

Complete Policy Title:
Lock Box Protocol for Personal Health Records

Approved by:
President

Date of Original Approval(s):
July 1, 2017

Responsible Executive:
University Privacy Officer

Policy Number (if applicable):

Date of Most Recent Approval:
July 1, 2017

Supersedes/Amends Policy dated:

Enquiries:
[University Secretariat](#)

DISCLAIMER: *If there is a Discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails*

Purpose

Section 20(2) of PHIPA makes it clear that individuals may withhold or withdraw their consent to the collection, use or disclosure of their personal health information by Health Information Custodians for the purposes of providing or assisting in providing health care. Further, under PHIPA, individuals may provide express instructions to health information custodians not to use or disclose their personal health information for health care purposes without consent in the circumstances set out in sections 37(1) (a), 38(1)(a) and 50(1)(e) of PHIPA.

These provisions have come to be referred to as the “lock-box” provisions.

This protocol is intended to explain the steps for handling lock boxes, the process of manually locking health records; situations when locked health records can be accessed; and, the process by which McMaster University ensures the security of locked information.

Policy

A capable client or their Substitute Decision Maker (SDM) may request that McMaster University and its staff not collect, use or disclose specified personal health information to another health information custodian for a particular purpose including the provision of health care.

Within this protocol, the right of the client or SDM to restrict the collection, use or disclosure of their personal health information is to be referred to as the “lock box” and “locking the health record”. Capable clients or their SDM can expressly instruct McMaster University not to collect, use or disclose information from a **particular visit(s)** contained in their health record, the content of their **entire health record**, or the disclosure of their personal health information to a particular health information custodian subject to the requirements of the *Personal Health Information Protection Act* (PHIPA).

Should there be a concern that the client's SDM has made a consent directive request which is not in compliance with section 24(1) of PHIPA which requires the SDM to act in the client's best interests, an application to the Consent and Capacity Board may be made.

Required Disclosures and Permitted Uses

PHIPA both requires and permits certain uses and disclosures of information without client consent, for which a lock-box **will not be effective**.

Required disclosures under PHIPA include:

- reporting to the Ontario Ministry of Health for payment or system planning purposes
- reporting to an authorized registry such as Cancer Care Ontario or the Cardiac Care Network
- responding to a warrant or court order served upon McMaster University for the locked information
- reporting the name of a client being treated for a gunshot wound to the police
- reporting certain diseases to Public Health
- reporting suspected child abuse

Procedure

If a client requests to withdraw consent or place restrictions on the use or disclosure of their personal health information they must be directed to the appropriate regulated health professional.

This protocol applies to all hard copy and electronic health records that McMaster University maintains as, or on behalf of, a Health Information Custodian (HIC).

Although PHIPA permits clients to make a verbal lock box request, it is the practice of McMaster University to obtain this request in writing from the client/SDM.

A lock-box request may request personal health information be locked in the following manner:

- the entire contents of the file (wherever possible); OR
- all documents/reports/notes contained in the file pertaining to visits within a specified time frame (wherever possible).

OR

A client record may be locked from:

- all McMaster University staff or other external health care provider(s); OR
- a specific individual or group of individuals within McMaster University or external to McMaster University (where possible).

The regulated health professional will meet with the client to discuss the request to lock personal health information. The regulated health professional will explain that McMaster University is committed to protecting the privacy, confidentiality and security of all personal health information with which it is entrusted.

The regulated health professional will thoroughly review the locking process with the client to ensure that they understand the potential implications for their future care if their personal health information is not available to healthcare professionals. In this context, the following implications for future care will be reviewed and explained to the client:

- locking a health record may result in time delays during visits;

- locking a health record may prevent staff and physicians from accurately assessing the client's health status, which may result in duplicate diagnostic procedures, or ineffective or insufficient treatment as a result of not having necessary information;
- when the University discloses personal health information to others, it is required to tell them when the information may be inaccurate or incomplete, including when the missing information could affect client care;
- in non-emergency situations, physicians are not obligated to treat a client about whom they have insufficient information;
- locked health information may be used and disclosed in an emergency situation without the express consent of the client, as required or permitted by law.

A signed lock box relates only to personal health information collected retroactively from the date the directive is signed. A lock box cannot be signed for future dated occurrences. Any future visits the requester wishes to lock require a signed lock box after each visit.

After reviewing the *Consent Directive - Express Instructions: Personal Health Information* (the Directive), the client will be asked to verify their identity in accordance with the *Guidelines for Verifying Identity*.

Following verification, the client or SDM will be asked to sign the Directive stating that they understand and accept the possible implications of locking access to their health record. The client will also be asked to indicate on the Directive what part(s) of their health record they wish to lock and the individual(s) from whom they wish to lock the information.

Also following verification, the regulated health professional will notify the treating area and the treating physician in writing that the client has begun the process of locking access to their health information and that no information should be accessed or released without the express consent of the client/SDM.

The regulated health professional will provide the client with a copy of the signed Directive and will ensure that a copy is appended to the client record. The records to be locked are to be removed from the paper chart and placed in a sealed envelope clearly marked – LOCKED CHART AT THE REQUEST OF THE CLIENT – DO NOT RELEASE WITHOUT EXPRESS CONSENT OF THE CLIENT *or* DO NOT RELEASE THIS CHART TO THE FOLLOWING PERSON(S). The locked records contained within the envelope are to be filed in a locked and segregated filing cabinet within the treatment area. A dated Notification Alert, listing the documents which have been removed from the chart, should be appended to the envelope.

If a patient has implemented a lockbox for electronic records, a lockbox message will appear when a user attempts to access the records through the electronic medical record system. A Notification Alert will be on the system and will identify whether all or a portion of the health record is locked. If the lockbox applies to everyone, then the electronic system will restrict access to that patient's record. If a lockbox restriction pertains to specific individuals, their access will be restricted. A list of unauthorized or "locked" persons will appear in the system. It is the responsibility of the regulated health professional to ensure that the password to the locked section of the chart is available in case of emergency.

Following completion of the lock box process, the regulated health professional will notify the client in writing that the request has been completed and that any subsequent request will require a similar formal process.

A client record may be unlocked at the request of the client or SDM. Any such request should be made to the appropriate regulated health professional who will have the client/SDM complete the *Altering Consent Directive- Personal Health Information* form (the Alteration Form). The original of this Alteration Form will be placed in the client record and the client and the regulated health professional will each have a copy. The treatment area will be advised to return the previously locked information to the client record or to regular storage.

A healthcare provider is permitted to access the locked information without the consent of the client in certain circumstances, where in his/her opinion, the access is necessary for the purpose of eliminating or reducing significant risk of serious harm to an individual or group of person. If the healthcare provider decides to unlock a health record s/he must document on the patient's health record the reason and authorization for "breaking" the lock and a detailed rationale must be provided in writing to the University Privacy Officer. Records which have been un-locked in an emergency situation as described above remain locked for all other purposes unless the status is changed at the request of the client/SDM.

The regulated health professional will conduct audits of all mediums of locked records to ensure that there has not been inappropriate access to the locked information. The regulated health professional will report any unauthorized access to locked records to the Privacy Officer, who will treat such unauthorized access as a Privacy Breach.

All activities related to the lock box request will be logged in a file maintained for this purpose by the regulated health professional.

Definitions

Lock box - The term lock-box is not defined in PHIPA. It is not an actual box but a method of describing a client's right under PHIPA to limit the collection, use and disclosure of their personal health information. Within PHIPA, a lock-box is referred to as:

- an individual's right to withhold or withdraw their implied consent for the collection, use and disclosure of personal health information for the purpose of providing health care pursuant to section 20(2) of PHIPA and/or
- an individual's right to expressly instruct a health information custodian not to use and/or disclose personal health information for the purpose of providing health care without consent, in these circumstances where the custodian is permitted to do so;

PHIPA – Personal Health Information Protection Act - means the 2004 (Ontario_ and the regulations made there under;

Record - means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record;

Substitute Decision Maker (SDM) - A substitute decision maker can request to restrict the collection, use or disclosure of personal health information on a client's behalf because the right the request such a restriction exists whether or not a client has capacity. A SDM will follow the same process as the client to request a restriction to the collection, use or disclosure of personal health information.