Patient Confidentiality and Privacy Policy

CLEAR MEDICAL IMAGING	REV Date: **04-MAY-2021**	REV Level: **C**
	Doc No.: **OP-PCP1**	Page: **1** of **11**

PURPOSE:

All patient information and medical records are personal and confidential. Clear Medical Imaging is responsible to comply with the Personal Health Information Protection Act and, as such is a "Health Information Custodian" responsible for "Personal Health Information" under its custody and control. The privacy rights under Personal Health Information Protection Act are granted to the patient, client, resident or an incapable patient's SDM.

SCOPE:

This policy applies to all staff and affiliates who:

(i) Have access to confidential information; or

(ii) Utilize Clear Medical Imaging-owned or personal-owned information devices to access or store confidential information.

Clear Medical Imaging reserves the right to audit and monitor to ensure compliance with this policy is maintained. Auditing may be carried out, without prior notice, for security reasons, to support ongoing operations, to maintain and upgrade technology resources, and to support approved investigative activities related to unacceptable use or legal issues. **Failure of an Employee or affiliate to take reasonable steps to secure confidential information may result in disciplinary action, up to and including termination of employment.**

DOCUMENT CONTENTS:

1. DEFINITIONS:

(a) "**Clear Medical Imaging**" means 2324317 Ontario Ltd. o/a Clear Medical Imaging;
(b) "**EPR**" means electronic patient record;
(c) "**IPC**" means the Information and Privacy Commissioner of Ontario;
(d) "**Personal Health Information Protection Act**" means the Ontario Personal Health Information Protection Act, S.O. 2004 c.3 Sched. A., as may be amended from time to time;
(e) "**Personal Health Information**" any identifying information with respect to an individual, whether living or deceased and includes details:
   i. Concerning the physical or mental health of the individual;
   ii. Concerning any health service provided to the individual;
   iii. Concerning the donation by the individual of any body part or any bodily substance;
   iv. Derived from the testing or examination of a body part or bodily substance of the individual;
   v. That is collected while providing health services to the individual; or
   vi. That is collected incidentally to the provision of health services to the individual.
(f) "**Privacy Officer**" means Dr. Igor Gaisinsky, and any successor or other Employee of Clear Medical Imaging who may be delegated such authority;
(g) "**SDM**" means a substitute decision maker who is a person that is:
   i. At least 16 years of age,
   ii. Capable with respect to the treatment,
   iii. Not prohibited by court order or separation agreement from having access to the incapable patient or giving or refusing consent on the incapable patient's behalf,
   iv. Available, and
   v. Willing to assume the responsibility of giving or refusing consent.

2. POLICY:

a) Patient Consent

All Employees are required to seek informed consent for the collection, use, and/or disclosure of a patient's personal information, subject to some exceptions set out in law. A patient may provide consent either orally or in writing. A patient's consent may also be implied through their conduct. For example, a patient's consent will be implied if they attend a Clear Medical Imaging office for diagnostic imaging services. In certain circumstances, as permitted or required by law, Employees may collect, use or disclose personal information without a patient's knowledge or consent. These circumstances include (where applicable):

(i) Where the patient is unconscious;
(ii) Where the patient is too sick or not lucid;
(iii) Where collection or use is clearly in a patient's best interest and consent cannot be obtained in a timely fashion;
(iv) To comply with a subpoena;
(v) Upon receiving a warrant or court order; and
(vi) As otherwise required and permitted by law.

b) Limiting Collection, Use, Disclosure and Retention of Personal Health Information

The collection of personal information is limited to that which is necessary. Similarly, personal information shall not be used or disclosed for purposes other than those for which the information is collected, except with the patient's expressed consent, or as required by law.

We retain patient records and films as required by law and regulations, including the regulations under the Independent Health Facilities Act.

c) Protection of Personal Health Information

Clear Medical Imaging requires all Employees take all reasonable precaution measures to ensure that a patient's Personal Health Information is kept safe from loss, theft, unauthorized access, modification, use, copying, disclosure or tampering.

Clear maintains safeguards to protect all Personal Health Information retained in each of its facilities, and during their disposal and destruction. These safeguards include, but are not limited to:

(i) **Physical measures** – locked filing cabinets, restricting access to our office, alarm systems;
(ii) **Technological tools** – passwords, encryption, firewalls, anonymizing software; and
(iii) **Organization controls** – security clearances, limiting access on a "need to know" basis, staff training, and confidentiality agreements.

d) Password Guidelines

- Length should be the minimum requirement, as determined by the software provider.
- Avoid words found in the dictionary and include at least one numeric character.
- Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords should not be maiden names, or names of children, spouses, or pets.)
- Do not write passwords down anywhere.
- Change passwords periodically, which at a minimum must occur at least once every ninety (90) calendar days.
- Do not include passwords in any electronic mail messages.

e) Storage of Confidential Information

Employees who have a role related reason to store confidential information on a portable information device, or on the hard/local/C drive of a computer are responsible to:

- Store only the minimal amount of information for the minimal amount of time necessary to complete the work.
- De-identify or encrypt confidential information. Password protection of confidential information is not adequate protection.
- Ensure that procedures for de-encrypting data and/or files linking unique identifiers with identifiable information are not stored in the same location/device as the encrypted data/de-identified data.
- Ensure the physical security of the device, e.g. locked cupboard in locked office. If a device must be left unattended in a vehicle, it should be locked in the trunk. Staff/affiliates must move the device to a more secure location as soon as possible and never leave it in a vehicle overnight. If the vehicle has no trunk, leaving the device in the vehicle is not a secure option.
- Ensure that, if the device is removed from service or redeployed for any reason, confidential information is removed from the device.

f) Patient Communication

Clear Medical Imaging is sensitive to the privacy of a patient's Personal Health Information and this is reflected in how our Employees communicate with both the patient and others involved in their care.

Telephone

A patient's preference with regards to phone messages will be taken into consideration. Unless a patient indicates otherwise, Employees should only leave their name and phone number on any message for the patient. Information must not be given over the phone to non-health providers (i.e., lawyers, insurers, and/or law enforcement agents). **Disclosure is permitted when a health care provider requests Personal Health Information for emergent or urgent patient care and does not have access to a secure fax line.**

Fax

All transmissions are sent via fax must be sent with a cover sheet that indicates the information is confidential. Employees are required to take reasonable steps to ensure that Personal Health Information is received only by a secure fax machine.

E-Mail

Any confidential information that we send via e-mail over public or external networks is encrypted. Clear Medical Imaging employs firewall and virus scanning software to mitigate against unauthorized modification, loss, or access. **Email is <u>not</u> a secure, private or confidential form of communication when being delivered to an address external to the Clear Medical Imaging email system, therefore disclosure of Personal Health Information is strongly discouraged.**

Post/Courier

When health information is transferred to another location it is **placed in a sealed envelope, marked as confidential, and directed to the attention of the authorized recipient**.

g) Access to Confidential Information

Employees of Clear Medical Imaging are responsible to:

- Access confidential information only if there is a need to do so as part of the role for which he/she has been hired or affiliated with the organization.
- Access information (electronically stored) using his/her own unique username and password.
- Protect the security of his or her username and password in accordance with Clear Medical Imaging's Password Guidelines, and by:
  - Not sharing it with others;
  - Not writing it down where others could gain access to it;
  - Creating strong, complex passwords that minimize the chance of being compromised; and
  - Change the password immediately and notify the administrative assistant in the event that he/she suspects that his/her password has been compromised.
- Suspend or log out of patient care systems, and systems containing confidential information, when the application is no longer in use (i.e., do not leave computer systems open and unattended).
- Position his or her computer screen such that unauthorized individuals cannot look over their shoulder and see the confidential information displayed.

- Access systems and networks containing confidential information from remote locations only if they have been granted authorization to do so.

In the event an Employee is provided access to confidential information for databases, research, quality assurance, or educational purposes, they are responsible to:

- Collect and store only the minimal confidential information essential to accomplish the purpose.
- De-identify the information as soon as possible.
- Secure the information using measures described in this policy.
- Report to the appropriate authorities and the Privacy Officer any loss, theft or unauthorized access to patient information.

Clear Medical Imaging will deactivate user accounts, without notice to the user, where the account has not been used in a predetermined period of time, as determined by Clear Medical Imaging in its sole and absolute discretion, for Employees on leave of absence, or for unacceptable use of the systems/networks. Audits of the electronic systems and networks are conducted to ensure compliance with this policy.

h) Patient Access to Personal Information

A patient may ask for access to any personal information we hold about them upon written request and with reasonable notice. Employees must require all patients and/or SDMs complete a Request for Personal Health Information form (**OP-PF01**). In completing this form, the Employee must verify the patient/SDMs identity prior to disclosing any Personal Health Information. If the patient/SDM presents in person, then the Employee must ask to see government issued photo identification. If the requesting patient/SDM is remote, the Employee must ask for a copy of government issued identification be sent to Clear Medical Imaging and schedule a call back once the requester's identity has been verified.

Upon granting access to a requesting patient/SDM, Clear Medical Imaging will also advise the patient whether we hold personal information about them, how the information has been used, and to whom it has been disclosed, upon written request and with reasonable notice (with only a few exceptions). If it is not possible to provide the patient with a specific list of third-party disclosures, we will provide them with a list of probable third-party disclosures.

Summary information is available on request. More detailed requests may be subject to a reasonable fee for photocopying, converting information to an alternate format (if applicable) and staff time. Employees must advise the patient of the approximate costs before processing their request. Employees are expected to respond to the patient's request within a reasonable period of time and must aim to be as specific as possible.

When a patient requests a copy of his/her chart or images, Employees must make the records available within five (5) working days. Clear Medical Imaging grants access to personal health information except in limited situations outlined by the Personal Health Information Protection Act and is responsible to respond to a patient's or patient's SDM request within the timeline set by the Personal Health Information Protection Act.

i) Disclosure Fees

There is a fee associated with requesting to view and/or obtain a copy of the health record for personal use (non-medical reasons). Clear Medical Imaging establishes fees for access on a cost recovery basis. **The requestor must be made aware of associated fees**. Payment of this fee

must accompany the written request to view and/or obtain a copy of a health record. No fee will be charged for the purpose of ongoing care (i.e. provision of images to take to a specialists' visit).

j) Denying Patient Access

A patient's rights to access their Personal Health Information is not absolute. Access can be denied for several different reasons, including:

- If doing so would likely reveal information about another individual, unless the other individual's information is severable;
- If doing so could reasonably be expected to threaten the life or security of another individual, unless the third-party information is severable;
- If the information is protected by solicitor-client privilege;
- If doing so would reveal confidential commercial information; and
- If the denial of access is required or authorized by law.

Reasons for Refusal of Access to Personal Health Information:

Use this chart for summarizing the various reason(s) for denying a patient's access request.

In each of the following situations, access should be provided to the part of the record that is not impacted by the reason for refusal and that can reasonably be severed from the record.

Reason for Refusal of Access	**Statement to give Requester**	
	Request refused (in whole or in part) and reason for the refusal	Refuse to confirm or deny the existence of any record
The record contains quality of care information	×	
The record contains information collected/created to comply with the requirements of a quality assurance program under the *Health Professions Procedural Code* that is Schedule 2 to the *Regulated Health Professions Act*	×	
The record contains raw data from standardized psychological tests or assessments	×	
The record (or information in the record) is subject to a legal privilege that restricts disclosure to the requester	×	
Other legislation or court order prohibits disclosure to the requester	×	
The information in the record was collected/created in anticipation of or use in a proceeding that has not concluded		×
The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded		×
Granting access could reasonably be expected to result in a risk of serious harm to the patient or to others (Where this is suspected you may consult a physician or psychologist before deciding to refuse access)		×
Granting access could lead to the identification of a person who was required by law to provide the information in the record		×

Reason for Refusal of Access	Statement to give Requester	
	Request refused (in whole or in part) and reason for the refusal	Refuse to confirm or deny the existence of any record
Granting access could lead to the identification of a person who provided the information in the record in confidence (either explicitly or implicitly) and it is considered appropriate to keep the name of this person confidential		×
The request for access is frivolous, vexatious or made in bad faith	×	
The identity or authority of the requester cannot be proven by the requester	×	

In the event that an Employee is required to deny a patient's request for access to their personal information, they must explain the reason for denial.

If a patient has any questions or concerns, or wishes to access their personal information, they should contact our Privacy Officer at:

Clear Medical Imaging
1568 Ouellette Avenue, Windsor, Ontario, N8X 1K7
519-256-4914
Attention: Privacy Officer

If unsatisfied with our response, the Privacy Commissioner of Canada can be reached at:
112 Kent Street
Ottawa, Ontario, K1A 1H3
1-800-282-1376

k) Disclosure of Personal Health Information

Disclosure of Personal Health Information must comply with legislative requirements and professional standards. **Employees of Clear Medical Imaging must not disclose records that exist in either hard copy or electronic form that originated from a visit and admission from another organization unless under specific exceptions, and only by Health Record Services/DI.**

Implied consent may be relied upon when Personal Health Information is collected, used or disclosed for the purpose of providing health care, unless the patient has placed restrictions on the disclosure of their information.

Express consent is required when collecting, using or disclosing Personal Health Information for purposes other than providing health care. **A fax or photocopy of the express consent is acceptable.** Express consent must be obtained from the patient or a patient's SDM prior to disclosure.

Disclosure of confidential information without appropriate consent from the patient or a patient's SDM may be cause for disciplinary action up to and including termination of employment.

In the event an Employee is uncertain as to whether collection, use or disclosure of Personal Health Information is permitted, they are strongly encouraged to speak with their Direct Manager prior to collection, use or disclosure.

l) Correcting Errors

If Clear Medical Imaging holds personal information about a patient and the patient believes that it is not accurate, complete and up-to-date, the patient can request to have it amended. Patients, or the patient's SDM, must show that the disputed entry is not correct or complete and provide the information necessary to make the correction.

m) Privacy Complaints and Reporting

It is the policy of Clear Medical Imaging to provide a process to address any individual's complaints regarding Clear Medical Imaging's privacy practices. Complaints can be an opportunity for learning and improvement, but when ineffectively managed can erode trust and confidence in Clear Medical Imaging, ultimately adversely impacting Clear Medical Imaging's ability to effectively undertake its business. The purpose of these policies and procedures is to manage privacy related complaints effectively.

n) Disposal of Confidential Information

All Employees are required to dispose of hard copy confidential information according to Clear Medical Imaging's Waste Management Policy and Procedures.

o) Incident Reporting

In the event that an Employee suspects or is aware of confidential information that has been lost, stolen, or accessed without authority, he or she must notify his or her Direct Manager as soon as possible.

3. PROCEDURES

a) Procedures to Correct Errors

i. Document Request for Correction.

- Patients/SDMs must first access subject record prior to seeking correction. If there has been no access, then facilitate access in accordance with Clear Medical Imaging's policy regarding patient access to Personal Health Information.
- Patients/SDMs must complete a Request for Access/Correction (**OP-PF02**).
- Assist patient/SDM if required.
- Create an event record in PHR.
- Provide completed form to Privacy Officer/designate.

ii. Verification of Identity and Status.

- Verify identity of patient/SDM. If presents in person, ask to see government issued photo identification. If remote, as appropriate to the circumstances, ask for copy of government issued identification to be sent to Clear Medical Imaging – and/or do a call back.
- If individual seeking correction is an SDM, verify status.
- Above information is captured in the Request for Personal Health Information Access/Correction form (**OP-PF02**).

iii. Review and Clarification (if required).

- Privacy Officer/designate shall review request within seven (7) days of receipt if non urgent and as soon as reasonably practicable if urgent.

- Ascertain whether request contains sufficient detail.
- If clarity required, Privacy Officer/designate may task personnel most knowledgeable about the requested records to assist requester to provide clarity. Communication shall be by directly speaking with the requester so that there is opportunity for back and forth dialogue and to resolve any issues on the spot, unless there is specific reason why a letter would be more appropriate.

iv. Correction.

- Correction to be undertaken if record demonstrated to be incorrect or inaccurate.
- Correction to be undertaken by person who created the record when possible.
- Record date of correction in record.
- Cross out incorrect information without obliterating it and if that is not possible date and label that information is not correct, severing the incorrect information from the record, storing it separately from the record and maintaining a link in the record that enables a person to trace the incorrect information, or if it is not possible to record the correct information in the record, ensure notation is made to inform a person who accesses the record that the information in the record is incorrect and to direct the person to the correct information.
- Document correction on Request for Personal Health Information Correction (**OP-PF03**) and create an event record in PHR for all requests, extensions, responses, and examination of original.

v. Respond to Requester and Others.

- The Privacy Officer/designate shall send a response letter (**OP-PF02**) to the requester, within thirty (30) days of receipt of the request or within the extended period of time.
- If correction is made then seek consent to also give written notice of correction to persons to whom Clear Medical Imaging has disclosed the subject information except if the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or other benefits to the individual. This is captured on the Request for Personal Health Information Access/Correction form (**OP-PF02**).
- Document response to Request for Personal Health Information Access/Correction (**OP-PF03**).

vi. Statement of Disagreement.

- If the correction is not made, provide notice to patient/SDM and provide an opportunity to the patient/SDM to prepare a statement of disagreement (**OP-PF04**).
- If the statement of disagreement is completed, provide a copy of the statement of disagreement to the Privacy Officer/designate who will file for retention.
- When patient/SDM requires (check PHR), include statement of disagreement whenever Clear Medical Imaging discloses information to which the statement of disagreement relates.
- When patient/SDM requires, Privacy Officer/designate shall make all reasonable efforts to disclose the statement of disagreement to any person who would have received notice of correction had correction request been granted.
- Document Statement of Disagreement on the Request for Personal Health Information Access/ Correction form (**OP-PF02**) and create an event record in the PHR for every statement of disagreement and for every disclosure of same.

b) Privacy Complaints Procedures

i. **Filing a Complaint.**

- Individuals may file a complaint to the Privacy Officer when:
  - Their Personal Health Information has been used or disclosed improperly;
  - A Clear Medical Imaging staff member has improperly handled their Personal Health Information; or
  - They have wrongfully been denied access to or opportunity to amend their Personal Health Information;
- A patient may file a privacy complaint by contacting Clear Medical Imaging Privacy Officer at twalsh@clearimaging.ca or by telephone at 519-256-4914 x 133.

ii. **Receiving a Complaint.**

- Thank the individual for bringing the complaint to Clear Medical Imaging's attention and assure the individual that Clear Medical Imaging values their input.
- Be sensitive to any barriers (i.e., language, illiteracy, disability) and accommodate as appropriate.
- Try to coordinate immediate opportunity for the individual to discuss the complaint with the Privacy Officer or designate. If there is not an immediate opportunity, coordinate a later opportunity.

iii. **Investigate and Make an Assessment.**

- The Privacy Officer, or designate, shall gather or cause to be gathered additional information as appropriate to fully and properly assess the complaint.
- The Privacy Officer, or designate, shall make an assessment as to an appropriate response to the individual complainant.

iv. **Follow-up.**

- The Privacy Officer, or designate, shall follow-up with the individual complainant to
- Communicate the investigation and assessment.
- Try to resolve the complaint to the complainant's satisfaction, taking steps as appropriate.

4. ASSOCIATED DOCUMENTS

i. Employee Handbook
ii. Code of Conduct
iii. Privacy Breach Policy #OP-PB01
iv. Privacy Audit Policy #OP-PA01
v. Request Access/Correct Form #OP-PF01
vi. Response Letter to Request for Access to Personal Health Information #OP-PF02
vii. Response Letter to Request for Correction to Personal Health Information #OP-PF03
viii. Statement of Disagreement #OP-PF04
ix. PHI Access Request Form #OP-PF01

5. REVISION CONTROL LOG

REV Level	REV Date	Pages Affected	Revised By	Approved by Licensee	Approved by Quality Advisor	Revisions Made
A	01-JAN-2018	All	Management	Tiffany Walsh	Dr. Hausmann	Initial Release
B	04-JUL-19	All	Director, HR	*Tiffany Walsh*		Reformatted, Associated Docs added, HR added
C	30-APR-21	All	Director, HR	Tiffany Walsh	Dr. Hausmann	Update Associated Documents

D	04-MAY-2021	Page 5	Director, HR	Tiffany Walsh	Dr. Hausmann	Correction in clause H, refer to Policy OP-PF02