# Hamilton Family Health Team

## Safeguards for Patient Information

At Hamilton Family Health Team we hold a lot of personal information about our patients.[1] This information is sensitive and valuable to our patients and we are obliged by law to treat it carefully. As part of our duties we must all take steps to keep patient information safe and make sure that it can be accessed only by those who need to see it for a proper reason.

This applies equally to our electronic medical record, paper copies of health records, reports, test results voice messages, and emails and any other ways patient information can be recorded. We have to protect this information from loss, theft, unauthorized access including any kind of disclosure to the wrong people.

These guidelines are part of Hamilton Family Health Team's Privacy Policy. Following them will minimize the risk of patient information falling into the wrong hands which could cause harm and distress to patients and legal consequences to the Hamilton Family Health Team and our related 15 Family Health Organizations. We require everyone who is affiliated with the Hamilton Family Health Team and Family Health Organizations, including all physicians, staff, volunteers, students and vendors (collectively "Team Members") to follow the best practices described here. Every team member has a role in keeping our patients' information secure, and we expect everyone to fulfill that role.

## Privacy Breach

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* ("PHIPA"). The most obvious privacy breaches happen when patient information is lost, stolen or accessed by someone without authorization.

For example:

- A fax with patient information is misdirected to a business where the fax number was entered incorrectly
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package of patient records is not delivered to the correct address
- An unencrypted USB key with an Excel spreadsheet with patient information or Word files is lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- A Team Member talks about a patient with a friend
- Team Member sends an email to a "help desk" attaching a worksheet with patient information but does not check the email address and instead of sending the attachment internally – sends it to the last help desk emailed which is at a bank
- Health records to be disposed of are recycled and not shredded

[1] We have used the term "patient" throughout the policy. It is possible that we hold PHI about individuals who are not Hamilton Family Health Team patients, and the safeguards policy would apply equally to those individuals

- Out of curiosity, a Team Member reviews a neighbour's health record
- A student or any other Team Member looks at health records of patients on a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise
- Health information is given to the media
- A Team Member makes a copy of an ex-spouse's health record without it being part of the Team Member's position to do so
- Team Members discuss patients in hallways and lunchrooms and other patients overhear (even colleagues overhear)
- Team Member releases information to another health care provider when a patient has said she doesn't want that provider to know
- Team Member releases information to a spouse when the patient doesn't want that spouse to know
- Team Member releases information to a child's parent when the child is capable of making his own decisions and said don't tell my parents

All privacy breaches must be reported immediately to a Privacy Officer (the Privacy Officers are the Executive Director of the Hamilton Family Health Team and the lead physician of each FHO). Please follow the Privacy Breach Protocol.

Please note:

- If a privacy breach happens within an individual family physician's office and it can be addressed there, then it should be. Where appropriate, a family physician may seek the support of their FHO Lead or contact the HFHT Privacy Officer directly.

- If a privacy breach cannot be managed within the family physician's office, the Privacy Officers can be contacted to assist.

- If you have any questions, contact one of the Privacy Officers.

Annually each FHO will submit a report to the Privacy Officers who will make a full report to the board of the Hamilton Family Health Team.

## Restricted Access to Patient Information

Access to patient information is provided on a need-to-know basis as appropriate to the Team Member's role and purpose for access.

No snooping!

Team Members must not access any health records unless authorized - which means only for legitimate reasons. Team Members may not access health records of their spouses, children, parents, friends or neighbours, or work colleagues unless that person is under the Team Member's direct care or the Team Member is authorized as part of their official duties (or if covering the shift or tasks for someone who is

authorized). Team Members may only access their own health record (if applicable) through the normal patient access channels and not directly.

Team Members must not:

- Access patient information for "self-education" or out of personal interest
- Edit, cut-and-paste, delete from or otherwise change any health records except for legitimate reasons

Team Members should know that all access to the electronic medical record is logged and audited.

## Accounts and Passwords

Our information technology systems are protected by the use of personal accounts and passwords. Individual accounts are given access to information required by the account holder. We require all Team Members to:

- Use only their own user account and password
- Not permit anyone else to use their account
- Help maintain security by choosing hard-to-guess passwords
- Contact a Privacy Officer if they suspect any kind of computer misuse

A good privacy password is a mix of numbers, upper and lower case letters and symbols. Avoid using your name in a password.

An unauthorized person trying to gain access to our health records may not be obvious. Data breaches have occurred in other organizations after "confidence tricks" convinced individuals to reveal passwords or other information to intruders, for example claiming to be the "IT helpdesk". Never tell anyone your password no matter who they say they are. If anyone you do not know requests information from you, you must verify their identity and their reason for asking, first. If you are left in any doubt contact a Privacy Officer immediately.

## Physical Security On-Site

We hold a large amount of patient information in printed format - on paper, in files and binders. Daytimers, schedules and notebooks may also contain patient information and are confidential just like patient files.

Access to patient information is permitted by individuals who require the information to do their authorized jobs. If patients or visitors are in areas where patient information is kept or in other private areas, politely challenge them as to their business. If there is any doubt as to someone's purpose, they should be asked to leave.

Patient information in paper format should be kept in a locked cabinet, container or room. If a filing cabinet or room where patient information is stored is not in constant use, it should be locked.

Where records are on desks in occupied rooms or in in-trays they should be turned over so they cannot be read by someone nearby.

Patient identifiable labels on files should not be visible to visitors.

Patient information that is being stored before secure destruction will be kept separate and clearly marked.

## Patient Information in Transit

Because of the serious risk of loss or theft, patient information will only ever be removed from the premises by those Team Members who have a real need to do so to carry out their duties (for example, Team Members who provide care to patients off site such as home visits or community settings). This applies to electronic files, paper copies and information on laptops, smart phones, disks and memory sticks (USB keys) and any other formats.

For electronic files, remote access to patient information should be through a secure server, where we can protect it. Every time patient information is saved to a laptop, disk or memory stick there is a chance it may be lost or stolen. Therefore we will do this only when absolutely necessary to carry out our jobs.

Where there is no choice but to take information off-site, patient information will be de-identified if possible. Otherwise, if Team Members are ever required to copy patient information onto a laptop, memory stick or other portable device strong encryption must be used. Strong encryption is more than just password protected. If you are not sure how to do this a Privacy Officer will show you how. For paper files, keep papers in a locked box or bag for transport.

When in public, steps should be taken to avoid drawing attention to the materials (such as keeping them in an unmarked bag or container).

Laptop computers, disks or files containing personal health information must not be left on the seat or in the trunk of an unattended car, even for just a few moments.

When transporting patient information, go directly to the destination, making the journey as short as practicable.

Patient information should not be stored at home except in very limited circumstances and if the Team Member is required to keep information at home, it must be held securely and care should be taken to avoid family or friends or other visitors from having any access. Team Members should not make printouts from remote access at home.

## Sending Patient Information

Special care must be taken when sending correspondence about a patient or containing patient information to anyone outside of the Hamilton Family Health Team - including to another health-care provider, to a third party, or to the patient.

Please note, sending a patient's chart number still constitutes identifiable health information. Merely removing a patient's name from a record does not necessarily anonymize the record.

In addition to this policy, physicians and integrated health providers (collectively, "clinicians") need to follow their own regulatory College's directives on confidentiality, security of personal health information and communicating with patients to ensure privacy is protected.

***External Emails and Text Messages***

Because of the insecure nature of emails, Team Members are not permitted to include patient information in any email or text sent to a recipient other than to a Hamilton Family Health Team email address or Team Member's phone, except as set out below.

***Patients***

Clinicians may send or give permission to a Team Member to send emails to their patients for the purposes of:

- Reminding patients about appointments and follow-up visits;
- Sending information or resources requested by a patient;
- For requesting feedback to programs, groups or services that a patient may have participated in; or
- Assisting a patient with self-management.

Any other information communicated with a patient via email will be done on a limited basis and through an approved, secure and encrypted method like Telus PS Suite and Ocean Cognisant MD platforms. No emails to patients should be sent through unapproved programs such as "gmail". This is important because it:

- Decreases the changes of typos in entering email addresses
- Ensures that a copy of the email is recorded in the patient's chart for continuity of care and legal purposes
- Ensures that the email is sent from an approved email address so that automatic reply functionality is working properly
- Ensures that any information not intended for the patient is not accidentally sent (such as can be the case with the "reply all" functionality of regular email chains.

Except in rare circumstances (such as an emergency where there is no other reasonable option), email (especially unencrypted email) should not be used to communicate diagnoses, provide information about test results or transmit other personal health information that will require a follow up visit to the Hamilton Family Health Team. Clinicians must take care to consider the sensitivity of the information being conveyed over email (especially unencrypted email). Clinicians should also consider that as the volume and frequency of emails increase – so too does the risk inherent in communicating by email.

If email is to be used for the authorized purposes, the following steps must be undertaken:

- The Team Member must register with the Privacy Officers as a patient email user (that means for physicians they declare to their FHO lead);
- The Team Member must have encryption software on his/her system that encrypts outgoing email messages and requires a password to be opened[2];
- The patient must sign a Hamilton Family Health Team Patient Consent and Release for Email Communication and it must be documented in the patient's health record (see Appendix A);
- There must be a disclaimer message at the end of the email message being sent (see Appendix B);
- The Team Member (or email method) must have an automatic response email for all incoming email messages (see Appendix C);
- Before sending, the Team Member must check the email address carefully to confirm it is going to the correct recipient (NOTE: email programs that "autofill" the recipient field can insert an address you did not intend to send to);
- The Team Member should avoid using the "reply-all" feature if responding to an email from a patient and limit the number of recipients to the minimum necessary. To avoid mistakes, the Team Member must check to see if there are any unexpected attachments to the email that will be sent (by clicking on "preview" to see the email content or otherwise reviewing the email before sending);
- If appropriate, the email message must be copied and entered into the health record or the clinician must write a note in the health record summarizing the clinically relevant information from the email communication;
- The email may only include the minimum amount of personal health information necessary for the purpose; and
- For group emails (emails to more than one patient such as for flu clinics or patient satisfaction surveys), the Team Member sending the email must check to see if there are any unexpected attachments to the email that will be sent (by clicking on "preview" to see the email content or otherwise reviewing the email before sending).

Similar issues arise with use of text messages. If you communicate with patients by text, please contact the Privacy Officers for recommendations.

---

[2] The CPSO policy on Medical Records reads in part: *"E-mails may not be secure. Therefore, physicians who wish to send personal health information by e-mail must obtain express consent to do so from the patient or their representative unless they have reasonable assurances that the information sent and received is secure. Physicians should use a secure e-mail system with strong encryption.*

### *Sending emails and texts to other health care providers outside the Hamilton Family Health Team*

Once Ontario has a secure shared electronic provincial health record, sharing identifiable patient information with external health care providers will become much easier. Until then, unencrypted email exchange and text messaging should not be used routinely for communicating with external health care providers. Consider all the issues discussed in this policy for communicating with patients and internally within the Hamilton Family Health Team. Extra care should be used to only include the minimum amount of personal health information necessary for the purpose.

***Emails Sent within Hamilton Family Health Team***

It is preferable to send messages about patients through the electronic medical record functionality wherever possible.

If sending emails within the Hamilton Family Health Team, limit the personal information included to the minimum necessary. Refer to patients by their initials rather than using their full names, if it is possible to do so.

When using the “reply-to” feature there is a risk of including more information than necessary by including a copy of the original email. Therefore, start a new email rather than responding to an email thread.

Carefully check the recipient before hitting the send button. Email programs that autofill the recipient field can insert an address you did not intend to send to.

Avoid using the "reply-all" feature and limit the number of recipients to the minimum necessary.

***Accessing Email on a Mobile Device***

If a Hamilton Family Health Team email address is to be accessible on a mobile device (such as a smart phone), the following steps must be undertaken:

- Team Members must have permission from one of the Privacy Officers to load a Hamilton Family Health Team email address account on a mobile device;
- The device must be password protected and ideally subject to a strong level of encryption;
- The device contents must be able to be erased remotely if lost or stolen (that means, all content from the device can be remotely deleted by Hamilton Family Health Team or the device owner);
- A “Return If Lost” sticker must be put on the device; and
- Any loss of the device must be reported immediately to the Privacy Officers to assess exposure and remotely delete the contents of the device if necessary

***Facsimile (Faxes)***

Misdirected faxes are easy to send and difficult to correct. They make up a significant proportion of privacy breaches. Therefore when sending patient information by fax, carefully check the fax number - multiple times - to ensure it is correct.

Include a cover sheet stating for whom the fax is intended. The cover sheet must ask a recipient to call if information is received in error.

Where appropriate, call the recipient prior to sending a fax so they can be waiting to retrieve it.

After sending a fax, collect and keep a confirmation receipt. If there is any question about a wrong number being used the receipt will make it much easier to check and to retrieve information sent to the wrong place.

A privacy breach occurs whenever patient information is sent to a third party without the patient's authorization or without being otherwise permitted or required by law. There can be particularly significant consequences in cases where clinicians repeatedly send patient information to a third party improperly.

In the event of a misdirected fax containing patient information, it is important to ask the wrong or unintended recipient to confirm **in writing** that the information was destroyed and not kept or shared with anyone. This should then be documented in the patient's chart.

Clinicians should use their judgment when it comes to implementing the Privacy Breach Protocol as a result of a misdirected fax. For single instances of a fax that is misdirected to another health care provider, ensuring that the recipient securely destroyed the fax may be sufficient. Clinicians may choose to put a reminder in the chart to discuss the breach (and actions taken to correct it) next time the patient visit the clinic. Clinicians should be aware that they may face increased consequences if they do not implement the full Privacy Breach Protocol whenever a breach occurs.

Please report all stray faxes to your Privacy Officer. And situations where there are repeated stray faxes must be reported to the Privacy Officers to assess whether a report to the Information and Privacy Commissioner is required and how to notify affected individuals.

***Social Media***

Team Members are advised to avoid posting information about patient-specific cases or and are advised against providing medical or other clinical **advice** online. Regulatory colleges and professional liability indemnity providers recommend that clinicians avoid posting comments in internet discussion forums or other online groups to avoid the perception of providing medical or health care **advice**. While it may be acceptable to provide general health-related **information** for public or professional educational purposes, those purposes should be clearly identified and clearly marked as not providing advice.

***Telephone***

Patients may ask us to relay their own health information to them by telephone. Calling a patient at home or at work or leaving messages carries a real risk to our patients' privacy. It may be difficult to verify the identity of the person who answers or control who hears a message.

To minimize these risks, ask patients every time they register for an appointment to check that their contact information is up to date so we have their most recent telephone numbers (and home address – see mail below). Ask if we can leave a message with someone or on an answering service and confirm the number.

If we have the patient's consent to leave a message and you are answered by a machine, listen for clues that you may have misdialed before leaving a message. For example, if the message repeats a name or number other than the one you expected to hear. If you are in any doubt leave a message only to say to call the office.

If a patient calls us we must take steps to confirm the caller's identity before providing information. Our patients expect it. If we are in doubt as to the identity of the caller, we can confirm the caller's identify by asking questions such as:

- When was your last appointment with us?
- What medications are you currently taking?
- What allergies do you have?
- What is your health card number?

***Mail***

Sometimes it is necessary to send patient information by mail or courier. When sending information in the mail, check the address to make sure it is correct. Also, mark the envelope or package "Attention <name>" on the outside to make sure it is opened only by the intended recipient.

Make sure that no health information can be read through the envelope or window, and consider whether there are any logos or other markings on the envelope that may identify the nature of the content enclosed.

For highly sensitive information, obtain a tracking number and follow up with the patient to make sure it was received. When sending regular patient information via mail, a tracking number is not mandatory, but should be used depending on the sensitivity of the health information being sent. For less sensitive information, clinicians may choose to mark envelopes with a CONFIDENTIAL stamp and include a return mailing address.

The easiest way to prevent the chances that a patient's mail will be lost or stolen (without using a tracking number system) is to call the patient and ask him/her to pick up the letter at the office. If they are not able to attend, the patient's home address can be confirmed at that time, and they will have notice that they will receive a letter in the next few days

## Filing Patient Information

Care should always be taken when tagging and filing electronic records or uploading paper copies of patient information to a patient's electronic health record to ensure the information relates to the correct patient. Check patient names and dates of birth carefully.

When patient information is filed in the wrong health record, it should be corrected immediately. It may be appropriate to choose *not* to enact the Privacy Breach Protocol when a test result is filed in the wrong chart, if a clinician feels confident that the misfiled information was not accessed by another healthcare provider to make healthcare decisions on behalf of the patient, and that no other patient would have had access to the information (for example, through a request for a copy of the chart). If it is possible that the information could have been used to make treatment decisions or could have been shared with an unauthorized third party, then the Privacy Breach Protocol should be enacted.

## Destroying Patient Information

When patient information is no longer needed we must make sure it is destroyed securely. Different methods of destruction are appropriate depending on how the data is stored:

| Material | Appropriate Method of Destruction |
|---|---|
| Paper (e.g., printouts, faxes, letters, labels, etc.) | Shredding |
| CDs, DVDs, disks, USB keys | Shredding or breaking into pieces |
| Audio or video tapes | Shredding |
| Pictures, slides | Shredding |
| Medication containers (bottles and bags) with ID labels | Shredding of label (or container) or return to supplier along with unused medications |
| IV bags | Label goes in shredding |
| Electronic devices with memory storage (e.g., laptops, PCs, printers, photocopiers, dictaphones) | Data wiping prior to redeployment or return to vendor |

Never recycle any paper or media which contains patient information. Never treat any paper which has been printed with patient information as reusable for scrap. When patient information is no longer needed, it should be securely destroyed.

## Third Party Vendors

When Hamilton Family Health Team or Family Health Organizations hire outside contractors to do data entry or provide information systems or to store, transport or destroy patient information we only use those that are bonded and insured and maintain a verifiable commitment to confidentiality. We make sure that the contractor uses the methods documented in the contract we have with them.

We only select contractors who commit under contract to:

- Agree to be a PHIPA agent of the applicable FHO

- Hold and follow written privacy policies and procedures saying how material is to be kept safe in transit, storage and destruction as applicable
- Have insurance coverage for their liabilities under contract
- Require their own personnel to sign confidentiality agreements
- Have appropriate training for their personnel on privacy policies and the procedures to implement them

## Breach of Privacy Safeguards

Failure by Team Members to adhere to the privacy safeguards and guidelines set out above may result in disciplinary measures, up to and including termination of employment or contract.

**Appendix A - Hamilton Family Health Team Patient Consent and Release for Email**

We are now able to offer the use of email for:

- Appointment reminders
- Sharing routine test results or home blood sugar testing and self management like insulin adjustments
- Nutritional counseling and questions

In addition physicians and health care providers may communicate with you by email with your permission . **Please read to the bottom of this page to submit your consent.**

If you intend to receive our emails, please remember to update your address book (with info@tmcdocs.info), and/or to check your junk/spam folder.

**Email Policy**

You have asked to use email with our office. There are some limits on what and when we can email you, which we will explain here.

- Email communication is not a substitute for meeting with your health care provider. Although technology is changing, the best way to share information with your health care provider is in person.

- Please tell us which email address you wish us to use. You must to keep this up-to-date and tell us of any changes to your email address.

- Email should never be used in an emergency. If you have an emergency, you should call 9-1-1 or go to your nearest hospital emergency room or health care provider immediately.

- Email should never be used for urgent problems (where you need a response from us by a certain time). If you have an urgent issue, you should make an appointment to see your Hamilton Family Health Team health care provider.

- We do not read our email messages 24 hours per day 7 days per week. We cannot guarantee any particular response time for an email. If you require a response to an email message, please call the Hamilton Family Health Team office.

- Emails should be short. If you have a problem that is complex – please call the office instead.

- You should not use email to tell us about sensitive health information. Please tell us if there are certain issues or types of information that you do not wish to discuss by email.

- There are some privacy risks in communicating by email:
    - Email may not be secure. While we try to protect our emails we cannot guarantee the security and confidentiality of any email you send to or receive from us. As the message

leaves Hamilton Family Health Team it is sent across the internet and it could be intercepted and read.

- More than just your health care provider may need to read your email. Administrative staff supporting your health care provider and people providing coverage for your health care provider (like a locum doctor) may also read any email you send.

- Emails may be filed on your health record depending on the content of the email message and can become a permanent part of your health record. Because they can become part of your health care record, emails may be shared within the Family Health Team or third parties, with your consent or if we are permitted or required by law (including with other health care providers and insurance companies).

- Email is easy to forge, easy to forward (sometimes accidentally and to many people) and may exist forever.

- If you use a work email, your employer may have a right to archive and inspect emails sent from their systems. We recommend you avoid using a work email address.

- We recommend you give us a personal email address that only you read. We recommend that you use an email address and system that is password protected. If you give us a family email address or share your email address with anyone else you should know that other people may also receive or read emails we send to you.

- Hamilton Family Health Team is not responsible for information loss due to technical failures.

- Hamilton Family Health Team may choose not to deal with you by email if you are not able to follow our email rules.

**Patient Acknowledgment, Agreement and Release:**

- I have read and fully understand this consent and release form.

- I understand the risks associated with using email with Hamilton Family Health Team and I accept those risks.

- I understand the limits set out for using email with Hamilton Family Health Team and I agree to follow those limits.

- I understand if I no longer wish to communicate with Hamilton Family Health Team by email, I will write to * .

- **I agree that Hamilton Family Health Team or the * Family Health Organization (and their physicians, staff, agents and officers) shall not be responsible for any personal injury including death, and/or privacy breach (outside the control of Hamilton Family Health Team or Family Health Organization) or other damages as a result of my choice to communicate with Hamilton**

**Family Health Team by email and I release the Hamilton Family Health Team and Family Health Organization (and their physicians, staff, agents and officers) from any liability relating to communicating with me by email.**

- If I had any questions about this form, I asked Hamilton Family Health Team those questions and agree that my questions have been answered.

- I understand I have the right to have legal advice about signing this form and what it means to me and have either sought that advice or have chosen not to seek such advice.

**SIGNATURE OF PATIENT/SUBSTITUTE DECISION-MAKER**

_____

**PRINT NAME**:_____**DATE:**_____

**Appendix B – Email Disclaimer Message**

This e-mail message is confidential and is intended only for the persons named above. If you have received this message in error, please notify the sender immediately and securely delete/remove it from your computer system. Any reading, distribution, printing or disclosure of this message if you are not the intended recipient is strictly prohibited. Thank you.

**Appendix C – Automatic Response Email**

Thank you for your message.

- If you are experiencing a medical emergency, please contact 9-1-1 or go to an emergency department or local hospital.
- All appointments with my office are made by phone to * (insert #) and I cannot accept email requests for new appointments.
- I do not monitor this email address 24 hours a day/ 7 days per week. There may be a delay in my ability to respond to your message.