

Subject: Lockbox	Date Approved: June 14, 2017
Approved by: Executive Director/ Medical Director	Date Revised:
Specific to: All Staff and Board of Directors	Next Review Date: September 2020

PRINCIPLE:

This policy is part of the Privacy Policy. It applies to all physicians, the Family Health Network, the Family Health Team and all staff, students, volunteers, and vendors. (“**Team Members**”)

POLICY:

Ontario’s health privacy law, the *Personal Health Information Protection Act* (PHIPA), provides individuals¹ with the right to make choices about, and control how, their personal health information (PHI) ² is collected, used, and disclosed.

PHIPA gives patients the opportunity to restrict access to any or their entire PHI by one or more Team Members³ or by external health care providers. Although the term “lockbox” is not found in PHIPA, lockbox is commonly used to refer to a patient’s ability to withdraw or withhold their consent for the use or disclosure of their PHI for health care purposes. The lockbox provisions of PHIPA are found in sections 37(1)(a), 38(1)(a), and 50(1)(e). The lockbox does not extend to other uses or disclosures that are permitted or required under PHIPA or other legislation.

This policy will help our Team Members understand and fulfill their role when addressing lockbox requests and providing care to patients who have implemented a lockbox. Lockboxes may affect clinical practice for physicians and the Family Health Team because access to information about patients may be restricted, and physicians and Family Health Team inter-professional health care providers may be asked not to share PHI with other health care providers inside or outside of the Family Health Team.

Requests for a Lockbox

Any current or former patient⁴ may request a lockbox to restrict sharing of all or some of their PHI by one or more Team Members or by external health care providers.

When patients ask about lockboxes, it is important for Team Members to address their concerns about the confidentiality of their PHI. Note that some patients may want to control who can access their PHI, but

¹ It is possible that we hold PHI about individuals who are not patients or who are former patients, and the lockbox policy would apply equally to those individuals.

²“PHI” is broadly defined under PHIPA. In our context it will mainly relate to a patient’s health record and we have used “health record” interchangeably with PHI throughout the policy. It is possible that the organization holds other PHI about an individual outside the health record and the lockbox policy would apply equally to that information, wherever it resides.

³ We refer throughout to “Team Members” – but this policy applies to the physicians, the Family Health Network and the Family Health Team’s staff, volunteers, students, and vendors.

⁴An individual’s substitute decision-maker may also request a lockbox and such requests are processed in the same manner.

may not know to use the term “lockbox.” Patients may want a lockbox when they use words such as “restrict,” “limit,” “don’t tell,” “exclude,” “shield,” or “block” when talking about their PHI. For example, patients may want a lockbox if they ask their health care provider or other Team Member:

- Not to tell their specialist that they are being treated at the Family Health Team
- To exclude certain clinical staff from seeing their information
- To “shield” their information
- To “restrict” their health record
- Not to let their family members or neighbours who work with the Family Health Team look at their health record

Patients may initiate the process for a lockbox by speaking with their physician or by contacting the Privacy Officer. Patients must submit their request for a lockbox in writing. Patients will be asked to complete a “Patient Lockbox Request” form. The completed form must be submitted to the Privacy Officer or designate.

The “Patient Lockbox Information” brochure should be given to patients who want more information. This brochure discusses the purpose, implications, and limitations of implementing a lockbox.

Lockbox requests can vary considerably. A patient may request that:

- Only some of the documents in their health record be locked
- All of their health record be locked
- All documentation created in the future be locked
- Only one Team Member be restricted from accessing PHI
- Several Team Members be restricted from accessing PHI
- All Team Members be restricted from accessing PHI
- One or more external health care providers not be given their PHI

Although PHIPA does not require that we lock documentation that does not yet exist, in practice, refusing to lock future documents may result in frequent lockbox requests from a patient if a lockbox will be requested every time a new document is created. For this reason, we will, where appropriate and if requested, lock documents as they are created. An example might be where a patient requests a future lockbox because one of their family members (or former spouse or partner) is a Team Member.

When patients request a lockbox, it often means they have concerns about their PHI and how it is being used and/or disclosed. Patients should be reminded that:

- We take privacy seriously and keep all PHI confidential and secure

- PHI is only accessed by Team Members on a need-to-know basis
- We conduct privacy audits regularly to ensure compliance with the need-to-know policy
- Where PHI is accessed without authorization, appropriate steps will be taken to prevent a reoccurrence and there would be disciplinary consequences
- PHI is disclosed only to external health care providers with whom the patient wants their PHI shared (unless the disclosure is otherwise permitted or required under PHIPA without consent, or by another law)

Sometimes a patient requests a lockbox when a lockbox is not necessary to resolve the patient's concern. For example, a lockbox is not necessary to restrict the sharing of PHI with non-health care providers (e.g., family, employers, insurers) because we need the patient's express consent (either in writing or if verbal, as documented by us) to share information with such recipients (unless, for example, a family member acts as the patient's substitute decision-maker). If a patient does not want us to share information with non-health care providers – we will not do so unless there is legal authority to do so.

As another example, if patients disagree with the information in their health records they can ask for a correction and/or append a statement of disagreement to the record. For that reason, they may not need a lockbox to solve their concerns about the accuracy of the information in their health record.

Implications of Implementing a Lockbox

If a patient chooses to move forward with a lockbox request, it is important that they understand the possible implications of the lockbox. There may be implications and risks to the patient and to their care. The Privacy Officer or designate or the patient's physician should discuss implications and risks with the patient. Examples may include:

- The patient not receiving the best possible service because health care providers may not have access to PHI that they need in order to provide the best possible care in a timely manner.
- The patient may have to undergo duplicate tests, procedures and/or health history questions, as applicable, if existing information is unavailable.
- We use a multidisciplinary team approach to providing care. Although each lockbox request is considered on a case-by-case basis, generally, a patient's choice to implement a lockbox should not prevent a team from providing care as per their standards of practice.
- There may be circumstances where clinicians providing health care ("**Clinicians**") cannot provide care in a manner that meets professional standards of practice if they do not have sufficient information. Such Clinicians may have to assess whether they can continue to provide care to a patient if there is insufficient information. However, the decision to discontinue care to a patient is a significant one and would only be made after thorough consideration of all the relevant information. Clinicians will try to maximize patient choice about how their PHI is used and

disclosed while at the same time allowing all of the Clinicians to uphold their commitments to deliver a high quality patient care and to meet their obligations to their regulatory colleges.

There may be other risks specific to particular patients, which should be explored and discussed with patients directly.

Decisions to Implement a Lockbox

All patient requests to implement a lockbox must be done on the ***Patient Lockbox Request Form***. The Privacy Officer or designate, together with the patient's physician/primary care provider, will review, approve, respond to, implement, and administer lockbox request.

The practical methods of implementing lockboxes are varied; therefore, lockbox requests are considered on a case-by-case basis. A decision to implement a lockbox will be based on the practicality of the solution, technological feasibility, and the specific circumstances.

The Privacy Officer or designate will notify in a timely manner any patient who made a lockbox request of the decision made in respect of the lockbox. If a decision has been to deny a lockbox request, the patient will be informed of the right to make a complaint to the Information and Privacy Commissioner of Ontario.

Lockbox Exclusions

Because the patient's physician is the health information custodian for purposes of PHIPA, a lockbox cannot be used to prevent the patient's physician from accessing the record.

A lockbox is limited under PHIPA to those providing care to the patient. It does not operate to prevent administrative functions from being carried out or the use or disclosure of PHI for other authorized purposes. For example, even where a lockbox is in place, it will not prevent the Family Health Network or Family Health Team from:

- Obtaining or processing payments
- Planning services
- Quality improvement
- Disposing of information
- Complying with a court order
- Litigation
- Research (with research ethics board approval)
- Teaching Team Members to provide health care

The above actions are permitted under sections 37-50 of PHIPA.

A lockbox does not prevent the physician or the Family Health Network or Family Health Team from using or disclosing PHI where there is a legal obligation to do so (for example, to fulfill mandatory reports to the Children's Aid Society or to the Ontario Ministry of Transportation). The physician and the Family Health Network and Family Health Team may also use or disclose PHI if there are reasonable grounds to believe that using or disclosing the information is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. There may be other circumstances where the use or disclosure of PHI is required or permitted by law. The Team Member should always consult with the Privacy Officer and physician.

Identifying a Lockbox

Before a Lockbox is implemented, the Team Member must ensure that the proper approval process has been followed (see "Decisions to Implement a Lock Box" above).

Team Members should be aware of how records are made subject to a lockbox and what a lockbox looks like.

Electronic Records:

If the entire health record is subject to a lockbox, the "Lock" function in eMR will be utilized. To lock a chart go to the Encounter Notes tab on the patients chart, click on the word "Patient" to the left of the patient's name. A pop up box will appear where "Selected users" should be selected which will allow for the patient's primary care physician to be selected as a select user who can view the patient chart. If the patient consents to other specific providers to also see their chart, they too can be selected. The physician **MUST** always be selected, the physician of the patient cannot be locked from a chart.

If a portion of the health record is subject to a lockbox, the relevant portion will be masked. (Note: Only clinical notes can be masked. Information such as medications, lab and diagnostic reports cannot be masked. The only way to protect this type of PHI is by locking the entire record). Any provider may mask a note. A provider may not mask the patient's physician from a note. A provider will know that the note that they are about to create must be masked by a pop up box in the eMR with specific instructions. To mask a specific note, go to the patient chart and to the virtual chart tab. Hold the "Alt" key down and click on the document you wish to mask. Click within the "Mask" checkbox so a checkbox appears. Then, click on the green plus to add users that the patient consents to viewing the document. The physician of the patient **MUST** always be authorized to view all documents and cannot be locked from a document.

Paper Records:

If the entire health record is subject to a lockbox, it will be in a sealed envelope (signed across the seal by the Privacy Officer or designate) with a label affixed to it that reads "Lockbox" and there will be a note in the eMR notifying the user that a Lockbox (paper record) exists.

If a portion of the health record is subject to a lockbox, the relevant portion will be in a sealed envelope (signed across the seal by the Privacy Officer or designate) with a label affixed to it that reads “Lockbox” and there will be a note in the eMR notifying the user that a Lockbox (paper record) exists. The eMR note will be electronically signed by the creator of the note and the paper record(s) that are locked will be in a double- locked area.

“Breaking” the Lockbox

If a Team Member is authorized to access information that is otherwise “locked”, the following instructions explain how to access the PHI.

Electronic Record:

To “break” a lockbox that a Team Member was previously locked from, whether an entire chart or documents within, and the team member is now authorized to access the health information that was otherwise locked, the Team Member will contact the organization’s Accuro Admin support in order for the authorization to be granted.

Paper Record:

To “break” a lockbox, a Team Member would open the sealed envelope with authorization to do so, and remove the paper records. Access to the health record is then available.

Any Team Member who accesses PHI that is protected by a lockbox must consult with the Privacy Officer before taking any action. The Privacy Officer would then consult with the Primary Care Physician to determine if appropriate. If it is determined appropriate for the Team Member to access the locked portion of the record, the reason must be documented on the patient’s health record along with the person(s) that authorized “breaking” the lock. All information subject to a lockbox will be monitored and there will be random audits of such files.

For paper health records, if the lockbox restrictions continue after the lock has been broken for a specific purpose, the PHI should be “locked” again in another sealed and signed envelope by the Privacy Officer or designate. The electronic record will continue with the assigned lockbox restrictions until they are removed.

Of course, a patient may choose to withdraw a lockbox request or unlock PHI in a lockbox. That decision must be in writing and must be documented on the health record.

Notice to External Health Care Providers

If a patient’s lockbox instructions state that the patient does not want all or some PHI shared with an external health care provider, the physician or Family Health Network will not disclose PHI to the restricted external health care provider unless:

- We are permitted or required by law to do so (for example, we need to disclose the PHI to the external health care provider in order to reduce or eliminate a significant risk of serious bodily harm to the patient or to another person or persons)
- The external health care provider has provided us with written proof of the patient's express consent to the disclosure.

If the physician or Family Health Network is prevented from disclosing PHI relevant to the provision of care to an external health care provider because of a lockbox, the physician or Family Health Network has an obligation to notify the receiving health care provider, on the referral to that provider, that not all the relevant PHI has been provided. The receiving health care provider is then able to explore the matter of the "locked" information with the patient and seek consent to have the locked information shared.

Audits

The organization's Privacy Officer or designate will conduct audits of locked health records to ensure compliance with patient lockbox instructions and to determine whether there has been inappropriate access to locked information. Any apparent unauthorized access to locked information will be investigated.

Breach of Privacy

Unauthorized access by a Team Member to a patient's health record constitutes a breach of privacy and may result in disciplinary action up to and including termination of employment or contract.

If there is a lockbox on a patient's health record and a Team Member is excluded from accessing the PHI, it is considered a breach for that Team Member to access the PHI without specific authorization from the physician and Privacy Officer or designate or unless otherwise permitted or required by law to use or disclose the information (such as in an urgent situation in order to prevent a significant risk of serious bodily harm).

The physician is obliged to notify any affected patient(s) of a privacy breach and their rights and will do so in accordance with the requirements of PHIPA.

Attachments

Appendix A – Patient Lockbox Information Brochure

Appendix B – Patient Lockbox Request Form

Appendix C - Lockbox Notification Sheet