorization??
  - Who will this action be reported to?
  - Will EMR privileges be revoked immediately until an investigation of the breach has been completed?
- Trustees should consider creating a progressive discipline policy that establishes penalties up to and including termination and/or reporting to the appropriate regulatory authority or body, depending on the seriousness of the violation

Auditing Users of the EHR

- Physician-trustees are also responsible for auditing the access to the EHR by employees, other health professionals, or medical students and residents at the medical practice who may include SLRR. PIP or the eHealth Portal.

Acceptable Use of Technical Resources

It is important for medical practices with EMRs to establish expectations for all employees, physicians, and third parties around the appropriate use of the practice's technical resources. The intent of an acceptable use policy is to ensure awareness and understanding of each person's accountability for using resources in a secure and privacy protective manner.

The medical practice's technical resources include the EMR, operating systems, storage media, network accounts, email accounts, Internet, and mobile technology such as laptops, cell phones, and tablets.

Inappropriate uses expose the medical practice to risks that include virus attacks, compromised network systems and services, and illegal activities.

Acceptable Use Agreement

Each user is assigned a user name and a password or some other method for the EMR to authenticate the user.

- Together a user name and password give each authorized user of the EMR a user account.
- Before a user is assigned a user name and password they are expected to sign an acceptable use agreement which explains the responsibility for appropriate use of technical resources.
- The acceptable use agreement is in addition to any confidentiality agreement the person might have signed.

Acceptable Uses

For purposes related directly to patient care and the administration of the medical practice.

All users are monitored for access to the EMR and other equipment, systems and networks where the password and user name are used.

User Responsibilities

Users are responsible for any and all use of their user accounts.

Users should ensure and safeguard against others obtaining unauthorized access to their accounts.

Users should not share passwords or any other access control information for their accounts.

Users are responsible for ensuring the confidentiality of all personal health information they have been granted access to, including:

- Ensuring the information is not observed by others while working at a computer,

- Ensuring they are logged out of their accounts when not at their computer,
- Exercising discretion when printing personal health information which can be viewed or observed by unauthorized persons,
- Refraining from copying, sending, duplicating or transmitting by any means, personal health information for any purpose other than patient care or a purpose identified to the patient or required by law.

Users are required to comply with all copyright and license conditions, such as:

- Refraining from moving, copying or transferring programs, files or other forms of software from one computing system to another without proper authorization to do so,
- Refraining from distributing, selling or making available software to any person where prohibited by copyright or license,
- Refraining from accessing and using software without proper authorization and license rights.

Passwords and Security

Employees and physicians are required to take all necessary steps to prevent unauthorized access to personal health information.

Keep passwords secure and do not share accounts or passwords. Change passwords at least quarterly.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the user leaves the computer.

Employees and physicians need to use extreme caution when opening e-mail attachments received from unknown senders, which can contain viruses, e-mail bombs, or Trojan horse code.

Personal Use

The physician-trustee should establish acceptable practices for employees to use the computers for personal activities such as e-mail and Internet access providing such activities do not interfere with the person's work schedule or responsibilities.

- The physician-trustee should not allow:
  - Any use that involves discriminatory, disparaging, defamatory or harassing comments,
  - Employees to access or view inappropriate content on the internet, such as websites that promote hate or that offer pornography, or to participate in electronic gambling,
  - Posting on Facebook, twitter, blogs, and other similar media cannot mention, harm or tarnish the image or reputation of the practice, its patients, employees or physicians,
  - Employees to use the practice's resources for streaming or downloading videos,

- Employees to use the practice's resources for personal gain.

Unacceptable Uses

Breaching legal protection provided by copyright and/or license to computer programs, technology or data.

Breaching security protections provided by all of the Acts and Codes of Saskatchewan or Canada that the medical practice and physicians are governed by.

Using technical resources to engage in any behaviour that might jeopardize the practice's security, including, but not limited to:

- Willfully bypassing or subverting the administrative, physical or technical electronic or procedural security controls,
- Attempting to alter or destroy resources (e.g. data, networks, electronics),
- Deliberately propagating malicious code (e.g. viruses, worms, Trojans),
- Generating or transmitting unsolicited commercial or advertising material such as spam or chain mail,
- Send anonymous messages.

Penalties

Violation of this policy should be considered to be grounds for disciplinary action. Trustees should consider creating a progressive discipline policy that establishes penalties up to and including termination and/or reporting to the appropriate regulatory authority or body, depending on the seriousness of the violation.

Examples of the Acceptable Use of Office Technology Policy

Technology	Core	Incidental	Incidental/ Unacceptable	Unacceptable	Against Existing Policy	Illegal
Phone	Making appointments for patients	Making a brief personal call	Spending a lot of time on personal calls resulting in work not being completed	Phoning 1-900 numbers on the clinic phone	Discussing personal health information in a manner or place that allows others to overhear.	Discussing personal health information with a drug rep
Mobile Phone	Making a work related call, email, text message or ping	Making a brief personal call, email, text message or ping	Making personal use of mobile phone that results in work calls or duties not being done	Phone 1-900 calls on a work mobile phone	Sending personal health information in an unencrypted email, text message or ping.	Sending personal health information in an email, text message or ping to a drug rep
Photocopier	Making copies of test results for a patient	Making a copy of a son's hockey schedule	Making copies of the hockey schedule for all the team members	Making a large number of copies of a garage sale	Copying a patient's chart without permission of the physician or privacy officer	Copying a patient's chart to give to a drug rep
Fax, including from the EMR	Faxing a referral letter	Faxing a trip itinerary to one family member	Faxing the full hockey team with the team's stats	Faxing your resume to potential employers	Faxing personal health information to another clinic without attempting to eliminate or minimize the amount of personal health information included in the fax	Faxing a list of patients to a drug rep
Email	Sending an email to a patient with education information requested by the patient	Emailing a friend to confirm lunch	Emailing the hockey team organizing rides to practices and games	Forwarding chain emails	Sending personal health information in an unencrypted email	Making libelous statements about co-workers in an email

Computer/ Tablet	Viewing a patient chart	Preparing a to do list for the kids' sitter	Writing a lengthy personal letter to a friend	Work is not done on time because you are playing solitaire	Viewing a patient's chart without permission	Installing a pirated version of software onto the office computer
Internet	Researching training courses and conference for the physician	Checking the hockey team's standing	Researching issues of personal interest during work hours	Watching YouTube during office hours.	Turning off the security features so you can play online poker	Downloading or sharing copyrighted movies or music
Social Media and Websites	Posting a job opening on a job site.	Checking Facebook on a coffee break	Watching videos that cause the network to operate slowly	Checking Facebook and Twitter during work hours	Tweeting about patients even if names are not used.	Posting personal health information about a patient who plays for the Rough Riders on a gossip website

Transmitting by Fax and Email

(HIPA s 16)

Medical practices need to transmit personal health information by fax and/or email many times a day. In doing so, physician-trustees need to recognize that this is a high risk activity that can result in a breach of personal health information. Some of the risks from using faxes and emails are

- Sending the document to the wrong number/email address resulting in the document being received by an unintended recipient without a legitimate 'need to know,.
- Sending the document to the correct number/email address but it is viewed by an unintended recipient (example, the faxed information is left unattended or the fax machine is located in an area where multiple people have access or the email address is one used by several people in the medical practice).
- The fax number/email address of the recipient has changed or the intended recipient is no longer employed by the organization.
- Emails pass through several points on the Internet during the transmissions that are not secure and are a potential breach point.

Actions to Reduce the Risks for Faxes and Emails

Only send the minimum amount of personal health information necessary and remove personal identifiers if possible.

When using emails for communications with patients CMPA recommends obtaining consent from the patient first. https://www.cmpa-acpm.ca/cmpapd04/docs/resource_files/infosheets/2005/com_is0586-e.cfm

Send email over secure channels.

- Use an email provider that supports secure, SSL-enabled POP and IMAP connections. Do not use Hotmail, Gmail or other free email for transmitting personal health information.
- Use person-specific email accounts. Do not use a general office email address to send or receive personal health information.
- Send personal health information as an attachment that is encrypted with strong encryption.

Always use a covering letter or text in the email and attach the personal health information as a second page in the fax or an attachment in the email.

- Ensure there is a warning that the information is only intended for the person identified as the recipient.

- Ensure the covering letter/email text includes the name of the intended recipient and the person sending the information.

Use saved speed-dial numbers for frequent fax recipients to prevent numbers being misdialed. Test these numbers periodically.

Put email addresses in the email address book. Confirm email addresses periodically.

For any new recipient, fax or email, verify the fax number or email address with a test sent before sending health information.

Develop policies on what to do if a fax was sent to the wrong place. (See breach management procedures).

Configure the fax machines to never save copies of received faxes.

Make sure that faxes do not remain on the fax machine after receipt, and that they are promptly delivered to the intended recipient.
Assign this responsibility to one or two employees.

Policies on the storage and destruction of records should include procedures for faxes and emails.

As with all disclosures of personal health information based on deemed consent, physician-trustees must only disclose personal health information to another health professional in accordance with the ethical practices of the profession and in accordance with their policies.

Fax and Email Upgrades

Use email encryption software, and consider the use of a fax machine or fax modem that encrypts transmissions

Ensure access to fax modems and emails are password protected.

Other advice

Provide CPSS with all changes in physicians fax numbers to reduce the possibility of receiving faxes in error.

Inform people who regularly fax or email personal health information of any changes in the fax number or email several times.

Establish procedures to addresses faxes and emails received in error.

Locate the fax machine, computers, and monitors in a secure location away from unauthorized browsing.

Regularly delete any information stored on the fax machine.

Review Privacy Considerations: Faxing Personal Information and Personal Health Information published by the Office of the Information and Privacy Commissioner athttp://www.oipc.sk.ca/resources.htm.

Wireless Devices and Networks

(HIPA s. 16)

The use of wireless devices is becoming more common in medical practices. Physician-trustees need to ensure they meet the highest standard of security for these tools if there is any possibility they will be used for viewing or storing personal health information. Today encryption is considered the standard for making information unreadable. More information about encryption is included in the discussion of General Security Software. Physicians and their IT support should monitor evolving best practices in this area to ensure continued security of the practice's network and wireless devices.

Risks of Wireless Networks

Unsecure wireless networks can provide access to the medical practice's network by a knowledgeable person.

- Only use secure wireless networks; those where a password is required to connect to the network.
- Only use secure websites when personal health information is involved; look for the padlock symbol in the address bar or the icon tray, or only use sites with an address that begins **https://** and has it on every page.

Data on unencrypted wireless networks is easily captured by an unauthorized person.

- Encrypt all information on wireless devices, although this only addresses information sent not received.

Use WPA2 security in the modems purchased for use in the medical practice and at home.

- Do not provide the wireless encryption key to people who do not have authorization to access personal health information at the medical practice.
- Use a minimum 128bit encryption standard.
- Have an IT professional test the wireless network periodically for weaknesses.
- Do not rely on WEP encryption.

Risk of Wireless Devices

Wireless devices such as laptops, Smart-phones, and tablets are easily lost and therefore require greater protection than stationary devices.

- Personal health information should not be stored on mobile devices except for those that are designed and will be used for long term encrypted storage.
- Occasionally personal health information and other confidential information are stored on mobile devices for short time periods.
    - Ensure the device is password protected and the information is encrypted.

- Some devices have software that allows for all information to be deleted from the device remotely if the device is lost.

Before a new wireless device is used an assessment should be made of its security. Ask questions such as:

- Does this device use encryption and if so how well tested is the encryption protocol?
- What is the cost of implementing a secure encryption protocol?
- Has this type of device been used on our network before?
- Can this device be configured to only allow authorized users to access it or the network through it?
- How easy will it be for an attacker to fool this device into allowing unauthorized access? What methods could be used?
- What secure authentication schemes are available and what cost or overhead is associated with their implementation and maintenance?
- How practical is wireless use considering the cost, potential loss, and added convenience?
- How secure is the authentication mechanism to be used?
- How expensive is the authentication mechanism to be used?
- How secure is the encryption mechanism?
- How sensitive is the data traveling through the wireless device?
- How expensive is the encryption mechanism?

The Office of the Information and Privacy Commissioner has published a report on Mobile Device Security. http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Best%20Practices%20-%20Mobile%20Device%20Security%20-%20March%202011.pdf

General Security Software

Encryption, Firewalls, Malware, and VPNs
(HIPA s 16, CPSS Bylaw 23.2(c)(xi))

Encryption

Encryption is the altering of data so that it is unreadable by anyone who does not have the key to unscramble the information.

- Encryption can be either hardware or software.
- It can be used on hard drives of servers, computers, and mobile devices
- It is very important to use encryption on laptops, USB keys, and other mobile devices like Smart-phones and tablets.
- There is also encryption software for email attachments.
- Web browsers will encrypt text automatically when connected to a secure server.
    - This is noted by a URL address beginning with ‘https,. The server decrypts the text upon its arrival. This however does not protect the text from being seen by employees who is not authorized to see the information.
- Without encryption, information passed over the Internet is not only available for virtually anyone to snag and read, but is often stored for years on servers that can change hands or become compromised in any number of ways.
- For more information see two publications from the Ontario Information and Privacy Commissioner, Healthcare Requirements for Strong Encryption, and Encrypting Personal Health Information on Mobile Devices.www.ipc.on.ca

Virtual Private Network

If the EMR is accessed remotely by physicians or vendors, physician-trustees are advised to set up a virtual private network. This can be accomplished through a hardware or software.

Virtual Private Networks or VPNs are strongly recommended if the physician is using a wireless network or if the backups are done remotely.

Security Software

Security software is essential for all computers.

- Physician-trustees are advised to work with an IT professional to determine the appropriate software for the medical practice and an update schedule.
- Updates to security software will be an ongoing cost to the medical practice.
- Install all vendor supplied updates
    - Physicians should get annual contracts for upgrades to firewalls, anti-virus, and malware.

Firewalls

A firewall is a device or set of devices, either hardware or software, designed to permit or deny network transmissions based upon a set of rules.

- Firewalls are used to protect networks from unauthorized access while permitting legitimate communications to pass.
- Medical practices should install a network firewall and personal firewall software on all computers.
- The medical practice should never turn off the firewall.

Anti-virus Software and Malware

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior.

Anti-virus software is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, Trojan horses, spyware, and adware.

- Ensure the anti-virus software is set to receive the latest virus definitions and scanning updates from your Internet service provider automatically.
- Purchase anti-virus software for computers and services and set to receive the latest virus definitions and scanning updates from the vendor of the product automatically.

General Office Security

(HIPA s 16, CPSS Bylaw 23.2(c)(xii))

The importance of the physical security of the medical practice's office cannot be overlooked.

Office Area

The full office needs to be securely locked after hours with a limited number of access keys available.

- Windows can be a point of entry and efforts should be made to secure these particularly if office equipment is visible through the windows.
- Ensure the landlord agreement includes conditions around when the landlord can access the office area.
- Consider locks that require using an access card and that records all people who access the office.
- Ensure keys are returned or locks changed when a employee, other health professional, medical student or resident ceases to work at the clinic.
- Larger medical practices should consider implementing security badges.

Office Equipment

Place monitors, printers, and fax machines where patients, unauthorized employees and others cannot see personal health information on them.

- If possible, keep office equipment in an office that can be locked.
- Place servers in an environmentally safe area and secure it to the floor or wall, or place in a locked cupboard.
- 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 these small storage media.
- Never leave portable equipment unattended when taken outside the office, such as in cars or hospital cafeterias.
- Require employees to set the lock screen or log off whenever they leave their workstation unattended.
- Ensure the computer cannot be opened again without a password.

College of Physicians and Surgeons of Saskatchewan Guideline

Appendix A: Transfer of Records

These CPSS Guidelines are included in the Handbook for the convenience of Physicians

Guideline: Provision of Patient Records to Patients

Preamble

This guideline has been developed jointly by the SMA and the College to guide physicians in dealing with the transfer of copies of patient records from a physician to their patients.

Patient medical records belong to the physician and not to the patient. Physicians have a responsibility to ensure that the record is secured and maintained accurately, and that information is not altered. The patient has a right to access the medical information in the chart, and to obtain a copy of documents in the chart, but not to obtain the chart itself.

Canadian courts have held that patients have a right of access to all of the information in their chart. This right of access includes all information in the file, including reports of consultants and other records.

The obligation to provide information to patients is also an ethical obligation. Paragraph 37 of the Code of Ethics of the Canadian Medical Association provides as follows:

Upon a patient's request, provide the patient or a third party with a copy of his or her medical record, unless there is a compelling reason to believe that information contained in the record will result in substantial harm to the patient or others.

The Guideline

1. Patients should never be given original medical records. This could result in loss of the file, removal of relevant portions of the patient file, and an inability for the physician to deal with future complaints, litigation or enquiries;

2. A copy of a requested record should be provided without undue delay;

3. A physician has a right to charge a fee in relation to photocopying a patient record. If a fee is to be charged, that fee should be fair and represent cost recovery including employees time and overhead costs. The Saskatchewan Medical Association publishes the Relative Value Guide, which on page A2 and Codes 510A and 516A on page A8 suggests what the Saskatchewan Medical Association considers to be a fair fee;

4. It has been customary not to charge a patient for a copy of relevant portions of a patient chart if the physician who has control of the record has moved or otherwise required the patient to transfer their care to another physician;

5. The physician should consider the patient's ability to pay when considering whether a fee will be charged and, if a fee will be charged, the amount of that fee:

6. Charging a fee for a copy of a record should never impede the orderly and timely transfer of required information.

7. If a fee is to be charged, and if the record is not immediately required for patient care or for some other pressing reason, it is reasonable for a physician to ask for some assurance of payment before a copy of the requested record is made.

Guideline: Transfer of Patient Records to Third Parties

Preamble

This guideline has been developed jointly by the SMA and the College to guide physicians in dealing with the transfer of copies of patient records from a physician to third parties.

Patient medical records belong to the physician, and not to the patient. Physicians have a responsibility to ensure that the record is secured and maintained accurately, and that information is not altered. The patient has a right to access the medical information in the chart, and to obtain a copy of documents in the chart, but not to obtain the chart itself. That includes a right to authorize other persons to obtain copies of their medical information.

Canadian courts have held that patients have a right of access to all of the information in their chart that is relevant to their medical care. This right of access includes all information in the file, including reports of consultants and other records.

The obligation to provide information to patients, or to a third party at the patient's request, is also an ethical obligation. Paragraph 24 of the Code of Ethics of the Canadian Medical Association provides as follows:

Upon a patient's request, provide the patient or a third party with a copy of his or her medical record, unless there is a compelling reason to believe that information contained in the record will result in substantial harm to the patient or others.

It is critical to ensure that either informed patient consent is obtained to transfer a record to a third party, or that the transfer is authorized by law (see paragraph 22 of the Code of Ethics of the Canadian Medical Association).

The Guideline

1. Physicians have an obligation to provide copies of patient charts to third parties if properly authorized by the patient;

2. Physicians should take appropriate steps to satisfy themselves that, if the request for a copy of a patient record is based upon the patient's request, the patient has given informed consent to the transfer;

3. If the authorization is in writing, and the authorization is dated a substantial time previous to the request, this may include an obligation to ensure that the patient still agrees to the transfer of the copy of the record;

4. If the request is made based upon a legal requirement, it is reasonable to expect that the person requesting the information will provide the authorization for the request, (court order, a copy of the legislation, etc.) before the documents are provided;

5. A copy of a requested record should be provided without undue delay;

6. A physician has a right to charge a fee in relation to photocopying a patient record. If a fee is to be charged, that fee should be fair and represent cost recovery including employees time and overhead costs;

7. If the record is not immediately required for patient care or for some other pressing reason, it is reasonable for a physician to ask for some assurance of payment before a copy of the requested record it made;

8. If, in addition to requesting a copy of a patient record, the third party requests an opinion, or wishes to speak to the physician pertaining to the care of the patient, it is reasonable for the physician to charge a reasonable fee for the time involved in discussing care provided to the patient, or in providing an opinion to the third party.

Guideline: Transfer of Patient Records Between Physicians

Preamble

The College and the SMA are regularly consulted with respect to disputes that arise when a physician leaves a medical practice and establishes a new practice. This guideline has been developed jointly by the SMA and the College to guide physicians in dealing with the transfer of patient records from one physician to another physician.

Courts have held that patient medical records belong to the physician and not to the patient. The physician has a responsibility to ensure that the record is secured and maintained accurately and that information is not altered. The patient has a right to access the medical information in the chart, and to obtain a copy of documents in the chart, but not to obtain the chart itself.

Information within a record cannot be disclosed to a third party without the consent of the patient unless the physician is required by law or by ethical principles to do so.

There are a number of situations in which a physician may need to access an old medical record. Examples include a billing review by the Joint Medical Professional Review Committee, complaints to the College of Physicians and Surgeons and legal proceedings. It is therefore essential that physicians maintain an ability to access medical records that they have created and assure their security.

The SMA, the College and CMPA all recommend that the clinic that owns the record should generally keep the original record, only providing a photocopy if requested. This is so for a variety of reasons:

1. The file could be lost in transit;

2. The patient may wish to return to the clinic for care, either on an episodic or permanent basis. The clinic will then need to obtain access to the medical file from the departing physician;

3. If the clinic needs access to the file at some later date, but the patient refuses permission to allow access, the person having control of the file may not be able to allow access;

4. The clinic has no control over the file after it leaves its possession and will have no proof of treatment given to the patient while at the clinic. This could make it very difficult to respond to complaints or court actions.

The SMA and College have concluded that the following principles apply to ownership of medical records:

1. Unless there is a specific agreement to the contrary, patient records belong to the owner of the practice where the patient is seen.

2. The same principles of ownership apply if the clinic is not owned by physicians. In the absence of an agreement to the contrary, the patient records associated with such clinics will be owned by the entity that owns the clinic (e.g. district health boards, corporations, etc.).

3. If a departing physician was an employee of the clinic, the physician is usually not entitled to take the charts for the patients that he/she will continue to see, unless the clinic agrees to transfer the patient records;

4. A departing physician who was a partner in a medical practice is not generally entitled to take any of the assets of the partnership, including patient charts. Usually, the physician leaving will not continue as a partner in the practice. Usually, the partnership will continue as a legal entity with the remaining partners. Usually, the assets of the partnership (including the patient charts) will continue to be owned by the partnership. The partners may agree to allow the departing partner to remove original patient charts for patients that he/she will continue to see;

5. Many physicians practice in an association. This means that the physicians in the practice will share expenses but will not join together to own the assets of the practice. Not all of these agreements are well-documented and it can be difficult in some circumstances to determine who owns what assets in the absence of a written agreement. When a physician leaves such an association, it can be difficult to determine exactly who is entitled to the patient records. As a general rule, if the patients in the practice are seen by more than one physician, it is likely that those patient records will continue to be owned by the clinic. This would mean that a departing physician does not have a right to take patient charts to a new location. If the patients were seen by only one physician, the right of that physician to take the patient records pertaining to those patients will be dependent upon the nature of the relationships within that association. In some circumstances, the right to remove patient charts may be determined by prior agreement between the physicians in the clinic.

Our Recommendations

The College and the SMA suggest that all medical practices should establish a written policy dealing with ownership of, and control over, medical records of patients who are seen at the clinic. Such a policy will help to avoid disputes and should address the following issues:

1. Who owns patient medical records if a patient is seen by more than one physician in the medical practice;

2. Who owns patient medical records if a patient is seen by only one physician in the medical practice;

3. If a physician who leaves the medical practice seeks a transfer of medical records pertaining to patients of the medical practice what charge, if any, will be made by the medical practice;

4. If copies of some records will be provided at no cost, what records will be so provided.

The Policy

The following principles apply to a request for a transfer from one physician to another physician. There may be unusual circumstances that make the application of these principles impractical, but generally physicians should follow these principles:

1. A medical practice should retain the original records in accordance with the requirements of the College bylaws;

2. Patient files should only be transferred to another physician with the express or implied consent of the patient. If there is any doubt about the consent of the patient, the clinic should obtain authorization from the patient:

3. A copy of a requested record should be provided without undue delay;

4. It has been customary not to charge a colleague for a copy of relevant portions of a patient chart. This is especially so if the physician who has control of the record has moved or otherwise required a patient to transfer their care to another physician.

5. A request for payment from another physician may be justified if there have been repeated requests for transfer of information relating to that patient, if the patient has transferred voluntarily to another physician in the locality, if the request is for a copy of a large portion of a patient file, or if the request requires considerable expenditure of physician or time.

6. If a fee is to be charged, that fee should be fair and represent cost recovery including time and overhead costs. The Saskatchewan Medical Association publishes the Relative Value Guide, which on page A2 and Codes 510A and 516A on page A8 suggests what the Saskatchewan Medical Association considers to be a fair fee;

7. Charging a fee for a copy of a record should never impede the orderly and timely transfer of required information.

8. If a fee is to be charged, and if the record is not immediately required for patient care, it is reasonable for a physician to ask for some assurance of payment before a copy of the requested record is made.

Additional Common Considerations Relating To This Guideline

There are some circumstances in which it may be more practical to transfer original patient files, rather than to transfer a copy of patient files to a physician.

If a physician with an established practice moves to another clinic and the departing physician has provided all, or nearly all, of the care to a patient, it may be more practical to transfer the entire file than to leave the file at the existing clinic. If patient care has been shared between the physicians in the clinic, but the patient will be transferring their care to the departing physician, the clinic may want to provide the patient file to the departing physician to allow that physician to photocopy relevant portions of the chart, and return the original.

There are some circumstances where a file will be sent to a hospital or other agency to assist in providing care for the patient at that location, with the file then returned to the clinic. In such circumstances the clinic should:

1. Consider whether patient authorization is required (see above);

2. List the patient files that have been so transferred and make a record when those files are returned;

3. Ensure that the files are transferred by a secure method to prevent loss in transit;

4. If the files are to be transferred temporarily to allow for them to be copied, the medical practice and the departing physician should agree on a date when those files will be returned;

5. If the clinic transfers the files permanently, the medical practice and the departing physician should enter into an agreement that the departing physician will, upon the request of the medical practice, allow the medical practice access to the patient files that were transferred if needed by the medical practice (this could be required to deal with litigation, a fee review by JMPRC, etc.)

NOTE: These guidelines are current as of May 4, 2012, but may be subject to amendment in the future.

Saskatchewan
Ministry of
Health

Appendix B: Overview of Consent Requirements in The Health Information Protection Act Prepared by Saskatchewan Health

July 2005

Table of Contents

N.B.: The Health Information Protection Act and this overview deal with consent for collection, use, and disclosure of personal health information; not with consent for treatment or service.

Please note that this Overview is provided for reference purposes only. The Overview discusses the intent of specific clauses and should not be considered an interpretation of the law. The Health Information Protection Act should be consulted for interpretations. Trustees should seek the advice of legal counsel as necessary.

Introduction

The requirement for consent for the collection, use, and disclosure of personal health information exists throughout The Health Information Protection Act (HIPA). In particular sections 26 and 27 regarding use and disclosure contain important requirements for trustees to consider regarding consent.

The following overview of consent in HIPA will provide the user with a basic understanding of how consent works in the Act.

Using the Act

Understanding the order of the Act is important for understanding how to interpret the consent provisions.

Part II - Rights of the Individual - this part identifies the rights that individuals have under the Act in regard to their own personal health information. Sections 5, 6, and 7 all provide important information regarding consent including what is required to make a consent a valid consent. Part II should be consulted when consent is required in other parts of the Act.

Part IV - Limits on Collection, Use and Disclosure of Personal Health Information by Trustees - this part provides rules regarding the collection, use and disclosure of personal health information by trustees including describing circumstances where consent is required. In particular Section 26 and 27 provide rules regarding use and disclosure of personal health information. Part IV should be consulted when considering collection, use or disclosure of personal health information or when developing policy for collection, use or disclosure.

Acting on a Consent collected by Others See Section 6 HIPA

The Act contemplates situations where a trustee will receive a consent from another trustee and enables that trustee to act on that consent without also seeking to confirm the consent or obtain an additional consent. Subsection 6(6) of the Act states

6(6) A trustee, other than the trustee who obtained the consent, may act in accordance with an express consent in writing or a record of an express consent having been given without verifying that the consent meets the requirements of subsection (1) unless the trustee who intends to act has reason to believe that the consent does not meet those requirements.

Consent can be Time-limited See Section 6 of HIPA

Section 6 provides for the option of making a consent "effective for a limited period." HIPA does not set a specific time frame for a consent to apply. An appropriate time limit will vary with the type of consent required. The circumstances of the request should be considered if a time limit is set.

Consent by Minors See Section 56 of HIPA

HIPA provides guidance for issues of consent regarding individuals less than 18 years of age. Specifically, the Act states that

Any right or power conferred on an individual by this Act may be exercised

- (c) by an individual who is less than 18 years of age in situations where, in the opinion of the trustee, the individual understands the nature of the right or power and the consequences of exercising the right or power;

- (d) where the individual is less than 18 years of age, by the individual's legal custodian in situations where, in the opinion of the trustee, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the individual;

The intent of subsection 56(c) is to allow a trustee to accept the consent of an individual less than 18 years of age, provided the trustee believes the individual understands the consequences of the decision. This is intended to reflect the common practice of providing certain health services to a minor provided he/she understands the nature of the service, without the consent of a parent or guardian.

Similarly, subsection 56(d) provides guidance for how to respond if a trustee receives consent from the parent or legal guardian for use or disclosure of personal health information of someone under 18 years of age. Specifically the intent of the section is to allow the trustee to disclose the information only if they believe it would not constitute an unreasonable invasion of privacy. In this case, if there is any doubt or uncertainty as to whether the minor would consent, it is probably not reasonable to conclude that it would not be an invasion of privacy. It is probably sensible to seek consent of the minor.

Consent by Others See Section 56 of HIPA

The Act anticipates that there will be circumstances in which an individual is not able to exercise their own rights and powers conferred by the Act, this includes the right to consent to the collection, use or disclosure of personal health information. In these circumstances, a trustee should be guided by Section 56 - Exercise of Rights by Other Persons. The section reads as follows:

Any right or power conferred on an individual by this Act may be exercised:

a) where the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate;
b) where a personal guardian has been appointed for the individual, by the guardian if the exercise of the right or power relates to the powers and duties of the guardian;
c) by an individual who is less than 18 years of age in situations where, in the opinion of the trustee, the individual understands the nature of the right or power and the consequences of exercising the right or power;
d) where the individual is less than 18 years of age, by the individual's legal custodian in situations where, in the opinion of the trustee, the exercise of the right or power would not constitute an unreasonable invasion of the privacy of the individual;
e) where the individual does not have the capacity to give consent:
   i. by a person designated by the Minister of Social Services if the individual is receiving services pursuant to The Residential Services Act or The Rehabilitation Act; or
   ii. by a person who, pursuant to The Health Care Directives and Substitute Health Care Decision Makers Act, is entitled to make a

health care decision, as defined in that Act, on behalf of the individual; or

f) by any person designated in writing by the individual pursuant to section 15.

Deemed Consent See Sections 26 and 27 of HIPA

The Act states that consent is not required to use or disclose personal health information if it is required to provide a service to an individual. This includes using or disclosing personal health information to:

- arrange for a service;
- assess the need for a service;
- provide a service;
- continue provision of a service; or
- support the provision of a service.

An individual's **consent is deemed to exist** where personal health information is required for these purposes. The service must be one which is requested or required by the individual.

Where an individual's consent is deemed to exist, it must be for the purpose for which the trustee collected the information or for a purpose that is consistent with that purpose. In addition to service delivery, consent can also be deemed to exist for the purpose of disclosing personal health information of an individual to that individual's next of kin or someone with whom the individual has a close personal relationship if the disclosure relates to health services currently being provided to the individual and the individual has not expressly stated that they do not want their information to be disclosed.

In circumstances where a trustee determines that an individual's consent is deemed to exist for service delivery, use or disclosure of the individual's personal health information by the trustee can only take place where:

- the use or disclosure is in accordance with established privacy and security policies and procedures; and
- if the use or disclosure is being made by a health professional, such access, use or disclosure must be in accordance with the ethical guidelines applicable to the health professional.

Specifically, subsections 27(1) to (3) read as follows:

27(1) A trustee shall not disclose personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section, section 28 or section 29.

(2) A subject individual is deemed to consent to the disclosure of personal health information:

- for the purpose for which the information was collected by the trustee or for a purpose that is consistent with that purpose;

- for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual; or
- to the subject individual's next of kin or someone with whom the subject individual has a close personal relationship if:
  i. the disclosure relates to health services currently being provided to the subject individual; and
  ii. the subject individual has not expressed a contrary intention to a disclosure of that type.

(3) A trustee shall not disclose personal health information on the basis of a consent pursuant to subsection (2) unless:

a) in the case of a trustee other than a health professional, the trustee has established policies and procedures to restrict the disclosure of personal health information to those persons who require the information to carry out a purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act; or
b) in the case of a trustee who is a health professional, the trustee makes the disclosure in accordance with the ethical practices of the trustee's profession.

Express Consent See Sections 6, 26, 27 & 29 (in particular) of HIPA

Where a consent is required by the Act (not deemed), it may be express or implied

Subsection 6(4) reads as follows:

> 6(4) Consent may be express or implied unless otherwise provided.

An express consent may be oral or written and must be consistent with the conditions laid out in Section 6.

Section 6 of HIPA places emphasis on the **process** of gaining consent, including the need for an express consent to be an informed consent. A consent form should not be the sole focus of the consent process. A consent form should only serve as a record of a valid consent being given. A signed consent form which results from a process that does not comply with Section 6 will not likely be treated as valid.

Implied Consent See Section 6 of HIPA

Where a consent is required by the Act (not deemed), it may be express or implied

Subsection 6(4) reads as follows:

> 6(4) Consent may be express or implied unless otherwise provided.

Where consent is implied, there must be the ability for a trustee to infer the consent of an individual in such circumstances. The intent of an implied consent is to enable a trustee to use or disclose personal health information for the purpose the information is collected without having to specifically ask if it is OK to use or disclose the information for that purpose. Yet consent is still considered.

The trustee must be able to form the opinion that the individual **would** consent to the use or disclosure if asked.

Risk Assessment – Trustees will need to consider if there is risk in relying on an implied or inferred consent. If a risk is identified it may be preferable to obtain an express consent.

Informed Consent See Sections 6 and 9 of HIPA

Consent is informed if "the individual who gives the consent is provided with the information that a reasonable person in the same circumstances would require in order to make a decision about the collection, use or disclosure of personal health information."

An express consent and an implied consent must be an informed consent.

Section 9 of HIPA also requires that trustees take steps to inform individuals of anticipated uses and disclosures of personal health information if collecting from the subject individual. This helps ensure an informed consent.

Revoking Consent See Section 7 of HIPA

Section 7 of HIPA ensures the right of individuals to revoke a consent already given. It is important to note that the Section does state that "no revocation shall have retroactive effect." The intent here is to ensure that a trustee is not in violation of the law if they have acted on a consent received and (for example) disclosed personal health information prior to the consent being revoked.

Valid Consent See Section 6 of HIPA

Where consent is required for the collection, use or disclosure of personal health information by the Act, it must be in accordance with Section 6. Specifically, the consent:

- must relate to the purpose for which the information is required;
- must be informed;
- must be given voluntarily; and
- must not be obtained through misrepresentation, fraud or coercion.

Written consent See Section 6 of HIPA

Section 6 clarifies that a consent can be express or implied and that a consent need not be in writing.

Appendix C: Trustees in the eHealth Environment

Ministry of Health

The Ministry of Health has a mandate to support Saskatchewan residents in achieving their best possible health and well-being. With direction from the Minister of Health, Saskatchewan Health establishes policy direction, sets and monitors standards, provides funding, supports regional health authorities and other organizations, and ensures the provision of essential and appropriate services.

The Ministry is the trustee for

- Pharmaceutical Information Program (PIP) and
- co-trustee with the Regional Health Authorities of the Saskatchewan Laboratory Results Repository (SLRR)
- Medical Services Branch (MSB) data
- Saskatchewan Immunization Management System (SIMS)

eHealth Saskatchewan

eHealth (formerly the Saskatchewan Health Information Network) was established on December 14, 2010, pursuant to Order in Council 734/2010. eHealth's prescribed objects and purposes are as follows:

(a) to lead Saskatchewan Electronic Health Record (EHR) planning and strategy for the Province of Saskatchewan;

(b) to procure, implement, own, operate or manage the Saskatchewan EHR and the associated provincial components and infrastructure;

(c) where appropriate, to procure, implement, own, operate or manage other health information systems for the benefit of the Province of Saskatchewan;

(d) to facilitate improved health provider and patient access and use of electronic health information for the purpose of enhancing the delivery of health care services in the Province;

(e) to establish the provincial health information and technology standards necessary for connecting local electronic health information systems to the Saskatchewan EHR and associated provincial components and infrastructure;

(f) to work and cooperate with regional health authorities, other health care organizations, providers, other organizations providing related services as agents, contractors or partners in health information systems and the public in the development and delivery of the Saskatchewan EHR and where appropriate, other health information systems;

(g) to provide data stewardship for the Saskatchewan EHR and where appropriate, other health information systems and databases, including, without limitation:

i. administering the rules for EHR data collection, use and disclosure;

ii. establishing and administrating provincial standards to protect the quality, confidentiality and security of EHR data;

iii. protecting the EHR data as a strategic resource; and

iv. acting as trustee and information manager for Saskatchewan EHR databases and services; and

(h) to pursue consistent funding for the Saskatchewan EHR, and where appropriate, other health information systems from all available resources, including, without limitation, Canada Health Infoway Inc. and to be accountable for the spending of such funds.

eHealth Saskatchewan, is an IMSP. It provides information technology and information management services to the Ministry of Health, RHAs and other health service providers and delivery agencies within Saskatchewan.

Regional Health Authorities

Health services are primarily delivered through 12 regional health authorities often referred to as health regions. The Regional Health Authorities (RHA) were established under *The Regional Health Services Act*. The Act came into force August 1, 2002 and sets out the powers and responsibilities for both the Minister of Health and the RHA. Each regional health authority has a governing board. The major areas of responsibility for the RHAs include:

- Hospitals;
- Health centres, wellness centres, and social centres;
- Emergency response services, including first responders, ambulance;
- Supportive care, such as long-term care, day programs, respite, palliative care and programs for patients with multiple disabilities;
- Home care;
- Community health services, such as public health nursing, public health inspection, dental health, vaccinations, and speech pathology;
- Mental health services; and
- Rehabilitation services.

The RHAs are the trustees of the personal health information in their custody or control in the above settings and also are source trustees for SLRR and the Radiology Information System (RIS) and Picture Archiving and Communications System (PACS)

Saskatchewan Cancer Agency

Cancer care services are primarily delivered by the Saskatchewan Cancer Agency. The Agency was established under *The Cancer Agency Act*. The Saskatchewan Cancer Agency has a governing board appointed. Its major areas of responsibility include:

- Assessing the cancer care and health care needs of the persons to whom the agency provides cancer care services;
- Co-ordinating the cancer care services it provides with health services, provided by regional health authorities and other providers of health services;
- Evaluating the cancer care services that are provided in Saskatchewan;
- Establishing provincial protocols and standards for cancer care services;
- Educating health care providers in the prevention, diagnosis, treatment and post-treatment of persons at risk of cancer or diagnosed with cancer; and
- Promoting and encouraging health and wellness.

The Cancer Agency is the trustee of personal health information in their custody or control.

Information Management Service Providers (IMSP)

There are many IMSPs in the eHealth environment. eHealth Saskatchewan is the largest IMSP, performing this role for PIP, SLRR, RIS-PACS, SIMS and other provincial information systems. EMR vendors are IMSPs when physicians select the ASP model for their EMR. Physicians may also use a local IT company to provide services to store or manage EMR data. Local companies that store paper and electronic information are also IMSPs. IMSPs must be fully aware of their responsibilities under HIPA and as set out in the agreement with the trustee whose information they are managing.

IMSPs are not trustees of the personal health information managed on behalf of trustee.

Designated Archives

When physician-trustees cease to practice they may wish to assign responsibility for their records to someone else. They may enter into an agreement with another physician or HIPA allows them to archive the records with designated organization. There are ongoing discussions between the Ministry of Health and the designated organizations as to their role. More advice is expected from the Ministry in the future.

The organizations designated as archives for records of personal health information under HIPA are:

- affiliates, as described in the *Regional Health Service Act*
- Department of Health
- Health professional bodies that regulate members of a health profession pursuant to an Act
- Regional health authorities
- Saskatchewan Archives Board
- Saskatchewan Health Information Network (eHealth Saskatchewan)
- University of Regina Archives

- University of Saskatchewan Archives

Health Professionals

In addition to physicians these other health professionals can be trustees when not employed by another trustee:

- Dentists
- Dietitians
- Licensed Practical Nurses
- Medical Laboratory Technologists
- Medical Radiation Technologists
- Midwives
- Naturopathic Physicians
- Occupational Therapists
- Optometrists
- Paramedics
- Pharmacists
- Nurses
- Psychiatric Nurses
- Speech-language Pathologists and Audiologists
- Physical Therapists
- Podiatrists
- Psychologists

Third Parties

Third parties are those 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 or residents. Physicians should enter into a written agreement with third parties that includes an obligation to protect the personal health information at the standard of the medical practice or higher.

Office of the Information and Privacy Commissioner

The Information and Privacy Commissioner is not a trustee but is an independent officer of the Saskatchewan Legislative Assembly. He oversees three different Saskatchewan statutes:

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

The OIPC has jurisdiction over Saskatchewan government departments; Crown Corporations; provincial agencies; health regions; universities, colleges and schools; municipalities; health information trustees such as physicians, pharmacies, laboratories, diagnostic clinics, and a number of other organizations. The OIPC has no authority over the federal government or the private sector other than private businesses that are health information “trustees”.

The OIPC ensures the privacy and access rights of the people of Saskatchewan are respected by:

- Informing members of the public of their information rights
- Mediating access and privacy disputes between individuals and public bodies
- Making recommendations on appeals from access to information decisions by public bodies
- Investigating and resolving privacy complaints
- Issuing recommendations on public bodies' policies and practices
- Commenting on proposed laws and policies