NorthWest Ontario
Counselling & Consulting

NorthWest Ontario Counselling & Consulting - Virtual Health Care and Lockbox Policy

Ontario's health privacy law, the Personal Health Information Protection Act ("PHIPA"), provides individuals [1] with the right to make choices about, and control how, their personal health information ("PHI") [2] is collected, used, and disclosed.

PHIPA gives clients the opportunity to restrict access to any or their entire PHI by one or more NorthWest Ontario Counselling & Consulting (NWOCC) Team members [3] or by external healthcare providers. Although the term "lockbox" is not found in PHIPA, lockbox is commonly used to refer to a client'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 NWOCC Team understand and fulfill their role when addressing lockbox requests and providing care to clients who have implemented a lockbox. Lockboxes may affect clinical practice for the professionals providing health care at the Agency because access to information about clients may be restricted, and such professionals may be asked not to share PHI with other health professionals inside or outside of the Organization. In addition, this policy will also provide additional information on the safeguards we have implemented for safeguarding and protecting PHI in our possession, and our protocol in the event of a privacy breach.

Requests for a Lockbox

Any current or former client of the NWOCC [4] may request a lockbox to restrict the sharing of all or some of their PHI by one or more NWOCC Team members or by external healthcare providers.

When clients ask about lockboxes, it is important for NWOCC Team members to address their concerns about the confidentiality of their PHI. Note that some clients may want to control who can access their PHI, but may not know to use the term "lockbox." Clients 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, clients may want a lockbox if they ask their health professional or other Team Member:

- Not to tell their specialist that they are being treated at the [insert practice name]
- To exclude certain of NWOCC's 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 NWOCC look at their health record

Clients may initiate the process for a lockbox by contacting NWOCC's Privacy Officer or by speaking to their therapist. Clients must submit their request for a lockbox in writing.

The NWOCC's "Lockbox Policy should be given to clients who want more information. This policy discusses the purpose, implications, and limitations of implementing a lockbox.

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

- Only some of the documents in their health record be locked
- All of their health records 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 healthcare providers not be given their PHI

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

- When clients request a lockbox, it often means they have concerns about their PHI and how it is being used and/or disclosed. Clients should be reminded that:
- NWOCC takes privacy seriously and keeps all PHI confidential and secure
- PHI is only accessed by Team Members on a need-to-know basis
- NWOCC conducts privacy audits regularly to ensure compliance with the policy
- Where PHI is accessed without authorization, appropriate steps will be taken to prevent a reoccurrence and there will be disciplinary consequences

- PHI is disclosed only to external health care providers with whom the client wants their PHI shared (unless the disclosure is otherwise permitted or required under PHIPA without consent or by another law)
- Sometimes a client requests a lockbox when a lockbox is not necessary to resolve the client's concern. For example, a lockbox is not necessary to restrict the sharing of PHI with non-healthcare providers (e.g., family, employers, insurers) because the Agency needs the client's express consent (in writing, as documented by the Agency) to share information with such recipients (unless, for example, a family member acts as the client's substitute decision-maker). If a client does not want the Agency to share information with non-healthcare providers – we will not do so unless there is legal authority to do so.

As another example, if clients 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 lock box to solve their concerns about the accuracy of the information in their health record.

Implications of Implementing a Lockbox

If a client 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 client and to their care. The NWOCC's Privacy Officer or agent should discuss implications and risks with the client. Examples may include:

- The client not receiving the best possible service because healthcare providers may not have access to PHI that they need in order to provide the best possible care in a timely manner.
- The client may have to undergo duplicate tests, procedures and/or health history questions, as applicable, if existing information is unavailable.
- There may be circumstances where clinicians providing health care at the Agency 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 client if there is insufficient information. However, the decision to discontinue care for a client is a significant one and would only be made after thorough consideration of all the relevant information. Clinicians will try to maximize client 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 high-quality client care and to meet their obligations to their regulatory colleges.

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

Decisions to Implement a Lockbox

The NWOCC's Privacy Officer or designate will review, respond to, implement, and administer lockbox requests (including on behalf of a NWOCC Team member, where applicable). Because the choice to implement a lockbox may have implications for the client's care, if applicable, the client's primary NWOCC Team member (e.g. counsellor) must be involved in processing the request as appropriate.

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.

NWOCC's Privacy Officer or designate will notify promptly any client 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 client will be informed of the right to make a complaint to the Information and Privacy Commissioner of Ontario.

Lockbox Exclusions

A lockbox is limited under PHIPA to those providing care to the client. 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 Agency from:

- Obtaining or processing payments
- Planning services,
- Quality improvement,
- Disposing of information,
- Complying with a court order,
- Litigation,
- Research (with research ethics board approval),

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

A lockbox does not prevent a NWOCC Team member or NWOCC 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 NWOCC and NWOCC's Team member 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. Lockboxing does not prevent the Agency from retaining records in adherence to the CRPO and/or OCSWSSW Guidelines, for the minimum retention period required. There may be other circumstances where the use or disclosure of PHI is required or permitted by law. NWOCC's team members will consult with the NWOCC's Privacy Officer when in doubt.

Identifying a Lockbox

Before reviewing a client's PHI, NWOCC's Team must always check to see if a lockbox has been applied.

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

Electronic Records:

If a client has implemented a lockbox:

- A note will be added to the client's chart, indicating the clients' request for lockbox.
- The HIC will confirm that only the HIC and the therapist (agent) have access to the client's chart file in the agency's EMR system, Jane. Other than the HIC and the therapist, the clients' chart file will not be viewable to any other team members.
- If the lockbox applies to NWOCC Team members then the electronic system will restrict their access to that client's PHI.
- When the HIC or therapist (agent) attempts to view the clients' chart file, each entry in the chart file would have an additional title labelled "LOCK BOX" to make it apparent to all viewers that the information contained therein is lock-boxed.

Paper Records:

At this time of policy creation, it is not NWOCC's practice to retain paper records. In the event that NWOCC begins implementing paper records, the following steps will be taken in this case.

- If the entire health record is subject to a lockbox, it will be in a sealed envelope (signed across the seal by a Privacy Officer or designate) with a label affixed to it that reads

"Lockbox" and a "Lockbox Notification Alert" form will be apparent and will include a list of unauthorized or "locked" persons.

- 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 a "Lockbox Notification Alert" form will be apparent and will include a list of unauthorized or "locked" persons.

"Breaking" the Lockbox

If an NWOCC Team member is authorized to access information that is otherwise "locked", the following instructions explain how to access the PHI.

Electronic Record:

Only the HIC and the agent (therapist) would have access to the file. To "break" a lockbox, an NWOCC Team member who does not currently have access would need to request that the HIC have permissions changed to enable access to the clients' chart file. The HIC would only adjust the permissions if it was required to do so by PHIPA, to execute their duties of the HIC or only if this was otherwise permitted or required by law to use or disclose the information (such as in an urgent situation to prevent a significant risk of serious bodily harm). Only then would permissions be changed and access to the health record be made available to the team member.

Each entry in the chart file would have an additional title labelled "LOCK BOX" to make it apparent to the viewer that the information contained therein is lock-boxed.

Paper Record:

At this time of policy creation, it is not NWOCC's practice to retain paper records. In the event that NWOCC begins implementing paper records, the following steps will be taken in this case.

To "break" a lockbox, an NWOCC Team member would open the sealed envelope and remove the paper records. Access to the health record is then available.

Any NWOCC Team member who accesses PHI that is protected by a lockbox must document on the client's health record the reason and authorization for "breaking" the lock. All information subject to a lockbox will be monitored and there will be random audits of such

files. If an NWOCC Team member is in doubt about whether they are legally permitted to break a lockbox, they should contact NWOCC's Privacy Officer.

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 client 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 Healthcare Providers

If a client's lockbox instructions state that the client does not want all or some PHI shared with an external health care provider, the Agency 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 client or to another person or persons)
- The external healthcare provider has provided us with written proof of the client's express consent to the disclosure.
- If NWOCC is prevented from disclosing PHI relevant to the provision of care to an external health care provider because of a lockbox, the Agency has an obligation to notify the receiving health care provider that not all the relevant PHI has been provided. As a note, the receiving healthcare provider is then able to explore the matter of the "locked" information with the client and seek consent to have the locked information shared.

Audits

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

Safeguards for the Protection of PHI

Listed below are various safeguards that we have implemented to protect PHI in our possession and control. We regularly review these safeguards to ensure that we are doing all that we can to protect PHI.

1. Technical safeguards:
    - only NWOCC pre-approved email, messaging, or videoconferencing accounts, software, and related equipment that comply with industry standards are used.
    - our staff will avoid the use of CC or BCC features when sending emails, as a means to avoid an accidental breach through accidental CC.
    - we utilize firewalls and protections against software threats. We encourage all of our staff to implement adequate firewall and antivirus protection on their electronic devices.
    - when accessing NWOCC email, or access to our EMR software system, our team members will only use secure, password-protected internet or wifi. Our team members will not use public or insecure WIFI networks when accessing anything related to clients.
    - we regularly update our software applications with the latest security and anti-virus software. Our EMR software system has regular updates, and our team member is urged to regularly update their electronic devices.
    - we encrypt data on all mobile and portable storage devices, both in transit and at rest. All of our team members use encrypted electronic devices.
    - we maintain, monitor, and review audit logs. Our Privacy Officer conducts regular audits, keeps an up-to-date audit log.
    - we use and maintain strong passwords. All electronically stored PHI in our possession and control is password protected.
    - we review and set default settings to the most privacy-protective setting. Jane Settings are set for enhanced privacy and Agents are encouraged to adjust privacy settings on their electronic devices.

2. Administrative safeguards:
    - we ensure our team members are properly trained to use secure email, messaging, and video conferencing platforms.
    - we ensure our team members are well aware of their ongoing obligation to avoid collecting, using or disclosing more PHI than is necessary
    - we ensure confidentiality agreements contain explicit provisions dealing with our team members' obligations when using secure email, messaging, or videoconferencing to deliver virtual healthcare
    - all email communication between our team members and clients is done through our own domain, and includes a confidentiality statement outlining the privileged nature of the information, intended only for the recipient, the process for destroying information

should it be the incorrect recipient and lastly, that sensitive information should not be shared via email.

- to minimize the use of PHI, our team members use, wherever possible, client initials or their EMR software system ID instead of identifying information such as names, phone numbers etc.
- we recommend clients use a password-protected email address that only they can access.

3. Physical safeguards:

- we keep all technology containing PHI, such as desktop computers and servers, in a secure location
- we keep portable devices containing PHI, such as smartphones, tablets, and laptops, in a secure location, such as a locked drawer or cabinet, when they are unattended
- we restrict office access, use alarm systems, and lock rooms where equipment used to send, receive or store personal health information is kept
- we do not lend technology containing PHI to anyone without authorization
- we ensure there are no unauthorized persons in attendance or within hearing or viewing distance
- any physical copy of PHI that is not electronically stored will be physically locked away when not in use.

4. Additional safeguards for video conferencing

- As a best practice, our team members will join videoconferences from a private location using a secure internet connection. This includes using a closed, soundproof room or an otherwise quiet and private place and having window coverings where and as appropriate. We use headphones rather than speakers on our devices to prevent being overheard by others, and we are mindful of where screens are positioned.
- Once logged into the videoconference, our team members check the meeting settings to ensure the meeting is secure from unauthorized participants. At the start of the video conference, our team members verify the identity of the client, inquire if anyone is accompanying the client, and confirm the client's consent.
- When videoconferencing, our team members use sufficiently high-quality sound and resolution to ensure they can collect information (including verbal and non-verbal cues) that is as accurate and complete as is necessary for providing health care.

Privacy Breach Protocol

In the event that there is a privacy breach, NWOCC has a comprehensive privacy breach protocol that involves four steps, generally outlined below. It is our commitment to ensure that all PHI remains confidential and is collected, used, disclosed and disposed of properly to the best of our abilities, however; in the unlikely event that a privacy breach does occur, we will adhere to our privacy breach protocol to ensure a timely remediation of said breach. If a privacy breach is suspected or known to have occurred, we will take the following actions:

Step 1: Ensure our team members are informed of the breach. We will:

- notify all relevant team members of the breach, including our Privacy Officer and determine who else from within our organization should be involved in addressing the breach,
- consider whether the Privacy Commissioner must or should be notified by reviewing the Commissioner's notification guidelines available at https://www.ipc.on.ca/wp-content/uploads/2019/09/2019-health-privacy-breach-notification-guidelines.pdf,
- prepare and maintain and formal report of all privacy breaches, and
- develop and execute a plan designed to contain the breach.

Step 2: Contain the breach. We will:

- attempt to retrieve any physical documents containing PHI disclosed due to the breach,
- verify whether any copies of these documents were made, and attempt to retrieve those copies,
- take steps to prevent any further unauthorized access to PHI stored electronically (e.g., restrict access, change passwords, temporarily shut down system).

Step 3: Notify affected individuals (consult with Privacy Officer or the HIC to decide who will inform). We will:

- consider the most appropriate way to notify affected individuals in light of the sensitivity of the information (e.g., by phone, in writing, at the next appointment),
- provide the contact information of our (Privacy Officer of HIC) in case affected individuals have further questions,
- inform all affected individuals if we have reported the breach to the IPC, and
- inform all affected individuals that they are entitled to make a complaint to the IPC and provide contact information for them to do so.

Step 4: Our Privacy Officer or HIC will further Investigate and remediate the problem.

- an internal investigation will be conducted by our Privacy Officer or HIC,
- a determination of what steps should be taken to prevent future breaches (e.g. changes to policies, additional safeguards required) will be made by our Privacy Officer or HIC,
- we will report the results of the investigation to any relevant regulatory Colleges if appropriate or required, and
- we will ensure our staff is appropriately trained to protect and safe PHI and conduct further training if required.

[1] It is possible that we hold PHI about individuals who are not clients or who are former clients, 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 client's health record and we have used "health record" interchangeably with PHI throughout the policy. It is possible that NWOCC 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 "NWOCC Team members" – but this policy applies to NWOCC, NWOCC's staff, volunteers, students, researchers and vendors.

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