PRIVACY POLICY

Public Statement of Information Practices | Effective September 1, 2026

Our commitment

Byrne Psychology Professional Corporation, operating as Connect Cognitive Therapy (the "Practice" or "CCT"), is committed to protecting the privacy, confidentiality, accuracy, and security of personal information and personal health information. This policy explains how we collect, use, disclose, retain, safeguard, and dispose of information, and how clients may exercise their privacy rights.

This document is intended to serve as the Practice's written public statement of information practices under Ontario's Personal Health Information Protection Act, 2004 (PHIPA). It applies to information in the custody or under the control of the Practice, including information handled by clinicians, administrative staff, supervised practitioners, and authorized service providers acting on behalf of the Practice. Specific clinicians may also have additional professional obligations arising from their regulatory College.

1. Who We Are and Who Is Responsible for Privacy

Byrne Psychology Professional Corporation operates Connect Cognitive Therapy and provides psychological, psychotherapy, social work, assessment, consultation, and related clinical services in person and virtually. The Practice includes regulated professionals and supervised/qualifying clinicians, as well as administrative personnel and authorized contractors or service providers.

Privacy Officer / Contact Person: Dr. Nelson Byrne, Byrne Psychology Professional Corporation
Suite 211, 168 Queen Street South, Mississauga, Ontario L5M 1K8
Telephone: 905-275-0665 | Fax: 289-206-0619
Email: reception@mailcct.com (please mark privacy-related correspondence "Confidential – Privacy Officer")

2. What Information We Collect

We collect only information that is reasonably necessary for lawful purposes connected with the services we provide and the operation of the Practice. Depending on the circumstances, this may include:

- identifying and contact information, such as name, date of birth, address, telephone number, email address, pronouns, and emergency contact information;
- personal health information, including mental and physical health history, symptoms, diagnoses, medications, family and social history, treatment goals, risk and safety information, and other information relevant to care;
- information obtained during assessments, including interview information, questionnaires, rating scales, psychological test data, collateral information, and reports;
- clinical records, including consent forms, appointment information, progress notes, treatment plans, correspondence, referrals, reports, consultation and supervision information where applicable, and records of disclosures;
- billing, insurance, payment, and administrative information, including information needed to process payments or provide receipts and invoices;
- communications with the Practice, including telephone, secure portal, email, text message, or other correspondence; and
- technical information generated when you use our website or online services, such as IP address, browser/device information, pages viewed, referral source, cookie identifiers, and website or booking-conversion events.

Personal health information is generally collected directly from the client. We may also collect information from another person or organization when the client has authorized us to do so, when consent can reasonably be implied for the provision of health care, or when collection is otherwise permitted or required by law.

3. Why We Collect, Use, and Disclose Information

We collect, use, and disclose personal health information primarily to provide and support care. Purposes may include:

- assessing needs, providing treatment, conducting psychological or other clinical assessments, and monitoring progress;
- coordinating or consulting about care with other health care providers when authorized or otherwise permitted by law;
- scheduling appointments, providing reminders, responding to inquiries, and communicating about services;
- maintaining the clinical record and meeting legal, professional, insurance, quality-assurance, and regulatory requirements;
- processing payments, insurance claims, receipts, accounting, and collection of unpaid accounts;
- supervision or consultation where relevant to the service, subject to confidentiality requirements;
- practice administration, quality improvement, auditing, security, and investigation of complaints or privacy incidents;
- complying with legal obligations, court orders, regulatory requirements, and permitted disclosures under PHIPA; and
- evaluating and improving our website and communications, including measuring the effectiveness of advertising and referral pathways, using technical and analytics information rather than clinical record content.

Data minimization. We do not collect, use, or disclose personal health information when other information would reasonably serve the purpose, and we limit information to what is reasonably necessary for the purpose.

4. Consent and Your Choices

Consent under PHIPA may be express or implied depending on the circumstances. We seek express consent when required by law or when the sensitivity or purpose of the information makes express consent appropriate. Consent must be knowledgeable, relate to the information and purpose in question, and be given without deception or coercion.

- You may ask questions before consenting and may withhold or withdraw consent to a future collection, use, or disclosure, subject to legal and professional limitations.
- Withdrawal of consent is prospective. It does not require the Practice to erase information that was already lawfully collected or that must be retained as part of the clinical record.
- You may place conditions on certain disclosures. In some circumstances, restricting information may affect what another provider can safely or appropriately do; where required by law, we may need to advise the receiving provider that relevant information has been withheld.
- Declining optional uses of information, including optional marketing communications or optional AI-assisted documentation, will not reduce the quality of care available to you.

Capacity and minors. The right to consent to the collection, use, or disclosure of personal health information depends on capacity and the applicable law, not simply on age. A capable person generally controls their own personal health information. Special rules apply to individuals under age 16 and to substitute decision-makers when a person is incapable of making a particular privacy decision.

5. Artificial Intelligence and AI-Assisted Documentation

The Practice may authorize clinicians to use approved artificial-intelligence tools, including an AI scribe or secure generative-AI platform, for limited clinical documentation purposes. The Practice currently expects to permit BastionGPT for approved uses, subject to its internal privacy, security, consent, and documentation requirements.

Where identifiable client information may be processed by an approved AI tool:

- the client's prior written consent is required before the tool is used with that client's identifiable personal health information;

- the client may decline or later withdraw consent for future AI-assisted documentation without losing access to care; an alternative documentation method will be used;
- the clinician remains responsible for the clinical record and must review, correct, and approve any AI-assisted draft before relying on it or incorporating it into the client record;
- AI tools are not authorized to make autonomous diagnosis, treatment, risk-management, or other clinical decisions on behalf of the clinician;
- depending on the approved function, information processed may include session audio, a temporary transcript, clinical notes, uploaded records, prompts, or draft outputs; only information reasonably necessary for the approved purpose should be provided;
- the Practice does not authorize client information to be sold, used for marketing, or used to train general-purpose AI models; under BastionGPT's current contractual terms, customer data is not used to train AI models;
- for Canadian customers, BastionGPT currently states that data is stored in Canada by default. Limited cross-border access or processing may occur in exceptional circumstances such as support, troubleshooting, failover, or disaster recovery, subject to contractual safeguards;
- temporary vendor-side processing or audit data may be retained for a limited period. Under BastionGPT's current published terms, certain processing data may be retained for up to 30 days; account settings and product features may affect how long user-visible items remain available; and
- CCT reviews approved AI vendors and their contractual, privacy, security, retention, data-residency, and breach-response terms. If the relevant practices change materially, the Practice will update its policies and consent information as appropriate.

De-identified information. The Practice does not currently authorize an AI vendor to use client information for model training, sale, or unrelated commercialization. If the Practice were ever to adopt a routine practice of sharing de-identified client information with an AI vendor or another third party for a separate purpose, we would first ensure legal authority, appropriate safeguards against re-identification, and appropriate transparency, and would update this public policy.

6. Electronic Records, Online Services, and Service Providers

The Practice uses electronic systems and third-party service providers to support clinical and administrative operations. These may include practice-management/electronic-record systems, online booking, secure communications, video platforms, payment processors, cloud hosting, IT/security services, accounting, legal services, website hosting, analytics, and approved AI tools.

Service providers are given access only to the information reasonably required for their role. Where they handle personal health information on our behalf, we select providers and use contractual, administrative, and technical safeguards appropriate to the sensitivity of the information and their role under PHIPA.

Storage or processing outside Ontario or Canada. Some service providers or their subprocessors may store, access, or process information outside Ontario or, in limited circumstances, outside Canada. Information processed in another jurisdiction may be subject to the laws of that jurisdiction. We assess the need for such processing and use reasonable contractual and security safeguards. Vendor-specific information that is material to consent, including approved AI tools, is provided when appropriate.

Payment information. Payment-card information is processed through approved payment systems. The Practice does not intentionally place full payment-card numbers in clinical notes.

7. Website, Cookies, Analytics, and Advertising

Our website may use cookies and similar technologies for essential site functions, security, analytics, and advertising measurement. Depending on your browser and the services in use, these technologies may collect technical or interaction information such as IP address, device/browser data, pages visited, referral source, approximate location derived from IP, and whether a booking or other conversion event occurred.

CCT does not intentionally send psychotherapy notes, assessment results, or other clinical record content to advertising or analytics platforms. Website and advertising analytics are maintained separately from the clinical

record unless information is deliberately submitted through a clinical intake, booking, or contact process. You can manage or block cookies through your browser settings, although doing so may affect some website functions.

When you leave our website for a third-party booking, payment, video, or other service, that provider's own privacy terms may also apply. CCT remains responsible for personal health information that is in its custody or under its control.

8. When We May Disclose Information Without Your Consent

We keep personal health information confidential and disclose it without consent only where permitted or required by law. Examples may include:

- where we believe on reasonable grounds that disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons;
- where child-protection legislation or another law requires a report;
- where a court order, summons, warrant, or other lawful authority requires disclosure;
- where disclosure is required or permitted to a professional regulatory College or other authorized regulator;
- where reporting obligations apply regarding specified professional misconduct, sexual abuse, incapacity, or other matters required by law;
- for legal advice, defence of a legal proceeding, or other proceedings where PHIPA permits disclosure;
- for payment, insurance, or funding purposes where the client has authorized the disclosure or the law otherwise permits it; or
- to a successor or potential successor to the Practice as permitted by PHIPA, subject to confidentiality and security requirements and notice obligations where applicable.

Any disclosure will be limited to the information reasonably necessary for the permitted or required purpose, unless the law requires otherwise.

9. Safeguarding Personal Health Information

We use administrative, technical, and physical safeguards appropriate to the sensitivity of the information and the nature of our practice. Safeguards include, as appropriate:

- role-based access and limiting access to persons who need information for their duties;
- password protection, multi-factor authentication where available, device security, encryption, and secure transmission methods;
- locked or access-controlled areas for any paper records and secure disposal of paper records;
- privacy/confidentiality obligations, training, and policies for clinicians, staff, supervised practitioners, and authorized contractors;
- vendor due diligence and contractual privacy/security requirements for service providers that handle personal health information;
- backups, audit capabilities, access monitoring, and incident-response procedures where supported by the relevant systems; and
- periodic review of privacy, cybersecurity, AI, retention, and information-handling practices.

No method of electronic communication or storage can be guaranteed to be completely risk-free. We therefore select and configure systems with regard to the sensitivity of the information and avoid using unapproved consumer tools for identifiable clinical information.

10. Privacy Breaches and Incident Response

If personal health information is lost, stolen, accessed, used, disclosed, or collected without authority, the Practice will take reasonable steps to contain the incident, investigate what occurred, reduce the risk of recurrence, and meet applicable notification and reporting obligations.

Where PHIPA requires it, affected individuals will be notified at the first reasonable opportunity and advised of their right to complain to the Information and Privacy Commissioner of Ontario. The Practice will also notify the

Commissioner and/or a regulatory College where the prescribed circumstances require it, and will maintain and submit annual privacy-breach statistics as required by Ontario law.

11. Retention and Secure Destruction

Clinical records are retained for at least the minimum period required by applicable law and professional standards. As a general Practice standard, individual clinical records are retained for a minimum of 10 years after the last professional contact or 10 years after the client reaches age 18, whichever is later, unless a longer period is required by law or reasonably necessary in the circumstances.

Different components of a record may be stored in different secure systems. Administrative, billing, tax, contractual, and business records may be subject to different retention requirements. Information that is subject to an active access request, complaint, investigation, legal hold, or other legal requirement will not be destroyed while the matter remains outstanding.

When information is no longer required, paper records are securely shredded or otherwise destroyed, and electronic information is securely deleted or rendered inaccessible using methods appropriate to the system. Where a service provider stores data for us, we require disposal or deletion practices appropriate to the service and applicable contractual requirements.

12. Access to Your Record

With limited exceptions set out in PHIPA and other law, you have a right to access records of personal health information about you that are in the custody or under the control of the Practice. You may contact the Privacy Officer to make an access request. A formal written request is recommended when you are seeking a copy of a record or a decision under PHIPA.

We will respond as soon as reasonably possible and generally no later than 30 days after receiving a formal access request. PHIPA permits a limited extension in specified circumstances. Before charging a fee, we will provide an estimate. Any fee will not exceed reasonable cost recovery as permitted under PHIPA.

Some information may be withheld or severed where an exception applies, for example because of legal privilege, a legal prohibition, serious-harm concerns, or protection of confidential third-party information. Psychological test materials and raw test data are subject to special rules. PHIPA may exclude raw data from standardized psychological tests from the statutory right of access, although the Practice may disclose raw data where permitted and professionally appropriate. Copyrighted or test-secure materials may be withheld or handled differently to protect test integrity and third-party rights.

13. Correction of Your Record

If you believe a record of personal health information is inaccurate or incomplete for the purposes for which the Practice uses it, you may request a correction. We will respond in accordance with PHIPA. The right of correction generally applies to factual information and does not require a clinician to change a professional opinion or observation made in good faith.

If we do not make a requested correction, you may be entitled to require that a statement of disagreement be attached to the record and, where applicable, provided to persons to whom the disputed information was disclosed.

14. Complaints and Questions

Questions, access/correction requests, or complaints about the Practice's privacy practices may be directed to the Privacy Officer listed in Section 1. We will review privacy complaints promptly and will provide a response appropriate to the circumstances.

You may also complain to the Ontario privacy regulator:

Information and Privacy Commissioner of Ontario (IPC)
2 Bloor Street East, Suite 1400, Toronto, Ontario M4W 1A8

Toronto: 416-326-3333 | Toll-free: 1-800-387-0073
www.ipc.on.ca

Concerns about the professional conduct of an individual clinician may also be raised with the clinician's applicable regulatory College, such as the College of Psychologists and Behaviour Analysts of Ontario, the College of Registered Psychotherapists of Ontario, or the Ontario College of Social Workers and Social Service Workers.

15. Legal Framework and Policy Updates

This policy is intended to reflect PHIPA, its regulation, applicable professional standards, and other privacy laws that may apply to particular activities. Ontario's PHIPA is the principal privacy law governing personal health information handled by health information custodians in the province. Federal privacy law, including PIPEDA, may apply to certain personal information or cross-border commercial activities in circumstances where PHIPA does not displace it.

We may revise this policy as our services, technology, vendor arrangements, professional standards, or legal requirements change. The current version will be made publicly available through our website. Material changes that affect consent or client choices will be communicated as appropriate.

Last reviewed: August 30, 2026