STANDARDS OF PRACTICE

PRIVACY & HEALTH INFORMATION

Name: Privacy & Health Information
Date Approved: 03/15/2019
Date Updated:
Number: SP-PM-8
Type: Practice Management
Reference: The Health Information Protection Act (HIPA)
http://www.publicationshttp://www.publications.gov.sk.ca/freelaw/documents/english/Statutes/Statutes/Ho-021.pdf
The Health Information Protection Regulations
http://www.publications.gov.sk.ca/freelaw/documents/English/Regulations/Regulations/Ho-021r1.pdf
The Freedom of Information and Protection of Privacy Act
http://www.publications.gov.sk.ca/freelaw/documents/English/Statutes/Statutes/F22-01.pdf
The Local Authority of Freedom of Information and Protection of Privacy Act
http://www.publications.gov.sk.ca/freelaw/documents/English/Statutes/Statutes/L27-1.pdf

The Saskatchewan Association of Optometrists endeavors at all times to ensure the privacy of all persons. Members have an obligation to be familiar with the Health Information Protection Act (HIPA) and to protect the privacy of their patients at all times.

Glossary of Terms Within HIPA

What follows is a list of common terms used in our HIPA regime in Saskatchewan. A few of these terms are defined in section 2 of HIPA. Many of these terms have meanings that are well established in Canadian jurisprudence and in decisions/orders of privacy oversight agencies developed over the last 25 years. Trustees should be familiar with the meaning of these terms and their purposes within HIPA.

Access is the right of an individual (or his or her lawfully authorized representative per section 56 HIPA) to view or obtain copies of records in the custody or control of a trustee. This is subject to limited exceptions in section 38 of HIPA. This is a fundamental element of HIPA and one which all trustees must organize to facilitate. This is quite different than the discretionary decision to disclose personal health information (phi) to a third party. The least amount of information necessary for the purpose and the need-to-know rules do not apply when responding to an access request under HIPA.

Applicant refers to an individual who has made an access request for his/her phi to a health information trustee.

Need-to-Know Sec 23(1) https://oipc.sk.ca/assets/ipc-guide-to-hipa.pdf
Need-to-know principle is self-explanatory. Trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an individual. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know the information for the purpose of delivering their mandated

services. A trustee should limit collection and use of phi to what he/she needs-to-know to do his/her job, not collect or use information that is "nice to know".

Circle of Care vs. Need-to-Know

Circle of Care is a popular term among Saskatchewan trustees. In this concept, the patient is at the center of the circle. Health care professionals involved in the diagnosis, treatment and care of the patient are also in the circle and would be entitled to view and use personal health information. However, need-to-know is the concept used in HIPA and is simpler and more accurate. A trustee should only view and use personal health information if they have a need-to-know. Need-to know will vary with each episode of care. When in doubt, ask yourself, "do I really need-to-know this information?"

Collection is defined by HIPA as to "gather, obtain access to, acquire, receive or obtain phi from any source by any means" (section 2(b) of HIPA).

Complainant refers to an aggrieved individual who makes a formal complaint to the Commissioner to investigate an alleged breach by that trustee pursuant to section 52 of HIPA.

Confidentiality is the protection of phi once obtained against improper or unauthorized use or disclosure. This is just one aspect of privacy and must not be conflated with privacy.

Consent in HIPA provides any trustee with 3 different options: (1) express consent (highest standard), (2) implied consent with a right to opt out (lower standard), and (3) no-consent or in section 27(2) described as "deemed consent". Except for three limited circumstances where express consent is required, trustees must determine, in accordance with their ethical codes and standards and the circumstances and urgency of the health service, which option is most appropriate. In an emergency room or ICU, no consent may be the most appropriate option. In the treatment of a diabetic patient where the patient must play a large role in his/her own treatment plan, express consent would be more appropriate.

Control is a term used to indicate that records that are not in the physical custody of the trustee are still within the influence of that body via another mechanism (i.e. contracted service, trustee employees working remotely, etc.).

Custody is the physical possession of a record by a trustee.

Disclosure is exposure of phi to a separate entity, not a division or branch of the trustee in custody or control of that information. For example, when a health region shares information with a family member, an insurer, media, SK Health, SK Cancer Agency, WCB, lawyer, police, etc. this amounts to a disclosure. Occasionally this will be mandatory (*The Gunshot and Stab Wound Mandatory Reporting Act* and *The Public Health Act*), but in most cases this requires the exercise of discretion on the part of the trustee. That discretion must be exercised mindful of the rule to disclose the least amount of phi necessary for the purpose.

Duty to Assist means responding openly, accurately and completely to an individual requesting access to their own phi. It does not allow a patient/client to specify which employee in a trustee organization explains terms in a health record.

Information Management Services Provider (IMSP) is defined in section 2(j) of HIPA. In Investigation Report H-2005-002 (Prevention Program for Cervical Cancer) the OIPC determined that a trustee that is acting as an IMSP for another trustee cannot use that phi it has received in that capacity for any of its own purposes. Generally, the sharing of phi with an IMSP is a use and not a disclosure since the trustee providing phi to the IMSP should be, by contract, exercising control over the phi in the temporary possession of the IMSP.

Personal Health Information includes information about one's physical or mental health and/or information gathered in the course of receiving a health service from a trustee. It includes information in an independent medical examination report.

Policies and Procedures for Technical, Physical and Administrative Safeguards refer to the reasonable measures that a trustee must take to protect phi in its custody or control. This is required by section 16 of HIPA. <u>These policies and procedures must be in writing.</u> The OIPC has indicated in the past that the Canadian Health Informatics Association (COACH) guidelines represent best practices. See also ISO/ISE 17799 Information Technology – Security Techniques – Code of Practice for information security management. These best practices evolve over time. For example, for portable computing devices such as laptops and PDFs, encryption is now seen as a requirement to meet the reasonableness threshold for phi.

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

Privacy Breach happens when there is an unauthorized collection, use or disclosure of phi, regardless of whether the phi ends up in a third party's possession.

Reasonable Fees, as permitted by section 39 of HIPA.

Review is the process by which the OIPC considers either a decision or failure of a trustee to provide an applicant with access to his or her phi.

Secondary Purpose refers to the use or disclosure of phi for a purpose other than that for which it was originally collected.

Severing is the exercise by which portions of a document are blacked out pursuant to section 38(1) of HIPA before that document is provided to an applicant.

Surrogate refers to someone other than the individual exercising rights or powers under HIPA on behalf of the individual. This is defined by section 56 of HIPA.

Technical Safeguards are the technology and the policy and procedures for its use that protect personal health information and control access to it.

Transparency Obligations refers chiefly to sections 9, 10 and 16 of HIPA. These obligations require trustees to provide information to patients/clients about how the trustee collects, uses and discloses information, the patient's/client's right of access to correction and their right to appeal to the OIPC if dissatisfied with the response of the trustee.

Trustee includes only those bodies particularized in section 2(t) of HIPA that have custody or control of phi.

Use indicates the internal utilization of phi by a trustee and includes sharing of the phi in such a way that it remains under the control of that trustee. For example, in a regional health authority and its facilities, the sharing of information between employees, volunteers and contractors, including physicians with privileges, constitutes "use" of the phi since the sharing happens under the control of the regional health authority.

Checklist for Compliance with HIPA

Optometrists should consider the following checklist to evaluate their compliance with privacy legislation:

1. Patients should know what information is being collected about them and why it is being collected.
    - A poster, sign or brochure should be freely available in the clinic that states:
        - Possible uses of patient information
        - Patients' right of access to their records
        - Patients' right to request amendments to their records
    - Information collected should be limited to that which is necessary for the care of the patient and for registration and billing purposes.

2. There should be a process for appropriate patient consent to collection, use and disclosure of information.
    - Consent must be informed and free of any coercion.
    - Deemed (or implied) consent is generally sufficient for the ongoing care of the patient after the original presentation, including referrals to other caregivers. Release of information within the care team should be on a need-to-know basis.
    - Express (usually written) consent should be obtained for use or disclosure of information for any purpose other than the original purpose for its collection.
    - Patients have the right to limit consent.
    - Patients can withdraw consent at any time. The consequences of withdrawal of consent should be discussed explicitly with the patient and documented.

3. The office must have a process to permit patient access to personal health information.
    - Patients must be permitted to see information in their records and to have copies of the records upon request. The optometrist should retain original documents.

- There are limited circumstances in which patients may be refused access to all or part of their record. Generally, this is limited to circumstances in which disclosure is likely to endanger the mental or physical health or safety of the patient or another person, would disclose confidential information about someone other than the patient, or would identify a third party who provided information to the optometrist in confidence.
- Prudent optometrists will ensure that patient access to records is supervised.
- Optometrists may charge a reasonable fee for providing access and/or copies.

4. There should be a mechanism to update and correct information in personal health records.
   - Registration and billing data must be updated as required.
   - Clinical records should be complete and accurate. Amendments to the clinical record should not erase any previous entries to the chart, should be dated and should indicate clearly that an addition or amendment is being made.
   - Corrections can be made to inaccurate or incomplete factual information. An optometrist is not required to make an amendment to a patient record merely because a patient disagrees with the optometrist's diagnosis or opinion.
   - Optometrists who use electronic medical records should ensure that their medical record software tracks additions/amendments.

5. All personal information (registration data, billing data, health records, staff/employee records, etc.) should be kept appropriately secure.
   - Consider locks, alarms and other physical security devices.
   - Electronic records should be password protected, and electronic systems should have appropriate firewalls and other electronic security mechanisms. Consider handcuffing (limiting access to portions of the electronic record to defined users).
   - Office policies and procedures should ensure that records are kept secure, that written information cannot be seen by unauthorized persons, that conversations cannot be overheard, and that all optometrists and employees understand the importance of complete confidentiality.
   - If an information manager (computer support person, offsite storage company, etc.) has access to patient information, a written agreement should be in place whereby the information manager agrees to ensure confidentiality and limit access to the records.

6. The office must designate an individual (ideally an optometrist) to act as Privacy Officer to oversee management of personal information.
   - The Privacy Officer should be familiar with the obligations under HIPA.
   - This individual should develop and implement the privacy policies for the clinic and provide clinic staff with advice regarding HIPA compliance.
   - All employees should know who this person is.

7. All staff should understand what types of information may be disclosed, to whom, and under what conditions.
    - Disclosure within the "circle of care" (i.e. among health care professionals in the course of providing patient care) does not generally require explicit consent; however, it should be on a need-to know basis.
    - HIPA allows disclosure without consent in a limited number of other situations (e.g. to a proxy for the patient in the case of advanced care directives, to a quality of care committee, for professional review/audit, to minimize danger to the health or safety of an individual). Disclosures of this type should be well-documented and overseen by the clinic's Privacy Officer.
    - The office should have explicit policies that define whether staff may respond to requests for information about patients.
    - Where information is shared among providers (or among trustees as defined in HIPA), consideration should be given to formal data sharing agreements signed by both parties. Data sharing agreements may be particularly important when data are shared electronically. Such agreements should bind both parties to comply with privacy requirements.
    - The default position should always be to require explicit consent from the patient prior to any disclosure.
    - When in doubt, staff should forward requests for information to the Privacy Officer.

8. Clinics should have a specific office policy for information management. All staff members should receive training about the policy and sign confidentiality agreements.
    - Staff policies and procedures should contain an explicit privacy policy. Non-compliance with the privacy policy should be grounds for disciplinary action.
    - Staff should receive regular in-service training on issues related to information handling.
    - Staff should be required to sign a confidentiality agreement at the time of hiring. Consider annual renewals of the agreement. The Agreement should state that:
        - The employee is familiar with the office privacy policies
        - The employee will not read, use or disclose information in any patient record unless required for patient care, or to fulfill their job responsibilities
        - The employee will not disclose any patient information to anyone except in accordance with the clinic's policies or as directed by the clinic's Privacy Officer
    - The clinic's privacy policy should be available to patients upon request.

9. The office should follow accepted guidelines for the retention and destruction of personal information.
    - Guidelines for retention are usually those determined by the licensing authority or other professional oversight body.
    - Destruction of personal information should always be by a method that removes personal identifiers and minimizes the chance of any inadvertent disclosure of information.
    - If the office utilizes a third party to store or destroy records, there should be a signed agreement in which the third party agrees to maintain confidentiality with respect to the information in those records.

10. A process should be in place for handling complaints about management of personal information.
    - The process should be defined in the office privacy policy, and usually should be handled by the Privacy Officer.
    - In the event that a complaint cannot be resolved, the Privacy Officer or designated individual should know the mechanisms for referral of the complaint to the Saskatchewan Association of Optometrists, attention of the Registrar or to the office of the Information and Privacy Commissioner.

11. Offices should have a clear and concise policy on how they will transmit and receive patient information. Patients should be made aware of the office policy. It is important for the custodians to understand risks when transferring patient information and to take steps to mitigate them before faxing and emailing documents.

Risks of Emailing

- Emailed to the wrong recipient
- Email is often accessed on portable devices, such as smart phones, tablets and laptops, which are vulnerable to theft and loss
- An email can be changed or altered without knowledge
- Emails are vulnerable to interception and hacking by unauthorized third parties

Addressing the Risks

Implement technical, physical and administrative safeguards to protect patient information.

- Encryption for portable devices
- Strong passwords
- Firewalls and anti-malware scanners

Physical Safeguards Include:

- Restricting office access, using alarm systems and locking rooms where equipment used to send or receive health information by email is kept
- Keeping portable devices in a secure location, such as a locked drawer or cabinet when they are unattended

Administrative Safeguards Include:

- Providing a notice in an email that the information received is confidential
- Providing instructions to follow if an email is received in error
- Communicating by email from professional rather than personal accounts
- Confirming an email address is up to date
- Ensuring the recipient's email address corresponds to the address proposed to be sent
- Regularly checking pre-programmed email addresses to ensure that they are still correct
- Restricting access to the email system and to email content on a need-to-know basis
- Informing individuals of any email address changes

- Recommending that individuals implement the above safeguards, including that individual communicate by email at an email address that is password protected and is accessible only to them

Custodians should also ensure compliance with the safeguards specified in any other policies and procedures, such as those related to bring your own devises to the workplace.

Email Encryption

Email encryption is an effective way to mitigate the risks associated with emailing personal health information. Encryption scrambles the contents of an email so that only those with access to a secret key or password can unscramble and read it. Encryption minimizes the risk of unauthorized collection, use or disclosure of information.
**Email protection information obtained from the Information and Privacy Commissioner of Ontario.*

Risks of Faxing

Risks of faxing are similar to emailing. Fax numbers should be verified prior to transmission. Pre-coded fax numbers should be checked periodically to ensure they are still active and correctly associated to the intended source.

What to do When a Breach of Confidentiality is Suspected or Determined

It is recommended to review https://oipc.sk.ca/assets/ipc-guide-to-hipa.pdf for advice and protocols to follow when a breach has been determined or suspected.

Privacy Policy – "Sample"

The privacy of personal information is an important principle to *<<insert your practice name>>*. We take care in how we collect, store and use your personal information that is collected to be able to meet your visual health needs as your optometrist. This document describes our privacy policies.

Your Personal Information

Your personal information describes you as an individual. Information that we gather relates to identification (age, gender, home address, phone number, family status, health services identification numbers), health (medical, ocular and family histories including present and past medications and allergies), activities (visual demands, hobbies and recreation) as well as other information that is unique to you that may influence both your visual performance as well as our ability to care for you.

Our Professional Team

Our team that cares for you begins with our optometrists and staff. We honor your privacy and will take care of your personal information. Occasionally, there may be other individuals that have access to limited portions of your personal information – this may include computer technicians and consultants, accountants, office security personnel, maintenance trades, building cleaning personnel and lawyers. We restrict access to personal information as best we can, and have assurances from these individuals that they will follow privacy principles.

Our Reasons for Collecting Personal Information

Our primary purpose for collecting personal information is to provide you with optometric services and care. We gather only the information that is necessary to perform these services in a responsible and professional manner. We may pass on information to other regulated health professionals as is necessary, such as in the case of a referral to an ophthalmologist or family physician – we do so with your consent. The only situation where we may share information without your consent would be in an emergency situation where as a patient, you may not be able to communicate.

There are other situations where we may collect, use and disclose information from your personal file. These include:

- Billing third party payment providers where coverage exists (Blue Cross, Saskatchewan Health, Health Canada, Private Plans)
- Sending practice correspondence to patients such as reminders regarding their next examination
- Advising patients of upcoming seminars, public health concerns regarding treatments or eye care products, office promotions and changes to office personnel and optometrists
- As a regulated health profession, evaluation teams from our provincial association may review office records and patient files to ensure a high standard of care and assist in improving practice performance
- Information may be passed on to agencies to assist in collection of funds related to unpaid bills for optometric services and treatments

Protecting Your Personal Information
We have taken the following steps to protect your personal information:

- Our employees are trained to collect, use, disclose and destroy personal information in such a manner to fulfill their duties and protect your privacy
- Paper information is under supervision or stored in a locked or restricted area
- Electronic information is either under supervision or secured in a locked or restricted area. Passwords and appropriate software safeguards are in place to restrict access to information.
- Paper information is transferred through sealed, addressed envelopes or boxes distributed by registered and reputable companies
- Care is taken to ensure information sent by fax is being sent to the appropriate destination by direct lines
- Care is taken to ensure verbal communication between you and our staff is in private and in confidence
- Your personal information is stored in our possession for a minimum of 6 (six) years – by law. Once your information is no longer necessary to our practice, or by law, we dispose of your information through shredding, in the case of paper files, or use a professionally trained source to eliminate any electronic records and information.

Access to your Information
You are fully entitled to your personal information. If you need a copy of your file or information from your file, please ask. You can expect that within a reasonable time, we will be able to respond to your request. We may ask for this request in writing, and there may be a charge for doing so, depending on how much information is required and how much preparation it may take.

Questions?
In addition to our privacy officer in our practice, you can contact the Saskatchewan Association of Optometrists at the following address:

<<Insert office information here >>

OR VISIT US AT OUR WEBSITE AT: _____

The Saskatchewan Association of Optometrists would like to thank the College of Optometrists of Ontario for the use of information, format and text from their Privacy Policy document.

Request for Information on the Following Patient – Sample

<<Insert originating office information here>>

TO: "Name of Dispensary" or "Your Business Name"
Fax:
Date:
RE: **Request for Information on the following patient:**

Name: _____

Address: _____

Phone: _____ Date of Birth: _____

Patient's Signature: _____

Licensed Ophthalmic Dispensers Name (Print): _____

Licensed Ophthalmic Dispensers Name (Signature): _____

Please provide the following information: _____

_____

Response:

Optical Prescription: OD _____ Add _____

PD_____ OD _____ Add _____

Prism _____ Special Instruction: _____

Date of Last Comprehensive Eye Examination: _____

Optical Prescription Expiry Date: _____

Optometrist Name (Print): _____

Optometrist Signature: _____

Response to a Request for Personal Information

<<Insert your office information here>>

Dispensary: _____ Date: _____

Dispensary Address/Fax: _____

Dispenser Name: _____ Signature: _____

You requested the following information regarding my patient:

Name: _____

Address: _____

Phone: _____ **Date of Birth:** _____

Optical Prescription: OD _____ Add _____

PD_____ OD _____ Add _____

Prism _____ Special Instruction: _____

_____

_____

Date of Last Comprehensive Eye Examination: _____

***Please note the optometrist is not responsible for the validity of this prescription if a year has expired since the last eye examination, as the prescription may no longer be accurate*

Patient's Signature: _____ Date: _____