Sample office privacy policy (*from CMA Privacy Wizard*)

Dr. Joe Smith, Family Physician
222 Smith Way, SmithFalls, ON
222-2222; Jsmith@email; Dr.Smith/mydoctor.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, protects and discloses 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 Patient information is sensitive by nature. Employees and all others in this office who assist with or provide care (including students and locums) are required to be aware of and adhere to the protections described in this policy for the appropriate use and disclosure of personal information.

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

- ☐ Office information management practices
  - ☐ Access is on a need to know basis
  - ☐ Access is restricted to authorized users
- ☐ third party obligations
  - ☐ contractual privacy clauses/agreements with third parties (including cleaning and security personnel, landlords, data processors, etc)

2.4 This office employs strict privacy protections to ensure that

- ☐ We protect the confidentiality of any personal information we access in the course of providing patient care.
- ☐ We collect, use and disclose personal information only for the purposes of providing care and treatment or the administration of that care, or for other purposes expressly consented to by the patient.
- ☐ We adhere to the privacy and security policies and procedures of this office.
- ☐ We educate and train staff on the importance of protecting personal information.

Collection, Use and Disclosure of Personal Information

3. Collection of personal information

3.1 We collect the following personal information

- ☐ Identification/Contact information, including
  - ☐ name
  - ☐ date of birth
- ☐ Billing information, including
  - ☐ Provincial/territorial health insurance plan (health card) number
  - ☐ private medical insurance details
- ☐ Health information, which may include
  - ☐ medical history
  - ☐ presenting symptoms

3.2 Limits on collection

We will only collect the 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.

4. Use of personal information

4.1 Personal information collected from patients is used by this office for the purposes of

- ☐ Identification and contact
  - ☐ emergency contact
- ☐ Provision and continuity of care
  - ☐ Historical record
  - ☐ Health promotion and prevention
- ☐ Administrate the care that is provided
  - ☐ Prioritization of appointment scheduling
  - ☐ Billing provincial health plan
- ☐ Professional requirements
  - ☐ Risk or error management, i.e., medical-legal advice (CMPA)
  - ☐ Quality assurance (peer review)
- ☐ Research studies and trials

5. Disclosure of personal information

5.1 Implied consent (Disclosures to other providers)

5.1.1 Unless otherwise indicated, you can assume that patients have consented to the use of their information for the purposes of providing them with care, including sharing the information with other health providers involved in their care. By virtue of seeking care from us, the patient's consent is implied for the provision of that care.

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

- ☐ other physicians in this practice
- ☐ other physicians in the after hours call group

5.2 Without consent (Disclosures mandated or authorized by law)

5.2.1 There are limited situations where the physician is legally required to disclose personal information without the patient's consent. Examples of these situations include (but are not limited to)

- ☐ billing provincial health plans
- ☐ reporting specific diseases
- ☐ reporting abuse (child, elder, spouse, etc)
- ☐ reporting fitness (to drive, fly, etc)
- ☐ by court order (when subpoenaed in a court case)
- ☐ in regulatory investigations
- ☐ for quality assessment (peer review)
- ☐ for risk and error management, e.g., medical-legal advice

5.3 Express Consent (Disclosures to all other third parties)

5.3.1 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.

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

- ☐ third party medical examinations
- ☐ provision of charts or chart summaries to insurance companies

5.3.3 Disclosure Log

Before a disclosure is made to a third party, a notation shall be made in the file that the patient has provided express consent, or a signed patient consent form is appended to the file.

5.4 Withdrawal of consent

5.4.1 Patients have the option to withdraw consent to have their information shared with other health providers at any time.

5.4.2 Patients also have the option to withdraw consent to have their information shared with third parties.

5.4.3 If a patient chooses to withdraw their consent, the physician will discuss any significant consequences that might result with respect to their care and treatment (e.g., possible negative impact on the care provided).

Office Safeguards

6. Security measures

6.1 Safeguards are in place to protect the security of patient information.

6.2 These safeguards include a combination of physical, technological (for offices where computers are in use) and administrative security measures.

6.2.1 We use the following **physical safeguards**

- ☐ limited access to office
  - ☐ monitored alarm system
  - ☐ deadbolt entry lock (or key card/key pad entry system
- ☐ limited access to records
  - ☐ need to know basis
  - ☐ locked file cabinets
- ☐ office layout/features
  - ☐ front desk privacy screens
  - ☐ soundproofing and/or white noise to ensure confidentiality

6.2.2 We use the following **technological safeguards**

- ☐ protected computer access for patient health information
  - ☐ passwords
  - ☐ user authentication
- ☐ system protections
  - ☐ firewall software
  - ☐ virus scanning software
- ☐ Protected external electronic communications - Internet
  - ☐ separate internet access (stand alone, not connected to operating system)
  - ☐ encrypted email for any external communication of patient health information
- ☐ secure electronic record disposal
  - ☐ safely dispose of computer hard drives
  - ☐ destroy all other removable media (diskettes, CD-R, DVD)

Wireless and mobile communication devices (e.g., laptops, PDAs, etc) are especially vulnerable to loss, theft and unauthorized access. We take extra precautions when using these devices for patient health information.

6.2.3 We use the following **administrative safeguards**

- ☐ Office information management practices
  - ☐ Access is on a need to know basis
  - ☐ Access is restricted to authorized users
- ☐ third party obligations
  - ☐ contractual privacy clauses/agreements with third parties (including cleaning and security personnel, landlords, data processors, etc)

6.2.3.1 Limits on third party access

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

6.2.3.2 Staff signed confidentiality agreements

- ☐ We also ensure that all staff have signed confidentiality agreements or clause as part of (or appended to) their employment contract.
- ☐ This confidentiality agreement or clause extends beyond the term of employment.

7. Communications policy

7.1 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.

7.2 We protect personal information regardless of the format.

7.3 We use specific procedures to communicate personal information by

7.3.1 **Telephone**

- ☐ Patient preference with regards to phone messages will be taken into consideration
- ☐ Unless authorized, we only leave our name and phone number on message for patients

7.3.2 **Fax**

- ☐ our fax machine is located in a secure or supervised area (restricted public access)
- ☐ we use of pre-programmed numbers to ensure fax received by proper recipient

7.3.3 **Email**

- ☐ any confidential information sent over public or external networks is encrypted
- ☐ firewall and virus scanning software is in place to mitigate against unauthorized modification, loss, access or disclosure

7.3.4 **Post/Courier**

- ☐ sealed envelope
- ☐ marked confidential

8. Record retention

8.1 We retain patient records as required by law and professional regulations (please refer to your College guidelines).

8.2 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 (age 18 or 19 in all jurisdictions).

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

8.4 Some colleges advise physicians that claims may arise beyond the stipulated regulatory period, and therefore may want to keep their records longer, particularly if they are aware of a potential claim.

9. Procedures for secure disposal/destruction of personal information

9.1 When information is no longer required, it is destroyed according to set procedures that govern the storage and destruction of personal information (please refer to your College guidelines).

9.1.1 We use the following methods to destroy/dispose of paper records

- ☐ According to provincial/territorial college regulations
- ☐ shredding

9.1.2 We use the following methods to destroy/dispose of electronic records
We seek expert advice on how to dispose of electronic records and hardware. At a 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, etc.)

- ☐ properly disposed of computer hard drive
- ☐ destroy all other electronic media storage (diskettes, CD-R, DVD)

9.2 Disposal log
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).

Patient Rights

10. Access to information

10.1 Patients have the right to access their record in a timely manner.

10.2 If a patient requests a copy of their records, one will be provided at a reasonable cost (please refer to your College guidelines for non-insured services).

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

10.4 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.

10.5 Patients can submit access requests

- ☐ verbally
- ☐ in writing

10.6 This office follows specific procedures to respond to access requests

- ☐ we acknowledge receipt of request
- ☐ we respond within
  - ☐ a timely fashion
  - ☐ 30 days

11. Limitations on access

11.1 In extremely limited circumstances the patient may be denied access to their records, but only if providing access would create a risk to that patient or to another person.

11.1.1 For example, when the information could reasonably be expected to seriously endanger the mental or physical health or safety of the individual making the request or another person.

11.1.2 Or if the disclosure would reveal personal information about another person who has not consented to the disclosure. In this case, we will do our best to separate out this information and disclose only what is appropriate.

12. Accuracy of information

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

12.2 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.

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

13. Privacy Complaints

13.1 It is important to us that our privacy policies and practices address patient concerns and respond to patient needs.

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

13.2.1 Patient complaints can be made

- ☐ verbally
- ☐ in writing

13.2.2 This office follows specific procedures for responding to patient complaints

- ☐ Our complaints process is readily accessible, transparent and simple to use
- ☐ Patients are informed of relevant complaint mechanisms

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

- ☐ provincial/territorial college
- ☐ provincial/territorial privacy commissioner

Physician Signature: _____

Date: _____