POLICY TITLE **Privacy and Information Security Policy**	
APPROVED BY: Director of Operations	
DATE APPROVED: April 4, 2019	**Operations Director SIGNATURE:**
DATE REVIEWED/REVISED:	

1. Introduction

Inner City Health Associates (ICHA) is firmly committed to protecting and preserving all personal health information and other confidential information that is collected, used, disclosed, and retained within its custody and control**.**

ICHA's obligations in regards to Personal Health Information (PHI) are outlined in Ontario's privacy legislation; the Personal Health Information Protection Act; (PHIPA) This Act contain provisions that require health information custodians to take reasonable steps to ensure that PHI is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing PHI are protected against unauthorized copying; modification or disposal.

This policy sets out requirements to ensure that personal health information in ICHA's custody is properly safeguarded. These requirements were formulated in the context of our legal and regulatory requirements.

In the course of carrying out its patient care, research, teaching and administrative functions ICHA collects, retains, uses, discloses, and ultimately disposes of personal and personal health information relating to its patients within its custody and control.

Our privacy measures are based on our legal and regulatory requirements and the Canadian Standards Association Model Code for privacy which outlines ten specific principles including:
1. Accountability for Personal Information
2. Identifying Purposes for the Collection for Personal Information
3. Consent for the Collection, Use, and Disclosure of Personal Information
4. Limiting Collection of Personal Information
5. Limiting Use, Disclosure, and Retention of Personal Information
6. Ensuring Accuracy of Personal Information
7. Ensuring Safeguards for Personal Information
8. Openness about Personal Information Policies and Practices
9. Individual Access to their own Personal Information
10. Challenging Compliance with ICHA's Privacy Policy and Practices

2. Definitions

- **Access** Defined as a staff member's ability to examine or obtain personal health information required to perform their job function; from a patient's perspective, it means their ability to examine or obtain their own personal health information.

- **Collection:** The process of gathering or obtaining private and confidential information, whether directly from the person or patient, or from other sources such as tests, images, samples, specimens or other care providers.
- **Confidential Information:** Confidential information is all information of a sensitive nature in any format which is created, received or disclosed by ICHA in the course of its business, including physical and electronic records in the custody of agents retained by ICHA.
- **Consent:** Voluntary agreement with what is being done or proposed. Consent can be "express", "implied" or via "notice". Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual. Notice includes situations whereby patients, families, visitors and staff are given written information explaining how their information may be used or disclosed, but are not asked to sign any form indicating that they have read the notice and agreed with its terms and conditions.
- **Disclosure** Means to make the information available or to release it to another person, organization or health care custodian outside of the organization.
- **Encryption** Encryption is the process of transforming plaintext information using an algorithm (called a cipher) to make it unreadable.
- **Patient:** Throughout this document, "patient" is understood to mean either the patient or, if applicable, a person legally authorized to make decisions on the patient's behalf, such as the substitute decision maker.
- **Personal Health Information (PHI):** For the purposes of this policy, personal health information (PHI) means oral or recorded identifying information about someone that related to a person's physical or mental health or family history or health care an individual receives, including who provided the health care.
- **Personal Information (PI)**: Recorded information about an identifiable individual.
- **Privacy:** The right of individuals to determine for themselves when, how and to what extent personal information about the individuals is communicated, and to be secure from unauthorized use or disclosure of their personal information**.**
- **Privacy Breach:** A privacy breach happens when personal health information or personal information is collected, used, disclosed or disposed of in a way that does not comply with PHIPA.
- **Staff:** ICHA medical staff, employees, trainees and any Host Agency staff who have access to ICHA's EMR- OSCAR.
- **Two-Lock:** The practice of physically securing PHI, when left unattended, behind two separate locks. e.g. If an office opens to a public corridor, sensitive information must be kept in a locked cabinet behind the locked door to the office.

.

3.0 Policy

ICHA is responsible for safeguarding the privacy and confidentiality of information, whether verbal, written, or electronic. All breaches are to be reported and will be dealt with in accordance with ICHA's practices as outlined in the Privacy Breach Protocol.

It is the responsibility of all ICHA staff working or carrying on activities on behalf of ICHA, to maintain the confidentiality and security of sensitive information. This is consistent with and supplementary to any applicable professional "codes of conduct" or "codes of ethics". Professional staff is additionally governed by their professional standards for privacy and confidentiality. Any person in possession of sensitive information must be diligent in protecting this information. Host Agencies Executive Directors (or the equivalent) are accountable for ensuring compliance with ICHA's privacy policies and procedures within their agencies.

Everyone is accountable for ensuring that sensitive information is only used as required to perform their necessary job duties, and that such information is not disclosed to anyone who does not have a legitimate need to have access to such information. It is inappropriate to access a patient's health record unless

you are **currently** providing or facilitating care to that individual. Any unauthorized access is a breach of confidentiality and is subject to notification requirements as outlined in PHIPA and through the professional regulatory bodies.

4.0 Guidelines
ICHA will conduct itself according to the following privacy principles:

Principle 1 - Accountability for Personal Information (PI) and Personal Health Information (PHI)
ICHA is responsible for PI/PHI under its custody or control and has designated a Privacy Officer, who is accountable for ICHA's overall compliance with privacy principles. The Privacy Contact's duties include:

- periodic assessments of information collection, use and disclosure practices
- developing policies, procedures and tools to carry out an organization wide Privacy Compliance Program
- oversee and/or conduct ongoing staff privacy training
- update/revise the Privacy and Confidentiality policies and procedures as required
- privacy impact and threat risk assessments and privacy audits of information use

ICHA will use contractual or other means to provide a comparable level of protection for information is collected used or disclosed by staff supporting ICHA's clinical operations.

Audits will be conducted periodically on records of a confidential nature to monitor compliance with this policy.

Principle 2 - Identifying Purposes for the Collection for Personal Information or Personal Health Information
ICHA, at or before the time PI/PHI is collected, will identify the purposes for which this information is collected, used, disclosed, and retained. The main purposes are and outlined for our patients in our Privacy Notice posted at all ICHA clinics as follows:

- To provide health care to you
- To improve the care we provide
- To teach future health care providers
- To conduct research
- To obey laws and regulations
- To receive payments for your treatments from government and other insurance providers

When PI/PHI that has already been collected is to be used for a purpose not previously identified, the consent of the individual will be obtained, unless the new purpose is required by law.

Principle 3 - Consent for the Collection, Use, and Disclosure of Personal Information or Personal Health Information
The knowledge and consent of the individual or substitute decision-maker is required for the collection, use or disclosure of their PHI, except where it may be inappropriate to seek consent due to legal, medical or security reasons. ICHA will make reasonable efforts to ensure that individuals are advised orally or in writing through the use of notice signs about the collection, use or disclosure of their PHI.

Expressed consent from the patient will be obtained for the release of PHI as outlined in ICHA's Release of Information policy==>

Principle 4 - Limiting Collection of Personal Information or Personal Health Information
The collection of PI/PHI will be limited to that which is necessary for the purposes identified by ICHA. Information will be collected by fair and lawful means. However, it should be noted that the minimum quantity of information needed to satisfy identified purposes may often be substantial.

Principle 5 - Limiting Use, Disclosure, and Retention of Personal Information or Personal Health Information

PI/PHI will not be used or disclosed for purposes other than those for which it was collected, except with the express consent of the individual. Only those individuals who need a record of PI/PHI in the performance of their work duties shall have access to it. Active OSCAR users are only to access information or records they are authorized to see or those which are required to do their jobs. Host Agency staff can only access OSCAR for the purpose of providing or facilitating direct patient care.

OSCAR access roles are as follows:

- Physician
- Health Care Professional/Medical Student
- Health Information Custodian Support Staff
- Non Health Information Custodian Support Staff
- Read only

Role assignment is based on the following criteria:

- Regulated health professional designation
- Agency staff role responsibilities to support ICHA clinic
- Agency Health Information Custodian status.
- Where applicable based on contractual obligations E.G. access agreements for REB approved research

Criteria for all Host Agency OSCAR users

- are currently employed by the Host Agency and require access to OSCAR in order to support clinic operations or direct patient care, and have been identified to ICHA, in accordance with ICHA's procedures for role identification
- are aware of their obligations under the current Host Agency agreement and under provincial law to protect privacy and security
- shall only collect use and/or disclose PHI as necessary in order to provide or to facilitate the provision of patient care
- shall only access PHI needed to fulfill their assigned duties related to the provision of care
- have reviewed ICHA's privacy policies, completed relevant ICHA OSCAR and Privacy training; and
- have signed ICHA confidentiality agreement

Principle 6 - Ensuring Accuracy of Personal Information or Personal Health Information

PI/PHI will be as accurate, complete and up-to-date as necessary and as reasonably possible for the purposes for which is it to be used.

An individual will be able to challenge the accuracy and completeness of his/her information and have it amended as appropriate. Such amendments will generally not involve deletions or alterations of the original record, but would take the form of addendums to the record. Where an individual believes their personal information (PI) contained in an ICHA record incorrect or inaccurate they may request a correction of that information. If ICHA disputes the correction, the individual shall have an opportunity to provide ICHA with a statement of disagreement that shall be attached to the record. Details of this procedure can be found in the ICHA's Requesting Corrections to the Medical Record Policy ==>

Principle 7 - Ensuring Safeguards for Personal Information or Personal Health Information

Security safeguards appropriate to the sensitivity of the information will protect PI/PHI against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. ICHA will protect PI/PHI regardless of the format in which it is held. The methods of protection include physical, organizational, and technological measures as follows:

- Each authorised OSCAR user will be assigned a two level password along with a Username
- Passwords:
    i. Must be unique and contain at least 8 characters with both letters and numbers or characters
    ii. It is prohibited to allow others to use Username and passwords specifically assigned to you. All users are accountable for any activity logged under their OSCAR account.
    iii. Will expire after one year.
    iv. If you have suspicions that your password has been compromised you must notify Virtual Office as soon as possible in order to have your password reset.
- OSCAR access must be cancelled whenever an OSCAR user ceases their employment or other relationship with the Host Agency, ICHA, or is on a Leave of Absence or Sabbatical, any exceptions must be approved by the Medical Director, Privacy Office and Host Agency lead.
- All portable electronic devices that store or have the potential to store personal health information must be encrypted.
- Web browsers, use a cache to improve performance of routinely accessed webpages. When a webpage is opened, the requested files are stored in your computer via the browser's cache. The browser **cache must be emptied** and cleared on a daily basis. This can typically be done using the browser's clear history function and/or in general settings.
- ICHA will establish through relevant contractual obligations and communicate, as necessary, the requirements that Host Agencies implement reasonable security standards for all computers that are used to access OSCAR.
- When transporting physical files containing PHI, files must be face down or in sealed envelopes or containers and marked "Confidential. If found please return to..."
- Open E-mail systems must not be used by staff to exchange PHI. Acceptable messaging systems includes:
    - Use of OSCAR Messenger
    - ONEMail Members: Emails exchanged with Healthcare organizations that are members of ONEMail. These are transmitted securely.
- Protect all physical files containing PHI in accordance with the Two-Lock practice when it's feasible to do so.
- Care will be used in the disposal or destruction of PI/PHI, to prevent unauthorized parties from gaining access to the information. All Host sites will have confidential bins available for this purpose.
- All breaches of confidentiality are to be reported to ICHA's Privacy Office as soon as reasonably possible Breaches will be managed in accordance with ICHA's Privacy Breach Protocol.

Principle 8 - Openness about Personal Information or Personal Health Information Policies and Practices

- ICHA will make readily available to individuals information about its policies and practices relating to the management of PI/PHI. New ICHA staff and any other individual doing work at ICHA will be made aware of this policy prior to being given OSCAR access.

Principle 9 - Individual Access to their own Personal Information or Personal Health Information

- Upon request, an individual will be informed of the existence, use and disclosure of his or her PI/PHI and will be given access to that information. ICHA will respond to such requests within 30 days and at minimal or no cost to the individual. Staff, who at some point may have been an ICHA patient and who now have authorized access to clinical systems are prohibited from directly accessing their own PHI or PHI of any relative for whom they may have access rights. All access requests are to be directed to ICHA's Privacy Office and managed according to requirements outlined in PHIPA and ICHA's Patient Requesting Access to Health Records policy.
- In certain situations, ICHA may not be able to provide access to all of the PI/PHI it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request.

Principle 10 - Challenging Compliance with ICHAs Privacy Policy and Practices

- An individual will be able to lodge a privacy complaint regarding the above principles to the Privacy Office, or appropriate designated individual. ICHA will investigate all complaints. If a complaint is found to be justified, ICHA will take appropriate measures. Complaints may also be lodged with the Office of the Information and Privacy Commissioner, Ontario.

5.0 References

The Information and Privacy Commissioner / Ontario website. http://www.ipc.on.ca/

Personal Health Information Protection Act, 2004. http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm

OHA Privacy Toolkit – Guide to the Ontario Personal Health Information Protection Act

COACH Guidelines for the Protection of Health Information

Freedom of Information and Protection of Privacy Act, 1990. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm