Policy Name:	Client Records, Confidentiality and Disclosure Policy
Originating:	Chapter 2: Program and Administrative Components
Approval Authority:	Board of Directors
Date of Approval of Original Policy:	September 04, 2012
Last Updated:	June 08, 2020
Mandatory Revision Date:	March 2024
Contact:	Privacy Officer

Policy

Hope Place Centres (HPC) is committed to protecting the privacy of personal information and is compliant with the Personal Health Information Protection Act (PHIPA), 2004, set out by the Government of Ontario. HPC shall ensure that the security and confidentiality of personal information is made a top priority.

Accountability

HPC is responsible for the personal information that it collects, holds, uses, discloses and destroys. HPC shall do what is deemed reasonably possible to ensure that personal health information is up-to-date, accurate and secure. HPC believes in privacy and confidentiality and is accountable to all those who access its services. As such, HPC shall appoint a Privacy Officer who is responsible for monitoring privacy, as well as HPC's compliance legislation. The Privacy Officer shall be appointed by and report to the Board of Directors. HPC shall ensure that the appointed Privacy Officer has the appropriate training necessary, in order to carry out the duties and responsibilities of the position. HPC shall ensure that the position holds a certain amount of authority in which to monitor compliance, manage complaints and alter privacy policies and procedures, as deemed necessary.

The duties and responsibilities of the Privacy Officer include:

- Ensuring compliance with legislation regarding privacy and confidentiality
- Creating and implementing policies and procedures dealing with privacy
- Training all staff and students on the privacy policies and procedures, including any changes made to the policies and/or procedures
- Monitoring and reporting compliance related to privacy and confidentiality
- Reporting non-compliance with the privacy policies and procedures to the Board of Directors
- Resolving conflicts and challenges to compliance
- Maintaining up-to-date knowledge of legislation dealing with privacy and confidentiality
- Being HPC's contact regarding privacy for its clients as well as the public
- Liaising with the Ontario Privacy Commissioner's office and government agencies

HPC shall ensure that the Privacy Officer is accessible to its clients and the public. HPC shall post on the HPC website under the Privacy link how to contact the Privacy Officer. The Privacy Officer's contact information shall be given to any persons upon request.

Identifying Purposes

HPC shall collect, use and disclose only the amount of information that is reasonably necessary to meet the purpose of providing quality services. This does not include personal information that is required by law. In the event that HPC requires the use of personal health information other than its intended purpose, the individual shall be asked for written consent and shall be given the exact nature of the use or disclosure. HPC collects and enters personal information into a province-wide electronic database registration system. The registration system is called Drug and Alcohol Treatment Information System (DATIS) which is a program that contains personal health information along with other personal information used to provide service to an individual. If individuals have any questions relating to the purposes of collection, use or disclosure of personal health information, they can be directed to the Privacy Officer who shall answer any questions they may have. DATIS is used to identify clients that have been registered for one or more of HPC's programs.

Consent

HPC shall obtain consent, either written or implied consent, when collecting, using, disclosing or destroying a client's personal information except in circumstances where the law does not require consent. The following circumstances are either permitted or required by law:

- Responding to a subpoena;
- Preventing serious injury to self or others (Duty to Warn under common law);
- Reporting communicable and reportable diseases (required under the Health Protection and Promotion Act);
- Suspected child abuse or neglect (required under the Child and Family Services Act);
- Suspected elder abuse;
- Health conditions that make it dangerous for an individual to drive (required by the Highway Traffic Act);
- Health conditions that make it dangerous for an individual to fly an airplane or to perform the duties of an air traffic controller (required by the Aeronautics Act);
- Sexual abuse by a regulated professional under the Regulated Health Professions Act (client consent is required for the disclosure of the client's name as required by the Regulated Health Professions Act);
- Termination or suspension of employment, for reasons of professional misconduct, incompetence or incapacity (as required by the Regulated Health Professions Act);
- When consent cannot be obtained in a timely manner and disclosure is reasonably necessary for the provision of health care.

There are four elements to consent which are set out by the Personal Health Information Protection Act (PHIPA), 2004 that HPC abides by:

1. Consent must be given by the individual. The information which is being collected, used or disclosed must be given consent by the individual to whom the information pertains or to a substitute decision-maker who has the best interests of the individual in mind.
2. Consent must be knowledgeable. The individual must be aware of the reasons for collection, use or disclosure and be aware of the option of giving or withdrawing/ withholding consent.
3. Consent must relate to the information collected, used or disclosed. Consent cannot be obtained for another purpose and be applied to any other information.
4. Consent must not be obtained through coercion or deception. The purpose of consent needs to be transparent.

In order for a substitute decision-maker to give consent on behalf of another, the individual must not be able to do the following:

- Understand information that is relevant to choosing to consent or not to consent to the collection, use or disclosure;
- Understand reasonable foreseeable consequences of giving or not giving, withdrawing or withholding consent.

In the event that an individual withdraws or withholds consent, the Privacy Officer must be notified and the withdrawal/withholding of consent must be recorded directly in the individual's file. Withdrawal/withholding of consent shall not be backdated but is effective as of the date it is signed.

Consent shall either be informed consent, where consent is specifically asked for or implied consent. ***Informed consent*** is specifically requested and shall be used for disclosure of personal information of any nature to any third party, unless it is required by law.
Implied consent shall be used when a person contacts HPC for service(s) and personal information is collected, held and used for these services. It is assumed that by contacting HPC, that an individual is giving HPC consent to collect, use, and hold personal information, unless otherwise stated.
HPC shall inform clients about DATIS, by sharing that their information is used to create statistics for reporting purposes and that no specific identifying information is used in creating the statistics.
Clients have the right to refuse to have their personal information from being entered into DATIS. In the event that a client has refused their information being entered, HPC shall not refuse them service and shall report that there was a refusal, in order for DATIS to monitor the number of refusals.

Limiting Collection
HPC requires that personal information be collected in order to provide quality services and to meet funders' requirements. HPC shall only collect information which is necessary to provide these services.
HPC may indirectly collect personal information for the following reasons:

- The individual consents to the collection;
- The information which is being collected is reasonably necessary for providing healthcare and it is not reasonably possible to directly collect the information from the individual;

- The information being collected is required by law.

HPC may collect information directly from the individual, even if the individual has a substitute decision-maker, if the information is reasonably necessary in order to provide healthcare and consent cannot be obtained within a reasonable time. In all other circumstances not listed above, consent shall be required for the collection of personal health information. HPC shall only have trained staff members and in some circumstances trained students, collecting personal information. HPC shall create an individual client file for every client that is registered in one or more of HPC's programs. In the client's file there shall be identifying information, including but not limited to A DATIS number, (in the event that a client refuses to have their information entered into DATIS there shall be no DATIS number), a client number that is given to the client upon registering for an HPC program. The HPC client number (DATIS number) shall remain with the client for the entire time accessing services. The creation of the individual client's file is the responsibility of the Admissions Department at both of HPC's 'live-in' sites. At the Community Treatment Centre site, it is the responsibility of the Case Manager who is going to serve that client to create the client file.

Limiting Use, Disclosure and Retention

Limiting Use

HPC shall only use the personal information it collects for its intended purpose. Should another purpose arise for the use of an individual's personal information, HPC shall obtain consent from the individual before using their personal information, unless its use is required by law. Only HPC staff members, including qualified students, shall use personal information. Outside service providers, shall not use any personal information that they may come into contact with while providing service to HPC. All outside service providers shall sign a Confidentiality Agreement.

An individual has the right to withdraw or withhold consent for HPC to use personal information. To ***withdraw*** consent means that consent has been granted, but later terminated, effective as of a certain date. To ***withhold*** consent means that consent was never granted by the client. This withdrawal or withholding consent shall be recorded in the individual's file and the Privacy Officer shall be notified.

Limiting Disclosure

HPC shall only disclose personal information to those named, once consent has been obtained from the individual or their substitute decision-maker. Only staff members, involved in providing services, shall disclose personal information. Outside service providers shall not disclose personal information that they may come into contact with while providing service to HPC. All outside service providers shall sign a Confidentiality Agreement. HPC shall not disclose any personal information in the event an individual has instructed HPC not to make a disclosure.

If the disclosure is considered reasonably necessary in order to provide the individual with healthcare, and consent cannot be obtained within a timely manner, HPC shall disclose only information that is necessary to carry out the healthcare being provided. HPC shall disclose personal health information in non-identifying form to the appropriate Minister or Local Health Integration Network (LHIN), only for the

purpose of funding or payment of Ministry provided service(s). In the event that an individual is injured, ill or incapacitated and is unable to give consent themselves, HPC shall disclose only that which is necessary to a relative, friend or potential substitute decision-maker of the individual. HPC shall disclose personal information about an individual, if the individual is deceased or reasonably suspected to be deceased for the following reasons:

- In order to identify the individual;
- To inform those to whom it would be reasonable to inform in the event that an individual is deceased or reasonably suspected to be deceased and/ or the circumstance surrounding the death, if appropriate;
- HPC shall disclose to the spouse, partner, sibling or child receiving the information what is reasonably required, in order to make decisions about the healthcare of themselves or their children

HPC shall disclose personal information if there is reasonable grounds to believe that an individual poses a significant risk of bodily harm to themselves or others. HPC shall disclose personal information to the appropriate authority in the event that an individual is being lawfully detained or to the person in charge of a psychiatric facility where an individual is being lawfully detained under the Mental Health Act. HPC shall disclose personal information in the event that a staff member is summoned or subpoenaed by the appropriate authorities to provide said personal information. HPC shall disclose personal information to the appropriate authorities for the purposes of determining capacity to consent. HPC shall use a Circle of Care Agreement and/or Consent to Release Personal Information, in order to obtain consent to disclose information, while a client is accessing services. This Agreement shall outline the following:

- The HPC site that is being given authorization to disclose information;
- The name of the individual that is consenting to the disclosure;
- The person(s) that information can be released to: contact name, phone and/or fax number and/or mailing address and/or email address (*as appropriate);
- The person(s) that information can be exchanged with: contact name, phone and/or fax number and/or mailing address and/or email address (*as appropriate);
- The person(s) that information can be obtained from: contact name, phone and/or fax number and/or mailing address and/or email address (*as appropriate);
- The specific information that is consent applies to or that is prohibited for release by HPC: attendance, progress reports, clinical case notes, medical information and/or other (please specify);
- The specific purpose of the disclosure: evaluation, assessment and/or coordinating treatment efforts;
- The beginning and the end of the time period in which the Agreement is active.
- Both the client and a witness shall sign and date the Agreement

The Circle of Care Agreement and/or Consent to Release Personal Information will be placed in the client's file.

HPC is dedicated to protecting its client's privacy and confidentiality. HPC recognizes and respects that individuals have rights pertaining to their personal information. In the event a client wishes to

withdraw/withhold consent, there is a form called Withdraw/ Withhold Consent that shall be explained and filled out with the client. Staff must explain and complete the following:

- Explain to the client the reasonably foreseeable consequences of withdrawing, withholding, limiting use and/or disclosure of personal information;
- Withdrawal is taking away consent that was previously given and withholding is having not given consent at all.
- Complete the Withdraw/Withhold Consent form with the client; both staff and client sign and date the form.
- If the file is closed, place the information in a manila envelope, seal it and attach the Withdraw/Withhold Consent form to the outside.
- If the file is open, place the information with the progress notes and attach the Withdraw/Withhold Consent form to the information.
- Explain to a third party (in person, by phone, or in writing) and/or other staff member(s) who are requesting the information, that some or all of the requested information is being withdrawn/withheld by the client.
- Document all interactions/ conversations pertaining to this withdrawal/withholding of consent in the client's file.
- The specific instructions shall be communicated to all staff involved in the client's care and a copy of the Withdraw/Withhold Consent form shall be sent to the Privacy Officer to be kept in a secure filing cabinet.

In the event that information is required by law or is necessary to prevent or reduce significant risk of serious bodily harm to themselves or another person and a client has given specific instructions not to disclose, HPC shall provide only that information which is required by the law or for the safety of the client and/or another person. Staff must complete the following:

- Disclose the personal information to the third party or staff member that is required by law or that is necessary to prevent or reduce the risk of bodily harm to self or others;
- Document the disclosure and the circumstances for it in the client's file;
- Contact the Programs & Services Manager and the Privacy Officer to inform them of the situation.

In addition to the above documentation, there shall be a Tracking System – Withdraw/Withhold Consent Checklist in the client's file. This is to ensure all of the appropriate steps have been taken to protect the client's rights and requests and that all of the legal obligations of the staff member(s) have been fulfilled. A copy of this Tracking System Checklist shall be sent to the Privacy Officer and kept in a secure filing cabinet.

Retention

HPC shall keep client files for ten years after the date of the last entry in the file, and after it is reasonable to believe that a client can no longer use any information within their file. This includes the date that a client requests information: it is 10 years after this date that the file can be destroyed. The client file shall be deleted, destroyed, shredded and disposed of in a manner that maintains the client's privacy and confidentiality. The destruction of a client's physical, paper file, will be conducted at the site where the

file is located, under the authorization and supervision of the Privacy Officer and/or designate. The client's physical, paper file, including the file folder, is to be destroyed by a cross-cut shredder. Upon shredding, the client's full name will be placed on a secure list on the HPC server that contains the date of the last entry in the file, as well as the date the shredding occurred. The deletion of a client's electronic, virtual file, will be conducted from any HPC location, under the authorization and supervision of the Privacy Officer and/or designate. The client's full name will be placed on a secure list on the HPC server that contains the date of the last entry in the file, as well as the date the deletion occurred. At the outset of providing services, HPC shall inform clients of how long their file shall be kept and how it will be deleted and/or destroyed.

Exchanging Information

HPC is a team oriented environment, meaning that staff members at each site exchange personal information about clients, with each other, in order to provide quality services. At HPC's Community Centre site, information is not exchanged with any co-located agencies/services, without the client's signed consent. Information is not shared with any internal service providers without signed consent. Personal information is only shared if it is required in order for other staff members to provide quality service to the client. Personal information is shared through written, verbal or electronic methods that maintain client privacy and confidentiality. Upon hiring, each staff member signs an Acknowledgement Form which specifically addresses confidentiality, ethics, privacy, duty to report as well as other relevant situations. In the event that a staff member must call a supervisor on the telephone, personal information shall be shared only if it is absolutely necessary to make a decision regarding care for the client. At HPC's Community Centre site, personal information may be relayed from this site to the women's 'live-in' site and vice versa, in order to provide quality care and make referrals to either site, in the event that both sites have a mutual client. Staff members who are sharing personal information about a mutual client may share through fax, phone, face-to-face, the HPC server or HPC's internal e-mail. Only information that is necessary to provide quality service to the client shall be shared.. Personal information shared amongst staff members or across sites shall be used only for the purposes that it was collected, unless required by law.

Accuracy

HPC shall strive to ensure that personal information is accurate to the best of staff members' abilities. Should a client move, change phone numbers, or change names for whatever reason, it is the client's responsibility to inform HPC. It is the staff member's responsibility to update the client's file and DATIS.

Safeguards

HPC shall take the necessary steps to protect the personal information it holds, whether it is physical, paper records or electronic, virtual records, from loss, theft, unauthorized use, disclosure, alterations, copying or destruction. Access to personal information shall be limited to those who are involved in providing services.

Data entry into DATIS is conducted by the following staff members:

- Admissions Department and those who conduct telephone screening or intake
- Case Managers; Support Workers – including Overnight and Peer Support Workers
- Students
- Programs & Services Managers

Board Members, staff, students, and clients shall all sign Confidentiality Agreements.

The Client Confidentiality Agreement shall clearly state:

- HPC's Confidentiality policy;
- How client files shall be kept, who has access to them, how long they will be kept, how and when they will be destroyed;
- The requirement of consent for disclosure, except obligations that are required by law;
- That the client agreed to keep fellow client's information confidential outside of HPC;
- Requirements to ensure client is capable of providing consent.

The client's Confidentiality Agreement shall be placed in the client's file after it has been signed and witnessed. All hardcopy information shall be kept in secure locked filing cabinets at whichever site the client is receiving services. All electronic information shall be on password protected computers on the HPC server and accessed by only those involved in providing service to the client. All electronic information shall be backed-up in accordance with data protection and maintenance standards, as prescribed in current policy/procedures of the integrated IT service provider partnered with HPC. Remote long-in access to the HPC server is restricted to personnel that have been specifically authorized by the Privacy Officer, and it can only be accessed through third party secured internet portal, which provides end-to-end data encryption and requires an added level of user authentication and firewall protection. The HPC server becomes inactive after security-specified period of inactivity, and requires repeat of user authentication process before it will restart. All records containing personal information shall be destroyed in a manner which maintains privacy and confidentially. When HPC replaces or disposes of a computer it ensures that all the data, including personal information is securely deleted. In the event that personal information is accessed by unauthorized persons, is lost, stolen or destroyed, HPC shall immediately notify the individual(s) who has been affected. The notification will be made informally in the most expedient manner (phone and/or text and/or internet), as well in writing, with a formal letter sent by courier/registered mail to the last address for client on record with HPC. The Privacy Officer shall be notified of the breach that has taken place and shall take the necessary steps in order to investigate, resolve, remediate (if possible) and report the outcome.

Openness

HPC believes in transparency and shall make a written statement regarding HPC's Privacy Policy available to the public. This shall be posted on HPC's website under the Privacy section and at each of HPC's three sites. A hard copy shall be made available upon request. The written statement to the public shall include:

- A description of HPC's information policies, procedures and practices;
- How to contact the Privacy Officer;
- How to access one's own personal file;
- The process of correcting incorrect information within one's personal file;
- How to make a complaint regarding compliance with HPC's Privacy Policy and legislation regarding privacy and confidentiality.

The Privacy Policy is available at www.hopeplacecentres.org and click on Privacy.
For more information on openness regarding HPC's privacy policy please contact the organization's Privacy Officer.

Access

Hope Place Centres believes (HPC) that clients have the right to ask to see a record of their file. HPC believes that for some clients this may be a detriment to their progress. Clients are not permitted to review their file without permission of a Programs & Services Manager or CEO. Clients who request permission to see their file are directed to submit a written request to a Programs & Services Manager. A Programs & Services Manager shall make an individual's file available upon request, unless there are reasons to deny such request including:

- The information within the file may cause potential harm to the recovery of the individual or cause bodily harm to self or others;
- May lead to the identification of an individual who provided information that was either required by law or given explicitly or implicitly and shall break the confidentiality of said individual;
- The file contains information that was collected or created for reasons of the law and all proceedings have not been concluded;
- The file cannot be found after a reasonable search;
- If there are reasonable grounds to believe that the request is frivolous, vexatious or made in bad faith. For more information, see PHIPA, 2004.

If a Programs & Services Manager has refused an individual's request he or she shall give a written notice to the individual, stating the reason for refusal and stating that the individual is entitled to make a complaint regarding the refusal to the Ontario Privacy Commissioner. The Programs & Services Manager shall give a response to the individual requesting access to their file, no later than 30 days after receiving the request. The time for granting access, may be extended to no more than an additional 30 days, for a total of 60 days after receiving the request. These additional 30 days are permitted if;

- The individual's request for access would interfere with the daily duties of the Programs & Services due to the amount of information to be located necessitating a lengthy search.
- The time required to complete the necessary consultation within the first 30 days would not be reasonable.

In the event a Programs & Services Manager has granted an individual's request to access their file, an individual can examine their file with the Programs & Services Manager present, who shall be there to explain any term, abbreviation or codes used within the file, or answer any direct questions immediately. An individual can request to retain a copy of their file, which shall be granted if it is reasonably practical. This request must be made to the Programs & Services Manager in writing and is subject to refusal based on the reasons for refusal of access. If an individual believes that their file is inaccurate or incomplete for the purposes for which the information was collected, used, disclosed or kept, then the individual may request in writing to the Programs & Services Manager for the information to be corrected. The Programs & Services Manager, after no more than 30 days, shall respond in writing to the individual requesting correction, whether the request has been granted or refused. An extension of 30 days, for a total of 60 days, shall be requested by the Programs & Services Manager if, replying to the request within 30 days would:

- Interfere reasonably with the Programs & Services Manager's daily activities;
- If the time to complete the necessary consultation within in the first 30 days would not be reasonable.

Reasons for refusal to correct the information include:

- The Programs & Services Manager was not the individual to create the original file and does not have sufficient information, knowledge or expertise to correct the file.
- The file consists of a professional opinion or observation that has been made in good faith about the individual.

Upon granting an individual's request for correction to their file, the Programs & Services Manager shall make said correction(s) by striking out the incorrect information in a manner that does not obliterate the information. If this is not possible, the incorrect information shall be labelled as incorrect and removed from the file, stored separately and a link shall be maintained that allows the incorrect information to be traced. If it is not possible to make the correction(s) in the individual's file then there shall be a practical system in which to inform a person who accesses the information that it is incorrect and the way in which to access the correct information. Once a correction has been completed according to a granted request, the Programs & Services Manager shall give written notice to the individual that the correction(s) have been made.

At the request of the individual, the Programs & Services Manager shall, within reason, contact those to whom the incorrect information was disclosed and provide them with the correction(s) to the information. Unless the correction(s) cannot be reasonably expected to have an effect on the ongoing provision of healthcare or provide other benefits to the individual, no attempt will be made to contact those to whom the incorrect information was given. In the event that a refusal has been made regarding correcting incorrect information, the Programs & Services Manager must prepare a written statement of disagreement that outlines the correction(s) that have been refused. This statement of disagreement shall be attached to the individual's file and shall become a part of the file. When information relating to this statement of disagreement is disclosed, the statement shall be a part of the disclosure. The Programs & Services Manager shall make all reasonable efforts to disclose the statement of disagreement to any

person who would have been notified if the correction(s) had been granted. The individual has a right make a complaint about the refusal to make corrections to the Ontario Privacy Commissioner.

Challenging Compliance

HPC is dedicated to protecting the privacy and confidentiality of its clients. Should an individual feel as though their privacy and/ or confidentiality has been compromised, HPC shall guide the individual in the process of challenging compliance with HPC's Privacy policy and PHIPA, 2004. Should any question or complaint arise regarding privacy or confidentiality an individual shall be directed to contact HPC's Privacy Officer. In the event that the appointed Privacy Officer cannot answer the question or deal with the complaint then the Privacy Officer shall direct the individual to the Board of Directors. If the complaint has not been resolved, then the Privacy Officer shall direct the individual on how to contact the Ontario Privacy Commissioner to make a complaint or to challenge HPC's compliance.