

<u>POLICY STATEMENT:</u>	Privacy Policy for Jewish Family and Child Service of Greater Toronto
<u>DATE ORIGINALLY APPROVED:</u>	December 3, 2019
<u>DATE OF REVISION:</u>	
<u>DATE TO BE REVIEWED:</u>	December 2020
WHERE TO FIND:	Privacy Manual

1. Policy Objective:

Jewish Family and Child Service of Greater Toronto (“JF&CS” or “Agency”) is a multi-service organization that provides a comprehensive set of individual and family services and operates a children’s aid society. The Agency is committed to protecting and respecting client privacy and maintaining the confidentiality of the personal health information (“PHI”) and personal information (“PI”) that it holds. The Agency is committed to carrying out its professional duties and obligations with integrity, objectivity and in compliance with all applicable privacy legislation and the Agency’s Standards of Conduct, including its Code of Conduct.

Definitions

“**Clients**” mean individuals who receive services from JF&CS

“**Client Information**” means personal health information under (*Personal Health Information Protection Act, 2004* (PHIPA) and personal information under the *Child, Youth and Family Services Act, 2017* (CYFSA).

“**CYFSA**” means the *Child, Youth and Family Services Act, 2017* and regulations thereunder.

“**Others**” means volunteers, consultants, interns, students, auditors, and vendors of the Agency when dealing with Client Information, and “Other” refers to any of them.

“**PHIPA**” means the *Personal Health Information Protection Act, 2004* and regulations thereunder.

“**Privacy Legislation**” means the CYFSA and PHIPA.

“**Privacy Officer**” means the Privacy Officer for JF&CS or their delegate.

“Privacy Procedures and Related Documents” means the list set out in Appendix A, all of which comprise part of this Privacy Policy.

A more fulsome glossary applicable to this Policy and the Privacy Procedures and Related Documents are set out in Appendix B.

2. Scope

This Privacy Policy deals with Client Information.¹ It applies to all employees of the Agency and Others. There are also Privacy Procedures and Related Documents, which are listed in Appendix A. All Agency employees and Others are required to abide by this Policy and the Privacy Procedures and Related Documents.

The Agency is a “health information custodian” (“HIC”) under PHIPA for many of its individual and family service programs and is governed by that legislation. As a children’s aid society, the Agency is a “service provider” under the CYFSA and is bound by new information protection laws² under Part X of that law. Privacy Legislation governs how Client Information may be collected, used and disclosed, as well as rights that clients have with respect to their Client Information. The Agency is accountable for compliance with Privacy Legislation and for the actions and omissions of employees and Others who are acting as agents of the Agency.

PHIPA³ and the CYFSA require that JF&CS take reasonable safeguards to ensure that Information of our Clients and former Clients in our custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that that client records are protected against unauthorized copying, modification or disposal.

Some Agency programs are not covered by Privacy Legislation. However, it is the Agency’s policy to treat all Agency programs, to the extent possible, in accordance with the privacy principles as required by Privacy Legislation and this Privacy Policy.

3. Principles

a) Context

The Agency collects, uses and discloses Client Information in order to provide effective and coordinated services to clients, to supervise and manage individual and family services as well as child welfare services, to obtain client feedback for quality improvement purposes, for accreditation, to comply with legal requirements and for other purposes permitted or required under law.

¹ Confidentiality of employee information is not covered by this Policy. Employee information is dealt with in part, in Policy 214, Standards of Conduct (Confidentiality).

² The changes to the CYFSA are scheduled to come into force on January 1, 2020.

³ See s. 12 of PHIPA.

b) Summary of Principles

The Agency is committed to:

- respecting the privacy of clients and maintaining the confidentiality of their Information;
- having privacy processes and practices that are transparent;
- providing clients with information to obtain knowledgeable consent;
- taking reasonable security measures to protect Client Information from unauthorized collection, use and disclosure;
- taking steps to ensure that clients are informed about their rights and how to exercise their rights;
- monitoring and responding to privacy issues through training, auditing information practices and processes, incident management and complaint procedures.

c) Commitment to the 10 Privacy Principles:

The Agency is committed to 10 Privacy Principles⁴ underlying Privacy Legislation. Set out below are the 10 Privacy Principles and how the Agency implements these principles.

1. **Accountability. The Agency is responsible for Client Information under its custody and control and shall designate an individual(s) who are accountable for the Agency's compliance with privacy principles.**

The Agency has designated a Privacy Officer position that reports to the Director of Research and Evaluation. The Privacy Officer manages compliance with this Privacy Policy and Privacy Legislation, with the support of the Privacy Advisory Committee, Senior Management and the Board of Directors.

In terms of privacy governance, a Privacy Advisory Committee (PAC) has been established. The purpose of the PAC is to serve as a decision-making authority that recommends and approves Procedures, Processes and Policies to be implemented as part of the implementation of Part X of CYSFA and PHIPA across JF&CS. The PAC will review all revised and new Policies and Procedures, and approve them for implementation. All Privacy Procedures are reviewed by the PAC and recommended for final approval by Senior Management.

Our commitment to privacy is demonstrated through our adherence to this Privacy Policy and Privacy Procedures and Related Documents and by educating our employees and Others about their privacy responsibilities.

2. **Identifying Purposes. The Agency shall identify the purposes for which Client Information is collected, at or before collection.**

⁴ The 10 Privacy Principles are modelled on *The Principles Set out in the National Standard of Canada Entitled Code for the Protection of Personal Information, CAN/CSA-Q830-96*. These principles are embedded within PHIPA and the CYFSA and set out in Schedule A to the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

The Agency collects Client Information primarily for the delivery of client care and to fulfill its responsibilities as a children's aid society. In addition, it uses Client Information for related purposes, including to:

- administer and manage Agency programs and services;
- process and make payments;
- seek client consent where appropriate;
- respond to or initiate proceedings;
- prevent, investigate, and or respond to child abuse and neglect of children under 18 years;
- evaluate risk of harm or actual harm to children and youth;
- assist families in offering supports to help keep their children safe;
- conduct research (in accordance with legislated requirements);
- do statistical reporting;
- do fundraising (in accordance with legislated requirements);
- conduct risk management;
- conduct training and quality improvement activities;
- comply with legal and regulatory requirements;
- fulfil accreditation requirements;
- support (on a de-identified basis) funding submissions and donor reports;
- comply with legal obligations; and
- carry out other activities as permitted or required by law.

The Agency has a Privacy Notice of Information Purposes statement that identifies the purposes for which Client Information is collected, used and disclosed which is posted on the JF&CS website and brochures.

When Client Information is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, consent will be required before the information can be used for the new purpose.

3. Consent. The knowledge and consent of the client are required for collection, use or disclosure of Client Information, except where disclosure is permitted or mandated by law.

Clients (or their substitute decision-makers) will be apprised of how the Agency collects, uses and discloses Client Information through the Agency's Privacy Notice and discussion of privacy practices by their workers, information brochures, posters and other information that will be developed and made accessible to clients. The Agency is committed to ensuring that consent is informed.

The Agency generally requires express (direct or sometimes referred to as explicit) consent in order to collect, use, or disclose Client Information. However, there are some cases where we may collect, use or disclose Client Information without consent as permitted or required by law (e.g. risk of imminent harm to self or others, emergencies, child protection concerns). See the Agency's "*Consent Management Procedure*".

Express consent will be sought if a client is enrolled in more than one Agency program, to share Client Information among all Agency providers involved in the client's care. See the "*Access and Correction Procedure– Release of Client Information*" section and the section on Sharing Client Information in the "*Consent Management Procedure*".

Express Client consent will be sought when a record is to be shared with external providers, unless the law requires or permits otherwise. See the "*Procedure on Disclosure to Third Parties*".

A client may choose not to give consent or to withdraw consent. If consent is given, a client may withdraw consent at any time, but the withdrawal cannot be retroactive.

Privacy Legislation gives individuals the right to restrict access by others to their Client Information– whether to specific staff of the Agency or other providers (referred to as a "**lockbox**"). See the Agency's "*Lockbox Procedure*".

- 4. Limiting Collection. The collection of Client Information shall be limited to that which is necessary for any identified purposes. Client Information shall be collected by fair and lawful means.**

We limit the amount and type of Client Information we collect to that which is necessary to fulfill the purposes identified. Information is collected directly from the client, unless the law permits or requires collection from third parties. For example, from time to time we may need to collect information from clients' other care providers in order to provide coordinated and effective service.

Client information may only be collected if necessary for a bona fide work purpose authorized by the Agency. Agency employees and Others are not permitted to initiate their own (or self-directed) projects to collect new Client Information from any source or to use Client Information for a new purpose, without the purpose being authorized by the Agency or the Privacy Officer.

- 5. Limiting Use, Disclosure and Retention. Client Information shall not be used or disclosed except for purposes for which it was collected, unless consent is obtained or permitted or mandated by law. Client Information shall be retained only as long as necessary for these purposes.**

Use and Disclosure

Client Information is not used or disclosed for purposes other than those for which it was collected, except with the consent of the client or as permitted or required by law.

Client Information may only be used or disclosed within the limits of each Agency employee's and Other's roles. Agency employees may not read, look at, receive or otherwise use Client Information unless they have a legitimate "need to know" as part of their position. Snooping is not permitted and will lead to consequences up to and including termination.

Retention

Client records are retained as required by law and professional regulations and to fulfill Agency purposes for collecting Client Information.

Client records will be disposed of when no longer necessary for the purposes for which collected, in accordance with legal, regulatory, litigation, professional and Agency requirements. Please see the Agency's "*Retention and Disposal Procedure*" and the "*Safeguards for Client Information Guidelines*".

6. Accuracy. Client Information shall be as accurate, complete and up-to-date as required for the purposes.

The Agency will take reasonable steps to ensure that information it holds is as accurate, complete, and up to date as necessary to minimize the possibility that inappropriate information may be used to make a decision about a client.

The Agency has a procedure whereby clients may request that inaccurate Client Information be corrected. See the Agency's "*Access and Correction Procedure - Release of Client Information*".

7. Safeguards. Client Information shall be protected by security and privacy safeguards appropriate to the sensitivity of the information.

The Agency has put in place safeguards for the Client Information it holds, which include:

- Administrative safeguards (such as permitting access to Client Information by Agency employees and Others only on a "need-to-know" basis and development of this Privacy Policy and Privacy Procedures and Related Documents);
- Technological safeguards (such as the use of passwords, encryption, and audits). The Agency will implement a privacy audit program to monitor compliance with our privacy requirements; and
- Physical safeguards (such as locked filing cabinets and rooms);

The Agency takes steps to ensure that the Client Information it holds is protected against theft, loss and unauthorized use or disclosure. The details of these safeguards are set out in the Agency's "*Safeguards for Client Information Guidelines*".

The Agency requires anyone who collects, uses or discloses Client Information on the Agency's behalf to be aware of the importance of maintaining the confidentiality of Client Information. This is done through the signing of confidentiality agreements, privacy training, and contractual means.

Care is used in the disposal or destruction of Client Information, to prevent unauthorized parties from gaining access to the information. See the Agency's "*Retention and Disposal Procedure*"

8. Openness. The Agency shall make information readily available to individuals about its policies and practices about Client Information.

The Agency shall make available the following information to clients and other members of the public:

- Information about our policies and practices relating to the management of Client Information, including the *Privacy Notice* and *Agency Rights and Responsibilities* document, consent discussions with clients, brochures, and posters;
- Provision of contact information for the Privacy Officer, to whom complaints or inquiries can be made;
- The process for obtaining access to Client Information the Agency holds, and making requests for its correction;
- A description of the type of Client Information we hold, including a general account of our uses and disclosures;
- A description of how a client may make a privacy complaint to the Agency or to the Information and Privacy Commissioner of Ontario; and
- Upon request, sharing copies of this Privacy Policy.

9. Individual Access. Upon request, clients shall be given access to their Client Information (unless access falls within a permitted exclusion). A client may challenge the accuracy and completeness of their PHI and PI and have it amended, if appropriate.

Clients may make written requests to have access to their Client Information, in accordance with the Agency's "*Access and Correction Procedure – Release of Client Information*".

The Agency will respond to a client's request for access within reasonable timelines and may charge reasonable costs to the client, as governed by law. Information will be provided subject to legislated exemptions from access (such as legal privilege). The Agency will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

Clients who successfully demonstrate the inaccuracy or incompleteness of their Client Information may request that the Agency amend their information. In some cases, instead of making a correction, clients may ask to append a statement of disagreement to their file.

10. Challenging Compliance. An individual shall be able to challenge the Agency's compliance with Privacy Legislation or the Agency's Privacy Policy/Procedures to the person designated by the Agency for privacy compliance.

Any person may ask questions or challenge the Agency's compliance with this policy or with Privacy Legislation by contacting our Privacy Officer

Compliance and Privacy Officer
Jewish Family & Child
4600 Bathurst St.
Toronto, Ontario M2R 3V3
Tel: 416-638-7800 ext. 6636
Fax: 416.638-7422
Email: privacy@ifandcs.com

The Agency will receive and respond to complaints or inquiries about our policies and practices relating to the handling of Client Information in a timely and responsive manner. The Agency will inform clients who make inquiries or lodge complaints of other available complaint procedures (e.g. to the Information and Privacy Commissioner of Ontario).

The Agency will investigate all complaints. If a complaint is found to be justified, the Agency will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees our compliance with Privacy Legislation. Any individual can make an inquiry or complaint directly to the Commissioner by writing to or calling:

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
Fax: 416-325-9195
www.ipc.on.ca

Cross References:

Policy 214A: Code of Conduct

Policy 214B: Conflict of Interest

Policy 214C: Confidentiality

Privacy Procedures and Related Documents set out in Appendix B to this Policy

Policy 902: Privacy Practices for Personal Health Information for The Jewish Hospice Program

Policy 701: Client Access to Records and Disclosure of Records to Others

Appendix A –Supporting Privacy Procedures and Related Documents

The following Supporting Privacy Procedures and Related Documents are referenced in the Privacy Policy and must be followed by Agency employees and Others:

	Privacy Procedures, Related Documents and Forms	Date of Approval by Privacy Advisory Committee	Date of Approval by Senior Management Committee
1	JF&CS Public Privacy Notice	September 16, 2019	October 30, 2019
2	JF&CS Lockbox Procedure	September 16, 2019	October 30, 2019
	<ul style="list-style-type: none"> • JF&CS Lockbox Information Sheet for Clients 	September 16, 2019	October 30, 2019
	<ul style="list-style-type: none"> • JF&CS Client Lockbox Request Form 		
3	JF&CS Safeguard Guidelines for Client Information		October 30, 2019
4	JF&CS Privacy Breach Protocol	September 16, 2019	October 30, 2019
5	JF&CS Consent Management Procedure (for collecting use and disclosure)	October 2, 2019	October 30, 2019
	<ul style="list-style-type: none"> • JF&CS Specific Express Consent Form 		
	<ul style="list-style-type: none"> • JF&CS General Express Consent Form 		
6	JF&CS Access and Correction Procedure - Release of Client Information	October 2, 2019	October 30, 2019
7	JF&CS Procedure on Disclosure to Third Parties	October 2, 2019	October 30, 2019
8	JF&CS Procedure on Working with Police	October 2, 2019	October 30, 2019
9	JF&CS Oath of Privacy Protection	October 2, 2019	October 30, 2019
10	JF&CS Retention and Disposal Procedure for Client Information	October 2, 2019	October 30, 2019

Appendix B –Glossary

This Glossary is for use with the Privacy Policy and Privacy Procedures and Related Documents.

“Access Audit Log” means the documented electronic record of Agency’s staff (or JF&CS Representatives) access to client information

“Auditing and Monitoring” means the process of reviewing all JF&CS Representatives’ case log details to detect any unauthorized access to client information. According to the IPC the process of logging, auditing and monitoring are effective deterrents to unauthorized access when JF&CS Representatives are well informed that all of their activities in relation to client information are logged, audited and monitored on an ongoing, targeted and random basis.

“Authorized person” means a person who has custody or control of client information as a result of or in connection with performing the person’s or organization’s powers or duties to meet the purposes for which the client information collected, used or disclosed.

“Business Day” means Monday to Friday from 9:00 am to 5:00 pm, exclusive of statutory holidays and the Civic Holiday in August.

“CAS” means Children’s Aid Society. CAS is a service provider under the *Child, Youth and Family Services Act, 2017* (“**CYFSA**”) and has statutory obligations to safeguard its service recipients’ Personal Information.

“Clients” means individuals who receive, or who have received, services from JF&CS

“Client information” means PHI under PHIPA and PI under CYFSA

“Circle of Care” means the term ‘circle of care’ is not a defined term in the PHIPA. It is a term commonly used to describe the ability of certain health information custodians to assume an individual’s implied consent to collect, use or disclose personal health information for the purpose of providing health care, in circumstances defined in PHIPA.”

“Collect”, means to gather, acquire, receive or obtain Client Information by any means from any source.

“Correction” means if a health information custodian has granted an individual access to a record of his or her personal health information and if the individual believes that the record is inaccurate or incomplete for the purposes for which the custodian has collected, uses or has used the information, the individual may request in writing that the custodian correct the record

“Confidentiality” means the obligation of an individual/the Agency to keep information provided in confidence, confidential.

“CPIN” means Child Protection Information Network

“Cyber-attack” means an electronic attack on, or exploitation of, a computer system or a network of computer systems by an unauthorized person(s) or hacker(s) whereby the system’s program codes are altered resulting in system or network malfunction. The primary motives for such attacks is fraud, to collect identifying information of an organization’s clients or customers,

intellectual property, access to passwords, system infiltration to cause denial of service(s), etc. Examples of such attacks are through the use of malicious codes or viruses, trojans, malware, phishing emails, spyware, fraud, ransomware, etc.

“Cyber Insurance” means an insurance policy to cover the financial consequences and damage to an organization’s reputation as a result of data privacy breach in business operations. The insurance may include an add-on of a third party (liability) coverage of the business cost incurred through liability claims.

“CYFSA” means Child, Youth and Family Services Act, 2017

“De-identify” in relation to the client information (PHI or PI) of an individual, means to remove information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

“Disclose” means to make Client Information in the custody or control of a person available or to release it to another to another person, but does not include using the information.

“Disposal” means client records will be disposed of when no longer necessary for the purposes for which it is collected, in accordance with legal, regulatory, litigation, professional and agency requirements.

“Final Disposition” means in the case of a court action, the action is finally disposed of (including all possible appeals); in the case of any other Proceeding, until the later of:

- the Proceeding has been completed and any subsequent hearing has been finally disposed of;
- if a separate legal claim may result from the incident that is the subject of the Proceeding,
- if a claim is made before January 1, 2004, 6 years (or, if involving a minor, until the minor reaches 18, plus 6 years); and
- otherwise, 15 years (or, if involving a minor, until the minor reaches 18, plus 15 years).

“Express (sometimes referred to as explicit) Consent” means consent that is given directly and may be given orally or in writing. The best practise is to document oral consent in the file. Under PHIPA, express consent is required if a HIC shares Client Information with a non-HIC, or two HICs share information for a purpose other than health care.

“Health information custodian” or **“HIC”** means a person or organization set out in PHIPA that has custody or control of personal health information as a result of, or in connection with, performing the person’s or organization’s powers or duties and includes regulated health professionals, registered social workers and social service workers, hospitals, JF&CS and other agencies that operate a program or service for community health or mental health, laboratories, pharmacies, etc.

“Incapable” means mentally incapable, and “incapacity”

“Information and Privacy Commissioner/Ontario” or “IPC” means the Information and Privacy Commissioner/Ontario, the entity charged with the administration of PHIPA and the CYFSA for privacy matters, among other provincial privacy statutes,

“JF&CS Representatives” means JF&CS staff, students, volunteers, researchers, auditors, vendors and other agents who may have access to Client Information.

“Joint Client” means a Client who is registered as a Client in more than one JF&CS program.

“Lockbox” means a client’s ability to withdraw or withhold their consent for the collection, use or disclosure of their Client Information.

“Matrix” means Matrix Case Management system for keeping client records

“Ministry” means Ministry of Children, Community and Social Services

“Non-Registered” means Clients who utilize some of JF&CS’ services (for example, customers who patronize the Just a Second Shop, and some clients of the Family Resource Centre, clients of Family Life Education, and clients that JF&CS staff may see at schools), but who are not registered in Matrix or CPIN as Registered Clients.

“Others” means volunteers, consultants, interns, students, auditors, and vendors of the Agency and “Other” refers to any of them.

“Personal information” means child welfare records that include demographic information about you, your contact information, your adoption, fostering and kinship information, record of visits, the care and support you received during those visits, health history, family history, educational, employment, etc. and information from other providers of care. These records are governed primarily by the CYFSA.

“Personal health information” means individual and family services records that include information relevant to your health and may include your date of birth, contact information, health number, health history, family health history, details of your physical and mental health, record of visits to clients, the care and support you received during those visits, any listed substitute decision-maker, and information from other health care providers.

“PHIPA” means the Personal Health Information Protection Act, 2004 and the regulations thereunder, all as amended from time to time.

“Proceeding” means a proceeding held in, before or under the rules of a court, a tribunal, an investigation, assessment, a commission, a justice of the peace, a coroner, inspection or other inquiry by a committee of a College within the meaning of the Regulated Health Professions Act, 1991, a committee of the Board of Regents continued under the Drugless Practitioners Act, a committee of the Ontario College of Social Workers and Social Service Workers under the Social Work and Social Service Work Act, 1998, an arbitrator or a mediator; (“instance”).

“Privacy” means to an individual’s right to be free from intrusion or interference by others and to control how their information is collected, used and disclosed.

“Privacy Breach” means an unauthorized collection, use or disclosure of personal health information under (PHIPA) or of personal information under CYFSA, or a breach of the JF&CS Privacy Policy or related privacy policies.

“Privacy Legislation” means CYFSA and PHIPA.

“Privacy Officer” means the Privacy Officer for JF&CS or their delegate.

“Retention Period” means the period for which agency keeps clients information for as long as necessary to allow clients to exhaust any recourse under privacy legislation that the client may have with respect to the request. Client records are retained as required by law and professional regulations and to fulfill agency purposes for collecting Client Information.

“Right of Access” means an individual has a right of access to a record of personal information or personal health information about the individual that is in the custody or under the control of a health information custodian subject to some exceptions.

“Safeguarding” means taking reasonable steps to protect client information in Agency’s custody or control against theft, loss or unauthorized collection, use, disclosure, copying, modification or disposal. There are three types of safeguards that are used to protect Client Information. These are classified as administrative, technical and physical safeguards.

“Substitute decision-maker”, in relation to an individual, means, a person who is authorized under Privacy Legislation to consent on behalf of the individual to the collection, use or disclosure of Client Information.

“Third Parties” means JF&CS partners, government agencies, police, children’s aid societies, regulatory colleges, courts, lawyers, consultants, external care providers, etc.

“Use” means to view, handle or otherwise deal with Client information, but does not include to disclose the information.

“Vendor Personnel” (for the purposes of these privacy and security terms and conditions) means the vendor’s employees, contractors, subcontractors, students, volunteers and agents. All Vendor Personnel who attend on-site at the JS&CA, will sign a Confidentiality Agreement.