POLICY

Community Support Connections believes that information gathered during the course of our work – about clients, volunteers, employees, independent contractors, and other stakeholders – is private and every safeguard should be taken to ensure that personal information and personal health information is kept confidential, in keeping with sound, ethical principles, leading practices, and governing legislation.

Community Support Connections collects, uses, discloses, retains, and protects personal health information (PHI) and is a health information custodian (HIC) under the Ontario Personal Health Information Protection Act, 2004 (PHIPA) and the federal Personal Information Protection and Electronic Documents Act, 2011 (PIPEDA). Under certain circumstances, Community Support Connections may also be subject to the Freedom of Information Freedom and Privacy Act, 1990 (FIPPA), which provides the framework within which people may access information from institutions.

PHIPA applies to PHI that is collected, used or disclosed by custodians. PHI includes oral or written information about the individual, if the information:

- relates to the individual's physical or mental health, including family health history;
- relates to the provision of health care, including the identification of persons providing care;
- is a plan of service under the Home Care and Community Services Act, 1994;
- relates to payment or eligibility for health care;
- relates to the donation of body parts or bodily substances or is derived from the testing or examination of such parts or substances;
- is the individual's health number; or
- identifies an individual's substitute decision-maker.

Any other information about an individual that is included in a record containing PHI is also included in the definition. Employee records of a custodian are excluded from the definition, provided that the records are used primarily for purposes other than providing health care. Also, the Act does not apply to information about a person if the information could not reasonably be used to identify the person. Other recorded information about a person that is not PHI and that is in the custody or under the control of an organization that is both a health information custodian and an institution or part of an institution is subject to FIPPA.

PIPEDA defines personal information as information about an identifiable person, but does not include the name, title, or business address or telephone number of an employee, or an organization.

Openness and Transparency
This policy is available for public viewing in the waiting rooms of all Community Support Connections' office locations and posted on our website. It describes how this office collects, protects, and discloses the PHI of clients and the rights of clients with respect to their PHI.

Questions regarding our privacy practices can be answered by contacting Community Support Connections' Privacy Officer.

Accountability
Community Support Connections collects, uses, and discloses PHI only for the purposes of providing service or the administration of that service or for other purposes expressly consented to by clients.

Collection, Use and Disclosure of Personal Information
Community Support Connections will only collect the information that is required to provide services, administer the service that is provided, and communicate with clients. Community Support Connections will not collect any other information, or allow information to be used for other purposes, without a clients' express consent - except where authorized to do so by law or the presence of risk to self or others. These limits on collection ensure that we do not collect unnecessary information.

Consent
Client consent – implied or expressed – is acquired at intake. Clients have the right to refuse consent to disclose their PHI that is not service specific without being denied services with Community Support Connections. Clients have the right to withdraw consent to have their PHI shared with other health providers or third parties at any time.

Safeguards
Safeguards are in place to protect the security of client information. These safeguards include a combination of physical, technological and administrative measures. Any other persons having access to client information or to Community Support Connections premises shall, through contractual or other means, provide comparable safeguards.

Record Retention
Community Support Connections retains client records as required by law and professional regulations.

Secure Disposal/Destruction of Information
When information (PHI, personal information and other information) is no longer required, it is destroyed or retained as required by law and professional regulations.

Client Rights
Clients have the right to access to their records in a timely manner. In extremely limited circumstances, clients may be denied access to their records, but only if providing access would create a risk to that client or to another person. For example, the information could reasonably be expected to seriously endanger the mental or physical health or safety of the individual making the request or another person.

Accuracy of Information
Community Support Connections makes every effort to ensure that client information is recorded accurately.

Privacy and Access Complaints
Clients who believe that Community Support Connections have not responded to their access request or handled their PHI in a reasonable manner, are encouraged to address their concerns with Community Support Connections' Privacy Officer.

Privacy Breach
A breach of confidentiality is defined as the inappropriate collection, access, use or disclosure of PHI. Community Support Connections will comply with legislated protocols relating to privacy breaches.

RESPONSIBILITY

Community Support Connections is responsible to ensure appropriate policies, procedures, practices and safeguards are in place to protect the privacy of PHI and other personal information we gather.

All volunteers, employee, and independent contractors providing services to Community Support Connections' clients, are responsible for adherence to the agency's privacy and confidentiality policy and the associated legislation.

All volunteers, employees, and independent contractors will read and sign a Confidentiality/Conflict of Interest Statement upon selection. Employees will sign annually thereafter.

PROCEDURES

Openness and Transparency
Community Support Connections has a designated Privacy Officer to answer any questions from clients, volunteers, employees, independent contractors or the general public regarding Community Support Connections' Privacy Policy.

Volunteers and employees are informed of the electronic location of the Policy and Procedure manual.

The Privacy Policy is available for public viewing in the waiting rooms at all Community Support Connections office locations and is posted on the Community Support Connections' website.

Public information regarding the Privacy Policy located in various collateral including brochures, will be linked to Community Support Connections' website for public viewing.

Accountability
Community Support Connections educates volunteers, employees, and informs independent contractors regarding the importance of protecting PHI, and receives their agreement to observe legislation and Community Support Connections policy, prior to granting access to PHI. Community Support Connections provides regular educational/informational updates thereafter (for employees, at minimum annually).

Community Support Connections ensures that independent contractors are aware and willing to comply with PHIPA and Community Support Connections' Privacy policies and procedures during the screening process.

All volunteers, employees, and independent contractors are required to sign a confidentiality agreement at hire/commencement which continues to apply even after employment/affiliation is terminated. Employees are required to sign annual updates.

All persons working for or through Community Support Connections, who have access to PHI, must adhere to the letter and spirit of PHIPA, including but not limited to the following information management practices:

- access is on a need to know basis;
- access is restricted to authorized users; and
- access is limited to hours of work as specified by position.

Volunteers and independent contractors are provided only that information which is required for the completion of their duties.

Volunteers, employees, or independent contractors who are found to inappropriately use PHI may warrant sanctions up to and including termination of employment/affiliation or removal from the independent contractor program. Breaches are investigated by the Privacy Officer.

Consent
Community Support Connections employees will seek informed consent to collect PHI necessary for service provision and to share that information with other providers from clients at intake. Employees explain that sharing information with other care providers is done to implement the care plan, improve service and minimize the need for clients to repeat their story unnecessarily.

Employees inform clients at intake that they may withdraw their consent to share information with other service providers at any time.

All information packages that go to new clients have a Privacy Brochure which outlines their rights regarding their PHI, as well as the process for withdrawing consent and the phone number to call in order for them to withdraw their consent to share PHI via the Integrated Assessment Record (IAR).

If a client refuses or withdraws consent to collect or share information, the designated employee will ensure the client understands any significant consequences that might result with respect to their service.

All consents or refusals are documented in AlayaCare. Information is not shared without future express consent.

When a client chooses to withdraw consent, Community Support Connections employees will document that decision in AlayaCare and advise the client of the telephone number for withdrawing IAR consent. Client information will not be shared with other providers after the withdrawal of consent.

Collection and Retention of PHI
Employees document only the information required for the purposes of providing services for the client and assisting in the formation of the care plan for clients. Information will only be collected indirectly if necessary, for the provision of services, with an individual's consent or if permitted/required to do so by law.

Accuracy of Information
All personal information is recorded in AlayaCare in a timely manner, including any/or all conversations/interactions with clients. Information is recorded either in the notes or narrative AlayaCare fields. Any amendments or changes to the client file are recorded in AlayaCare.

Disclosure
The Community Support Connections Privacy Officer will review requests for client information and provide requested information if the request is mandated or authorized by law using the following procedures.

Client Access to Information
Clients are informed of their rights, including the right to review their file, at intake.

Clients are permitted to view their files in a secure location. When clients request to see their file, Community Support Connections will provide the Consent to View form. Once the form is returned, Community Support Connections will respond within twenty (20) business days.

If the request is approved, a designated employee will pull the written file and make copies of the relevant documents in the file, ensuring that any/all references to any other clients are deleted.

The original paper files and documents shall remain in the client's file until the file is destroyed (10 years after termination of service). Electronic files, if available, will be archived.

If the request is declined, the Community Support Connections Privacy Officer will explain to clients why access to the records requested is not possible.

Disclosures to other providers by implied consent
When Community Support Connections' clients receive assessments, their PHI is shared and stored on a centralized electronic sharing system with community health service providers.

During preliminary intake, Community Support Connections employees explain to clients that unless otherwise indicated, Community Support Connections assumes that clients have consented to the use of their information for the purposes of receiving service, including sharing the information with other health/service providers involved in their care. By virtue of seeking service from Community Support Connections, a client's consent is implied for the provision of that service. Relevant PHI is shared with other providers involved in client care, including, but not limited to:

- other community support services; and
- the provincial Integrated Assessment Record (IAR)

The Integrated Assessment Record (IAR), is used by local Health Service Providers to share client assessment data as part of service delivery.

Disclosures mandated or authorized by law (without consent)
There are limited situations where Community Support Connections is legally required to disclose PHI without client consent. Examples of these situations include, but are not limited to:

- billing provincial health plans;
- reporting specific diseases;
- reporting abuse;
- reporting fitness to drive, fly, etc.;
- by court order, including coroner's warrants;
- in regulatory investigations;
- for quality assessment (peer review); and
- for risk and error management.

Disclosures to all other third parties by Express Consent
Clients' express consent, oral or written, is required before Community Support Connections will disclose PHI to third parties for any purpose other than to provide service or unless authorized to do so by law or risk to self or others.

Examples of situations that involve disclosures to third parties include, but are not limited to:

- police without warrant or subpoena; and
- Client service summaries to insurance companies.

Disclosure Log
Before a disclosure is made to a third party, a notation shall be made in the electronic file that a client has provided express consent, or a Client Consent form is signed and scanned into the file.

Community Support Connections will maintain a confidential Disclosure Log of requests and disclosures.

Safeguards
Information regarding persons should not be available on desks, computers, photocopiers, or any location that enables casual observation.

All client, personnel and donor files are kept in locked file cabinets, AlayaCare and/or appropriate secured electronic repositories.

Only those volunteers and employees who need to access these files as part of their job are able to access these files and only within their prescribed working hours.

There are designated employees who open the file cabinets at the beginning of a work day and to lock them at the end of the day.

Client, personnel and donor information may not be left unattended on desks.

Access to electronic client, personnel or donor files is controlled by unique user names and passwords. Employees are not allowed to share passwords. Passwords or employee recognition at a comparable level (such as finger print scans) are changed on a regular basis. Volunteers may be assigned a more generic user name and password, but these credentials only work from a Community Support Connections computer and provide limited access.

Employees are required to log out of AlayaCare or lock their computer when leaving their desks and to log out of AlayaCare and shut down their computers at the end of the work day. Employees are required to ensure volunteer workstations are similarly shut down at the end of the work day.

If a client file is taken off site, it is to be kept in a secure location and then brought back to the office. Personnel files may not be taken off site. Community Support Connections laptops are encrypted.

Transmission of PHI to other service providers will be done by secure means such fax, Integrated Assessment Record (IAR) or Health Partner Gateway (HPG). Transmission of PHI via email is prohibited except for the transmission of limited PHI (name, address, and destination) to volunteers or independent contractors via encrypted emails.

Employees, volunteers and independent contractors are not allowed to store client, personnel or donor information on their personal computers/devices.

Limits on third party access
All Community Support Connections offices have a security system with unique user identification, and only designated employees have keys to the office(s).

All client information is protected in the office(s), by usage of locked file cabinets and IT protocols identified above.

Record Retention
Current paper record retention requirements are:

- client records - 10 years;
- financial records - 7 years; and
- board minutes – indefinitely.
- employee personnel files – as per the Employment Standards Act (ESA)

Electronic client records and other types of records will be stored indefinitely.

Secure Disposal/Destruction of Information
When information is destroyed and/or disposed of, it must be shredded either by the employee or disposed of by an authorized vendor. Community Support Connections will keep detailed logs of destroyed records including who destroyed or disposed of the shredded records and when this action took place.

Privacy and Access Complaints
Clients may call the Community Support Connections Privacy Officer or provide a written statement of their complaint. Client complaints will receive a response within twenty (20) business days.

If clients are not satisfied with the resolution of the complaint, the Privacy Officer will provide information about how to contact the Executive Director with their complaint. The Executive Director will respond to complaints within twenty (20) business days of receipt of the escalated complaint.

If clients are not satisfied with the resolution of the complaint, the Executive Director will provide information about how to contact the President of the Board of Directors with their complaint. The President of the Board will respond to complaints within twenty (20) business days of receipt of the escalated complaint.

If clients are still not satisfied with the resolution of their complaint, the President of the Board of Directors will provide information about how to make a formal complaint with the Privacy Commissioner of Ontario.

Reporting Breaches

The most common privacy breaches are:

- unauthorized collection of PHI;
- unauthorized or unsecured disposal of PHI; and
- unauthorized disclosure of PHI through:
  - loss (a file is misplaced);
  - theft (a laptop is stolen); or
  - error (a letter addressed to one person gets faxed/emailed to and received by the wrong person).

Volunteers, and employees, will be trained regarding what constitutes a breach of privacy, and the severity of breaches.

Volunteers, employees, independent contractors are required to immediately notify the Community Support Connections Privacy Officer when there is privacy breach. The Community Support Connections Privacy Officer will:

- call the complainant and gather necessary facts as part of the investigation process;
- complete the Privacy Breach Reporting Form;
- notify the Executive Director (and/or President of the Board of Directors) of the breach and resulting actions/outcomes; and
- report breaches to the Ontario Privacy Commissioner as required.

Volunteers, and employees, will be trained on privacy and confidentiality, and are expected to report all privacy breaches. Reports will be completed, reviewed, and followed up upon.

Privacy Audits

The Privacy Officer and/or delegate will run the following audits to ensure that Community Support Connections complies with applicable legislation and policies:

- AlayaCare files reviews – quarterly;
- IAR User PHI Assessors forms – at hire and termination; at regular intervals; and
- IAR Privacy Breach Trending Report.

RELATED POLICIES AND PROCEDURES

3500 – Client Complaint Resolution

RELATED DOCUMENTS

Confidentiality Agreement
Consent to View
Privacy Breach
IAR User PHI Assessors Report
IAR Privacy Breach Trending Report
Intake Forms - Consent of Collection/Use/Disclosure Internal
IAR Client Privacy Rights Complaint
IAR Client Privacy Rights Update Form

Policy History

Date	Reviewed	Amended	Approved by
March 29, 2021		Leadership	Executive Director
May 15, 2018	Quality Cte	Staff	Executive Director
October 11, 2016		Quality Cte	Executive Director
November 3, 2015		Quality Cte	Executive Director
August 21, 2014			Board