Dawson Travel and Immunization Clinic

PRIVACY POLICY

Your Personal Health Information (PHI) includes data that identifies you and reports about the care and services you receive at the Dawson Travel and Immunization Clinic. *Your record at the clinic is the property of the Dawson Travel and Immunization Clinic, but the information in your file belongs to you.*

The Dawson Travel and immunization Clinic takes steps to protect your personal health information from theft, loss and unauthorized access, copying, modification, use, disclosure and disposal.

This policy describes how health information about you may be used, collected and disclosed and how you can get access to this Information. It applies to all of the records, both electronic and paper, about your care. Please review it carefully.

WHAT PERSONAL INFORMATION DO WE COLLECT?

- **Identification** and **Contact** information (name, address, date of birth, emergency contact, etc)
- **Billing** information (for provincial plan and/or private insurer)
- **Health** information (symptoms, diagnosis, medical history, test results, reports and treatment, record of allergies, prescriptions, etc)

WHEN AND TO WHOM DO WE DISCLOSE PERSONAL INFORMATION?

Implied consent for provision of care: By virtue of seeking care from us, your consent is implied (i.e., assumed) for your information to be used by the Dawson Travel and Immunization Clinic to provide you with care, and to share with other providers involved in your care. It Includes all information created by Dawson Travel and Immunization Clinic clinicians, Physicians, other health care professionals, and other support staff.

Disclosure to other health care providers: Relevant health information is shared with other providers involved in your care, Including (but not limited to) other physicians and specialists, pharmacists, nutritionists.

Disclosures authorized by law: There are limited situations where we are legally required to disclose your personal information without your consent. These situations include (but are not limited to) billing provincial health plans, reporting infectious diseases and fitness to drive, or by court order.

Disclosures to all other parties: Your express consent is required before we will disclose your information to third parties for any purpose other than to provide you with care or unless we are authorized to do so by law. Examples of disclosures to other parties requiring your express consent include (but are not limited to) third party medical examinations, provision of charts or chart summaries to insurance companies, enrolment In research studies and trials

YOUR RIGHTS REGARDING YOUR PERSONAL HEALTH INFORMATION

Can you withdraw consent?

You can withdraw your consent to have your information shared by other health care providers or other parties at any time, except where the disclosure is authorized by law. However, please discuss this with your physician first.

How do you access the personal information held by this office?

You have the right to access your record in a timely manner. If you request a copy of your record, one will be provided to you at a reasonable cost. If you wish 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. Patient requests for access to the medical record must be made in writing to the privacy officer. In extremely limited circumstances you may be denied access to your records.

What if you feel your record is not accurate?

We make every effort to ensure that all of your Information is recorded accurately. If an inaccuracy is identified, you can request that a note be made to reflect this on your file.

Can you restrict access?

In some circumstances, you can tell us not to use, share or give out some or all of your personal health information to other people who provide you with health care. If access is restricted, we are required to tell other providers when we think the information is inaccurate or incomplete, including when we think the missing information could affect your health care.

For More Information, Access Requests or Complaints

If you would like more information, to request access to your records, or believe that the organization has not handled your personal information in a reasonable manner, please address your concerns in writing to:

Dawson Travel and Immunization Clinic, C/O Kevin McGuirk Privacy Officer
83 Dawson Road, Guelph, Ont N1H1B1

If you are not satisfied with the privacy officer's response, you have the right to complain to the Information and Privacy Commissioner of Ontario. The Commissioner can be reached at 1.800.387.0073 or visit the IPC website www.ipc.on.ca

Dawson Travel and Immunization Clinic

PRIVACY POLICY

DETAILED CLINIC POLICIES FOR THE PROTECTION OF PERSONAL (HEALTH) INFORMATION

Dawson Travel and Immunization Clinic
83 Dawson Road Suite 101
Guelph, Ontario
NlH 1B1, Canada
phone: S19-840-0106
fax: 519-763-4315
email:
website:www.dawsontravelclinic.com

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. This policy applies to PHI in verbal, written and electronic forms

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

   1.6. A public-friendly, 2 page summary version of this document is available In each clinic.

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 restricted to authorized users
   - Staff signed confidentiality agreements (as part of employment contract Appendix 5)
   • Staff are aware of and understand requirements to protect personal information.

Appropriate sanctions for failure to fulfill requirement

- 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 respect the requirements of each staff members role and grant access to PHI only as necessary
- 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.
- We engage in annual privacy updates and reminders at staff meetings

2.5. This office employs strict repercussions for inappropriate use of PHI, up to and including termination of employment/affiliation

2.6. Employees who are terminated, or who pursue other employment opportunities, are held to the same privacy protection standards as they were when they were employed

3. Privacy Breaches

3.1. A privacy breach occurs when there is unauthorized access to/of collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if is occurs in contravention of Personal Information Protection Act 2004. The most common privacy breach happens when personal information of patients or employees is stolen, lost or mistakenly disclosed.

3.2. In the event of a privacy breach, the event will be completely documented by using the form In Appendix 4

3.3. Patient will be contacted and informed if any of their information was, or may have been, Involved in a privacy breach

4. Privacy Audits

4.1. The Dawson Travel and Immunization Clinic will regularly conduct privacy audits to ensure staff are using their access to Personal Health Information appropriately

4.2. Audits will be conducted using the privacy audits features found in Practice Solutions 5.15

4.3. Questionable access to PHI will prompt the privacy officer to interview the staff member whom accessed the chart

4.4. If the staff member does not provide sufficient reasons for accessing PHI, they risk termination.

Collection, Use and Disclosure of Personal Information

5. Collection of personal information

5.1. We collect the following personal Information:

- Identification and Contact information including
  - Name
  - date of birth
  - address
  - phone and/or fax and/or email
  - **emergency contact information**
  - record of patient appointment times
- Billing information including:
  - Provincial/territorial health insurance plan (health card) number
  - private medical insurance details
- Health Information, including:
  - medical history
  - presenting symptoms
  - physical examination findings
  - relevant medical history of family members
  - test requisitions and results (laboratory tests and x-rays)
  - reports from specialists or other health providers
  - diagnosis and treatment notes (including prescriptions)
  - allergies
- Information to be provided to third parties at the patients request (e.g., workers compensation, reports for legal proceedings, insurance claims, government claims)

6. Use of personal information

6.1. This office uses Personal information collected from patients for the purposes of:

- Identification and contact Emergency contact Provision and continuity of care Historical record
- Health promotion and prevention
  Referral to specialists or other treating physician
- Requesting laboratory investigations
- Requesting diagnostic tests
- Generating prescriptions
- Referral to other health care providers
- Referral to Home Care agencies
- Home care supervision
- Administrate the care that is provided
- Prioritization of appointment scheduling
- Billing provincial health plan
- Billing third parties
- Facilitate reimbursement of patient claims (at patient's request)
- to allocate resources to our programs

- Professional requirements
- Risk or error management, i.e., medical-legal advice (CMPA)
  - Quality assurance (peer review)
- Maintenance of competence
- Generate anonymous statistics for the MOHLTC

7. Disclosure of personal information

7.1. Implied consent (Disclosures to other providers)

7.1.1 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 searching care from us, the patient's consent is implied for the provision of that care.

7.1.2 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 afterhours call group
- locums
- medical students and residents
- nursing or other health care students
- other physicians and specialists
- Pharmacists
- Nutritionists
- program coordinators and support staff

7.2. Without consent (Disclosures mandated or authorized by law)

7.2.1 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 or similar, as per Appendix 2)
- in regulatory investigations
- for quality assessment (peer review)
- for risk and error management, e.g., medical-legal advice

7.3. Express Consent (Disclosures to all other third parties)

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)

- third party medical examinations
- provision of charts or chart summaries to insurance companies
- enrolment in research studies and trials

7.3.3 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.

7.4. Withdrawal of consent

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

7.4.2 Patients also have the option to withdraw consent to have their Information shared with third parties.

7.4.3 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).

7.5. Substitute Decision Makers (SDM)

- An SDM is a person who has the lawful authority to make a decision for another person who lacks the mental capacity to make that decision

- In the event that it is unclear which SDM has the authority to make a decision regarding consent, 'Substitute Decision-Maker Raking Guide' in Appendix I.

7.6. Patient Death

- If a patient dies and there is a request of information for the medical file, only the executor of the will can legitimately release the file; and we would need to see the will and identification of the person named on the will;
- Any other requests can come from the coroner; subpoena and/or warrant.

- In the event that any other individual is asking and does not meet the above criteria and decides to complain, we shall point them to the Information Privacy Commissioner's office.

Clinic Safeguards

8. Disclosure of personal information

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

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

8.2.1 We use the following **physical safeguards**

- limited access to office
- key fob/keypad electronic entry
- authorized access only
- limited access to records
- need to know basis

8.2.2 We use the following **technological safeguards** protected computer access for patient health information:

- Passwords
- user authentication
- audit trails

- o system protections
- o firewall software
- o redundancy systems (backups)
- o regular backups
- o encrypted
- o Protected external electronic communications - Internet
- o encrypted email for any external communication of patient health information
- o secure electronic record disposal
- o Where electronic records are retained rather than destroyed, we follow College requirements for secure retention and disposal of medical records

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.

A password policy has been implemented (Appendix 3) to ensure the safe maintenance of passwords.

8.2.3 We use the following **administrative safeguards**

- Office Information management practices
- Access Is restricted to authorized users
- Records should only be printed in hard copy when necessary and must be disposed off securely onsIte
- staff signed confidentiality agreements (as part of employment contract, Appendix 5)
- staff are aware of and understand requirements to protect personal information
- appropriate sanctions for failure to fulfill requirements
- third party obligations
- No contractual privacy clauses/agreements with third parties (Including cleaning and security personnel, landlords, data processors, etc)

8.2.3.1 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.

8.2.3.2 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.

8.2.3.3 Identity Verification

Any individual submitting consent directives (granting or limiting access to PHI) will undergo Identification verification to protect privacy and unauthorized distribution of information.

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**

- secure office voicemail system
- no audible playback of voice messages in office

9.3.2 **Fax**

- our fax machine is located in a secure or supervised area (restricted public access)
- we use pre-programmed numbers to ensure fax received by proper recipient
- a cover sheet indicates the Information is confidential

9.3.3 **Email**

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

9.3.4 **Post/Courier**

- sealed envelope
- marked confidential
- addressed to the authorized recipient

10. Record retention

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

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 (age 18 or 19 In all jurisdictions).

11. Procedures for secure disposal/destruction of personal information

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

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

- Shredding

11.1.2 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) o destroy all other electronic media storage (diskettes, CD-R, DVD) o Electronic records are retained rather than destroyed, and we follow College requirements for the secure retention of medical records

Patient Rights

12. Access to information

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

12.2. If a patient requests a copy of their records, one will be provided at a reasonable cost.

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

12.4. 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.

12.5. Patients can submit access requests In writing to:

Dawson Travel and Immunization Clinic C/O Kevin McGuirk, Privacy Officer 83 Dawson Road, Guelph, Ont. N1H 1B1

12.6. This office follows specific procedures to respond to patient access requests

- we acknowledge receipt of request
- we respond within 30 days

12.7. In exceptional circumstances, where a written request is not possible, access to information verbally should be done by contacting the privacy officer at **519-766-1360**

13. Limitations on access

13.1. 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. 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.

13.2. 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.

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 and Access Complaints

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

15.2. 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.

15.3. Patient complaints can be made in writing to:

Dawson Travel and Immunization Clinic C/O Kevin McGuirk, Privacy Officer 83 Dawson Road, Guelph, Ont. N1H 1B1

15.4. The Dawson Road Family Medical Clinic follows specific procedures for responding to patient complaints

- We acknowledge and respond to patients In a timely fashion
- All complaints shall be investigated
- If justified, remedial measures will be taken, such as amending policies, procedures and practices

15.5. Patients who wish to pursue the matter further are advised to direct their complaints to the Information and Privacy Commissioner of Ontario. The Commissioner can be reached at 1.800.387.0073

Dawson Travel and Immunization Clinic Privacy Officer

Signature:

Date:

Appendix 1 - Substitute Decision-Maker Raking Guide

Substitute Decision Maker Ranking Guide

This is a guideline to refer to if sufficient grounds exist to believe that client is incapable to consent to the release of information in order to attain sufficient authority to release personal information.

1. Guardian with authority to consent/refuse
2. Attorney for personal care if POA (Power of Attorney) gives authority to consent/refuse
3. Representative appointed by CCRB (Consent and Capacity Review Board) if it has authority to consent/refuse
4. Spouse (at least one year of cohabitation, a child or a cohabitation agreement or a partner (one year cohabitation and close personal relationship which is primary importance in both persons' lives.
5. Child or parent, Family and Children Services or other person lawfully entitled to give consent/refuse (does not include access parent).
6. Access parent
7. Brother or sister.
8. Any relative (by blood, marriage or adoption - s. 20 (1).

Substitute Decision must follow **Health Care Consent Act (HCA)**

- prior wishes (capable and at least 16 years old)
- if impossible to follow or unknown, then act in the client's best interest (s.21 (2))

If principles not followed, service provider may apply to the Privacy Officer to determine compliance by Substitute Decision Maker (SDM)

Appendix 2- Procedure When Releasing PHI to Police

Procedure When Releasing PHI To Police

Releasing PHI to the Police: Ground Rules

This section provides the fundamentals regarding the release of personal health information (PHI) to the police. As a general rule, If the police present one of the following pieces of documentation, PHI **must** be released to the police upon completion of the steps (as applicable) below:

- A valid court order, or
- A Search Warrant, or
- A Subpoena, or
- A Coroner's Writ, or
- A Production Order, or
- An original written authorization of the patient allowing release of the Information requested. To verify the identity of the patient this form must be accompanied by a copy of patient photo identification.

- If you receive on of the above documentation you must complete the following steps (as applicable) prior to releasing any PHI.
- Ensure that the document clearly states the purpose of the request.
- You must notify your director/manager, risk coordinator and/or privacy officer when a police officer arrives on site with documents
- If the warrant is for health records, police must be directed to the Release of Information Office
- Requests for PHI by the police must be directed to Health Information Management (HIM) department during regular business hours.
- Requests for PHI by the Coroner (or Police Officer acting on his/her behalf) must be directed to the HIM department. As part of an investigation a coroner can authorize a police officer to exercise all or any of his/her powers including the inspection, extraction and copying of PHI relating to the deceased [Coroner's Act, Section 9(1,2), 16(4)].
- The information provided pursuant to a warrant should only include that part of the record requested in the warrant.
- The following information must be included In the Release of Information document
    - Name and division of the police force; and
    - Name and badge number of police officer requesting information release form)

- A contact telephone number for the Police officer; and
- A copy of the legal document (e.g., warrant, court order, signed patient release form)

Dawson Travel and Immunization Clinic Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Dawson Travel and Immunization Clinic's entire network. As such, all Travel Clinic employees (including Guelph Family Health Team employees, contractors and vendors who have access to Dawson Road Family Medical/Dawson Travel and Immunization systems)) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at Dawson Road Family Medical Clinic facility, has access to the Guelph Family Health Team network, or stores any non-public Dawson Road Family Medical Clinic information.

Genera

1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must
   be changed on at least a quarterly basis.
2. All production system-level passwords must be part of the administered global password management
   database.
3. All user-level passwords (e.g., email, web, desktop computer, etc) must be changed at every four months.
4. No user account with full administrative privileges shall be allowed to logon the network. Administrative tasks must be "run as" the administrator.
5. Passwords must not be inserted into email messages or other forms of electronic communication.
6. All user-level and system-level passwords must conform to the guidelines described below.

Password Creation Guidelines

Passwords are used for various purposes at Dawson Travel and Immunization Clinic. Some of the more common uses Include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Dawson Travel and Immunization Clinic", "sanfran" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and tower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !©«$%*&*()_+1~-
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmytOe).
- Are not a word in any language, slang, dialect, jargon, etc
- Are not based on personal information, names of family, etc

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2RI^{n} or "TmbIW>r" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for Dawson Road Family Medical Clinic accounts as for other non-Dawson Road Family Medical Clinic access (e.g., personal ISP account, option trading, benefits, etc). Where possible, don't use the same password for various Dawson Road Family Medical Clinic access needs. For example, select one password for the Lab systems and a separate password for IT systems.

Do not share Dawson Road Family Medical Clinic passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Dawson Road Family Medical Clinic information.

Here is a list of “dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don’t reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don’t reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- If someone demands a password, refer them to this document or have them call someone in the Information Security Department

^o

- o Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Internet Explorer), o Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption
- o If an account or password is suspected to have been compromised, report the incident to Management and change ail passwords.

Management or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?<r>*@TrafficOnThel101Was$&fflfThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix 4 - Privacy Breach Reporting Form

PRIVACY BREACH REPORTING FORM

A privacy breach occurs when there is unauthorized access to/of collection, use. disclosure or disposal of personal information. Such activity is "unauthorized" if is occurs in contravention of Personal Information Protection Act 2004. The most common privacy breach happens when personal information of your clients or employees is stolen, lost or mistakenly disclosed. Examples include when a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong person. Upon receipt of this form, you will be contacted by the Dawson Road Family Medical Clinic Privacy Officer.

Note: All fields must be completed before you submit this form to the Dawson Travel and Immunization Clinic Privacy Officer. Submit form by fax to (519) 763-4315. If a question does not apply to your situation, or you do not know the answer now, please indicate this. Append added pages if necessary. Upon receipt of this form, you will be contacted by the Dawson Travel and Immunization Privacy Officer.

Receipt of Returned Personal Hearth Information

1. Contact Person (Individual who received and/or processed the Breach)

Name: _____ Extension: _____

Service:

Position:

Date PHI received/awareness of breach

Risk Evaluation

Incident Description 1.

Type of Breach:

Service to Service Misdirect (Medium)
Correspondence Misdirected & Not Opened - (Low)
Correspondence Opened by other than client - (High)
Stolen Laptop (Unencrypted) with PHI on it-(High)
Other: indicate risk rating (describe) _____

2. Date of incident:

3. **Date if incident discovered:** _____

4. **Location of incident** _____

Personal Information Involved

5. **Describe the personal information involved (e.g. name, address, CID, financial, medical).**

Safeguards

6. **Describe physical security (correct address on file and software) in place.**

Harm from the Breach

7. **Identify the type of harm(s) that may result from the breach:**

- **Identity theft**

(most likely when the beach includes loss of SIN. credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud)

- **Risk of physical harm**

(when the loss of information places any individual at risk of physical harm, stalking or harassment)

- **Hurt, humiliation, damage to reputation**

(associated with the loss of information such as mental health records, medical records, disciplinary records)

- **Loss of business or employment opportunities**
  (usually as a result of damage to reputation to an Individual)

- **Breach of contractual obligations**
  (contractual provisions may require notification of third parties in the case of data loss or privacy breach)

o **Future breaches due to similar technical/system failures**
(notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)

o **Failure to meet professional standards or certification standards**
(notification may be required to professional regulatory body or certification authority)

Other (specify):_____

Notification

8. **Has your Supervisor/Manager and Privacy Officer / Manager of Information and Privacy been notified?**

Yes Who was notified and when?____
No When to be notified?_____

Management/Privacy Officer Action"

9. **Risk Manager has been notified depending on potential risk level of Breach (e.g., media awareness, meets high risk criteria)**

   Details:

10. **Breach information been forwarded to appropriate Manager/Supervisor and/or delegate.**

    Name: _____
    Affected individuals are notified. Name individual(s):
    Yes Form of notification: _____
    No Why not? _____

11. **Describe the notification process (e.g. who was notified, the form and content of notification): _____**

If you have completed a security audit, please forward to the Dawson Travel and Immunization Clinic C/O Privacy Officer, Kevin.McGuirk@drfmc.ca.

Password protect your document by providing the password in a separate e-mail.