afhto association of family health teams of ontario

Privacy Toolkit for the

Quality Improvement Decision Support Program

in Family Health Teams

Written by:

DDO HEALTH LAW

Kate Dewhirst

March 2014

Disclaimer

This toolkit is for general information purposes only. It is not intended as legal or professional advice or opinion. Family health teams who are integrating Quality Improvement Decision Support Specialists into their workplaces and who have specific concerns about privacy or legal issues are advised to seek their own legal or professional advice based on their particular circumstances.

AFHTO and Dykeman Dewhirst O'Brien LLP are not responsible or liable for any harm, damage, or other losses resulting from reliance on these materials or from the use or misuse of the general information contained in this toolkit.

Acknowledgements

AFHTO acknowledges the following members of the QIDS Specialist Contact Group and additional advisors for their contributions to this toolkit: Randy Belair, Sunset Country Family Health Team Executive Director; Stephanie Dudgeon, Brockton and Area Family Health Team Manager of Finance and Administration; Dr. Michelle Griever, North York Family Health Team; Sherry Lynn Harrington, Primary Health Care Services of Peterborough Director of Program Innovation and Evaluation; Monique Hancock, STAR Family Health Team Executive Director; Kavita Mehta, South East Toronto Family Health Team Executive Director; Jill Murphy, Thames Valley Family Health Team Quality Improvement Decision Support Specialist; Melonie Young, Sunset Country Family Health Team Quality Improvement Decision Support Specialist.

And we also acknowledge the contributions of our own AFHTO staff: Tim Burns, Provincial Lead – QIDS Specialist; Jessica Hedges-Chou, QIDS Research Analyst; Carol Mulder, Practice Lead, Quality Improvement and Decision Support; Denise Pinto, Improvement Programs Assistant; and Clarys Tirel, Provincial Lead – Governance and Leadership.

Principal 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 and nurse practitioner led clinics on privacy, patient/family complaints, physician performance, quality improvement, risk management, legal compliance, health records, documentation, and governance.
Email: kd@ddohealthlaw.com Twitter: @katedewhirst

Contributing Authors from DDO Health Law

DDO Health Law is a law firm serving health care organizations including family health teams and nurse practitioner led clinics in Ontario. www.ddohealthlaw.com

Kathy O'Brien focuses on corporate, commercial, regulatory and charitable law issues for the health sector. In particular, she advises on collaborative relationships.

Maria McDonald advises family health teams and nurse practitioner led clinics on all issues relating to their human resources and employee relations.

Table of Contents

CHAPTER 1: Introduction

The purpose of this toolkit is to provide general information to family health teams (**FHTs**) about how to best navigate privacy issues when working with Quality Improvement Decision Support Specialists (**QIDS Specialists**). This toolkit answers questions such as:

- What obligations do FHTs and their affiliated physicians have to protect patient privacy when engaged in the activity of quality improvement and data analysis?
- What steps need to be taken if QIDS Specialists are to be shared among multiple FHTs?
- Who can make decisions about whether a QIDS Specialist gets access to the electronic medical record (**eMR**)?

Format

This toolkit is designed in a Frequently Asked Question format. AFHTO canvassed key stakeholders to find out the issues they were facing in integrating QIDS Specialists in their community. We have organized the toolkit into four chapters:

In Chapter 1, we introduce the topic of QIDS Specialists and privacy issues and how the toolkit works.

In Chapter 2, we highlight the background to QIDS Specialists in Ontario. This may be useful information to share with your FHT Board and with your affiliated physicians so that they understand the purpose and benefits of working with QIDS Specialists. This toolkit is not the full authority on the QIDS Program. For more information, go to the QIDS Program on the AFHTO members' only page.

In Chapter 3, we explain the *Personal Health Information Protection Act, 2004* and the ten privacy principles that FHTs and their affiliated physicians must follow when dealing with personal health information and quality improvement activities. We then explain how the privacy rules apply to QIDS Specialists.

In Chapter 4, we explain how multiple FHTs can share a QIDS Specialist. Attached as Appendix I is a template *QIDS Specialist Collaboration and Data-Sharing Agreement*. Chapter 4 further explains how the template can be used.

Links

The toolkit is loaded with links. Where there is a hyperlink in this toolkit – right click it to find on-line resources.

Language about Affiliated Physicians

We have referred throughout the toolkit 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 (**BSM**); these physicians do not form a separate organization. In some parts of this toolkit it will matter if the physician group is employed by the FHT or not. Where that distinction matters, we will alert the reader.

Language about Patients

Throughout this toolkit, we will refer to individuals served by FHTs as "patients". In your FHT you may refer to them as "clients". When we discuss privacy rules, 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.

Privacy Homework

When reading this toolkit or implementing the *QIDS Specialist Collaboration and Data-Sharing Agreement*, you may realize you have some work to do to become compliant with PHIPA. You may discover that you may not have basic privacy processes in place to meet your existing obligations as health information custodians under PHIPA. If you need assistance, ask a privacy lawyer or privacy consultant to assist you to do the privacy homework needed. You may also want to look at our Chapter 3 and Appendix II: *Privacy Impact Assessment Template for Family Health Teams* and Appendix III: *General Privacy Resources* for more general information about privacy compliance.

CHAPTER 2: Quality Improvement Decision Support Specialists (QIDS Specialists)

What is the provincial QIDS initiative?

The Quality Improvement Decision Support (**QIDS**) Program is a provincial initiative to advance performance measurement and quality improvement in Ontario FHTs.

The goals of the QIDS Program are to improve primary care and enable the sector to lead healthcare transformation.

The primary intervention arm of the program is a cadre of 33 QIDS Specialists who are employed directly by host FHTs to provide service to both the host FHT and other participating FHTs.

The provincial QIDS Program includes:

- Provincially funded QIDS Specialists through the Ministry of Health and Long-Term Care (**MoHLTC**);
- A provincial QIDS Steering Committee of AFHTO that works with FHTs and other health sector partners to set specific objectives and priorities to advance best practice and optimize performance measurement capacity across the sector;
- A provincial QIDS staff team of four AFHTO employees to support and align local QIDS initiatives and coordinate, mentor and otherwise support QIDS Specialists in the field; and
- An expectation from the MoHLTC that FHTs will enter into formal QIDS collaboration arrangements with peers to share resources and build strategic capacity in the sector.

How many QIDS Specialist FHT Models are there in Ontario? And what are they?

There are 33 QIDS Specialists in Ontario at this time to be shared among 155 FHTs.

AFHTO knows of at least two models used by FHTs to engage QIDS Specialists:

Sharing QIDS Specialist Model

A group of FHTs share one or more QIDS Specialists. The FHTs work collaboratively to share the QIDS Specialist position so that each FHT benefits from the QIDS Specialist's expertise. If your FHT is going to share a QIDS Specialist with another FHT, you need to have a collaboration and data-sharing agreement (as explained in Chapter 4). Each participating FHT may also have work to do with their FHO* or

FHOs* to determine who is the health information custodian (described in Chapter 3) and who can authorize the QIDS Specialist to access the eMR. You may still need to have a services agreement between your FHT and FHO* or FHOs* to explain what the QIDS Specialist is permitted to do.

Example: STAR Family Health Team in Stratford, Ontario is sharing one QIDS Specialist with seven other FHTs.

Example: The FHTs in the Champlain Local Health Integration Network are sharing multiple QIDS Specialists.

Single FHT QIDS Specialist Model

A FHT engages its own QIDS Specialist. If you have your own QIDS Specialist and you do not share with another FHT, there is no need for a collaboration agreement (and you will not need to use the template Collaboration and Data-Sharing Agreement). However, there are still privacy issues to be addressed (including determining who the health information custodian is and who can authorize the QIDS Specialist to access the eMR). You may still need to have a services agreement between your FHT and FHO* or FHOs* to explain what the QIDS Specialist is permitted to do.

Example: Guelph Family Health Team has its own QIDS Specialist working only for that FHT.

What does (can) a QIDS Specialist do?

QIDS Specialists assist FHTs and their affiliated physicians with quality improvement planning, decision making and implementation. A QIDS Specialist acts as an internal resource to improve clinical data quality, data integrity and clinical performance management outcomes and processes within a FHT.

There may be a great deal of variation in the job descriptions of QIDS Specialists across the province. This toolkit does not define or prescribe what QIDS Specialists are allowed or not allowed to do. We have instead provided some ideas of what your QIDS Specialist may be authorized to do.

See Appendix I: *QIDS Specialist Collaboration and Data-Sharing Agreement* and its Schedule A for a sample Job Description for a QIDS Specialist.

For example, a QIDS Specialist may (this is not a required or an exhaustive list):

- Access an eMR in order to collect and use personal health information for the purpose of performing data analysis and decision support for quality improvement purposes exclusively for that FHT
- Conduct patient surveys and collect new personal health information directly from patients
- Improve the flow and use of information by FHTs by standardizing information entered in the eMR (such as common language, terms, nomenclature)
- Develop queries and analytical products that support FHT boards and leaders in their quality improvement goals and support clinical teams in clinical outcome improvements and process changes
- Improve the data quality within a FHT by harmonizing data entry and data codes so that information can be compared within the FHT
- Harmonize quality indicators within a FHT and within a group of FHTs
- Share de-identified (anonymized) data within a group of FHTs to identify best practices for quality improvement and clinical performance

Who decides what a QIDS Specialist can do?

The answer to that question will depend on your situation. Usually, a QIDS Specialist will report to the Executive Director and have a workplan of "authorized" activities. Depending on the QIDS Specialist FHT model you are using, the activities of the QIDS Specialist may be directed by:

- **Sharing QIDS Specialist Model**: If multiple FHTs are sharing one or more QIDS Specialists, the group of FHTs should decide who can instruct the QIDS Specialist. In the template *QIDS Specialist Collaboration and Data-Sharing Agreement* we have proposed that there be a Steering Committee to approve the workplan(s) for the QIDS Specialist to ensure each FHT gets the work they need done. But the group does not have to have a Steering Committee and can make different arrangements. For example, they may choose to allow each participating FHT to instruct the QIDS Specialist directly. However, it may be difficult to ensure each FHT is receiving an appropriate amount of services without central coordination.

- **Single FHT QIDS Specialist Model**: In cases where a single FHT has one QIDS Specialist, the Executive Director of the FHT (or some other individual) will determine the workplan for the QIDS Specialist just as the FHT would do with any other employee or independent contractor.

To avoid confusion it should be made clear to QIDS Specialists whether they are allowed to take instructions directly from individual physicians or interprofessional health care providers (**IHPs**) to examine the needs of that physician or IHP's patients.

Also, as you will read in Chapter 3, the "health information custodian" or HIC is also able to make decisions about the kind of information that QIDS Specialists are allowed to access.

CHAPTER 3: Privacy Rules

General Privacy Rules

In Ontario, the *Personal Health Information Protection Act, 2004* (**PHIPA**) and its regulation govern the collection, use and disclosure of personal health information (**PHI**) by health information custodians (**HICs**). The Information and Privacy Commissioner of Ontario (**IPC/O**) oversees PHIPA compliance and enforces the law. Any quality improvement activities by FHTs must be done in accordance with PHIPA.

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 in working with QIDS Specialists:

1.	Accountability	A HIC is responsible for PHI under its control and must designate an individual who is accountable for the HIC's compliance with PHIPA (usually a Privacy Officer)
2.	Identifying Purposes	The purposes for which PHI is collected must be identified by the HIC at or before the time the information is collected
3.	Consent	The knowledge and consent of the patient (or any person about whom the HIC holds PHI) are required for the collection, use, or disclosure of PHI, except where otherwise permitted or required by law
4.	Limiting Collection	The collection of PHI must be limited to that which is necessary for the purposes identified by the HIC, and PHI may only be collected by fair and lawful means
5.	Limiting Use and Disclosure and Retention	PHI must not be used or disclosed for purposes other than those for which the PHI was collected, except with the consent of the patient or as otherwise permitted or required by law, and PHI may be retained only as long as necessary for the fulfillment of those purposes
6.	Accuracy	PHI must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used
7.	Safeguards	PHI must be protected by security safeguards appropriate to the sensitivity of the information

8.	Openness	A HIC shall make readily available to the public including its patients specific information about the HIC's policies and practices relating to the management of PHI
9.	Individual Access	Upon request, a patient shall be informed of the existence, use, and disclosure of his or her PHI and shall be given access to that information, and a patient shall be able to challenge the accuracy and completeness of the PHI 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 HIC's compliance

This toolkit explains how FHTs and FHOs* should approach their work with QIDS Specialists to respect these privacy principles.

Health regulatory colleges also set out privacy guidelines and expectations for their members. For example:

- The College of Physicians and Surgeons of Ontario
- The College of Nurses of Ontario
- The Ontario College of Social Workers and Social Service Workers

If there is ever a conflict between College guidelines and PHIPA, PHIPA overrides the College guidelines.

What is a HIC?

A **health information custodian** or **HIC** under PHIPA is the person or group ultimately responsible to protect the PHI it holds. A HIC is a defined term under PHIPA (see section 3 of PHIPA) and 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.

FHTs have been recognized as "a person who operates a group practice of health care practitioners"[1].

So, is the FHT the HIC? Is the FHO* the HIC? How do we know?

Privacy Homework

You may need legal advice to answer this question.

Many FHTs still have to settle this question with their affiliated physicians.

If you have not done this yet – you will need to do it now, whether or not you go ahead with QIDS Specialists. This is part of your privacy homework.

The exercise involves determining between the FHT and the FHO* which is going to be the HIC. As set out above, HIC is a defined term under PHIPA and includes a person who operates a group practice of health care practitioners. You have to determine who "owns" the health records and who is responsible for compliance with PHIPA. Often it is the FHO*. Sometimes each individual physician is a HIC. Sometimes the FHT is the HIC. The analysis depends on:

- The agreements between the physicians and the MoHLTC
- The agreement between the physicians (if any – such as the FHO* agreement)
- Agreements the FHO* has with the FHT for services (if any)
- Agreements the FHT may have already signed with your other partners (such as a hospital or university)
- An understanding reached between the FHT and its affiliated physicians

Privacy Homework

Decide as between the FHT and the FHO* (or individual physicians) who is the HIC and document that decision (NOTE: you may need professional advice to decide this)

Please note if physicians are employees of the FHT, the FHT will most likely be the HIC.

---

[1] See H. Perun, M. Orr and F. Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act* Toronto: Irwin Law Inc. 2005 at 23.

If the FHO* is the HIC (or individual physicians are the HICs), 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 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).

Privacy Homework

If the FHO* is the HIC (or individual physicians are the HICs), it is best practice to have a PHIPA agency agreement to explain the purposes for which the FHT is authorized to access the health record and any privacy services the FHT will provide to the FHO* (NOTE: you may need professional advice to do this.)

How do I know if our FHT (or the FHO* or individual physicians) is PHIPA privacy compliant?

Finding the answer to this question is part of your privacy homework and should be done whether or not you take on QIDS Specialists.

You need to complete Part A of a PHIPA Privacy Impact Assessment. See Appendix II: *Privacy Impact Assessment Template for Family Health Teams.* Whoever is the HIC (see above) is responsible for doing this. But, often even if the FHT is not the HIC, the FHT may choose to help the HIC to understand PHIPA and fulfill the steps that must be taken to be privacy compliant.

Privacy Homework

Complete Part A of the PHIPA Privacy Impact Assessment (NOTE: you may need professional advice to do this)

Here is a short-list of the steps the HIC needs to take[2]:

Step 1: Choose a Privacy Officer: The Privacy Officer is the person (or people) with the responsibility of privacy compliance within the organization. See section 15 of PHIPA. A Privacy Officer is responsible for:

- Facilitating the HIC's compliance with PHIPA
- Ensuring that all agents of the HIC are appropriately informed of their duties under PHIPA
- Responding to inquiries from the public about the HIC's information practices
- Responding to requests from patients for access to their health records (and to make corrections)
- Receiving and responding to privacy complaints

The choice of Privacy Officer should be documented in writing and must be communicated in policies. Everyone working in the FHT should know who the Privacy Officer is. Often the FHT Executive Director and the FHO* Lead Physician are chosen to be co-Privacy Officers.

Step 2: Policies: You need privacy policies to explain to your staff, your "agents" (described below), your patients and the public about your privacy practices.

Step 3: Communication: You need to advise your patients of their privacy rights. There are free posters and brochures available through the IPC/O. You can order free copies to be delivered to you.

- Privacy Brochure
- Privacy Poster

[2] These are obligations of the HIC. If the FHT is the HIC – the FHT has to do these activities. If the FHO* is the HIC, the FHO* does these activities. If each affiliated physician is a HIC, each physician is responsible for each of these tasks.

Step 4: Training: Under PHIPA, you are required to train all your staff and agents about privacy and your privacy policies and expectations. This should be done formally every 3-4 years and there should be a plan of action for reminding staff and agents about privacy issues in an ongoing way.

Step 5: Contracts: Your contracts with vendors (especially your eMR provider, shredding contracts and off-site health records storage contracts) must address privacy issues. Any independent contractor who has access to PHI should have a written contract with privacy clauses.

Step 6: Privacy Breaches and Complaints: You must have a privacy breach policy or practice to follow.

Step 7: Insurance: There is specific insurance you can get to cover your organization for privacy breaches (sometimes called "cyber insurance"). You may want to speak to your existing insurer or seek other advice about insurance options.

There are many resources available to HICs to fulfill these obligations. See Appendix III.

What are the consequences for a privacy breach?

A privacy breach happens whenever a person contravenes a rule under PHIPA or a privacy policy. The most obvious privacy breaches happen when PHI is lost, stolen or accessed by someone without authorization. For example:

- A USB key with identifiable patient data is lost
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package with health records is not delivered to the correct address
- A staff member talks about a patient with a friend
- Health records to be disposed of are recycled and not shredded
- Out of curiosity, a staff member reviews a neighbour's health record
- Health information is given to the media
- A staff member makes a copy of an ex-spouse's health record without the permission of the patient and outside the proper release of information channels

If there is a privacy breach, patients may complain to the HIC and then to the IPC/O (which is a provincial agency charged with oversight of PHIPA compliance). Consequences of failing to comply with PHIPA include:

- IPC/O has power to initiate investigations
- IPC/O has broad order-making powers
- Court may award monetary damages
- PHIPA offences carry fines of up to $50,000 for individuals and $250,000 for corporations
- Self-regulatory bodies (i.e., regulated health profession colleges) have power to take disciplinary action
- HIC may take action including termination of employment or contract

Privacy Rules for Quality Improvement Activities and QIDS Specialists

Does PHIPA apply to quality improvement activities of a FHT?

Yes. If the activity of quality improvement requires the use of clinical information (see below), anyone engaged in a quality improvement activity, including a QIDS Specialist, must comply with PHIPA.

A QIDS Specialist is considered a **PHIPA agent**; therefore, PHIPA applies to his or her activities. Agent is a defined term in PHIPA. It means a person who, **with the authorization of the HIC**, acts for or on behalf of the HIC in respect of PHI.

That means that a QIDS Specialist may only collect, use or disclose PHI with the authorization of the HIC. And the QIDS Specialist must follow privacy rules and practices of the HIC when doing his or her work.

Did you know?

Using PHI to perform quality improvement activities is a legally permitted use of PHI without consent of patients.

What role does a FHO* or individual physicians play in authorizing a QIDS Specialist to access the eMR for quality improvement activities?

You may need to have your own legal advice to answer this question. And there may be cultural issues for you to navigate in addition to the privacy considerations set out in this toolkit.

From a privacy perspective, the HIC makes the decision about who is authorized to access the health record (including an eMR) and for what purposes.

- If physicians are employed by the FHT, the FHT will likely be the HIC. Therefore, the FHT will make decisions about the QIDS Specialist's access to the health records.

- If the FHO* is the HIC or individual physicians are HICs, the FHO* or individual physicians must approve the circumstances under which the FHT and its staff or agents (such as a QIDS Specialist) may access health records. It is best practice for this to be done through a services agreement or PHIPA agency agreement. Because FHT IHPs also provide care to patients, quality measurement and improvement are necessary uses of PHI by the FHT. Services agreements and PHIPA Agency agreements should allow FHTs to perform these legitimate and legally permitted activities.

Practice Tip

It is best practice for services agreements and PHIPA agency agreements between FHTs and FHOs* to allow FHTs (and QIDS Specialists) to access the eMR for quality measurement and improvement activities.

The answer becomes complicated because FHTs and FHOs* often share an eMR. Some PHI will be entered in the eMR by FHT employees (such as IHPs). In situations where the FHT is not the HIC and a FHO* or individual physician as HIC does not grant permission to the FHT for a QIDS Specialist to access their patient information, the QIDS Specialist would be limited to using the PHI entered in the eMR by the FHT IHP to review and measure the FHT's own performance and that of the FHT IHPs, but not physician performance. Since it is virtually impossible to limit eMR access according to who authored an entry, this may cause technical problems. In such cases, the QIDS Specialist should be informed that they are not permitted to run reports or make inquiries that would produce results that would identify physician performance.

However, there may be cases where a FHT has mandatory reporting obligations (such as to Health Quality Ontario or to the MoHLTC) and will require access to the eMR to fulfill those obligations. If the FHO* is the HIC or individual physicians are the HICs the FHT should explain those obligations to the HIC to explain why the FHT (through its QIDS Specialist) must have reasonable access to the eMR. It is best practice to anticipate these scenarios through a PHIPA agency agreement or services agreement between the FHT and the FHO* and explain how such access will be permitted so that the details and safeguards are worked out in advance**.**

What is "personal health information" (PHI)? And should QIDS Specialists be allowed to look at PHI?

PHI is a defined term under PHIPA. PHI is oral or recorded information about an individual that (among other things):

- Relates to physical or mental health
- Relates to providing health care to the individual or identifies the provider of health care
- Relates to payments or eligibility for health care
- Relates to donation of body parts, bodily substances or is derived from the testing or examination of such
- Is a health number
- Identifies a substitute decision-maker

Did you know?

Anything in the eMR or in paper patient health records is definitely PHI. But, if patient information is de-identified or anonymized, it is no longer PHI.

In order to improve clinical data quality, clinical data integrity and clinical performance management outcomes and processes, a QIDS Specialist will need to use clinical data. Generally speaking, that means the QIDS Specialist will need to use identifiable patient information and will likely do that by accessing an eMR.

It is possible that a QIDS Specialist could work with only de-identified information – but if a QIDS Specialist were only allowed to use de-identified information, this would significantly limit the effectiveness of the QIDS Specialist and what he or she can help the FHT to measure.

In some cases, the QIDS Specialist may also directly contact patients to collect new information – such as patient satisfaction survey data.

What other confidential or sensitive information might QIDS Specialists need?

Depending on the activities assigned, the QIDS Specialist may also need access to other FHT activity information (that isn't identifiable patient information) such as:

- Financial information
- Infection control data
- Utilization data
- Clinical protocols
- Scheduling data
- Service agreements
- Committee reports
- Quality improvement data

FHTs should be clear about the categories of information that a QIDS Specialist may and may not use to perform his or her duties.

Who is responsible for the privacy aspects of the QIDS Specialist's activities?

The HIC is ultimately responsible for the PHI under its control and for who accesses the eMR and under what circumstances.

The table on the following pages highlights the ten privacy principles. For each principle, it explains the privacy responsibilities of the HIC and the QIDS Specialist and it identifies considerations for host FHTs in Sharing QIDS Specialist Model arrangements. References in the table to the template agreement are to Appendix I: *QIDS Specialist Collaboration and Data-Sharing Agreement.*

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
Accountability	The HIC is responsible for PHI under its control and must designate an individual who is	The QIDS Specialist must know who the Privacy Officer is for each FHT where he or	The host FHT may be tasked to ask all participating FHTs to document the HIC for

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
	accountable for compliance with PHIPA (usually a Privacy Officer). The HIC is responsible to ensure the QIDS Specialist, as its PHIPA agent: • Receives PHIPA training • Understands the HIC's privacy policies • Complies with PHIPA and the policies • Understands the limits of what PHI he or she can collect, use or disclose.	she is providing services. If a HIC chooses the QIDS Specialist to be the Privacy Officer, that decision would give the QIDS Specialist much more responsibility and authority within the FHT/FHO than most QIDS Specialists currently have. If a QIDS Specialist is a Privacy Officer, he/she is responsible for ensuring the FHT/FHO*'s compliance with PHIPA.	their FHT/FHO* and the Privacy Officer and may be tasked to share that information with the QIDS Specialist. See s. 1.d. of the template agreement. The host FHT may be responsible for general privacy orientation for the QIDS Specialist on behalf of the participating FHTs. See s. 6.c.iii. of the template agreement.
Identifying Purposes	The HIC must have a poster and/or policy available to the public that lists "quality improvement" as one of the activities or purposes for which it uses PHI. See free Privacy Poster.	The QIDS Specialist should know for what purposes he or she is authorized to collect, use and disclose PHI (the main purpose will be for quality improvement).	The host FHT may be asked to coordinate with the other participating FHTs to determine the purposes for which the QIDS Specialist may collect, use and disclose PHI (the main purpose will be for quality improvement).
Consent	The HIC must ensure the QIDS Specialist understands and complies with rules for consent for collection, use and disclosure of PHI. However, for the most part, the HIC will not be required to have the consent of individual patients to allow the QIDS Specialist to provide quality improvement services because such activities are permitted under PHIPA without consent	The QIDS Specialist must follow the consent rules provided by the HIC.	The host FHT should clarify for the QIDS Specialist when consent of patients is required for quality improvement activities (if it is).

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
	(See Limit Collection and Limit Use and Disclosure below).		
Limiting Collection	A HIC may ask a QIDS Specialist to collect new PHI from patients (such as for patient satisfaction surveys). When they do this activity, it is considered a "collection" under PHIPA. The HIC should decide whether the QIDS Specialist needs "identifying information" or "de-identified" information to do the quality improvement activities. Identifying information is defined under PHIPA. It means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. To de-identify or anonymize data means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual. Removing a patient's name from a list is likely not enough to de-identify an individual.	QIDS Specialists should only collect the amount of PHI necessary to perform the function – and no more. If a QIDS Specialist only needs de-identified information to do the work – he or she should not have access to PHI (or should not collect new PHI).	The host FHT should be careful to ensure that it does not inadvertently "collect" PHI belonging to other participating FHTs by virtue of the QIDS Specialist saving or storing PHI on the host FHT's server or in hard copies at the host FHT's offices. (See Limiting Retention below). Your *QIDS Specialist Collaboration and Data-Sharing Agreement* should explain that, when the QIDS Specialist provides services to other FHTs, the QIDS Specialist is the agent for the participating FHT. See s. 9.c. of the template agreement.
Limiting Use	Quality improvement is a "permitted use" without consent under PHIPA. That means that HICs do not require the consent of patients to allow QIDS Specialists to use identifiable patient data for quality improvement purposes.	QIDS Specialists should be very clear about what information (including PHI and other confidential information) they are authorized to use and are not authorized to use.	Host FHTs may need to ensure all staff and FHO* physicians are aware of the concept of "permitted use" to avoid perceptions of breaches of privacy. Multiple FHTs can share a QIDS specialist

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
	It is possible that a QIDS Specialist could work with only de-identified information – but it would be difficult to structure a QIDS Specialist position in that way. If a QIDS Specialist were only allowed to use de-identified information, it would significantly limit the effectiveness of the QIDS Specialist and what he or she can help the FHT to measure.	QIDS Specialists should only use the amount of information necessary to perform the function – and no more. If a QIDS Specialist only needs de-identified information to do the work – he or she should not have access to PHI. The QIDS Specialist may also be given the task of de-identifying PHI for use by the HIC.	to "use" patient information for quality improvement purposes – but there must be a data-sharing PHIPA agreement between the FHTs. See Chapter 4. As long as the QIDS Specialist is not expected to share identifiable patient information from one FHT with another FHT, most of the activities of the QIDS Specialist will be considered a "use" of PHI for quality improvement purposes and the QIDS Specialist activities can occur without consent of the patients of each FHT.
Limiting Disclosure	A HIC is not permitted to disclose PHI (meaning share it outside the HIC) without the consent of the patient unless the disclosure is permitted or required by law. Quality improvement is not a "permitted disclosure" without consent under PHIPA. However, there are many other permitted disclosure activities under PHIPA. A HIC may authorize a QIDS Specialist to disclose PHI on its behalf in those permitted circumstances (such as to comply with a law). If patient information is de-identified before it is shared by a QIDS Specialist outside the HIC, it is no longer considered PHI, and the activity is not	QIDS Specialists should be very clear about what information (including PHI and other confidential information) they are authorized to disclose and are not authorized to disclose. QIDS Specialists should only disclose the amount of information necessary to perform the function – and no more. If a QIDS Specialist only needs de-identified information to make a disclosure - he or she should not disclose PHI.	Host FHTs should ensure there is an agreement in place to explain what information may and may not be shared by the QIDS Specialist with the participating FHTs to avoid actual and perceptions of breaches of privacy. If the QIDS Specialist is expected to share patient identifiable information between the FHTs for the purpose of quality improvement – that activity would be considered a "disclosure" under PHIPA, and it would

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
	considered a "disclosure" under PHIPA.	The QIDS Specialist may also be given the task of de-identifying PHI for disclosure by the HIC.	require express consent of the patients of each FHT.
Limiting Retention	The HIC should tell the QIDS Specialist for how long it wants its quality improvement reports retained. (The HIC may have a record retention policy that sets out applicable retention periods.) The HIC should provide a safe and secure place for the QIDS Specialist to store its PHI (in paper and electronically).	The QIDS Specialist should save his or her reports and raw data as directed by the HIC and in accordance with record retention policies of the HIC. The QIDS Specialist should securely dispose of any PHI if it is no longer needed.	In situations where FHTs share a QIDS Specialist, reports should probably not be saved on the host FHT's server. Instead they should be securely saved on the server of the participating FHT to whom the information belongs. If the QIDS Specialist must save information on the host FHT's server or in paper copies at the host FHT's site, it should be clearly explained in your *QIDS Specialist Collaboration and Data-Sharing Agreement* between the FHTs that the host FHT does not have a right to access the other FHT's data. If the host FHT does access the data, it would be considered a privacy breach.
Accuracy	The HIC has an obligation to ensure the PHI it holds is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. HICs may use QIDS Specialists to improve data quality and accuracy of the PHI they hold.	QIDS Specialists may be given the responsibility to improve data quality and accuracy on behalf of a HIC.	There may be a role for a host FHT to provide leadership in improving data standardization among participating FHTs sharing a QIDS Specialist and across the province.

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
Safeguards	The HIC must ensure PHI is protected by physical, administrative, and technical security safeguards appropriate to the sensitivity of the information. When engaging a new person such as a QIDS Specialist to do an authorized activity such as quality improvement data analysis in patient records, it is best practice for the HIC to put in place safeguards such as: • Have a job description for the QIDS Specialist and ensure that person understands the job • Have the QIDS Specialist sign a confidentiality agreement • Explain the HIC's privacy policies to the QIDS Specialist • Explain what PHI or other business-sensitive information is "off limits" to the QIDS Specialist • Explain what constitutes "de-identified" or "anonymized" information and what does not • Provide technical supports that will allow the QIDS Specialist to do the job and protect patient privacy such as: o A virtual privacy network to work remotely o Encryption software for protecting mobile devices • Explain that identifiable information should never leave the building in paper format or electronically if it is not encrypted	The QIDS Specialist must: • Complete required privacy training • Comply with privacy policies • Sign confidentiality agreements if requested to do so • Follow privacy breach protocols	There may be a role for the host FHT to work with participating FHTs to harmonize their privacy safeguards to make it easier for the QIDS Specialist to comply with PHIPA and each FHT's privacy rules. The IPC/O has resources available with respect to security of mobile devices that should be reviewed if a QIDS Specialist is expected to travel or transport PHI between FHTs (instead of using a virtual private network).

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs

	• Explain what data (or level of detail) can and what cannot be shared with:
	  o Others within the HIC
	  o Other FHTs
	  o Health Quality Ontario or the MoHLTC
	  o The public
	• Conduct a privacy impact assessment to determine whether any risk management strategies should be put into effect to protect the PHI (see Appendix II: *Privacy Impact Assessment Template for Family Health Teams*)
	• Explain where data should be stored
	• Ensure there is a way to audit the QIDS Specialist's activities in the patient records and conduct routine audits
	• Have a protocol to follow if there is a privacy breach		

Openness	A HIC must make readily available to the public (including its patients) specific information about the HIC's policies and practices relating to the management of PHI. If anyone (such as patients, staff, public, clinicians, regulatory bodies) asks about the activities of the QIDS Specialist, the HIC should be open about its quality improvement activities and explain that quality improvement activities are permitted without consent under PHIPA.		
Individual Access	The HIC must ensure that a patient is informed of the	The QIDS Specialist may play a role in improving	The role of the QIDS Specialist in a shared

Privacy Principle	Responsibility of the HIC	Responsibility of the QIDS Specialist	Considerations for Host FHTs
	existence, use, and disclosure of his or her PHI and shall be given access to that information and must ensure that a patient is able to challenge the accuracy and completeness of the PHI and have it amended as appropriate. The role of the QIDS Specialist will not impact a patient's right to access his or her own health record.	data quality and accuracy.	environment will not impact a patient's right to access his or her own health record.
Challenging Compliance	The HIC must have a process to respond to patient complaints about privacy. The HIC must also have a privacy breach protocol to follow. The HIC is responsible in law for the activities of its agents including the activities of the QIDS Specialist. If the QIDS Specialist has committed a privacy breach, the HIC may take action including termination of employment or contract. The HIC would be responsible for any costs or damages associated with responding to a privacy breach or for fines.	The QIDS Specialist should report any privacy breach to the HIC in accordance with the privacy breach protocol.	As the employer of the QIDS Specialist, the host FHT may bear some vicarious liability for the activities of its employee. The host FHT should ensure the *QIDS Specialist Collaboration and Data-Sharing Agreement* considers how the participating FHTs will manage a privacy breach. See s. 9.g. of the template agreement. There may be a role for the host FHT to work with participating FHTs to harmonize their privacy breach protocols to make it easier for the QIDS Specialist to comply with PHIPA and each FHT's privacy practices.

Is there any time when the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (the federal privacy legislation) takes precedence over PHIPA?

In Ontario, PHIPA has been declared substantially similar to PIPEDA. So, with respect to patient information and PHI generally FHTs and FHOs* need to comply with PHIPA and not PIPEDA.

Do we need to do a PIA before a QIDS Specialist starts at our FHT? If so, how do I do one?

A "PIA" is a privacy impact assessment. Anytime a HIC introduces a new technology or a new way of doing business, it is best practice for a PIA to be performed. A PIA will help you to understand whether there are any gaps in your privacy policies or practices and will help you proactively identify and mitigate risks to your organization. We have provided a sample PIA at Appendix II.

Since there is a provincial mandate, what information will be shared between QIDS Specialists?

The QIDS Specialists were released to FHTs to support the goals of the QIDS Program, which has a provincial reach across all AFHTO members. So while QIDS Specialists are hired by and managed by host FHTs, collectively they have a mandate to support the achievement of the QIDS Program goals across the AFHTO membership. For that reason, just as FHTs share "general" information with other FHTs about a range of issues, it may be appropriate for FHTs to share information about their quality improvement activities and collaborate on ways to improve practices. QIDS Specialists may come together from time to time and discuss in high level terms the kinds of quality improvement work they are doing to share best practices within the QIDS Specialist community to better serve their own collaborating FHTs as well as contribute to the overall goals of the QIDS Program.

However, identifiable patient information must never be shared among QIDS Specialists or with other FHTs, even if those FHTs belong to a community sharing a QIDS Specialist (unless express consent from patients has been obtained – which would not be a usual occurrence).

Practice Tip

Identifiable patient information must never be shared among QIDS Specialists or with other FHTs without the express consent of the individual patients. If data is de-identified, it may be shared.

At what point should a QIDS Specialist de-identify data?

See the ten privacy principles chart above and the sections "Limit Collection", "Limit Use" and "Limit Disclosure". The basic rule is that QIDS Specialists should only collect, use and disclose the amount of PHI necessary to perform the function – and no more. If a QIDS Specialist only needs de-identified information to do the work – he or she should not have access to PHI (or should not collect new PHI). The QIDS Specialist should consider this question for each assignment.

At the very least, as mentioned in the answer above, identifiable patient information must never be shared among QIDS Specialists or with other FHTs without the express consent of the individual patients to whom the information relates. And therefore, the QIDS Specialist must de-identify any PHI before sharing reports or general data outside the FHT.

If a FHT stores old patient health records (from patients who are no longer with the FHT or FHO*) should the QIDS Specialist still be allowed to access those records for quality improvement purposes?

It depends. The HIC should be consulted. It may be that patient records relating to former patients should be disposed of in accordance with record retention policies. However, from a privacy perspective there is nothing wrong with a QIDS Specialist accessing former patient records for the purposes of quality improvement and data analysis as long as the activity is approved by the HIC.

What is allowed if a HIC wants the QIDS Specialist to assist with research activities?

Research is a defined term in PHIPA. It means a systematic investigation designed to develop or establish principles, facts or generalizable knowledge and includes the development, testing and evaluation of research. Research activities have different rules under PHIPA than quality improvement activities.

If research is an authorized activity by the HIC, a QIDS Specialist or researcher may collect, use or discloses PHI for research purposes with the consent of the research participant.

If consent of the patients is not contemplated (such as for a retrospective chart review), there are special privacy rules to follow. Research is a "permitted use", with rules (ss. 37(1)(j), 27(3), 37(4) and 44 of PHIPA). Before a HIC uses PHI for research without consent, the HIC must prepare a research plan and have it approved by a Research Ethics Board. The researcher must carry out the research and follow certain rules.

Research is also a "permitted disclosure", with rules (s. 44 of PHIPA). Before a HIC discloses PHI for research without consent, the HIC must:

- Receive from the researcher:
  - an application in writing
  - a research plan
  - a copy of the decision of Research Ethics Board approval
- Enter into a research agreement with the researcher

If you expect your QIDS Specialist to assist the FHT or FHO* with research, you should consider seeking professional advice.

Should QIDS Specialists be allowed to email patients? Such as to conduct patient satisfaction surveys?

Before making direct contact with any patient, the QIDS Specialist should be sure that he or she is authorized to do so by the HIC. The reason for the communication with the patient must also be lawful.[3]

There is nothing in PHIPA that allows or restricts communication with patients by email. PHIPA just requires that HICs take appropriate precautions with PHI. A number of regulatory Colleges and associations have set out guidelines about communicating with patients by email, and FHTs and FHOs* should follow those rules. For example, see (not an exhaustive list):

- College of Physicians and Surgeons of Ontario
- Canadian Medical Protective Association
- Canadian Medical Association
- Canadian Medical Association Policy
- College of Nurses of Ontario

[3] If the QIDS Specialist intends to contact a patient to conduct a patient satisfaction survey – that would be considered a lawful activity.

- Ontario College of Pharmacists
- College of Dieticians
- College of Psychologists of Ontario

CHAPTER 4: Collaborating Among a Group of FHTs to Share a QIDS Specialist

FHTs engaged in the Sharing QIDS Specialist Model (see Chapter 2), with more than one FHT sharing a QIDS Specialist, must have a collaboration and data-sharing agreement to explain how the QIDS Specialist will be shared.

See Appendix I: *QIDS Specialist Collaboration and Data-Sharing Agreement*

How do I know if the template will work for our situation?

The template is designed for groups of FHTs that are sharing a QIDS Specialist.

You do not need this template agreement if one QIDS Specialist will be working only for your FHT (Single FHT QIDS Specialist Model). If that is the case, you will still need to address the privacy issues set out in Chapter 3. But you do not need a collaboration and data-sharing agreement with other FHTs.

Why do we need an agreement? Can't we just allow a QIDS Specialist to access each of our records?

Contracts do not need to be in writing to be binding on the parties. But without a written contract, the terms of your collaboration may be uncertain. It is best practice to have an agreement so that you address key issues. This is especially important for host FHTs who employ QIDS Specialists to explain how costs and liability for the QIDS Specialist are intended to be shared. During a dispute is the worst time for you to sort out the details of what you intended.

You could go without a formal agreement, but that likely does not meet your obligations under PHIPA to ensure there are necessary safeguards in place to protect the PHI you hold and to allow the QIDS Specialist to access the eMRs of the participating FHTs. Please see section 9 of the template dealing with data sharing.

Do we have to use the template? Can we change the parts we do not like/need?

No, you do not have to use the template. This template is for general information purposes only.

The only section you must include in order to fulfill your PHIPA obligations is section 9 dealing with data sharing. Otherwise, you can change anything in the agreement to suit your needs. We recommend you get legal advice to ensure the agreement meets your purposes, whether you keep it as it is or make changes.

Why is it called a "Collaboration Agreement" and not a "Partnership Agreement"?

The word "partnership" has a legal meaning. In a partnership, assets are considered to be pooled and, as a result, all parties to a partnership are liable for the obligations of all of the partners. For example, this means the host FHT could be responsible for another FHT's liability even if the liability is not the fault of the host FHT. This is why it is not recommended to use the word "partnership".

In sharing a QIDS Specialist, FHTs are working together or "collaborating".

Can we have as many FHTs sign the agreement as we like? Is there a limit to how many FHTs can be part of a collaboration?

Yes, you can have as many FHTs sign your *QIDS Specialist Collaboration and Data-Sharing Agreement* as you would like. There is no limit, except that you will want to ensure your QIDS Specialist can accommodate the workload of all of the participating FHTs.

Why are the FHTs signing this agreement? Shouldn't it be the FHOs* (or the physicians) signing?

The main collaboration is actually between the FHTs that are sharing the QIDS Specialist. To have the FHOs* or individual physicians included as parties to the agreement makes the agreement too cumbersome and overly complicated because much of the agreement does not apply to them.

Of course, FHOs* and physicians are important stakeholders in the QIDS initiative. And they have an important part to play with respect to privacy, especially if the FHO* or individual physicians are the HIC for the health records that the QIDS Specialist will access to do quality improvement work. See Chapter 3.

In the template agreement at section 1.d., in order to become part of the QIDS Specialist collaborative, each FHT must do its homework and organize behind the scenes to identify who is the HIC for purposes of PHIPA and who can agree to allow the QIDS Specialist access to the health records. In order for a FHT to participate in the collaborative, it must either provide the host FHT with a letter confirming that it is the HIC for its patients or confirm that the FHO* (or physicians) are the HICs. This can be achieved through something as simple as an email. See Chapter 3 for a discussion on how to determine who the HIC is.

If the physicians are employees of the FHT, the FHT will most likely be the HIC. If the FHO* is the HIC or individual physicians are the HICs it is best practice to have a PHIPA agency

agreement to explain the purposes for which the FHT is authorized to access the health record and any privacy services the FHT will provide to the FHO* or the individual physicians.

As a group of collaborating FHTs, do we have to have a local Steering Committee?

No. You are not required to have a local Steering Committee. However, we recommend that you do have one in order that you have clarity around how decisions will be made about the QIDS Specialist and a forum for discussing issues that arise in the collaboration. Without a Steering Committee, you may not have clarity around who can make decisions, how tough decisions will be made, and how disputes may be resolved.

Does the Steering Committee have to make decisions by consensus? Can we do majority rules?

Your local Steering Committee can be organized however you like. There is no right or wrong model of decision-making.

> **Consensus**: If you operate by consensus, it means that each representative has the power to veto a decision because unless everyone agrees, you cannot act.
>
> **Majority**: If you operate by majority, it means that as long as most of you (50% +1) agree to a decision, it carries. It means that some of the FHTs may be carried along despite not agreeing.
>
> **One FHT Decides**: If you operate where one FHT decides (such as the host FHT), then basically the host FHT holds meetings to share information only.

How often should the Steering Committee meet?

The timing and frequency of the Steering Committee meetings is up to you.

What should the QIDS Specialist do?

The template agreement provides a sample job description. However, there may be a great deal of variation in the job descriptions of QIDS Specialists across the province. The template list of duties for the QIDS Specialist is neither required nor exhaustive. The role and activities that the QIDS Specialist performs can be tailored by the group to suit your needs.

What information should be shared between FHTs?

This can be decided within your group. However, identifiable patient information must never be shared by QIDS Specialists among themselves or with other FHTs (unless express consent from patients has been obtained – which would not be a usual occurrence). See Chapter 3 and the "Limiting Disclosure" principle.

Can a QIDS Specialist combine information from separate FHTs?

The QIDS Specialist should only combine information from separate FHTs if doing so is an authorized activity (as directed by the Steering Committee or other authorized person).

However, as explained above, PHIPA does not allow sharing PHI outside the HIC for quality improvement purposes without the consent of the individual patients to whom the information relates. As long as a QIDS Specialist does not share PHI (that is identifiable health information) from one FHT to another FHT, it may be permissible for the QIDS Specialist to combine information from separate FHTs, de-identify it and share the de-identified results with the group.

From whom should the QIDS Specialist take instructions?

This can be decided within your group. We have recommended in the template agreement that each FHT identify a manager to whom the QIDS Specialist will report within that FHT. Otherwise, we recommend the QIDS Specialist will take instructions only from the Steering Committee and from his or her manager within the host FHT.

How should we protect our "confidential information" if we share a QIDS Specialist with other FHTs?

In an arrangement where the QIDS Specialist works at multiple FHT sites, the QIDS Specialist is not only going to have access to patient information that needs to be protected. The QIDS Specialist will also be privy to confidential business information about a FHT and its affiliated FHOs* that should not be shared with other FHTs and FHOs*.

You need to think about whether you want the QIDS Specialist to share with the other FHTs in the collaborative your:

- Internal policies and procedures
- Types of services provided to patients (e.g., types of clinics being run)
- Financial information
- Infection control data

- Utilization data
- Clinical protocols
- Scheduling data
- Service agreements
- Committee reports
- De-identified quality improvement data

See section 5 of the template agreement. “Confidential information” is intentionally much broader than patient health information. Each FHT should be very clear with the QIDS Specialist what it considers to be “sensitive” or “confidential information” that is not to be shared with other FHTs including with the host FHT.

In the case of a privacy breach by a shared QIDS Specialist, who will be held responsible?

Where a QIDS Specialist is shared, this may be a difficult question to answer.

As the employer of the QIDS Specialist, the host FHT may have vicarious liability for the activities of its employee.

Under PHIPA, the HIC is always responsible to protect the PHI it holds from loss, theft and unauthorized access. The HIC is responsible for the activities of its agents, and would be responsible for the activities of the QIDS Specialist. However, responsibility for the costs of a privacy breach may be assigned or shared through a PHIPA agency agreement or the *QIDS Specialist Collaboration and Data-Sharing Agreement*. This is an important issue to address and should be addressed before a privacy breach occurs.

Why are there two options listed for “Liability and Indemnification”?

Indemnity refers to one party agreeing to pay damages of the other party in specific situations. This section of the agreement is written in order to allocate risk amongst the parties. Indemnity payments are meant to restore a party to the state they were in before the loss. Indemnity is often subject to a limitation of liability (see Limitation of Liability below) and is typically supported by insurance so that the party is able to honour the indemnity.

Section 16 of the template offers two options to allocate risk through indemnity. Option #1 limits the circumstances in which one party can claim indemnity from another. These circumstances are only: where one party has acted very badly (in bad faith or outside the authority of the agreement) or where a third party (such as a patient) is seeking damages. Otherwise, the parties will look to their insurance (and not to each other) if there are damages resulting from the agreement or another party’s breach of the agreement. This

indemnity is much more limited than you would find in a typical commercial agreement. This limited indemnity may make sense given that this isn't a commercial arrangement (money is not changing hands) and everyone is cooperating in good faith.

Option #2 allows the parties to claim indemnity against each other in broader circumstances, such as for damages resulting from the other party's own negligence. This is much more like the indemnities you would expect to find in commercial agreements.

Limitation of Liability in a contractual relationship provides that, in given situations, the parties will **not** be responsible for each other's damages or will only be responsible up to an established limit or under certain circumstances.

What insurance do we need when we are sharing a QIDS Specialist?

You should seek professional advice from your own insurance provider about a shared QIDS Specialist. There is also specific insurance you can get to cover your organization for privacy breaches (sometimes called "cyber insurance"). Again, speak with your insurance provider about potential options.

Parties to a contract are often required to have insurance as a pre-condition to the contract and to maintain insurance as an ongoing condition of the contract. It is possible for one party to be responsible for the insurance of both parties. In this case, the non-insuring party can be added to an insurance policy as a **named insured**. This may not cost extra. Before the contract takes effect, a **certificate of insurance** (i.e., a signed document from the insurance company confirming the existence of the required insurance) is often necessary. Again, such a certificate usually does not cost extra.

What should we do if we already have a partnership agreement without privacy issues addressed?

If you already have an agreement in place, you should review the agreement to see how "amendments" are to be addressed. You may be able to add privacy clauses to the existing agreement through an amendment or as a schedule. You may choose to terminate your existing agreement and start a new agreement with the privacy issues addressed. However, you may wish to seek professional advice before terminating an existing agreement.

Appendix I: QIDS Specialist Collaboration and Data-Sharing Agreement – Template

Click here to access the link.

Appendix II: Privacy Impact Assessment Template for Family Health Teams

Privacy Impact Assessment Template for Family Health Teams[4]

For: [Insert name of the information system, technology or program for which the PIA is being prepared]
Author's name:
Author's title:
Author's contact information:
Author's email address:
Date:

Part A: Organizational Privacy Management

The questions in Part A relate to privacy management throughout the Family Health Team and the affiliated Family Health Organization(s). They are not limited to the information system, technology or program being reviewed. Specific questions related to the information system, technology or program appear in Part B.

#	Question	Yes	No	In Progress
A1	Is there a Family Health Team strategic plan or business plan that addresses privacy protection? *Note*:			
A2	Does the Family Health Team have a written privacy policy or statement of information practices? *Note*:			
A3	Have privacy policies or procedures been developed for various aspects of the Family Health Team's operations? *Note:*			
A4	Do the privacy policies or procedures that we identified in response to questions A2 and A3 ensure the following: - Personal health information is collected in accordance with *PHIPA* and other applicable legislation; - Individual consent is obtained in accordance with sections 18 of *PHIPA* where consent is required; - A written public statement about the Family Health Team's information practices, who to contact with privacy questions or complaints, and how to obtain access or request correction of a record of personal health			

[4] Based on the Information and Privacy Commissioner/Ontario, "Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act", 2005
(Available online: http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf)

	information is readily available to individuals, as outlined in section 16 of *PHIPA*; - Individuals are entitled to request access to and correction of their own personal health information as provided for under sections 52-55 of *P H I PA*, subject to certain exceptions; - There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained as well as procedures outlining the manner by which personal health information will be securely destroyed. *Note:*			
A5	Are administrative, technical and physical safeguards in place at the Family Health Team to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal pursuant to section 12 of *PHIPA*? *Note:*			
A6	Is there an appointed privacy contact person in the Family Health Team? *Note:*			
A7	Does a reporting process exist to ensure that the Family Health Team's management is informed of any privacy compliance issues? *Note:*			
A8	Are senior executives actively involved in the development, implementation and/or promotion of the Family Health Team's privacy program? *Note:*			
A9	Are employees or agents of the Family Health Team and related Family Health Organization(s) with access to personal health information provided training related to privacy protection? *Note:*			
A10	Have policies and procedures been developed concerning the management of privacy breaches, including the notification of individuals when the confidentiality of their personal health information has been breached? *Note:*			

Part B: Project Privacy Management

The questions in this section relate to the information system, technology or program being reviewed.

#	Question	Yes	No	In Progress
B1	Has a summary of the proposed or existing information system, technology or program been prepared, including a description of the requirements for the system, technology or program and a description of how the information system, technology or program will or does meet those needs? *Note:*			
B2	Has a listing of all personal health information or data elements that will be or are collected, used or disclosed in the proposed or existing information system, technology or program been prepared? *Note:*			
B3	Have diagrams been prepared depicting the flow of personal health information in the proposed or existing information system, technology or program? *Note:*			
B4	Have documents been prepared showing which persons, positions, or employee categories will have access to which elements or records of personal health information? *Note:*			
B5	Does consent from the individual or an authorized substitute decision-maker provide the primary basis for the collection, use and disclosure of personal health information for the proposed or existing information system, technology or program? *Note:*			
B6	Have we documented the purposes for which personal health information will be or is collected, used or disclosed in the information system, technology or program? *Note:*			
B7	Is personal health information collected, used, disclosed or retained exclusively for the identified purposes and for purposes that an individual would reasonably consider consistent with those purposes? *Note:*			
B8	Will personal health information in the proposed or existing information system, technology or program be linked or cross-referenced to other information in other information systems, technologies or programs? *Note:*			

B9	Will personal health information collected or used in the information system, technology or program be disclosed to any persons who are not employees or agents of the Family Health Team? *Note:*			
B10	Have we made arrangements to provide full disclosure of all purposes for which the information system, technology or program will collect personal health information? *Note:*			
B11	Have communications products and/or a communications plan been developed to fully explain the information system, technology or program to individuals and how their personal health information will be protected? *Note:*			
B12	Does the proposed or existing information system, technology or program involve the collection, use or disclosure of any personal health information beyond Ontario's borders? *Note:*			
B13	Has an assessment been completed to identify potential risks to the privacy of individuals whose personal health information is collected, used, retained or disclosed by the proposed or existing information system, technology or program? *Note:*			
B14	If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the design and/or implementation of the proposed or existing information system, technology or program? *Note:*			
B15	Has an assessment been completed to identify whether other Family Health Teams (or other health information custodians) have implemented the same or a similar information system, technology or program, the risks to privacy experienced by other Family Health Teams or health information custodians and the means implemented by these other Family Health Teams or health information custodians to avert or mitigate these risks? *Note:*			
B16	Have key stakeholders been provided with an opportunity to comment on the sufficiency of privacy protections and their implications on the proposed or existing information system, technology or program? *Note:*			
B17	Will users be trained in the requirements for protecting personal health information and will they be made aware of the relevant			

	notification procedures if personal health information is stolen, lost or accessed by unauthorized persons? *Note:*			
B18	Have security policies and procedures to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal been documented? *Note:*			
B19	Have privacy policies or procedures been developed for various aspects of the operations for the proposed or existing information system, technology or program? *Note:*			
B20	Do the privacy policies or procedures that we identified in question B16 ensure the following (if so, please enclose): - Personal health information in the proposed or existing information system, technology or program is collected in accordance with *PHIPA* and other applicable legislation; - Individual consent is obtained in accordance with section 18 of *PHIPA* for the proposed or existing information system, technology or program where consent is required; - A written public statement about the purposes for which the proposed or existing information system, technology or program collects, uses or discloses personal health information is readily available to individuals as outlined in section 16 of *PHIPA;* - Individuals are entitled to request access to and correction of their own personal health information in the proposed or existing information system, technology or program as provided for under sections 52-55 of *PHIPA*, subject to certain exceptions; - There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained in the proposed or existing information system, technology or program, as well as procedures outlining the manner by which personal health information in the proposed or existing information system, technology or program may be securely destroyed. *Note:*			
B21	Does the proposed or existing information system, technology or program provide functionality for the logging of the insertion, access, modification or disclosure of personal health information as well as an interface to audit those logs for unauthorized activities? *Note:*			
B22	Have policies and procedures been developed for the enforcement of privacy rules relating to the proposed or existing information system,			

	technology or program, including fulfillment of the commitments made in this PIA? *Note:*			

Appendix III: General Privacy Resources

Canadian Mental Health Association Privacy Toolkit

College of Physicians and Surgeons of Ontario Confidentiality Policy

eHealth Ontario Guide to Information Security for the Health Care Sector Information and Resources for Small Medical Offices

Information and Privacy Commissioner of Ontario (IPC/O)

- Privacy Diagnostic Tool from IPC/O
- Privacy Impact Assessment Tool from IPC/O
- Privacy Poster from IPC/O
- Protecting Personal Health Information on Mobile and Portable Devices from IPC/O

Ontario College of Social Workers and Social Service Workers Privacy Toolkit

Ontario Hospital Association/Ontario Medical Association Privacy Toolkit

OntarioMD Privacy and Security Guide and Workbook Electronic Medical Records – Transition Support Program

- Privacy and Encryption Tutorial from OntarioMD
- Sample Privacy Policy from OntarioMD
- Sample Office Privacy Handout from OntarioMD
- Confidentiality Agreement for Physician Office Employees from OntarioMD
- Sample Contractual Privacy Clauses for Employees and Third Parties from OntarioMD

Appendix IV: Acronyms

AFHTO – Association of Family Health Teams of Ontario

APP – Alternative Payment Plan

BSM – Blended Salary Model

eMR – Electronic Medical Records

FHG – Family Health Group

FHO – Family Health Organization

FHT – Family Health Team

HIC – Health Information Custodian

IHP – Interprofessional Health Care Provider

IPC/O – Information and Privacy Commissioner of Ontario

MoHLTC – Ministry of Health and Long-Term Care

PHI – Personal Health Information

PHIPA – *Personal Health Information Protection Act, 2004* (Ontario)

PIA – Privacy Impact Assessment

QIDS – Quality Improvement Decision Support

RNPGA – Rural and Northern Physician Group Agreement