Kitchener Downtown Community Health Centre

Type of Policy:
[] Administration (A)
[] Financial (F)
[] Board of Directors (B)
[] Human Resources (H)
[] Information Systems (I)
[] Occupational Health and Safety (S)
[] Volunteers (V)

Client Services
[X] General (CG)
[] Programs (CP)
[] Medical Services (CM)

Policy No.: Client Privacy

Title: CG0403

Policy

In order to provide clients with the services and supports the Kitchener Downtown Community Health Centre (KDCHC), will require personal information. KDCHC will work to respect the privacy and confidentiality of any information we have. Any information we have about a client is protected by this policy.

Clients who have questions about our Privacy Policy or practices or would like to review or correct personal information can contact the Privacy Officer at (519) 745-4404 or cadams@kdchc.org.

For the purpose of this policy "client" is defined as anyone who receives services from KDCHC for which they must provide personal information and for which KDCHC must document the service delivery.

Clients will be supported by staff to help them understand this policy or to file a privacy complaint. Clients are welcome to ask staff for assistance as needed.

This policy will be posted on the KDCHC website.

Definitions

Agent: Individual that acts on behalf of the health information custodian (KDCHC) in respect to the personal health information that is collected, used or disclosed

Consent Directive: Direction provided by the individual to withhold or withdraw, in whole or in part, his or her consent to the collection, use or disclosure of the personal health information in the electronic health record

Consent Override: A health information custodian (HIC) or agent of the HIC seeks to collect personal health information in the electronic health record that is the subject of a consent directive

Program Office: The organization that manages and delivers a shared program or system (e.g. eHealth Ontario is the program office that operates the ConnectingOntario program)

Personal Health Information

Personal health information is any identifying information about clients that is verbal, written or electronic form. Clients do not have to be named for information to be considered personal health information. Information is "identifying" if a person can be recognized, or when it can be combined with other information to identify a person. Personal health information can also be found in a "mixed record" which includes personal information other than that noted above.

The purpose of the collection, use or disclosure of personal health information by the health information custodian (KDCHC) must be for the provision of health care or assisting in the provision of health care to the individual.

Identified Purposes – Why We Need Information

We use personal information to:

- Provide clients with primary care services and treatments, including referrals
- Provide personal and community health promotion services
- Decide who can use our services
- Prepare general reports for the Ontario Ministry of Health and Long Term Care ()
- Meet any legal or regulatory requirement
- Communicate with clients

Collection – Who We Get Information From and Why

When we can, we get information about a client directly from that client. With a client's consent, we may collect information from others such as other health care providers.

Only information from external sources (e.g. shared electronic health record systems) that is collected, used or disclosed for the purpose of providing or assisting in the provision of health care to the individual to whom it relates can be considered as implied consent.

Information received from third parties (eg employer, insurer, educational institution) is not considered to be received with consent of the client unless a signed consent to release information form is received with the information.

We collect only the personal information we need to provide a client with the services they want. We collect personal information only by fair and lawful means.

Consent – Is It OK For Us To Get and Use Information?

For a definition of types of consent, please see KDCHC Policy #CG1301 Consent to Medical Primary Health Care Services.

We will ask clients if it is OK for us to collect, use and share their personal information. We will answer any questions, and provide an interpreter if necessary, so that clients can understand the consent that they are being asked to give.

If a client voluntarily supplies personal information to KDCHC (e.g., request for eligibility screening to become a client), we believe that they are giving us consent to use that information for the purpose for which it was given.

A custodial parent or legal guardian may give consent and provide information about their child. A legal guardian may give consent and provide information for a person who does not have the capacity to give consent.

KDCHC as an organization serves our clients health needs. Because of this, it is necessary for information about clients to be shared among the staff. Staff will only use the specific information that they need to do their job.

All client inquiries related to how KDCHC may contribute or obtain information from provincial repositories (e.g. ClinicalConnect) will be directed to eHealth Ontario. KDCHC will provide the responsible program office's Privacy Department with supporting information to respond to inquiries or complaints within 14 days of request.

Documenting and Tracking Withdrawal of Consent

Individuals are permitted to block personal health information provided to particular individuals or organizations including staff at the KDCHC. This means the individual expressly withholds or withdraws consent for release of personal health information. This might include an item of information or their entire record. This is referred to as a "lock-box" provision.

If the client requests that personal health information not be forwarded to particular individuals or organizations, and the provider agrees, the provider must:

a) explain to the client the reasonably foreseeable consequences of a refusal to consent to the disclosure
b) if the provider feels the third party needs the information, advise the third party or staff member of KDCHC (in person, by phone or in writing) that some relevant information has been withheld at the direction of the client. This is what is called the "lock-box provision" and the Withdrawal of Consent Form is completed – see form on next page.
c) note conversations in the client's chart

The receiving health information custodian or staff member of KDCHC may choose to explore the matter of the "locked" personal health information with the individual and seek consent to

access and use that information. If the client informs the third party or staff member at KDCHC that the client agrees to have the information "unlocked":

a) the disclosing health information custodian would need to obtain the written consent of that individual to then disclose the locked information.

If the provider believes that disclosure is necessary to eliminate or reduce significant risk of serious bodily harm to a person or persons, he/she must:

a) disclose personal health information to the third party or staff member of KDCHC
b) note disclosure and circumstances surrounding it in client's chart and, if appropriate, inform the client that disclosure has occurred

If the withdrawal of consent involves a shared electronic health record system, the request will be forwarded to the Privacy Officer who will:

Confirm the client is aware of the consequences of a consent directive

Complete a Consent Directive Request form will be submitted to the responsible program office (e.g. eHealth Ontario) within 4 days of the client request; Agent-level consent directives will be forwarded to the program office within 7 days of consent directive validation

Once the consent directive is applied by the program office, provide written notification to the client confirming the consent directive was applied and its date of application

Document in KDCHC's Consent Directive log and ensure a copy of the notification is stored in the client's medical record

Should a patient wish to place a consent directive on personal health information contributed to the shared system by a health information custodian other than an agent of KDCHC the Privacy Officer will redirect the individual to the responsible program office.

Personal health information collected as the result of a consent override in a shared system may only be used for the purpose for which the override occurred. Express consent must be obtained from the client when completing a consent override unless there is risk of harm to self or others. Printed documents that are added to the client record should include a label that the information is not to be used or disclosed for other purposes.

Should a KDCHC staff member complete a consent override they must follow the process, as identified by the system. If a staff member completes a consent directive override, the program office will notify KDCHC's Privacy Officer who will:

Follow up with the staff person who completed the override to confirm that it was appropriate

Work with the program office to provide timely notification of the override to the client, if appropriate, and document the notification

Where a consent directive override is completed to prevent risk of bodily harm to other individuals, notify the IPC/O. This notification should not include identifying information of the client or other individual(s)

Information required by law (eg Family and Children's Services) cannot be blocked by a client.

Note: This information is based on the requirements of the Personal Health Information Protection Act (PHIPA).

SAMPLE WITHDRAWAL OF CONSENT FORM

Information Tracking System - Withdrawal of Consent to Disclose to Outside Providers ("lock-box" provision)

Based on the Personal Health Information Protection Act, 2004

Individuals are permitted to block, at least partially, personal health information which may be perceived negatively by a third party or staff member at KDCHC. This means the individual expressly withholds or withdraws consent for release of some or all of their personal information.

If the client requests that personal information not be forwarded to a third party or staff member of KDCHC, and the practitioner agrees, the practitioner must:

✓		Task	Date / Initials
	1.	Explain to the client the reasonably foreseeable consequences of a refusal to consent to the disclosure	
	2.	Place a label on the front of the chart saying "See special info sharing instructions"	
	3.	Notify the Privacy Officer directly or advise the client to contact the Privacy Officer who will initiate a lock-box request	
	4.	If the client does not allow the release of some information to a third party, or staff member of KDCHC, and the practitioner feels the third party needs the information that has been excluded, the practitioner advises the third party or staff member of KDCHC (in person, by phone or in writing) that some relevant information has been withheld at the direction of the client. This is what is called the "lock-box provision"	
	5.	Note conversations in the client's chart	

If the practitioner believes that disclosure is necessary to eliminate or reduce significant risk of serious bodily harm to a person or persons, he/she must:

✓		Task	Date / Initials
	1.	Disclose personal health information to the third party or staff of KDCHC	
	2.	Note disclosure and circumstances surrounding it in client's chart	
	3.	It is advisable to contact the Program Manager to advise them of the situation.	

Use and Disclosure – How We Will Use Client Information and How We Will Share It

KDCHC will use and disclose (share) the information only for the reasons for which consent was provided or when we have to by law (See KDCHC Policy # CG0903 Duty to Warn). We do not sell, barter or exchange any personal information for profit.

Disclosure to Police

It is not mandatory for staff to provide confidential material to the police in the absence of a legal obligation. At these times, the general rules regarding consent and disclosure apply, meaning that express consent, either from the client directly, or the substitute decision-maker, will be required before the police are provided with personal health information.

PHIPA allows the disclosure of personal health information without client consent under certain circumstances. However, staff are not prohibited from seeking the client's consent. For this reason, staff will make every reasonable effort to obtain the client's consent before disclosing the information.

A staff member can only disclose the client's personal health information:

• when staff has the client's or substitute decision-makers consent and it is necessary for a lawful purpose;

• where it is permitted under legislation, without the client's or substitute decision-maker's consent; or

• where it is required by law.

Summonses, Subpoenas and Court Orders

In the course of litigation, staff may be required by a summons, subpoena or a court order to disclose a client's personal health information and patient records. The staff member should read the summons, subpoena or court order carefully and not do more than it requires. For example, a summons may require a staff person to attend a court at a particular time and to take a specific patient chart. The summons does not authorize the staff member to discuss the client's care with, or show the record to, anyone in advance of the court appearance.

When personal health information is disclosed to the police, staff members are encouraged to record the officer's name and badge number, the request for information, the information provided, and the authority for the disclosure (e.g., consent, reporting obligation, search warrant or summons). A photocopy of any search warrant or summons should be included in the client's medical record. The police or Crown attorney will usually take the originals but leave the staff member with copies of the record so that ongoing care can be given.

HIPA permits a Heath Information Custodian to disclose to the appropriate persons, including police, personal health information about a person where the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

Use for Other KDCHC purposes

We will only share the information with other health care providers that they need to provide a specific service.

With the client's consent contact information may be given to program volunteers such as peer support volunteers.

KDCHC does occasionally have auditors, information technology (computer), or other contractors on-site. When they are here they might have access to personal information. They only have access for a limited amount of time and they must follow this policy. They will be required to sign a confidentiality agreement as per KDCHC policy

Retention and Disposal – How We Will Keep and Destroy Client Files

Please see KDCHC policy # B0701 Records Maintenance and Retention

Safeguards – How We Protect Client Information

Everybody who works or volunteers at KDCHC must sign a 'Confidentiality Agreement'. This agreement says that they won't share or use any personal information except as agreed by the client. Everybody also gets training. Anybody who knowingly misuses personal information will be disciplined.

Client files are stored in rooms that only staff have access to and are locked at the end of each day. Electronic files are protected by passwords, firewalls and other means. We will tell clients if there is any loss of personal information or if anyone who doesn't have permission sees your information.

Accuracy and Access – Keeping Client Information Correct and Letting Clients See It
KDCHC tries to ensure that personal information is correct and as up-to-date as necessary. Clients have a right to see their personal information and to request updates and corrections.

KDCHC may limit access to a client's file if the file contains confidential information about somebody else, information protected by law, or information that could result in serious harm or interfere with law enforcement. Clients will be told the reasons for limiting access. KDCHC may charge a fee if there are costs to produce the information or make copies.

Satisfaction
We welcome client feedback on this policy and its implementation. Clients who have any questions, concerns or wish to file a complaint under this policy are invited to contact the Privacy Officer.

Procedures

Collection, Consent, Use and Disclosure

Clients of Kitchener Downtown Community Health Centre must give their consent for the collection, use and disclosure of personal information as outlined in the KDCHC Privacy Policy. It is KDCHC's responsibility to advise clients of the purpose(s) for which their information is being collected and will be used.

Consent can be in various forms – written, oral, and implied.

In general, anyone who is over 16 years of age and competent may give consent for the collection, use and disclosure of their information. Custodial parents, legal guardian or legal substitute decision-makers can also give consent. In addition, children under sixteen years of age has the right to give and refuse consent to release information if the provider deems them to be competent to make that decision.

1. All clients accessing KDCHC will be told why we are collecting information and how it will be disclosed. This can be achieved by explaining the purpose and use orally and, where appropriate, providing them with a copy of our Privacy Policy - Summary.

   All clients accessing KDCHC will be asked to provide their general consent to collection and use of their information. This can be achieved by getting a signed consent (at intake, see "New Client Consent and Intake" form), or when written consent is not practicable or feasible, orally with oral consent documented.

2. When proposing to share information with other KDCHC staff: advise the client of the information to be shared, with whom and for what purpose. Given that the general "Consent and Authorization" included on the New Client Intake form makes reference to KDCHC as an organization, consent has already been documented. If the client objects to the sharing of information, advise them of any resulting service limitations.

3. Consent for disclosure of information for the purpose of providing health care or assisting in the provision of health care to an individual is implied between health information custodians (including health care practitioners, laboratories, x-ray, long term care homes, community care access centres, hospitals, including psychiatric facilities, pharmacies, ambulance services, Ontario Agency for Health Protection and Promotion). **Staff will inform clients of this implied consent when offering external provision of service.** Consent for disclosure of information to government agencies or other third parties will be confirmed by signature on a "Release of Information" form (see attached). In some situations written consent for disclosure of information to a third party may not be possible from the client, but an oral consent can be provided. In these situations, document the consent.

4. While the circle of care for implied consent applies to all health information custodians, other agencies or individuals may be identified by the client as part of their circle of care. The contact names/information should be noted in the client record. A consent to release information form should be signed by the client if possible. Oral consent by the client

needs to be documented. Staff should periodically review the extended circle of care information to ensure that it is current and still appropriate for the client.

5. When requesting information from an external service provider/third party: advise the client of what information is to be requested and what it will be used for. Consent for request for information will be confirmed by signature on a "Consent to Obtain Information" form (see attached).

6. When a client refuses consent or wishes to withdraw consent, advise the client of the consequences of withholding or withdrawing consent. Refusal or withdrawal of consent must be documented and tracked on an ongoing basis as appropriate.

Retention and Disposal

See KDCHC Policy B0701 Records Maintenance and Retention

Safeguards

All staff/volunteers/students and vendors contracted to work on site at KDCHC must be oriented to and sign a confidentiality agreement when they start their employment/service. Privacy policies and procedures will be reviewed during orientation and the implications of any breach of confidentiality are to be explained to the employee/volunteer/student and vendors. Documentation related to the above orientation will be maintained by the Director of Human Resources.

Annual privacy training refreshers will be delivered to all staff. Non-compliance may result in restricted access or the removal of access to KDCHC systems and/or shared systems.

Client-related records will be maintained in a locked room or file cabinet accessible only to staff. Files are not to be removed from the KDCHC property. Limited files to be transported to outreach sites will remain in the custody of KDCHC staff at all times and will be returned to KDCHC for filing immediately following the end of outreach visitation.

Programmatic client files that do not include medical or primary health information may be accessed by specific volunteers for specific uses under supervision of staff, such as contact information used by the Volunteer Coordinator volunteer assistant.

Electronic files are protected by firewalls and passwords.

Auditing

An audit is a technical safeguard for personal health information stored in an electronic health record system. Audits are completed to ensure that users are only accessing information that is required to support in the provision or administration of health care, to deter inappropriate access and support in privacy investigations.

The Privacy Officer or a delegate will:

- Conduct regularly scheduled or trigger audit reports, as needed
- Maintain documentation of audits conducted and results of follow up, if necessary
- Request audit reports for both agents and clients on a quarterly basis from the responsible program office for shared systems. In addition, activity audits for clients who have consent directives in shared systems will be requested, as needed
- Follow the privacy breach protocol outlined below if inappropriate access is detected and confirmed in any electronic health record system

Appointment of Privacy Officer

The KDCHC is accountable for the protection of personal information that it has in its possession and control and appoints an individual with the responsibilities of a Privacy Officer, to monitor and ensure agency compliance with privacy laws and regulations.

The Privacy Officer will be accountable to the Executive Director and Board of Directors, who make the appointment.

The organization will ensure that the Privacy Officer has appropriate training to carry out the responsibilities of the role. The organization will also ensure the position carries meaningful authority to monitor compliance, handle complaints, and communicate changes to agency privacy policies, if required.

Duties and Responsibilities of the Privacy Officer:

- Leadership for the privacy program
- Conducting or overseeing privacy risk assessments and audits
- Developing and implementing privacy policies and procedures
- Ensuring that all staff and volunteers have training in the organization's privacy program
- Monitor systems development and operations for security and privacy compliance
- Ensure compliance related to privacy, security and confidentiality
- Track and report on compliance related to privacy, security and confidentiality
- Provide counsel related to third party agreement and service contract development with other agencies
- Resolve allegations of non-compliance
- Maintain knowledge of all privacy legislation and regulations
- Manage public perception of data protection and privacy practices for the organization
- Liaise with government agencies and privacy commissioner's office.

Privacy Breaches

A privacy breach occurs when there is unauthorized access to collection of, use, disclosure or disposal of personal information. The most common privacy breach happens when personal information is stolen, lost or mistakenly disclosed.

In the event of a breach or perceived breach of personal information, staff are to contain the breach, if possible, and then advise a Director immediately. That Director will advise the Privacy Officer. The Privacy Officer will immediately take action to:

- Contain the breach
- Assess the size and scope of the breach and the risk issues
- Contact the affected clients to inform of the breach and the actions taking to address the situation. This would be done within a reasonable amount of time, usually within a business week.
- Conduct a full investigation to identify issues that lead to the breach and actions that can be taken to prevent a future breach.

For a breach involving a shared system, the Privacy Officer will:

- Inform the responsible program office's Privacy Department by the end of the next business day after becoming aware of the incident
- Support in breach containment, as required
- Contact affected clients to inform of the breach and when complete, provide a summary of the results of the investigation, as required
- Conduct an investigation, implement remediating activities and complete a Privacy Breach Report, as required

It will be the role of the Privacy Officer to inform the Executive Director about the breach, the risks or potential risks of the breach and the actions taken to address it.

Any client believing that their personal information has been breached should contact the Privacy Officer (see information at the beginning of this policy). The Privacy Officer will address the complaint quickly following the above steps. The Privacy Officer will contact the client once the results of the investigation have been completed.

Accuracy and Access

Staff at KDCHC will take reasonable efforts to ensure the accuracy of the information contained in the client files. Clients should be asked during visits if the basic information (contact information, OHIP number, name) is correct.

Clients have the right to see the information contained in their file and to append comment or correction to the file, and to have the file copied. Clients have a right to access a copy of their record for review within 30 days, (or 60 days in the case of complex searches), to request a correction of information, to obtain a copy of their record, and to have assistance in interpreting their record. They do not have the right to remove the file from the possession of KDCHC. Essentially, the information contained in the file is the property of the client, while the paper the information is on is the property of KDCHC. Clients can make requests to review their file to

the Privacy Officer or their primary care provider. The Privacy Officer should be advised in advance of all requests to review files. Request is to be documented in the client file.

KDCHC reserves the right to charge the client for the cost of copying a file.

If a client requests to review their file, an appointment will be made with a qualified staff member to review the file. This is done to ensure that the client is made aware of and understands the content of the file.

The client may request corrections to the file. Depending upon the nature of the correction requested, the correction can be made (eg. - to the address), a request for correction and correct information appended to the file in a separate letter, or a notation made and duly executed in the progress notes by the health care provider (such corrections will only be corrections of fact). The Privacy Officer will determine the method of correction.

All requests for access and correction will be logged and maintained by the Privacy Officer.

KDCHC reserves the right to limit client access to their record if: the record contains confidential information about somebody else; the information in the record is protected by law; the information in the record could result in serious harm or interfere with law enforcement. The Privacy Officer will advise the client of the reason for limited access.

Shared Systems

If a client or Substitute Decision Maker requests to access or correct their personal health information in a shared electronic health record (EHR) system (e.g. ClinicalConnect),

The Privacy Officer will:
Document the request in the CHC's access and correction log
Forward the request to the responsible program office (e.g. eHealth Ontario) within 21 days of receiving the request to ensure the client receives a response within 30 days. The program office will communicate with the client and complete all administrative tasks.
Notify the client if KDCHC has completed a correction in a shared system. If the correction is medically relevant, the responsible program office will be informed to enable notification to all HICs who have viewed the information.

Where multiple organizations are involved in a request for access or correction to a shared system, KDCHC will respond by providing the client with information for the privacy contact at the responsible program office.

Office of the Information and Privacy Commissioner of Ontario

You are also welcomed to contact the Office of the Information and Privacy Commissioner of Ontario for information related to privacy, legislation on Privacy and to make direct complaints to the Commissioner.

Mailing Address: 2 Bloor Street East, Suite 1400 Toronto, ON M4W 1A8
Email address to reach the IPC or the Commissioner**:** info@ipc.on.ca

Phone Numbers:
Toronto Area: 416-326-3333
Long distance: 1-800-387-0073
TDD/TTY: 416-325-7539

Fax: 416-325-9195

Website address: www.ipc.on.ca

Reference Documents:
New Client Consent and Intake Form
KDCHC Privacy Policy Summary for Clients
Release of Information Form
Consent to Obtain Information Form

Approved by: Eric Goldberg, Executive Director **Date**: June 20, 2018

_____