taproot
Community
Support Services

Data Security and Privacy

Taproot Community Support Services (Taproot) is responsible for the protection of all personal information that is collected or controlled by agency employees, practicum students, volunteers, or contractors ("personnel") and systems. Only trained and authorized Taproot personnel may collect, access, or disclose personal or confidential information following law and agency policy.

Taproot has multiple procedures and safeguards in place to ensure that the personal information of current and former persons served, their families, and Taproot personnel is protected against the risks of a data / privacy breach.

Collection and Disclosure of Personal Information

Except where permitted by law, Taproot personnel must obtain the informed written consent of the individual or their representative before any personal information about them may be collected or disclosed. To be considered "informed" consent, the individual must understand why the information is being collected and how it will be used.

When requesting their consent, personnel must inform the individual that they may **withdraw their consent** at any time, but by doing so they may prevent Taproot from providing services or offering employment to them.

Taproot personnel must only…

- **collect information that is necessary and relevant to the service being provided, and**
- **store information in secure locations with controlled access.**

Taproot may only use the information for a purpose that aligns with the individual's written consent.

Storage and Retention of Personal Information

All electronic and hard copy records that contain personal information about persons served or personnel must be stored in a secure location with controlled access. Taproot protects electronic records and information using authentication, password protection, and frequent system imaging and backups. Hard copy records are secured in locked locations that only authorized personnel may access.

Taproot may not dispose of person served records without authorization from funders and must return records to funders at the end of the service contract. Taproot retains personnel records following applicable provincial regulatory requirements. All closed / inactive files are stored in a secure location with controlled access.

Any loss or unauthorized access or destruction of a confidential person served or personnel record must be reported as a data / privacy breach.

Data Security

Taproot has multiple data security safeguards in place to protect against the risks of a data breach, including password-protection and encryption software, virus and threat detection software, and secure storage and data sharing procedures for all computer and communication devices used for agency purposes.

If a data breach is discovered, Taproot must notify affected individuals, funders, and government ministries as soon as possible. Taproot also maintains records of every data breach, including a timeline of events, responses, and notices given.

Requests for Access or to Correct Information

Person Served Information

In BC and Alberta, persons served or their guardians must submit requests for access or correction directly to the government ministry that funds their services (the "funder") for access to or copies of the personal information contained in Taproot or funder records.

In Ontario, under the Child, Youth, Family Services Act, agencies that provide child/youth services are authorized to process written requests for information or correction from persons served or their guardians, but all requests must be documented, and the number of requests must be reported to the government annually. Please contact Taproot program management in Ontario for specific information about their process.

Information About Personnel

Except as required by law and in controlled circumstances for third-party reviews (accreditation, inspections, audits), Taproot and our personnel will not provide personal information about any agency personnel or associates—including references or to verify employment—without prior written authorization from the individual following agency policy. Requests for correction must be made in writing to the HR department.

Information About Taproot

If you have more specific questions about Taproot and our services, you may submit them to us using the 'Get in Touch' option on our website or by phone or email to our 'Contact Us' addresses. Taproot personnel will not provide personal or other confidential information and will not answer media inquiries without direct authorization from agency leadership.

Privacy Complaints

Persons served or personnel who have questions or concerns about Taproot's data and privacy policies are encouraged to discuss them with program management or their supervisor following our Open Door Policy.

Formal privacy complaints may be submitted by email to the Taproot Privacy Officer (our CEO) using the Taproot Complaint Form (personnel) or the Person Served Complaint Form (persons served or family), which are included in the person served orientation package and available on request to program management. If you are not satisfied with Taproot's response or if you prefer, you may submit your complaint directly to the Office of the Information and Privacy Commissioner for your province.