Office Privacy Policy

Dr. Adam Fogel

info@mobilemedicalclinic.ca

Protecting Personal Information

1. Openness and Transparency

1.1 We value patient privacy and act to ensure that it is protected.

1.2 This policy was written to capture our current practices and to respond to federal and provincial requirements for the protection of personal information.

1.3 This policy describes how this office collects, uses, discloses and protects the personal information of patients and the rights of patients with respect to their personal information.

1.4 We are available to answer any patient questions regarding our privacy practices.

2. Accountability

2.1 The physician is ultimately accountable for the protection of the health records in his/her possession.

2.2 Our office privacy contact person is Dr. Adam Fogel and can be reached at info@mobilemedicalclinic.ca, Our privacy contact person is responsible for:

- 2.2.1 Facilitating compliance with PHIPA
- 2.2.2 Ensuring that all individuals affiliated with this office are aware of their obligations under this policy and PHIPA
- 2.2.3 Receiving complaints or inquiries from patients about our privacy practices
- 2.2.4 Responding to requests for access to or correction of medical records.

2.3 Employees and all others in this office who assist with or provide care (including locums and volunteers) are required to be aware of and adhere to the protections described in this policy for the appropriate use and disclosure of personal information.

2.4 All persons in this office who have access to personal information must adhere to the following information management practices.

- 2.4.1 Office information management practices.
  - a) Access is on a need to know basis.
  - b) Access is restricted to authorized users.

2.4.2 Third party obligations

a) Contractual privacy clauses/agreements with third parties (including cleaning and security personnel, landlords, data processors etc.)

2.5 This office employs privacy protections to ensure that:

a) We protect the confidentiality of any personal health information that we acquire in the course of providing patient care.
b) We collect, use and disclose only as much information as is necessary to provide patient care.
c) We collect, use and disclose personal information only for the purpose of providing care or treatment or for other purposes expressly consented to by the patient.
d) We educate and train all staff and those affiliated with this office on the importance of protecting personal health information and the manner in which to do so.

Collection, Use and Disclosure of Personal Health Information

3. Consent

Personal health information is extremely sensitive. Unless required or permitted by law, we only collect, use or disclose personal health information with the express or implied consent of the individual to whom the information belongs or their substitute decision maker.

3.1 Implied consent can generally be relied on when personal health information is being collected, used or disclosed for the purpose of providing or assisting in the provision of health care to that individual.

3.2 If the purpose of the collection, use or disclosure of personal health information is something other than providing health care to the individual, express consent is generally required.

4. Withholding and Withdrawing Consent

4.1 Patients have the right to withhold or withdraw their consent to the collection, use or disclosure of their personal health information at any time.

4.2 The withholding or withdrawal of consent can take many forms, including prohibiting the collection, use or disclosure of particular item of personal health information or prohibiting the disclosure to or use of personal health information by a specific person,

4.3 If consent is withdrawn, the personal health information becomes “locked” and cannot be disclosed or used without the express consent of the individual.

4.4 If we are prevented from disclosing information to another health information custodian because it is “locked” we must inform the other health information custodian that the

information is locked if we believe that the information is reasonably necessary for the provision of care.

4.5 If the patient's decision to withdraw consent will compromise patient care, discuss the effect of withdrawal with the patient.

4.6 The withdrawal of consent and discussions related to withdrawal will be carefully documented.

5. Collection of Personal Health Information

5.1 We collect personal health information about patients from the patient or from a person acting on the patient's behalf. Occasionally, we collect personal health information about patients from other sources if we have obtained their consent to do so or if the law permits.

5.2 We collect the following personal health information.

5.2.1 Identification/Contact information, including:

a) Name
b) Date of Birth
c) Address

5.2.2 Billing information, including

a) Provincial/territorial health insurance plan (health card) number
b) Private medical insurance details

5.2.3 Health information, which may include:

a) Medical history
b) Presenting symptoms

5.3 Limits on Collection

5.3.1 We only collect personal health information that is required to provide care, administrate the care that is provided and communicate with patients. We will not collect any other information, or allow information to be used for other purposes, without the patient's express consent – except where authorized to do so by law. These limits on collection ensure that we do not collect unnecessary information.

6. Use of Personal Health Information

6.1 Personal health information collected from patients is used and disclosed by this office to:

a) Treat and care for patients,
b) Get payment for patient treatment and care (from OHIP, WISB, private insurer or others),
c) Plan, administer and manage our internal operations, including electronic medical records,

d) Risk or error management
e) Conduct quality improvement activities (like patient satisfaction surveys),
f) Teach,
g) Compile statistics,
h) Comply with legal and regulatory requirements
i) Fulfil other purposes permitted or required by law

7. Disclosure of Personal Health Information

7.1 Disclosure shall be done only in accordance with the uses described above at section 6.1 or as otherwise permitted by law.

7.2 Implied consent to disclose personal health information

7.2.1 Unless otherwise indicated, we can assume that patients have consented to the disclosure of personal health information to other providers involved in their care (i.e. within the circle of care). By virtue of seeking care from us, the patient's consent is implied for the provision of that care.

7.2.2 Relevant health information is shared with other providers involved in the patient`s care, including (but not limited to)

a) Other physicians in this practice
b) Other physicians in the afterhours call group

7.3 Express consent to disclose personal health information

7.3.1 The patient's express consent (oral or written) is required before we will disclose personal information to third parties for any purpose other than to provide care or unless authorized to do so by law

7.3.2 Examples of situations that involve disclosures to third parties include (but are not limited to)

a) Third party medical examinations
b) Provisions of charts or chart summaries to insurance companies

7.3.3 Before a disclosure that requires express consent is made, a notation should be made in the patient's medical record that they provided express consent or a signed consent form should be attached to the file.

7.4 Disclosures permitted without consent

7.4.1 In some circumstances, the disclosure of personal health information is permitted or required, even if no express or implied consent has been given.

7.4.2 Examples of such situations include (but are not limited to)

a) Billing provincial health plans
b) Reporting communicable diseases
c) Reporting abuse (child, elder, spouse, etc.)
d) Reporting fitness (to drive, to fly etc.)
e) By court order (when subpoenaed in a court case)
f) In regulatory investigations
g) For quality assessment (peer review)
h) For risk and error management (e.g. medical-legal advice)

Protection of Personal Health Information

8. Security Measures

8.1 We use physical, technological and administrative safeguards to protect the security of patient health information.

8.2 We use the following physical safeguards

8.2.1 Limited access to the office

a) Monitored alarm system
b) Deadbolt entry lock (or key card/key pad entry system)

8.2.2 Limited access to records

a) Restricting access on a need to know basis
b) Locked file cabinets
c) Maintain log of those who are granted access to electronic medical records

8.2.3 Office layout/features

a) Front desk privacy screens
b) Sound proofing and/or white noise to ensure confidentiality

8.3 We use the following technological safeguards

8.3.1 Protected computer access for patient health information

a) Strong passwords
b) Limited search functions
c) User authentication

8.3.2 System Protections

a) Firewall software
b) Virus scanning software

8.3.3 Protected external electronic communications – Internet

a) Separate internal access (stand alone, not connected to operating system)
b) Encrypted email for any external communication of patient health information

8.3.4 Secure electronic record disposal

a) Safely dispose of computer hard drives
b) Destroy all other removable media (CD-R, DVD, diskettes)

8.3.5 Privacy notices and warning flags

a) Prior to accessing certain electronic medical records, a privacy notice will be displayed
b) Privacy warning flags can be attached to specific files at the request of the individual or where there is reason to believe that the information is particularly susceptible to a privacy breach (e.g. celebrity patient)

8.3.6 Auditing and monitoring of personal health information

a) We audit and monitor the collection, use and disclosure of personal health information on an ongoing basis
b) We conduct random reviews of access to medical records, including reviews of: all agents who accessed the medical record of a specific individual during a specific period of time, all the records accessed by a specific patient during a specific period of time and all agents who access a health record of an individual with the same last name as the agent (i.e. a family member)
c) We audit the access of medical records that contain consent directives and/or a privacy warning flag

8.3.7 Mobile computing devices (e.g. laptops, USB keys, smartphones)

a) Personal health information should only be stored on mobile computing devices with the authorization of the privacy contact person
b) If personal health information is stored on a mobile computing device, the information should be encrypted

8.4 We use the following administrative safeguards

8.4.1 Office information management practices

a) Access is on a need to know basis
b) Access is restricted to authorized users

8.4.2 Third party obligations

a) Contractual privacy clauses/agreements with third parties (including cleaning and security personnel, landlords, data processors etc.)

8.4.3 Limits on third party access

a) Any other persons having access to patient information or to these premises (e.g. cleaners, security staff, and landlords) shall through contractual or other means provide a comparable level of protection.

8.4.4 All staff and others affiliated with the office (volunteers, locums) have signed confidentiality agreements

a) We also ensure that all staff have signed confidentiality agreements or clauses as part of (or appended to) their employment contract
b) This confidentiality agreement or clause extends beyond the terms of employment
c) Confidentiality agreements will be renewed annually

9. Communications Policy

9.1 We are sensitive to the privacy of personal information and this is reflected in how we communicate with our patients, others involved in their care and all third parties.

9.2 We protect personal information regardless of the format.

9.3 We use specific procedures to communicate personal information by

9.3.1 Telephone

a) Patient preference with regards to phone messages will be taken into consideration
b) Unless authorized, we leave our name and phone number on messages for patients

9.3.2 Fax

a) Our fax machine is located in a secure or supervised area (restricted public access)
b) We use pre-programmed numbers to ensure that faxes are received by the proper recipient

9.3.3 Email

a) Any confidential information sent over public or external networks is encrypted
b) Firewall and virus scanning software is in place to mitigate unauthorized medication, loss, access or disclosure

9.3.4 Post/Courier

a) Sealed envelope
b) Marked confidential

10. Record Retention

10.1 We retain patients' medical records as required by law and professional regulations. The CPSO requires:

10.1.1 The medical records of adult patients must be kept for 10 years from the date of the last entry in the record.

10.1.2 The medical records of children must be kept until 10 years after the day on which the patient reached or would have reached the age of 18 years.

10.1.3 Notwithstanding the above requirements, the CPSO recommends that records be maintained for a minimum of 15 years.

10.2 The Canadian Medical Protective Association (CMPA) advises members to retain their medical records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority (18 or 19 years in all jurisdictions).

10.3 We use secure offsite record storage (locked, fireproof, etc.)

11. Secure Disposal and Destruction of Personal Health Information

11.1 When the obligation to retain the medical record has come to an end, the medical records may be destroyed.

11.2 The CPSO requires that paper medical records be destroyed by cross shredding.

11.3 We use the following methods to destroy/dispose of electronic records

11.3.1 We seek expert advice on how to dispose of electronic records and hardware. At minimum, we ensure that all information is wiped clean where possible prior to disposal of electronic data storage devices (e.g. surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMs, USB sticks etc.)

a) Properly disposed of computer hard drives

b) Destroy all other electronic media storage (diskettes, CD-R, DVD, etc.)

11.4 Disposal log

11.4.1 Before the secure disposal of a health record ,we maintain a log with the patient's name, the time period covered by the destroyed record, the method of destruction and the person responsible for supervising the destruction (if applicable).

12. Access to Information

12.1 A patient has the right to access his or her medical records in a timely manner.

12.2 Patient requests for access should be directed to the privacy contact person

12.3 If a patient requests a copy of his or her records, one will be provided at a reasonable cost.

12.4 Access shall only be provided upon approval of the physician.

12.5 If the patient wishes to view the original record, one of our staff must be present to maintain the integrity of the record and a reasonable fee may be charged for this access.

12.6 Patients can submit access requests verbally or in writing.

12.7 This office follows specific procedures to respond to access requests.

12.7.1 We acknowledge receipt of the request.
12.7.2 We respond to a request for access within 30 days of receipt of the request.
12.7.3 If replying to a request within 30 days would be unreasonable or impractical, an extension of 30 days may be granted. Notice of such an extension must be provided, in writing, to the requestor.

13. Limitations on Access

13.1 Patients may be denied access to their records where it is permitted or required by law.

13.2 Legal exceptions to the right of access include situations where:

13.2.1 Granting access could reasonably be expected to result in a risk of serious harm to the patient or to others,
13.2.2 Providing access would reveal personal information about another person who has not consented to the disclosure,
13.2.3 The record contains raw data from standardized psychological tests or assessments,
13.2.4 The information in the record was collected/created for an inspection/investigation/similar procedure authorized by law that has not concluded,
13.2.5 The request for access is frivolous, vexatious or made in bad faith.

13.3 If only a portion of the record is covered by a legal exception, we will do our best to separate out the exempted information and provide access to information that can be disclosed.

14. Accuracy of Information

14.1 We make every effort to ensure that all patient information is recorded accurately.

14.2 If an inaccuracy is noted, the patient can request changes in their own record and this request is documented by an annotation in the record

14.3 No notation shall be made without the approval or authorization of the physician.

15. Privacy Education and Training

15.1 We conduct annual privacy training to ensure all those who provide care or assist in this office are aware of their obligations under this policy and PHIPA and that they fulfil those obligations.

15.2 Our training includes information about

a) The purposes for which employees and others affiliated with this office are permitted to collect, use and disclose personal health information,
b) The limitations, conditions or restrictions on collection, use and disclosure of personal health information,
c) The privacy policies and procedures implemented and followed by this office
d) Obligations imposed under PHIPA,
e) The duty to notify the privacy officer at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons
f) Auditing and monitoring the collection, use and disclosure of personal health information
g) The consequences of a breach of this policy or the obligations imposed by PHIPA
h) The administrative, technical and physical safeguards implemented to protect personal health information

16. Privacy Complaints

16.1 It is important to use that our privacy policies and practices addresses patient concerns and respond to patient needs

16.2 A patient who believes that this office has not responded to their access request or handled their personal information in an appropriate manner is encouraged to address their concerns first with their doctor.

16.2.1 Patient complaints can be made verbally or in writing.

16.2.2 This office follows specific procedures for responding to patient complaints.

a) Our complaints process is readily accessible, transparent and simple to use.
b) Patients are informed of relevant complaint mechanisms

16.2.3 Patients who wish to pursue the matter further are advised to direct their complaints to

a) Provincial college
b) Information Privacy Commissioner of Ontario

17. Breach of Privacy Policy

17.1 Consequences of a breach of this policy or PHIPA include (but are not limited to):

17.1.1 Suspension or termination of employment with this office
17.1.2 Discipline by regulatory college
17.1.3 Conviction under PHIPA (including a fine up to $100,000 for a person and $500 000 for an organization)
17.1.4 Legal action from the individual affected
17.1.5 Order from the Information and Privacy Commissioner of Ontario