Skylark Children, Youth & Families

POLICY SECTION Programs & Services	POLICY NAME Consent to Release Information and Client Access to Records	POLICY # PS 824
SUBSECTION Client Related	RESPONSIBILITY Senior Director of Children's Mental Health	APPROVED BY Chair of the Board November 2018
EFFECTIVE/REVISED DATE November 2018	LAST DATE REVIEWED November 2018	NEXT REVIEW DATE June 2022

POLICY:

Skylark takes steps to ensure it meets privacy principles and requirements with respect to personal health information under applicable privacy legislation. The purpose of this policy is to ensure that clients are informed about how we collect, use, disclose and protect their personal health information.

Skylark supports the sharing of useful and relevant client information, when it will help the client with other service providers and community resources. However, the agency respects the client's right to confidentiality and privacy. Except where permitted by law such as under the Child Youth and Family Services Act, information will not be released without the signed consent of the client and/or their guardian.

PROCEDURES:

Personal Information We Collect

Skylark and its employees collect personal health information in a number of circumstances in the course of providing services. These employees are referred to as Health Information Custodians under the Personal Health Information Protection Act. Personal health information we collect is contained in a clinical file that includes:

- Name, address, telephone number(s), other business and residential contact information;
- Birth date;
- Client/family health history relevant for client case assessment, treatment planning and treatment provision;
- Other information we may collect with consent or as permitted or required by law.

At intake, staff will review the agency's policies and practices regarding the collection, use, release, and protection of personal information with clients and/or legal guardian and/or substitute decision-maker when they sign the "Consent and Agreement to Participate in Service".

Use of Personal Information

The information provided will primarily be used to deliver services, for professional supervision and quality assurance purposes, including accreditation, and to keep the client/family informed about Skylark programs, services and special events.

Skylark uses a team approach to service delivery, including students, trainees, and volunteers. In many situations we provide integrated care with other agencies and in order to provide the best care to client/family we may share information with other service providers within the network of care. Client/family will be informed that information may be shared among members of the team, both internal and external to the agency.

Unless otherwise directed not to do so by the client, the information may also be used by individuals engaged in reviews of the agency's practices including quality assurance; evaluation; research; accreditation; and licensing procedures. These individuals are required to sign a confidentiality agreement and will not remove client files from the agency's premises. In addition, information is used to provide data related to funding needs, volunteer opportunities, and to publicly recognize donations supporting Skylark. Staff may only collect and use personal information for the purposes listed above and within legal limits such as requirements to follow guidelines related to duty to report.

Disclosure of Personal Health Information

Skylark will not willingly disclose information obtained in confidence from an individual without proper consent, or unless required by law. Skylark may breach confidentiality if it is believed there is a significant risk that a client may seriously harm self or others.

All clients and/or a legal guardian or substitute decision maker will be required to sign the "Consent to Disclose and Receive Personal Health Information" form when agreeing to the sharing of information between Skylark and another external service provider.

Only the Skylark *Consent to Disclose and Receive Personal Health Information* or a form from another organization that contains all of the required information will be accepted as authorization to release or obtain client information. The consent form will clearly identify the name of the organization and staff person releasing and obtaining the information, the client name, the specific information being released or obtained, and the purpose for which it is required. Information on the form will identify any limits on consent such as time period or limits on use of the shared information. The form will be properly signed, dated, and witnessed with an expiry date not exceeding one calendar year. The signed consent will be kept in the client file. When unable to sign the form, at the client's request, expressed verbal consent will be accepted and noted in the file. The worker noting the consent will fill out the required form noting date, time and client's request. Clients are able to request a restriction on certain uses and disclosure of personal health information, or withdraw authorization to use or disclose their information, unless restricted by law. This request will be noted in the client file, and the client will be informed if it can be followed as long as the request does not render service futile or harmful.

Clients 12 years of age or older who are receiving counselling services and understand the concept of consent, are able to sign the *Consent to Disclose and Receive Personal Health Information* without parental or guardian consent. For children under the age of 12, parental or guardian

consent is required. When a request for information is received from another service provider, police, or a third party, the case manager or primary worker will review the client's file with the client and the Program Manager before releasing any information.

Every effort will be made to protect information relating to a third party participant (i.e. sibling, step-parent, etc.) unless Consent *to Disclose and Receive Personal Health Information* is signed by the identified participant. Information received by this agency from another service provider will not be released unless the client has provided consent. Where the information sharing is in the client's best interests and supports continuity of care, the worker will discuss the benefits and risks the client derives from sharing this information with other health-care professionals and/or those who form the client's "Circle of Care". Skylark will always request expressed consent to share information. Psychiatric or any other specialized reports, which are written on behalf of Skylark, may be released but only after consultation with the report's author.

Following receipt of the signed *Consent to Disclose and Receive Personal Health Information*:

- A progress note listing the documents released will be entered in the clinical record or;
- A cover letter/fax sheet listing the documents released will be included in the package to the service provider with a copy of the letter placed in the client's file.

If Toronto Police Services, or police services from another jurisdiction, requests information about a client it must be with consent or required by law.

Skylark does not sell or trade any personal information including mailing lists.

Security

Skylark ensures that records of personal information in its custody are retained, transferred and disposed of in a secure manner. The requirements for these procedures are contained in Skylark's policies related to record retention and storage.

Personal Health Information is protected using physical, electronic or procedural security measures appropriate to the sensitivity of the information in our custody or control. This will include safeguards to protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

Client Access and Correction to the Clinical File

Clients who wish to request access to or make a correction to their personal information in our custody or control, can address this request in writing to the attention of the Privacy Officer.

The right to access a clinical file is subject to applicable restrictions. The Privacy Officer may deny all or part of a request based on several criteria such as:

- Parents/guardians of clients 12 years of age or older who initiated their own counselling do not have the right to access the youth's clinical record without the youth's consent;
- In the opinion of the Privacy Officer or their designee, viewing the record could result in physical or emotional harm to the client or another individual;

- Is subject to a legal proceeding or court order and the agency has been ordered not to release information;
- The information was collected or created during an inspection, investigation or similar procedure;

A client may request information contained in their record be corrected if they believe it is inaccurate or incomplete. A correction will be made except when:

- The record was not created by Skylark;
- The record consists of a professional opinion made in good faith.

Corrections should record the correct information by striking out incorrect information or labelling it incorrect. Once corrected, the client can request that, if reasonable, anyone with whom the information was shared is informed of the correction.

If Skylark does not agree to the correction the client may prepare a statement of disagreement which will be attached to the record.

Skylark will respond within 30 days of receiving a client request to access or correct a file and will provide reasons should access or the requested correction be denied. Any changes to a file will be initialed by the Privacy Officer. Inquiries or complaints related to personal health information practices can be addressed in writing or by telephone to the Privacy Officer at 40 Orchard View Blvd, Ste 255, Toronto, ON M4R 1B9 or 416-482-0081.

Privacy Officer

The Skylark privacy officer is the Chief Executive Officer.

Privacy Breach

Clients will be notified if their information is lost, stolen, or used without authorization. Staff are required to inform the Privacy Officer in the event of a real or suspected privacy breach. In the event of a privacy breach Skylark will make efforts to contain it to the best of its ability. A Serious Occurrence Report will be filed with the appropriate Ministry as required. Risk avoidance measures will be taken to lessen further breach possibilities. Clients and the public are made aware of the agency's privacy breach procedures on the agency website.

Compliance

Staff will understand and comply with the provisions of the Personal Health Information Protection Act. Skylark will annually review and assess compliance by means of a random file audit and during supervision. Non-compliance by staff or agency partners may result in corrective action including termination of employment or working agreement.