afhto association of family health teams of ontario

ANSWERS TO FIVE PRIVACY QUESTIONS

AND FIVE PRIVACY TOOLS

FOR FAMILY HEALTH TEAMS

Written by:

DDO HEALTH LAW

Kate Dewhirst

February 2016

Author

Kate Dewhirst is a founding partner with the Toronto health law firm Dykeman Dewhirst O'Brien LLP (**DDO Health Law**). Kate advises family health teams (**FHTs**) and nurse practitioner-led clinics on privacy, patient/family complaints, physician performance, quality improvement, risk management, legal compliance, health records, documentation and governance.
Email: kdewhirst@ddohealthlaw.com Twitter: @katedewhirst

DDO Health Law

DDO Health Law is a law firm serving health care organizations including FHTs and nurse practitioner-led clinics as well as hospitals, mental health and addictions agencies, long-term care homes, community health centres and shared services organizations in Ontario. www.ddohealthlaw.com Twitter: @DDOHealthLaw

Disclaimer

This document is for general information purposes only. It is not intended as legal or professional advice or opinion. FHTs that have specific concerns about their privacy obligations and compliance are advised to seek their own legal or professional advice based on their particular circumstances.

AFHTO and DDO Health Law are not responsible or liable for any harm, damage, or other losses resulting from reliance on this document or from the use or misuse of the information contained in this document.

Language about Affiliated Physicians and Use of Term "FHO*"

We have referred throughout this document to groups of physicians affiliated with FHTs but organized separately from FHTs as Family Health Organizations (**FHOs***). However, with the "*" we acknowledge that physicians may be organized in other configurations of physician payment organizations such as Family Health Networks (**FHNs**), Rural and Northern Physician Group Agreements (**RNPGAs**), Family Health Groups (**FHGs**) or Alternative Payment Plans (**APPs**). Some of the family physicians affiliated with your FHT may also belong to larger physician practices with specialists who are not affiliated with the FHT. For ease of reference, we refer to FHOs* but we intend to include these other models in that term. We also acknowledge that some FHTs employ physicians directly through the Blended Salary Model; these physicians do not form a separate organization.

Language about Patients

Throughout this document, we will refer to individuals served by FHTs as "patients". In your FHT you may refer to them as "clients". The privacy legislation applies broadly to "individuals to whom information relates" and our use of "patient" is intended to be broadly applied to include all individuals whose personal health information FHTs or FHOs* hold (including prospective patients and former patients). The use of the term "patient" is also used to include substitute decision-makers who make decisions for individuals who have been found incapable of making their own choices. The language is streamlined for ease of reading.

TABLE OF CONTENTS

PRIVACY BACKGROUND

Privacy Legislation and the 10 Privacy Principles

In Ontario, the *Personal Health Information Protection Act, 2004* (**PHIPA**) and its regulation govern the collection, use and disclosure of personal health information by health information custodians. The Information and Privacy Commissioner of Ontario (**IPC/O**) oversees PHIPA compliance and enforces the law.

PHIPA is based on ten privacy principles, modeled on the "Canadian Standards Association Model Code for the Protection of Personal Information". These principles provide a privacy roadmap for FHTs and their affiliated physicians and FHOs*:

1.	Accountability	A health information custodian is responsible for personal health information under its control and must designate an individual who is accountable for the custodian's compliance with PHIPA (usually a Privacy Officer)
2.	Identifying Purposes	The purposes for which personal health information is collected must be identified by the health information custodian at or before the time the information is collected
3.	Consent	The knowledge and consent of the patient (or any person about whom the health information custodian holds personal health information) are required for the collection, use, or disclosure of personal health information, except where otherwise permitted or required by law
4.	Limiting Collection	The collection of personal health information must be limited to that which is necessary for the purposes identified by the health information custodian, and personal health information may only be collected by fair and lawful means
5.	Limiting Use and Disclosure and Retention	Personal health information must not be used or disclosed for purposes other than those for which the information was collected, except with the consent of the patient or as otherwise permitted or required by law, and personal health information may be retained only as long as necessary for the fulfillment of those purposes
6.	Accuracy	Personal health information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used
7.	Safeguards	Personal health information must be protected by security safeguards appropriate to the sensitivity of the information
8.	Openness	A health information custodian shall make readily available to the public including its patients specific information about the custodian's policies and practices relating to the management of personal health information
9.	Individual Access	Upon request, a patient shall be informed of the existence, use, and disclosure of his or her personal health information and shall be given access to that information, and a patient shall be able to challenge the accuracy and completeness of the personal health information and have it amended as appropriate
10.	Challenging Compliance	A patient shall be able to complain concerning compliance with the above principles to the designated individual(s) accountable for the health information custodian's compliance

Five Privacy Questions and Five Privacy Tools

In this document, we answer five privacy questions commonly asked by FHTs and provide five practical privacy tools to assist FHTs with their privacy compliance:

1. How do we decide with our affiliated physicians who will be the Health Information Custodian?

   Privacy Tool 1: An annotated template FHT FHO* PHIPA Agency Agreement

2. How do our staff know if we are allowed to leave a voice message for a patient?

   Privacy Tool 2: Communicating with our Office by Phone

3. At what age can children make their own decisions about their information?

   Privacy Tool 3: FAQs about Privacy and Working with Children in a Family Health Team Environment

4. If we allow our staff to use text messages or email to communicate with patients, what do we need to know and put in place?

   Privacy Tool 4: Sample Patient Consent and Release for Email Communication

5. What should we have our staff sign as evidence that they understand our privacy policies?

   Privacy Tool 5: Sample Annual Confidentiality Pledge

QUESTION I: How do we decide with our affiliated physicians who will be the Health Information Custodian?

What is a Health Information Custodian?

A **health information custodian** under PHIPA is the person or group ultimately responsible for compliance with the legal requirements of the Act. A health information custodian is a defined term under PHIPA (see section 3 of PHIPA).

For example, the following are health information custodians (and there are others):

- Health care practitioners (including group practices)
- Public and private hospitals
- Psychiatric facilities
- Independent health facilities
- Community Care Access Centres
- Community health or mental health centres, programs or services (if their primary purpose is the provision of health care)
- Long-term care homes
- Placement coordinators
- Retirement homes
- Pharmacies
- Laboratories
- Specimen collection centres
- Ambulance services
- Operators of care homes (residential tenancies)
- Homes for special care
- Community support services provider (under *Home Care and Community Services Act, 1994)*

As you will note, FHTs and FHOs* are not specifically listed above. But the definition includes "a health care practitioner or a person who operates a group practice of health care practitioners". Health care practitioner is also a defined term in PHIPA and includes, among others, members of regulated health professions under the Regulated Health Professions Act, 1991 and social workers and social service workers. When a health care practitioner works alone, he or she is a health information custodian. If health care practitioners work together in a group practice, the group may be a single health information custodian.

Why is it complicated for FHTs and FHOs* to determine who is the health information custodian?

Some arrangements are easier than others to determine who acts as the health information custodian. For example, in a Blended Salary Model FHT where physicians are employees of the FHT, the FHT will most likely be the health information custodian (and the physicians will be the FHT's agents as that term is understood under PHIPA). If a FHT is a department of a hospital and not a separate legal entity, the hospital may be the health information custodian and the FHT staff and affiliated physicians may be the hospital's agents.

But for the vast majority of FHTs and FHOs*, the FHT and the FHO* physicians are technically separate entities from each other even though they are designed to work together to provide completely

integrated care by the physicians of the FHO* and the interdisciplinary health professionals of the FHT to a shared group of patients. To patients and key community partners and the public, the FHT and the FHO* often look like one entity. FHTs and FHOs* may even brand the premises and use signs and a website and communicate in other public ways as a single entity under the name of the FHT. Those FHTs and FHOs* have two options:

1. Identify as two separate health information custodians; or

2. Identify as a single health information custodian to recognize the completely integrated nature of their relationship (and this option has three sub-options).

Many (if not most) FHTs and FHOs* who have done this exercise already have chosen the second option.

How do we decide who is the health information custodian?

You may need legal advice to answer this question.

First, gather all the relevant documentation to help you make a decision. These documents may not provide you with conclusive evidence one way or another as to who should be the health information custodian. But, they may provide you with clues to help you in your decision-making.

Documentation	What to Look For
The agreement between the physicians and the Ministry of Health and Long-Term Care	• Does the agreement identify the FHO* as a health information custodian? (if yes, the FHO* is more likely the custodian) • Does the agreement state that the physicians are employed by the FHT? (if yes, the FHT is more likely the custodian) • Does the agreement include language that patients are rostered to a particular physician who is part of a group practice FHO*? (if yes, the FHO* is more likely the custodian or the physicians may wish to remain individually responsible under PHIPA)
The agreement between the FHT and the Ministry of Health and Long-Term Care	• Does the agreement identify the FHT as a health information custodian? (if yes, the FHT is more likely the custodian) • Does the agreement state that the FHT will provide administrative services and interdisciplinary health professional services to the FHO* or affiliated physicians? (if yes, the FHO* is more likely the custodian)
The agreement between the physicians (if any) – such as the FHO* agreement	• Does the document identify the FHO* as a health information custodian? (if yes, the FHO* is more likely the custodian) • Does the document explicitly state the physicians do not wish to permit joint decision-making among them or hold joint liability or responsibility (if yes, the individual physicians may indicate they do not wish to operate as a group health information custodian, but

Documentation	What to Look For
	instead remain wish to remain individually responsible under PHIPA)
The agreement the FHO* has with the FHT for services (if any)	• Have the FHT and FHO* already explained this PHIPA relationship in a services agreement?
Agreements the FHT has already signed with other partners (like a hospital or university)	• Is the hospital the health information custodian for the FHT and the FHT's patients? • What has been said to date about the relationship between the FHT and the FHO* in agreements with others?
Agreements signed with other groups like Clinical Connect or HealthLinks or other data sharing agreements	• These agreements may have already communicated a message that either the FHT or the FHO* is the health information custodian • Be careful to note who has signing authority to bind either the FHT or the FHO*
Who owns the electronic medical record (**eMR**)?	• If only the FHT originally paid for the eMR that it shares with the FHO* – the FHT is more likely the custodian • If only the FHO* originally paid for the eMR that it shares with the FHT – the FHO* is more likely the custodian • Who decides which individuals will be granted access to the eMR and when individuals come off the eMR? • If both the FHT and the FHO* jointly paid for the eMR and share the costs – that is important to know. Although that arrangement does not indicate which of you should be the custodian, it does suggest that you operate as a single group with respect to health information

Second, consider the pros and cons of each arrangement:

1. **THE TWO CUSTODIAN MODEL: The FHO* and the FHT are separate health information custodians.** Each is responsible for its own activities and its own members and its own staff.

   PROs

   - Each of the FHT and the FHO* maintain control over its own privacy practices.
   - Each group is only exposed legally and financially for its own privacy actions – not the actions of the other group.

CONs

- The sharing of personal health information between FHT and the FHO* would be a "disclosure" and not a "use" and therefore there would be fewer options to share identifiable personal health information between them without consent of the patients– **this is probably the main reason not to follow this model as it does not maximize integrated care and administration between the FHT and FHO*.**
- This model is potentially confusing to patients. Patients may not appreciate that there are two separate entities. If there is a privacy breach or concern patients may be told to go to the other organization for resolution. And there may be different privacy rules for patients to be told about and to understand.
- This model does not encourage harmonization between the two entities for privacy policies or practices.
    - There could be a variety of different standards and practices applying to health information in a shared eMR environment.
    - This environment could be confusing to staff if there are multiple sources of rules.
- Privacy breaches may span across both organizations – and if that happens – both custodians must coordinate their responses. It might be difficult to determine liability and the two organizations might have to sue each other.
- Patient requests for access to health records would need to be processed by two separate health information custodians.
- This model makes it very hard to coordinate with third parties (like hospitals, HealthLinks and with insurance companies and law firms etc.) because they will have to have two separate and potentially different agreements for sharing personal health information.

2. **SINGLE CUSTODIAN MODEL:** If you have a shared eMR, and if the FHO* and FHT provide integrated clinical services to shared patients and cobrand and in order to simplify who is the health information custodian for the joint patients, it is usually recommended that there be a single health information custodian. Who acts as the health information custodian as between the FHT and the FHO* is a decision you can make.

PROs

- This model best reflects the integrated nature of the care provided by the FHT and FHO*. Because of the shared eMR and integrated nature of the clinical care provided by the physicians and the interdisciplinary health professionals and the integrated relationship between the FHO* and FHT, sharing of personal health information is seen to be a "use" and not either a "collection" or "disclosure" as those terms are understood under PHIPA. This allows much easier and broader use of the shared eMR and personal health information of joint patients – **this is the main reason to follow this model.**
- This model is easier for patients. Patients are told about one set of privacy rules. Patients can come through any door to inquire about privacy or make a privacy complaint – and there is a coordinated response for the patient.

- This model encourages harmonization between the FHO* and FHT.
    - You have privacy policies that apply to everyone.
    - You coordinate responses to privacy breaches.

CONs

- Only one group is the ultimate decision maker and so the "agent" group loses some control to the health information custodian – this is potentially a problem if one group does not agree with the other group's privacy decisions.
    - The agent must follow the custodian's rules and restrictions imposed.
- One group takes on legal and financial liability for privacy issues – and could be exposed if a staff member of the other entity "goes rogue" (although this exposure can be managed through insurance and contracts).

There are three sub-options to this model:

a. The FHO* is the health information custodian (the FHT is the PHIPA agent).
    - Often this is the model that best incents the physicians to take privacy seriously and to attend privacy training.
    - Physicians make the ultimate decisions about privacy rules and practices.
    - Physicians collectively maintain their control over their rostered patients' information.
    - Physicians can still ask the FHT to do administrative privacy tasks for them and have a FHT staff member (like an Executive Director) act as the Privacy Contact person.
    - Often in this model, the FHT would still find itself with significant investment of resources and time to assist the physicians meet their privacy obligations.

PLEASE NOTE: Many FHTs and FHOs* have chosen this sub-option (a). And this is the option for which we have developed the FHT FHO* PHIPA Agency Agreement tool that is attached to this document.

A further sub-version of this option is where individual physicians maintain health information custodian status and do not act as a collective group custodian as a FHO*. This can be a complicated choice and there can be health information network provider consequences of this choice under PHIPA. If physicians wish to remain as individual health information custodians, seek legal or other professional advice.

b. The FHT is the HIC (the FHO* is the PHIPA agent).
    - Often this model presents a practical struggle because the physicians may not follow the FHT's mandatory requirements for privacy training and policies and the FHT may not have the authority to enforce compliance.
    - The FHT makes all privacy decisions.

- Physicians have to follow the FHT's rules but would be consulted to ensure nothing compromises the physicians' collective and individual responsibilities to patients and College of Physician and Surgeons of Ontario rules.
- This model often best reflects who takes the lead on privacy issues – as the physicians may not have enough time to make timely decisions about privacy policies and issues.

c. The FHO* and FHT apply to be a single health information custodian under PHIPA.
   - This option might best reflect the unique situation of FHTs and FHO*s and would recognize that FHTs and FHOs* are different entities that have come together for a shared purpose.
   - But, this is a highly unusual option. We have not heard of many groups doing this. There is a process under PHIPA that allows for this. If you wish to pursue this option, seek legal or other professional advice.
   - All decision making would be shared.
   - There may be some additional costs for this model and the application process may take a while.

What needs to be in a PHIPA Agency Agreement?

If the FHO* is the health information custodian (or individual physicians are the health information custodians), you will then need a PHIPA agency agreement between the FHO* (or individual physicians) and the FHT to explain what the FHT is going to do on behalf of the FHO* and the obligations of each party. This PHIPA agency agreement sets out the circumstances under which the FHT can access the clinical record (such as for legitimate clinical purposes of the FHT's IHPs and legitimate business purposes of the FHT such as quality improvement activities) and consequences for breach of privacy by the FHT or its staff/agents (such as the FHT may need to indemnify the FHO* for costs incurred in responding to the privacy breach). This may alternatively be done as part of a services agreement between the FHT and the FHO* (or individual physicians).

Tool 1: Sample FHT FHO* PHIPA Agency Agreement (see separate attachment)

QUESTION 2: How do we know if we are allowed to leave a voice message for a patient?

Calling a patient at home or at work or on a cell phone or leaving messages carries a risk to patient privacy. It may be difficult to verify the identity of the person who answers or control who hears a message.

To minimize these risks, consider the following:

1. Ask patients every time they register for an appointment to check that their contact information is up to date so you have their most recent telephone numbers (and at the same time you may wish to confirm home address). Ask them to complete or update your form for communicating with your office and to let you know if you can leave a message with someone or on an answering service.
    a. Use Tool 2: Communicating with Our Office by Phone

2. If you 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.

3. If a patient calls your office, you should take steps to confirm the caller's identity before providing information. You can do this 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?

This is a sample. Edit to reflect your own circumstances.

Tool 2: Communicating with Our Office by Phone

Name: _____

Alternate Names Used: _____ (such as maiden/married names or nicknames used)

Phone Calls: If the FHT needs to reach me by phone, my phone number is:_____

If the first number does not work, I would like the FHT to call my other phone numbers:

_____ or _____

Voice Messages: The FHT can leave voice messages for me at the above phone numbers EXCEPT I do not want voice messages left for me at the following phone numbers:

_____ or _____

Detail:

- ☐ Choice 1: The FHT should <u>not</u> leave any information on voicemail for me (no voice message)
- ☐ Choice 2: The FHT is only allowed to leave a voice message to call the FHT back
- ☐ Choice 3: My voicemail is confidential and the FHT can leave me voice messages with information about (check all that apply)
    - ☐ Scheduling appointments with any health care providers
    - ☐ Test results
    - ☐ Follow up health instructions
    - ☐ Opportunities to participate in research studies
    - ☐ Opportunities to participate in health clinics/programs

  (*Please list any exceptions*): _____

My Family and Friends:

- ☐ Choice 1: It is okay for the FHT to leave a message with the following people:

  _____

- ☐ Choice 2: I do not want the FHT to share any information with anyone except me

Making Appointments:

- ☐ Choice 1: Only I am allowed to make my appointments
- ☐ Choice 2: The following people are allowed to book appointments for me

  _____

IMPORTANT: I will tell the FHT immediately if this information changes.

DATE:

QUESTION 3: At what age can children make their own decisions about their information?

The following is a practical tool that describes the circumstances under which children make their own health information decisions.

Tool 3: FAQs about Privacy and Working with Children in a Family Health Team Environment

Q1. What is a "health information" decision?

A health information decision deals with whether identifiable health information about a patient may be collected, used or disclosed and to whom. Such as, decisions about whether the FHT can share information with anyone who is not the patient (such as family members, insurance companies, schools, and other health care providers).

Q2. Is there an age of consent where children start to make decisions about their own health information?

No. Just like consent to treatment, there is no magic age in Ontario at which a child automatically starts to make his or her own health information decisions. A child may make information decisions if he or she is "capable".

Q3. How do I know if my patient who is a child is "capable" of making information decisions? What is the legal test for capacity to consent to information decisions in Ontario?

The test for capacity to make health information decisions is found in the *Personal Health Information Protection Act, 2004* (PHIPA)

First, all patients are presumed to be capable to make health information decisions, unless it is not reasonable to presume capacity. For example, babies are never capable of making health information decisions. Very young children are rarely able to make their own health information decisions. But as children age they may become more capable of making their own choices about their own health information.

It is a two-part test; to be considered capable a child must have the ability to:

- understand the information that is relevant to the decision to collect, use or disclose his/her health information, and
- appreciate the reasonably foreseeable consequences of his or her choices about the collection, use or disclosure of his/her health information (giving, not giving, withholding or withdrawing the consent).

If the child fails either part of the two-part test, the child is incapable of making health information decisions.

Q4. Who can make decisions about the collection, use and disclosure of a child's health information?

This can be complicated. If you would like to refer to the original text, see section 23 of PHIPA.

Let's start with an **incapable child**. If a child is found to be incapable of making information decisions, only the child's substitute decision maker (SDM) can make decisions on that child's behalf. The ranked list of who can be a substitute decision maker is in section 26 of PHIPA. Most of the time parents act as SDMs for their incapable children. The ranked list includes:

- The incapable child's guardian of the person or guardian of property, if the guardian has authority to give or refuse consent to health information decisions (***note,*** *very few people have a "guardian of the person" – this is not the same as "legal guardian" as used in other contexts like school notes*)
- The incapable person's attorney for personal care or attorney for property, if the consent relates to the attorney's authority to make a decision on behalf of the individual (***note****, children under the age of 16 cannot execute a power of attorney for personal care –so they will not have one. Children under the age of 18 cannot execute a power of attorney for property – so they will not have one. A power of attorney for personal care and a power of attorney for property are both documents - if someone claims to have the authority to act as an attorney for personal care or an attorney for property you should ask to see a copy of the document)*
- The incapable person's representative appointed by the Consent and Capacity Board (CCB), if the representative has authority to give or refuse consent to the information decision (***note****, very few people have a personal representative appointed by the CCB)*
- The incapable person's spouse or partner (***note****, most children do not have a spouse or partner*)
- **A** child or **parent of the incapable person**, or a children's aid society or other person who is lawfully entitled to give or refuse consent to the information decision in the place of the parent. **This paragraph does not include a parent who has only a right of access**. **If a children's aid society or other person is lawfully entitled to give or refuse consent to the information decision in the place of the parent, this paragraph does not include the parent.**
- A parent of the incapable person who has only a right of access.
- A brother or sister of the incapable person.
- Any other relative of the incapable person.

A SDM must be at least 16 years of age, unless the parent of an incapable child.

In most cases for incapable children, their parents will make their information decisions for them.

Now, we'll deal with a case where a **child is "capable"**:

- A capable child may make decisions about his or her own health information

  AND

- If the capable child is over the age of 16, he or she may authorize someone else to act on his or her behalf to consent to the collection, use or disclosure of health information (that person must be at least 16 years of age) (***note**, for example, a 17 year old may write to the FHT that his or her friend who is also 17 can authorize sending information to an insurance company while the patient is away at school out of town*)

  AND

- If the capable child is under the age of 16, his or her parent (or CAS or other person lawfully able to make decisions instead of a parent) may also make information decisions **UNLESS** the information relates to:

  - treatment about which the capable child made a decision on his or her own under the *Health Care Consent Act* OR

  - counseling about which the child participated on his or her own under the *Child and Family Services Act*

  OR UNLESS the capable child says he or she does not want the parent to make that decision. A capable child's decision to exclude his or her parents from making health information decisions trumps the permission of a parent to make some decisions.

  This is complicated. Let's work through some examples:

  Example 1: A school needs information about a 14 year old's vaccinations. Express consent is needed for the FHT to release that information to the school (the school is not a health information custodian).

  The FHT can rely on the following people to sign the form:

  1. If the 14 year old is incapable of making the decision and the parents are substitute decision makers for the child, the parents would be asked to sign the form.

  2. If the 14 year old is capable of making the decision to release the information to the school – the 14 year old can sign the form.

3. If the 14 year old is capable of making the decision, but the records about the vaccinations have to do with when the child was a baby and very young and not making his or her own decisions about the vaccinations, the parent could also sign the form (UNLESS the 14 year old said, no I don't give permission for my parent to do that).

Example 2: A parent asks to see a 15 year old child's health record – or to be told about a child's diagnosis or why the child came to the FHT.

1. If the 15 year old is incapable of making decisions about treatment and the parent is the SDM, the parent stands in the shoes of the child and gets access to all relevant information in order to make decisions about the child's treatments. And the parent can have access to information for releasing to anyone else.

2. If the 15 year old is capable of making the information decisions – the child may not want his or her parents to see the health record, or know a diagnosis or know why he or she came to the FHT. If the child made his or her own treatment decisions or counseling decisions, a parent cannot get automatic access to the child's information. It can only be shared with the child's consent. Generally speaking the FHT should consult with capable children about how they would like their parents involved in their decisions and how much information they would like shared with their parents.

3. If the 15 year old is capable of making the decision, but the records relate to when the child was a baby or young child and not making his or her own health care, the FHT can release information to the parent UNLESS the 15 year old does not give permission for the parent to have that information. Generally speaking the FHT should consult with capable children about how they would like their parents involved in their decisions and how much information they would like shared with their parents.

Here is a table:

AGE	CAPACITY	DECISION MAKER
Person of any age	If capable	Can make decisions about release of everything in his/her own health record
Person of any age	If incapable	Needs a substitute decision-maker to release anything in health record
Under age of 16 (birth to 16 less a day)	If capable	Can make decisions about release of everything in his/her own health record AND A parent can also consent to release of information about any treatment or counseling that child did not consent to on his/her own BUT NOT IF THE CAPABLE CHILD OBJECTS TO PARENT MAKING SUCH DECISIONS

Q5. When a child is incapable, do parents have to make information decisions together? What if they disagree?

If two parents are both substitute decision-makers for their incapable child, they make information decisions together. If they do not agree, then they should be encouraged to try to agree. If they cannot agree, ultimately they may lose the right to make information decisions and the health care practitioner would go to the Public Guardian and Trustee for decisions on the child's behalf.

Q6. What happens if a child's parents are separated or divorced? Who makes information decisions for the child?

Please note, in cases of separation or divorce there may be a separation agreement or court order relating to decision-making and sharing information about a child. If one parent says there is such a document the health care practitioner should be given a copy and should read it carefully.

Remember, if the child is capable – the child makes information decisions even if there is a court order that says one or both parents have custody. A capable child may say he or she does or does not want parents involved.

If the child is incapable (and there are no higher ranking SDMs):

- If both parents have custody, they both make information decisions
- If one parent has custody and the other parent has only access, the custodial parent makes information decisions.

But all that said, court documents have to be read carefully. Sometimes a court orders a FHT to release information to the court even about a capable child. Sometimes you will need legal advice to get the answer right.

QUESTION 4: If we allow our staff to use text messages or email to communicate with patients, what do we need to know and put in place?

Patients seem to be increasingly comfortable communicating with their health care providers by text or email. FHTs and their affiliated physicians need to consider whether they permit communicating with patients using text or email and be clear about the rules in policies.

1. Managing Patient Expectations

Introducing or permitting communication with FHT and FHO* staff by text and email for clinical purposes, especially where patients are given staff cell phone numbers (work or personal) and/or personal email addresses for staff, potentially raises patient expectations that FHT and FHO* staff will be available to them 24 hours a day/7 days a week/365 days a year. This is an expectation that may persist despite efforts to manage it. Furthermore, it is an assumption that impacts FHT and FHO* staff – the way they work, their ability to interact with other onsite patients, and their ability to manage the information that is being communicated to them. In addition, while patients may assume that "anything goes" with respect to what they can and cannot communicate with their FHT or FHO* staff contact, this is not the ideal practice for the FHT or FHO*.

2. The Documentation Of Clinically Relevant Information Received By Email Or Text

Information that is received from a patient that is clinically relevant must be documented (i.e. put in the chart) and acted upon as necessary. The FHT and FHO*'s goal would be to ensure that no matter how a patient communicates with the FHT and FHO*, patient care continues to be provided with all relevant patient information available when necessary. As such, clinically relevant information received via text message or email would have to be added to the chart in timely manner so a patient's chart is complete and up-to-date. Email messages could be printed and scanned or otherwise uploaded into the electronic medical record. It is possible that texts could be transcribed or a screen-print taken and added to the chart. In either case, processes would have to be put in place to make sure that new information is added to the chart as quickly as possible and that other relevant providers are alerted as appropriate.

3. Emergency Practices and Procedures

Adopting a practice of communication via email and text message requires thinking about how to respond if and when a patient reaches out through one of these means during a clinical crisis. For example, despite setting boundaries, a patient who has the email address or cell phone number of a FHT of FHO* staff member may send an email or a text outside of business hours (i.e., on weekends or evenings). Not responding to clinically relevant information, especially in a crisis situation, could jeopardize the safety of the patient and exposes the FHT or FHO* staff member, other health professionals and the FHT or FHO* or physician to liability.

4. Use by FHT or FHO* Staff of Personal Cell Phones

Some FHT or FHO* staff may consider giving out personal cell phone contact details for patients. However, providing a personal contact can blur the lines of professional boundaries. It may also create the expectation that the FHT or FHO* staff member is available at all times. There would be additional concerns about the privacy security of the device (e.g. personal devices might not be encrypted) or the accessibility of the device to non-FHT or FHO* staff members (such as family and friends).

5. Privacy Issues Related to the Security of Email and Text Communication

Nothing in the health privacy legislation in Ontario, the *Personal Health Information Protection Act, 2004* (PHIPA), explicitly prohibits the use of email and text messaging as means by which personal health information can be communicated or exchanged between health care providers and patients. Rather, the legislation is concerned with ensuring that any means by which this kind of information is shared or transported has in place the appropriate privacy controls to prevent inadvertent disclosure, loss or theft.

Unfortunately, neither text messaging nor email are secure means of communicating and there can be interceptions of either type of message. Without the proper measures taken by the FHT and FHO*, personal health information contained in email communication and text message transmissions will not be secure against interception and access by unauthorized third parties.

Also, many email programs have an auto-fill function that completes a partially entered email address. This may result in information being communication to someone other than the intended recipient, which could lead to a privacy breach for which PHIPA notification obligations and sanctions could apply.

FHTs and FHOs* that intend to permit staff to communicate with patients by text or email or both should seek legal advice and should consider the following:

1. **Disclaimers**: The FHT/FHO* should require that patients sign a disclaimer which:

    a. Confirms that text or email is not a secure method of communicating.

    b. Outlines the content the FHT/FHO* considers appropriate for email communication. For example, patients may be allowed to communicate appointment availability but not to communicate urgent clinical information.

    c. Sets out the timelines within which messages will be returned (and not outside of business hours).

    d. Explains how emergency services should be sought.

    The value of a well-crafted disclaimer is that where the patient subsequently opts to communicate outside of those guidelines or someone else intercepts the communication, the FHT/FHO* can make the case that it has satisfied its responsibilities towards to that person. However, a disclaimer would

not protect the FHT/FHO* from all liability or prevent someone making a privacy complaint or prevent someone from suing the FHT/FHO* for negligence or malpractice.

2. **Auto-reply function:** If you wish to permit email or text message communication, the FHT/FHO* should give some thought to establishing an auto-reply process so that when FHT/FHO* staff are unavailable to patients, their unavailability is instantly communicated as well as alternative emergency contact info (such as instructions to call 911). This may be easier with respect to email since an out-of-office alert could be turned on. Similar technology may exist for received text messages – although its acquisition and installation could be at a significant cost to the FHT/FHO*.

3. **Encryption**: To the extent that a FHT/FHO* decides to institute a practice of receiving email and text communication from their patients, only encrypted (or similarly privacy protected) work cell phones and computers should be used. Typically, personal cell phones will not have the requisite level of privacy protections necessary to safely transmit personal health information.

If a FHT/FHO* email address is to be accessible on a mobile device (such as a smart phone), the following steps should be undertaken:

- Team Members must have permission from the Privacy Officer[s] to load a FHT/FHO* email address account on a mobile device;
- The device must be password protected and subject to a strong level of encryption;
- The device contents must be able to be erased remotely (that means, all content from the device can be remotely deleted by the FHT/FHO*);
- 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

Be aware of the following examples of email communication standards:

- ☐ CPSO Medical Records Policy
- ☐ CMPA Using email communication with your patients: legal risks
- ☐ CMA Physician Guidelines for Online Communication with Patients Policy
- ☐ CNO Confidentiality and Privacy – Personal Health Information
- ☐ CoD Communicating with Clients Via Email

This is a sample. Edit to reflect your own circumstances.

Tool 4: Sample Patient Consent and Release for Email Communication

You have asked to communicate with us via email. There are some limitations on how we can communicate with you by email, which we will explain here.

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

- You should let us know of the email address you wish us to use. You are responsible to keep this up-to-date and let us know of any changes to your email address. It is probably best not to use a work email (if your employer has the right to view your emails) or an email that you share with others.

- You should not use email to share detailed or sensitive health information with us. And please tell us if there are certain types of information that you do not wish to discuss by email.

- We do not communicate by email diagnoses, test results or transmit other personal health information that will require a follow up visit to the Family Health Team.

- There are some privacy risks in communicating by email:
    - Email is not considered a secure method of communicating with us. Emails can be intercepted and we cannot guarantee the security and confidentiality of any email communications that you send to or receive from us.
    - 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, they may be shared within the Family Health Team or third parties if permitted or required by law (including with other health care providers and OHIP for example).
    - Email is easy to forge, easy to forward (sometimes accidentally) and may exist indefinitely.
    - Individuals other than your physician or health care provider may read emails especially to cover for vacation, illness and other absences and for administrative purposes.

- Email should not be used to communicate emergencies or time-sensitive health care issues. If you are experiencing an emergency, you should call 9-1-1 or go to a hospital or health care provider immediately. If you require a less urgent consultation, you should make an appointment to see your health care provider at the Family Health Team. We do not have 24 hours per day 7 days per week monitoring of email messages. We cannot guarantee any particular response time for an email. If you require a response to an email message, please follow up by phone call to the Family Health Team's office.

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

- If you no longer wish to communicate with us by email, please notify • in writing.

Patient Acknowledgment, Agreement and Release:

- I acknowledge that I have read and fully understand this consent and release form.
- I understand the risks associated with communicating with the Family Health Team by email and I accept those risks.
- I understand the limits set out for email communication with the Family Health Team and I agree to follow those limits.
- **I agree that the Family Health Team and their physicians, staff, directors, officers and other agents shall not be responsible for any personal injury including death, and/or privacy breach (outside the reasonable control of the Family Health Team) or other damages as a result of my choice to communicate with the Family Health Team by email and I release the Family Health Team and their physicians, directors, officers and other agents from any liability relating to communicating with me by email.**
- I have had the opportunity to ask any questions I had about this form and any questions I had have been answered to my satisfaction.
- 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:**_____

QUESTION 5: What should our staff sign as evidence that they understand our privacy policies?

Tool 5: Sample Annual Confidentiality Pledge

This is a sample. Edit to reflect your own circumstances.

ANNUAL CONFIDENTIALITY PLEDGE – YEAR

For Staff/Physicians/Students/Board Members/Volunteers

I pledge to keep confidential any information obtained during the performance of my duties at <NAME OF FAMILY HEALTH TEAM>. I understand that confidential information includes information relating to:

- Patients (and patient information would include health records (paper or electronic), health information in any format, conversations, registration information, financial history, the fact that someone is, has been or may become a patient of <NAME OF FAMILY HEALTH TEAM>, the name of a substitute decision-maker, etc.);
- <NAME OF FAMILY HEALTH TEAM> employees, physicians, students, volunteers, contractors or vendors (such as employee records, disciplinary action, performance reviews, quality reports, etc.);
- <NAME OF FAMILY HEALTH TEAM> business information (such as contracts, financial information, memos, peer review information, etc.).

I agree that I have read and agree to follow the following <NAME OF FAMILY HEALTH TEAM> policies:

<LIST HERE>

I understand that the policies were updated from last year in the following ways:

<LIST HERE>

If I need help understanding these policies, I will ask my supervisor or the <NAME OF FAMILY HEALTH TEAM>'s Privacy Officer.

I also understand and agree that:

- I am only allowed to collect (including to receive, look at, access, ask for, view, copy, record, print, read, listen), use and disclose confidential information on a "need to know basis" only, and even then only the minimum amount required, as required for my role or as I have been authorized to do in writing or as required by law.
- I will not communicate confidential information either within or outside <NAME OF FAMILY HEALTH TEAM>, except to persons authorized to receive such information and only for the purposes of performing my duties.
- I will not collect, use or disclose the confidential information of family, friends, co-workers or any other individual, unless they are under my direct care or I am authorized as part of my official duties at <NAME OF FAMILY HEALTH TEAM> and not for my own purposes.
- I will only access my own health information in the custody or control of <NAME OF FAMILY HEALTH TEAM> through the method approved for the public in the <NAME OF POLICY>.

- If I am a patient's substitute decision-maker, I will only access the patient's health information through the method approved for the public in the <NAME OF POLICY>.
- I am not allowed to engage in self-study (such as learning how to document or learning about our patients and the services we offer them or learning how others provide services) with personal health information in the custody or control of <NAME OF FAMILY HEALTH TEAM> without written permission from my supervisor or the Privacy Officer.
- I will not share my passwords to electronic information systems with anyone. I understand I am responsible for protecting those passwords and access to <NAME OF FAMILY HEALTH TEAM>'s systems and records and that I am responsible for all actions performed when the electronic information system has been opened using my password.
- I will access, process and transmit confidential information using only authorized hardware, software, or other authorized equipment. I understand that I may not save confidential information on an unencrypted USB key or other portable device.
- I shall not remove confidential information from <NAME OF FAMILY HEALTH TEAM> premises (including taking it home to work on) except as authorized by my supervisor or a Privacy Officer. If authorized, I shall securely store the information and ensure it is in my custody and control at all times.
- I will not alter, destroy, copy or interfere with confidential information, except with authorization and in accordance with <NAME OF FAMILY HEALTH TEAM> policies and procedures.
- I shall immediately report all incidents involving loss, theft or unauthorized access to confidential information to my immediate supervisor and to <NAME OF FAMILY HEALTH TEAM>'s Privacy Office.

I understand that the <NAME OF FAMILY HEALTH TEAM> conducts regular audits to ensure confidential information is protected against unauthorized access, use, disclosure, copying, modification or disposal.

I understand any breach of my duty to maintain confidentiality may result in corrective action. Such corrective action taken may include retraining, loss of access to systems, suspension, reporting my conduct to the Information and Privacy Commissioner of Ontario or a professional regulatory body or sponsoring agency, school or institution, restriction or revocation of privileges, and up to and including immediate dismissal. I understand there could also be notification of affected persons. I understand a privacy breach could also result in me being fined, prosecuted or sued and other consequences.

I understand and agree to abide by the conditions outlined in this pledge, and they will remain in force even if I cease to be employed by or have an association with <NAME OF FAMILY HEALTH TEAM>.

Name: _____

Date: _____

PRIVACY RESOURCES

Association of Family Health Teams of Ontario

- Privacy Toolkit for the Quality Improvement Decision Support Program in Family Health Teams
- Statutory Compliance Toolkit for Boards of Family Health Teams and Nurse Practitioner-Led Clinics

Information and Privacy Commissioner of Ontario

- 45 Minute PHIPA Training Video for all health sector staff
- PHIPA Fact Sheets
- PHIPA Orders

College of Physicians and Surgeons of Ontario

- Confidentiality of Personal Health Information
- Medical Records
- Appropriate Use of Social Media by Physicians

College of Nurses of Ontario

- Confidentiality and Privacy – Personal Health Information
- Social Media

Canadian Medical Protective Association

- Privacy and Confidentiality
- Documentation

Ontario Hospital Association and Ontario Medical Association

- Hospital Privacy Toolkit

OntarioMD

- Privacy & Encryption Online Tutorial

DDO Health Law

- 3 day Privacy Officer Training for the Health Sector
- 3 hour Privacy Training for Family Health Teams
- 1 hour Privacy Training for the Health Sector (online streaming video) – Coming March 2016
- Legal Issues for Family Health Teams Monthly Teleconference