INTERNAL OFFICE PRIVACY MANUAL

Eyes360

MEDICAL EYECARE • FASHIONABLE EYEWARE

“We value each and every one of our patients, and understand the importance of privacy to you. We are committed to collecting, using, and disclosing your personal information responsibly and keeping it secure in the best ways possible"

CONTENTS

INTRODUCTION

Privacy of our patient's health information is principle important to Eyes 360. We are committed and accountable to collect, use, disclose and protect a patient's health information in a confidential and appropriate manner.

DEFINITIONS

a) Affiliates – Includes all employees, volunteers, students and other individuals contracted to provide services for custodians.
b) Custodians – In 2010, the *Health Information Act* (HIA) was amended to designate all optometrists as custodians. A custodian is an individual or organization who is defined or designated as a custodian in the HIA and HIR. Optometrists may be considered an affiliate to another custodian if they meet the definition of affiliate under HIA Section 1(1(1)(a).
c) Health Information is defined as:
    - Registration information.
    - Diagnostic, treatment and care information.
d) *Health Information Act* – referred to as the HIA
e) *Health Information Regulation* – referred to as the HIR
f) Information Manager (IM) – A person or body that:
    - Processes, stores, retrieves or disposes of health information, or,
    - Strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, in accordance with the regulations, or,
    - Provides information management or information technology services.
g) Information Manager Agreement (IMA) – A written agreement between a custodian and an information manager that covers:
    - Services to be provided by the information manager.
    - All requirements specifically listed in the *Health Information Regulations*.
    - That the information manager must comply with the HIA, the HIR and the agreement with the custodian.
h) Privacy Impact Assessment (PIA) – A PIA is required in order to access Netcare or whenever a custodian updates or implements an administrative practice or information system that may impact the collection, use or disclosure of information.

TRAINING AND RISK ASSESSMENT

Our office:

- Holds training sessions for all new employees upon hiring. All new hires are required to read and sign privacy policies.
- Holds regularly scheduled training session for all doctors and staff to maintain compliance with office policies and the HIA. All documents will be updated yearly and staff is updated, April of each year.
- Conducts a periodic risk assessment to ensure that health information stored at our clinic is maintained in a safe and confidential manner.
- Staff is required to routinely log off of computer and ensure no patient records are left visible and unattended.

Doctors and staff who do not follow required procedures and policies will be given a warning along with remedial education sessions. Serious privacy breaches may result in immediate termination of employment.

COLLECTION OF INFORMATION

Our clinic collects health information in accordance with the HIA. Specifically, we only collect as much health information as is essential and necessary to carry out the purpose for which the information is being collected as follows:

- Collect only essential information.
- Collect with the highest degree of anonymity.
- Collect in a limited manner.
- Identify authority to collect individually identifying information.
- Collect directly from the individual unless indirect collection is authorized.

Personal information including name, age, phone number, e-mail address and Alberta Health Care number may be asked at the reception desk. If you prefer, you may ask to provide this information at the time when we collect health information.

We may also send recall notices in the mail, with the above collected information, to remind you to book your next appointment. These recall notice will only be sent if we were unable to get a hold of you by phone, email or SMS. Recall notices contain minimal information, and this includes name and address.

HEALTH INFORMAITON

PROTECTION OF HEALTH INFORMATION

Our clinic protects health information in accordance with the HIA. We have taken all reasonable steps to maintain administrative, technical and physical safeguards to protect your health information including:

- Not allowing any paper/computer record to be inadvertently seen by other patients.
- Conduct periodic risk assessments to test effectiveness of our office policies and procedures.
- Hold regularly scheduled staff meetings to maintain compliance.
- Restrict access to computers with passwords and usernames.
- Log-out on computer terminals when leaving a patient exam room.
- Shred paper charts if the health information is no longer required.
- Dispose of computer hard drives and other storage devices in an appropriate manner to ensure no information remains after destruction.
- Implement controls to protect wireless networks from eavesdropping.
- Implement appropriate malware protection, firewalls and other communications security measures.
- Have appropriate Information Manager Agreements.
- Have appropriate Custodianship of Patient Records Agreements.
- Back up all computer information in a confidential and appropriate manner.

USE OF HEALTH INFORMATION

Our clinic uses health information in accordance with the HIA to perform one or more of the following:

- Provide a health service.
- Determine or verify a person's eligibility to receive a health service.
- Manage internal operations.
- Conduct research.
- Educate other health service providers.

All custodians and affiliates in our clinic are authorized to share health information for the purposes of providing the above listed services. We will be

diligent to use only the minimum amount of health information essential to provide adequate and optimal care.

DISCLOSURE OF HEALTH INFORMATION

Our clinic discloses a patient's health information to other custodians and other entities in accordance with the HIA.

Generally, our clinic may disclose a patient's health information to other health care practitioners who have been designated as custodians under the HIA without the patient's consent as part of the patient's diagnosis, treatment and care regimen. We will only disclose that information which is deemed essential to the patient's continuing care and note this disclosure in the patient chart.

Patient health information will be provided to other health care practitioners solely for the purpose of patient's diagnosis, treatment and care. This is mainly done through fax, but in some cases may also be provided by email, or referral websites such as MDcollaborate. If patient requests any diagnostic testing, we may provide these by the way patient requests.

In addition, a patient's health information may also be disclosed where required or allowed by law without the patient's consent to:

- Other health care providers who are not subject to the HIA.
- Regulatory authorities, where such information may assist in the investigation of a complaint or a review of standards of care.
- Governmental authorities (e.g. CCRA, Office of the Information and Privacy Commissioner of Alberta, Human Rights Commission, etc.) who have it in their mandate to access your file.

ACCESS TO HEALTH INFORMATION

Our clinic allows access to a patient's health information in accordance with the HIA. All patients have the right to access their health information at any reasonable time (e.g. during regular office hours). Our Privacy Officer deals with all access requests. The privacy officer will notify the patient's doctor, who will then communicate directly with the patient, or may direct a staff member to provide patient access to their health information.

We will make all reasonable attempts to respond to all formal, written access requests from patients within 30 days of receiving the request in accordance with the HIA. Informal, unwritten access requests are discussed with the patient and recorded on the patient chart.

If a fee is to be charged for accessing health information, an estimate of the total fees to be charged will be given to the patient before providing the services. Our clinic abides by the HIR fee schedule. Our clinic retains the discretion as to whether fees will be charged or not, and in what amount.

CORRECTING OR AMENDING HEALTH INFORMATION

It is our duty to ensure that health information is accurate and complete. As such, our clinic responds to correction and amendment request in accordance with the HIA. All patients have the right to request a correction or amendment to their health information. We will make all reasonable attempts to respond to all written correction and amendment requests from patients within 30 days of receiving the request.

A request does not guarantee a correction or amendment. Corrections and amendments apply to factual information and not professional opinions that may have been recorded. All corrections and amendments are recorded on the patient file. If our office does not agree with the correction or amendment, we will include a brief statement on the patient file recording both opinions. If the custodian refuses to make a correction, the requestor must be told they have right to either ask for a review by the Commissioner, or submit a statement of disagreement of 500 words or less that will be attached to the record.

RECORDS RETENTION

Our clinic maintains patient records and disclosures for a minimum of ten (10) years after the patient's last eye examination and/or two (2) years after the death of the patient. In addition, records of disclosure of information must also be kept for ten (10) years after disclosure.

PRIVACY IMPACT ASSESSMENT

Privacy impact assessments have been submitted to the Office of the Information and Privacy Commissioner that explain the privacy protection, legal authorities and risk mitigation of our internal practices and information systems. PIA's will be reviewed on a periodic basis; and, updated and resubmitted should any changes have occurred in our clinic, paper record system or computer system.

RESEARCH

As per ACO Guideline 1.2.2f, if a patient's health information is to be used for research purposes, our clinic must follow the rules prescribed under HIA Part 5, Division 3 and Section 27(1)(d). In addition, Netcare has its own research protocols.

The HIA allows optometrists to use health information already in their custody or under their control for research without a research agreement. If you wish to use the information held by the clinic for research purposes, please send us a written statement and details of purpose of use. We will only provide information that is within the rules prescribed under HIA.

A research agreement is only required when disclosing health information to a third party for research purposes. If an affiliate receives a request for disclosure of information for records, they will promptly notify our Privacy Officer. The Privacy Officer is required to pass information on to and receive approval from all shareholders prior to proceeding with any requests.

PRIVACY BREACHES & INCIDENT RESPONSE

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Upon notification or suspicion of a possible breach, custodians and affiliates must immediately notify the privacy officer, and our Privacy Officer will:

- Take immediate common sense steps to contain the breach.
- Assess what information may have been inappropriately accessed.
- Evaluate the risks associated with the possible breach.
- Notify affected patients of the possible breach
- Identify the internal or external source of the breach.
- Update the office privacy safeguards to prevent future occurrences of a similar nature.

As not all privacy breaches are mandated to be reported to the OIPC, the Privacy Officer will make a determination on whether to report or not. The Privacy Officer will also make a determination on whether to report the incident to Police, other contracted entities and the Alberta College of Optometrists.

GUIDELINES TO THE ACO STANDARDS OF PRACTICE

Our office abides by the rules and provisions of the Alberta College of Optometrists Guidelines to the ACO Standards of Practice.

PRIVACY OFFICER

Our Privacy Officer is Dr. Ranbir Sond