# PRIVACY AND CONFIDENTIALITY POLICY

## PREAMBLE

Confidentiality is at the heart of the professional-client relationship, and a relationship of trust leads to better service. Where clients have the opportunity to consent to collection, use or disclosure, they can be secure in their belief that confidentiality will be maintained, which enhances the relationship of trust.

Contact Brant recognizes the importance of privacy and the sensitivity of the personal information service participants give us about themselves and their families to allow us to provide services.

> Our Consent Policy ensures that consent is secured, and the purposes of collection, use and disclosure are made clear to each client.
>
> Our Privacy and Confidentiality Policy sets professional expectations for making clients fully aware of our privacy and confidentiality practices, disclosure, safeguarding and managing personal information, as well as digital communications; client access to and correction of personal information; and processes for any breach of privacy.

This policy recognizes that appropriate sharing of information to plan and provide services is essential for creating successful outcomes for children and families. Contact Brant collects personal information about clients through the intake, referral and service coordination processes directly from clients and their parents/another person authorized to act on their behalf, as well as from other sources/professionals, if we have obtained consent to do so or if the law permits. Contact Brant facilitates the effective access to appropriate services through the disclosure of information with informed consent, and maintains a record of personal information and contacts with all clients served.

Contact Brant follows legislation, including but not limited to the Child, Youth and Family Services Act (CYFSA), the Personal Health Information Protection Act 2004 (PHIPA), and the Canadian Anti-Spam Legislation. The CYFSA references 'personal information' while PHIPA specifies 'personal health information' - our privacy practices are intended to cover all personal information collected about clients.

> The Child Youth and Family Services Act, Section X, regarding Personal Information, was developed to protect the privacy rights of children, youth and their families; to clarify how personal information can be collected, used and shared; and to enable the better use of data to understand sector outcomes. The paramount purpose of the CYFSA is to promote the best interests, protection and well-being of children. It recognizes that appropriate sharing of information to plan

and provide services is essential for creating successful outcomes for children and families. Children and youth receiving services under the CYFSA have rights, including the right:

- To express their views freely and safely about matters that affect them
- To be consulted on the nature of the services provided and participate in decisions about services provided to them
- To raise concerns or recommend changes to their services, and to receive a response without interference or fear of coercion, discrimination or reprisal.

Under the Personal Health Information Protection Act, Contact Brant is a **Health Information Custodian** (HIC) as defined in PHIPA. A Health Information Custodian is responsible for collecting, using and disclosing personal health information on behalf of clients, when that personal information:

- Relates to an individual's mental or physical condition, including family medical history,
- Relates to the provision of care to the individual,
- Is a plan of service for the individual,
- May include the individual's health number (when required by a provider)
- Identifies a health care provider or a substitute decision-maker for the individual.

The CYFSA and PHIPA are very similar in their expectations for the manner in which personal information (CYFSA) or personal health information (PHIPA) may be collected, used and disclosed. Contact Brant follows PHIPA related to the collection, use and disclosure of personal health information, and follows the CYFSA related to the collection, use and disclosure of personal information that is not defined as personal health information.

Collection means to gather, acquire, receive or obtain personal information by any means from any source (verbally, written, electronic). Collection can be direct from the person to whom the information relates or their substitute decision-maker, or indirect from a third party.

Use means to handle or deal with the information in the custody or under the control of Contact Brant (e.g., review a file for continuity between staff; review information when meeting with a family, providing the information to a supervisor or other employee when reasonably necessary for carrying out that purpose). Use does not include disclosure.

Disclosing or sharing means to make the information in the custody of Contact Brant available to another service provider or person. Consent for disclosure must be explicit; it can be written or verbal consent which must be recorded within the client's EMHware record.

Where federal laws such as the Criminal Code or Youth Criminal Justice Act prohibit disclosure of personal information, they prevail over CYFSA and service providers cannot disclose information. The YCJA publication ban overrides consent and access to information as laid out in PHIPA.

The personal information that we collect may include, but is not limited to:

- Race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual
- Education or the medical, psychiatric, psychological, criminal or employment

history of the individual or information relating to financial transactions in which the individual has been involved

- Any identifying number, symbol or other particular assigned to the individual
- Address, telephone number, fingerprints or blood type of the individual
- Correspondence sent to a service provider by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence
- The personal opinions or views of the individual except where they relate to another individual
- The views or opinions of another individual about the individual
- The individual's name where it appears with other personal information relating to the individual, or where the disclosure of the name would reveal other personal information about the individual
- An individual's health card number – Note: A health card number can only be shared with health care providers that require this number for their provision of service.

Personal Information can be recorded or unrecorded information about an identifiable individual. *Recorded Information* is information recorded in any format, such as paper records and notes, electronic records, photographs, or videos. *Unrecorded Information* is collecting information that is not recorded, such as information collected through a phone call or an intake interview. An individual can be identified if:

- Information reveals something of a personal nature about the individual, or
- It is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information).

CYFSA and PHIPA also set out rules regarding privacy and access to personal information. With limited exceptions, Contact Brant must have consent to collect, use or disclose personal information; must take steps to safeguard this information; and must notify people if there is a breach of their privacy. Contact Brant must give individuals access to their records of personal information on request, subject to limited exceptions, and must respond to requests for correction of inaccurate or incomplete records.

General Privacy Principles

Privacy legislation is based on internationally accepted standards, including:

- **Accountability**: An organization is responsible for personal information under its custody or control.
- **Identifying Purposes:** Organizations must identify purposes for personal information collection before collecting.
- **Consent:** Knowledge and consent for the collection, use and disclosure of personal information is required.
- **Limiting Collection:** Personal information collection must be limited to what is necessary for purposes identified and collected by fair and lawful means.
- **Limiting Use and Disclosure and Retention:** Personal information use and disclosure must be limited to purposes for which it was collected, unless consent is provided or otherwise permitted by law. Personal information should only be retained as long as is necessary to fulfill the organization's stated purposes.

- **Accuracy:** Personal information must be as accurate, complete and up-to-date as needed for the purposes it is being used.
- **Safeguards:** Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
- **Openness:** Organizations must make information about its policies and practices relating to personal information management publicly and readily available.
- **Individual Access**: Upon request, individuals must be informed of the existence, use and disclosure of their personal information and be given access to that information. Individuals can also challenge the accuracy of their personal information and request amendments, as appropriate.
- **Challenging Compliance**: Individuals must have the right to challenge compliance of the organization with the above privacy principles.

Also refer to the Contact Brant Consent Policy, AD-02. The Contact agencies consulted with Lonny Rosen, LLP, to develop our Consent and Privacy policies.

*In this policy we use the terminology 'personal information' to include both 'personal health information' and 'personal information' described in both PHIPA and CYFSA.*

*The term 'Contact Brant' is used in this policy statement and procedures to reflect Contact Brant employees, students and volunteers.*

## POLICY

Contact Brant is a Health Information Custodian (HIC) and will adhere to the expectations set out in the Personal Health Information Protection Act, as well as the Child Youth and Family Services Act, to collect, use and disclose personal information in order that clients can access programs and services.

Contact Brant respects privacy and holds personal information confidential. Contact Brant will:

- Ensure knowledgeable consent and purposes for the collection, use and disclosure of personal information
- Ensure people are made fully aware of our confidentiality and privacy practices
- Limit collection, use and disclosure to what is necessary for purposes identified
- Ensure personal information is as accurate, complete and up-to-date as needed for the purposes it is being used
- Take all reasonable measures to safeguard personal information in our custody and control
- Recognize client's rights for access to and correction of personal information
- Identify and address any breach of privacy.

## PROCEDURES

1. In accordance with CYFSA and PHIPA, Contact Brant follows the standards for collection, use, and sharing of personal information to protect the confidentiality and privacy of individuals with respect to that information, and take reasonable steps to safeguard the information they maintain, while facilitating the effective provision of services.

2. Personal information includes any identifying information about an individual in oral, paper and/or electronic form that relates to:
    - The physical or mental health of an individual including their medical, clinical, and psychological history; social or demographic information; and family-related information
    - Providing care, including identifying a provider of care
    - Identifying a substitute decision-maker
    - An individual's health card number
    - Any observation, assessment, care, or service that is carried out or provided to treat or maintain an individual's physical or mental condition, prevent injury or to promote health.
3. Informed Consent will be obtained for the collection, use, and disclosure of personal information, unless legally obligated to without consent. Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Refer to *Consent Policy, AD 02*.
    - Contact Brant may disclose a client's personal health information to other health care providers in their "circle of care" (refer to PHIPA legislation), when they need to know certain information to help provide a client with services, and we cannot gain consent in a timely manner. The "circle of care" includes health care professionals (client's physician, psychologist) or if the client has been in hospital, the hospital staff.
      The circle of care does not include any health care provider who is not a part of the direct or follow-up team, a teacher or employee of a school board, a Children's Aid Society or CAS workers, medical officer of health or a board of health, an assessor under the Substitute Decisions Act, 1992 or any Ministry or Government Agency.
4. Even with consent, there are three limits on when and how much personal information can be collected, used or disclosed. Contact Brant must:
    i. Ensure, to the best of their knowledge, that the collection, use or disclosure is necessary for a lawful purpose.
       For example, even if a client gave consent to use their personal information "in any way you please," you may only use it where necessary for a lawful purpose.
    ii. Only collect, use or disclose as much personal information as is reasonably necessary to provide a service.
       For example, even with consent it would not be appropriate to collect information about clients' political affiliations, unless you somehow need this information to provide service.
    iii. Not collect, use or disclose personal information where non-personal information will serve the same purpose.
       For example, if applying for a grant and need evidence of successful client outcomes, provide de-identified or statistical information. In this case, there would be no need to disclose clients' personal information in the application.
5. Contact Brant will take all reasonable steps to ensure the information is as accurate, complete and up-to-date as possible. When disclosing information, recipients will be informed of any limitations on the accuracy, completeness, or up-to-date character of the information.

6. In accordance with professional standards, Contact Brant will maintain a record of services and contacts with all clients served. Refer to AD 09 *Retention of Records Policy*. Records containing personal information include but are not limited to:
    - The Intake Report that includes information that a client has provided or authorized us to receive
    - Referral information
    - Service and transition plans, including Coordinated Service Plans
    - Assessments, including the interRAI, or assessments completed by others
    - Consent forms or documentation of verbal consent
    - Confirmation of diagnosis
    - Case notes that outline direct contacts and service provided
    - Service related communication.
7. Unauthorized use of information is not allowed. Access to personal information including the review of client records whether in electronic or written form is **restricted to a "need to access" basis**. Contact Brant staff, students and volunteers, only have the authority to access the client's records only in accordance with their unique roles and responsibilities. Employees, students and volunteers reading records for reasons not related to the performance of their duties is an unauthorized use of information and is not permitted under legislation.
    - Snooping due to curiosity about a familiar name or any other reason not related to the performance of duties is not allowed. Any snooping is cause for disciplinary action.
    - The Chief Executive Officer may access any record for the purposes of review of staff work, or client information in accordance with the CEO roles and responsibilities.

**Disclosure of Personal Information**

8. Contact Brant will operate in a culture of privacy. Contact Brant will never discuss unnecessarily with other Contact Brant employees, students or volunteers.
9. Staff should inform clients they have an obligation to disclose information where a person is deemed to be at risk:
    - Disclosure to Children's Aid Societies – information shared should only include the facts and circumstances surrounding the worker's observations and informant's statements.
    - Disclosure to Police – a warrant is required to allow disclosure and production of information to police. If police request information, disclosure is not required unless a clear duty to report exists.
    - Disclosure to a parole officer can only occur with express consent or pursuant to a court order.
10. Disclosure of personal information must be documented in EMHware Contacts. It is also recorded in the Referral tab when a referral is sent through EMHware.
    - When disclosure without consent is reasonably necessary to reduce a risk of serious harm, a record of what information was disclosed, when and to whom, along with the reason for doing so will be completed in EMHware Contacts tab.

11. Employees, student and volunteers will sign a Confidentiality Statement and Promise of Commitment to commit to protect the confidentiality of the information; protect the privacy of individuals with respect to that information; facilitate the effective provision of services through appropriate collection, use, and disclosure of information; and safeguard the information. If an employee discloses or fails to take reasonable efforts to protect confidential information, they will be subject to disciplinary action up to and including termination.
12. Employees, students and volunteers will not disclose any information during or after ceasing employment or placement at Contact Brant to any third party for any reason, except with informed consent by the appropriate person.
13. Contact Brant can:
    - Use Personal Information for our own service planning purposes - Supporting system service planning is part of explicit consent that Contact Brant requests from each client.
      (System/service planning includes activities related to planning services such as analyzing individuals' personal information to allocate resources, manage, evaluate or monitor programs and services).
    - Use personal information for research purposes if a research plan is developed that meets requirements outlined in legislation, and approval of the research plan is obtained from a research ethics board that has at least five members, with at least one member that is knowledgeable in privacy issues. (Research is performing a methodical study in order to prove or disprove a hypothesis).
    - Disclose personal information to a Prescribed Entity or a First Nations, Inuit or Métis person or entity (FNIM entity) for system/service planning purposes under certain circumstances, as listed in CYFSA.
14. **The Youth Criminal Justice Act limits disclosure** of children age 12 – 17 years of age who have been convicted on criminal offenses.
    - A youth's voluntary self-disclosure of criminal behaviour or actions which have not received formal court involvement or charges under the YCJA, do not fall under these guidelines.
    - Contact Brant would typically identify "police involvement".
    - Contact Brant will not release any client information related to youth justice involvement or charges. All information received from the youth or others that would serve to identify the youth as having youth criminal justice involvement will not be released, including but not limited to identifying convictions, probation, and court diversion decisions.
    - Contact Brant is permitted to record and store information related to the youth's criminal behaviour or charges as part of delivery of services. To ensure that this information is not shared, this information should only be noted in Contacts/Case Notes and never in the Intake Report or Coordinated Service Plan.
        - If the client's file was subpoenaed, the case notes identifying involvement with the YCJA must be redacted.
    - Records, which contain YCJA information, will be destroyed when the youth turns 28 years of age.

**Safeguarding and Managing Personal Information**

15. Contact Brant will take all reasonable steps to protect personal information by ensuring it is appropriately stored and protected against theft, loss and unauthorized use or disclosure; protecting against unauthorized copying, modification or disposal; and ensuring that all records are retained, transferred and disposed of in a secure manner. This includes, but is not limited to, electronic records, emails, written files and notes. Safeguard measures include but are not limited to:
    - Collecting information sent to the printer immediately.
    - Private area for photocopying and printing.
    - Not including personal information in emails, and encrypting documents sent by email.
    - Locking desks, cabinets, filing systems, and offices where personal information is stored.
    - Reasonable steps outlined in policies and procedures to protect personal information from theft, loss, unauthorized use/disclosure, and unauthorized copying, modification or disposal.
    - Limiting faxing of personal information unless this is the required format of the recipient. A fax cover sheet will always be completed, clearly identifying the sender and recipient, as well as a warning that the information is confidential and intended for the named recipient only and to contact the sender if the communication is misdirected
    - Using screensavers and individualized login and passwords to access computers, databases, portable devices. Passwords should be changed at least two times annually.
    - Making electronic files accessible to employees off-site through password access - this must be used instead of transporting notes and files wherever possible.
    - Only taking personal information out of the office when necessary and limiting this to needed information (for example, case conference minutes, CSPs for distribution). Employees must transport any personal information maintaining confidentiality and security through use of a brief case/bag, locking the file/information in the trunk of car, ensuring the information is with the employee at all times, and protecting against unauthorized access.
    - Ensuring that personal information is disposed of in a secure manner through shredding.
    - At least annual assessment of potential threats and risks associated with the collection, use and disclosures of personal information.
    - Privacy and security policies and procedures.
    - The Chief Executive Officer ensures employees, students and volunteers review policies at hire and annually thereafter. Additionally the CEO ensures staff training on hire and annually thereafter on privacy and security as well as confirmation of confidentiality declarations.
    - The Chief Executive Officer at least annually audits information and security practices.
    - Protecting the premises by lock and alarm, and procedures that ensure the building is secure when closing the building

- Ensuring anti-virus, firewall and security measures are maintained on all computers as well as external databases
- Storing records in a locked filing system in a locked file room marked "Employees Only"
- Ensuring that all contracts with outside parties that may have access to technological equipment, records, or private areas of the office include an expectation and agreement of confidentiality.
- Securely destroying records when appropriate by irreversible shredding of paper records and by engaging an expert for electronic records. Refer to Retention of Client Records Policy, AD-09.
    - The Chief Executive Officer will ensure agents engaged in disposal of records, have a written agreement that sets out the obligations for secure disposal and requires the agent to provide written confirmation once secure disposal has been conducted.
- A "lock box" system through EMHware or hard copy record, to be used for information that allows only prescribed access. This may include when a client is directly related to a staff member, or a person has restricted the use that may be made of personal information or who can see and use part or all of the person's personal information.

  Measures will include:
    - Sealing restricted information in an envelope within the person's file and labelled with the details of the restriction
    - The client related to a staff will have files secured in a separate location with only the Chief Executive Officer and staff directly involved with that client having access to the file while the file is active; after closure only the Chief Executive Officer will have access to the file; information will not be discussed at staff meetings or with other staff. If the Chief Executive Officer is to be excluded, an alternate will be identified, usually the Executive Assistant.
    - Wherever possible electronic files will be protected by limiting access to specific client files.

**Access to and Correction of Records**

16. Contact Brant recognizes individuals have a right to access and review their record of personal information, or where a restriction on access applies, to access that part of the record that can be severed. Individuals also have the right to request correction and amendments to their record:
    - An individual of any age who is deemed capable of giving consent;
    - Parents/guardians of a client who is under the age of 16.
    - Parents/guardians of a client of any age who is deemed incapable.
17. Contact Brant will respond within 30 days to an access request, preferably in writing. Contact Brant will expedite the response where it is necessary for the individual's request.
    - Contact Brant will verify the individual's identity prior to access to the record.
    - A Contact Brant employee will be present while the individual is reviewing their records due to the confidential nature of information about other individuals

contained within the database, and the importance of ensuring that paper records are not lost.

- Contact Brant will make a copy of part of the record or the complete file to provide to the individual if they request a copy; the client will not be given the original record. There will be no cost charged for providing a copy.

18. An individual may be denied access to all or part of their personal record:
    - Granting access could reasonably be considered to result in risk of serious harm to the treatment or recovery of the individual, or risk of serious bodily harm to the individual or another person
    - Lead to the identification of a person who was required by law to provide information or a record
    - Lead to the identification of a person who provided information explicitly or implicitly in confidence and the employee in consultation with the Chief Executive Officer considers it appropriate to keep that person's identity confidential
    - A provincial or federal Act, or a court order, prohibits disclosure of the information to the individual
    - The parent/guardian of a client under 16 may designate specific information that is in the record that relates to the parent as information that will not be disclosed to the child.
19. An individual may request a correction informally; however, requests must be in writing for an individual to invoke the rights and requirements in the CYFSA, including having a service provider respond within a specified timeline or having the right to appeal a refusal to make a correction.
    - The individual must demonstrate that the record is inaccurate or incomplete for the purposes for which Contact Brant uses the record, and provide the necessary information for the correction
    - Employees in consultation with the Chief Executive Officer must correct the record within 30 days when a request is received in writing. If an extension is required, Contact Brant can extend up to 90 days (for a total of 120 days) with written notice of the extension, the length of extension, and the reason for it.
    - Corrections should not destroy the erroneous information; staff will not use white out or delete the information. Documentation in the client's EMHware Contacts will record the information that was identified as incorrect, and the date the record was corrected.
    - A notice of the correction will be provided in writing to the client, and to any organization/person who received the original record.
20. Contact Brant is not required to make corrections when they consider that:
    - A professional opinion or observation was made in good faith about the individual
    - The record was not originally created by Contact Brant and deem we have insufficient knowledge, expertise or authority to make the correction; or
    - Contact Brant believes on reasonable grounds that the request is frivolous, vexatious or made in bad faith.

21. When Contact Brant refuses a request for a review or correction, the individual must be informed in writing of the refusal including:
    - An explanation of the decision
    - Their right to appeal the refusal to the Contact Brant Board
    - Their right to attach a statement of disagreement.
    - Contact Brant must attach this to the client's record and disclose this whenever we share information to which the statement relates.
    - Their right to make a complaint to the Information and Privacy Commissioner; the IPC contact information will be provided.
    - The Contact Brant complaints brochure will accompany this letter.
22. Employees will document in the client's record in EMHware Contacts:
    - All requests for reviews or corrections and dates
    - All items reviewed and dates
    - Decisions made about requests and corrections including refusals for and the reasons
    - Identification of all records items reviewed or photocopied and dates
    - Outcomes of requests and reviews.

23. **Privacy Officer** - The Chief Executive Officer is the agency's Privacy Officer.
    - Employees, students and volunteers will direct people to the CEO if they have complaints about the agency's privacy and confidentiality practices.
    - Issues will be dealt with according to Contact Brant's complaints procedures (Refer to *Complaints Policy, AD 08,* and *Feedback and Complaints Brochure*).
24. The CEO will ensure the required statements related to Contact Brant's information privacy practices are publicly posted on our website and in the Contact Brant office area (Refer to the Privacy and Consent Statement):
    - General description of the agency's information practices for the collection, use, and disclosure of personal information;
    - Describe how to contact the service provider;
    - The process for accessing and correcting personal information;
    - The process for making a privacy complaint to the agency and the IPC.

25. **Digital Communication** - The Canadian Anti-Spam legislation outlines expectations for any form of digital contact from an organization to an individual for the purpose of solicitation of almost any kind. It is important to consider the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message. Employees, students and volunteers will consider the content of the message, the hyperlinks in the message to content on a website or other database, and the contact information contained in the message. (refer to the *Anti-Spam Policy, AD 13*)

    Contact Brant must:
    - Obtain consent to send a message using any means of telecommunication. When requesting a client's email, staff must request consent to use the email to send QSS, PSS, letters, or other specific communication. This will be recorded in EMHware in the 'Client' tab, using the 'Flagged Note' text box –

include the person's name that provided the consent, the date and the purpose identified to use this email.

- Clearly identify the employee's name as well as the agency in all means of telecommunication. This must include using a standard 'signature' on emails that will include name, position, and email as well as agency logo, address, phone and website.
- Every telecommunication message sent must provide a way for recipients to 'unsubscribe' from receiving messages in the future.

26. **Breach of Privacy** - A privacy breach occurs when there is unauthorized access to or collection, use, or disclosure of personal information; this occurs when personal information is:
    - Lost
    - Stolen
    - Used without authority
    - Disclosed without authority.
27. In any occurrence of a suspected privacy breach, the Chief Executive Officer, or alternate, will act immediately to contain the breach:
    - Breach containment includes but is not limited to retrieving hard copies of information that has been disclosed, and changing passwords to protect against further unauthorised access.
    - Commence an investigation to decide the most appropriate response including identifying who, if anyone, should be notified, and identify steps to prevent future breaches.
28. When a Privacy Breach is deemed to have occurred, Contact Brant will notify the individual(s) of the breach at the first reasonable opportunity that will include:
    - A general description of the breach, in plain language;
    - A description of the action taken to address the breach and mitigate impact;
    - The contact information of an employee who can provide additional information; and
    - A statement that the individual is entitled to make a complaint to the Information and Privacy Commissioner.
    - This will be documented in Contacts in each client's EMHware record.

    Note: Contact Brant has insurance that may cover the costs of notification and managing communication and risks related to a Privacy Breach.
29. Information and Privacy Commissioner (IPC) - The IPC is responsible for the oversight of information sharing and privacy protection by service providers including resolving complaints; receiving notification of significant privacy breaches; publishing annual statistics; and supporting implementation. The Commissioner reports to the Legislative Assembly, and is independent of the government.

    Contact: Information and Privacy Commissioner of Ontario: https://www.ipc.on.ca; 416-326-3333
30. The CEO or designate will notify the Information and Privacy Commissioner, as well as the Ministry Program Supervisor(s) when:
    - The breach is significant as determined by the service provider after

assessing the sensitivity, volume, number of persons impacted, and number of service providers involved.

- Personal information was used or disclosed by someone who knew or should have known they were doing so without authority.
- The service provider has reasonable grounds to believe the personal information was stolen.
- The service provider has reasonable grounds to believe the breached personal information has been or will likely be used or disclosed again without authority, or there is a pattern of similar breaches.
- The breach led to an employee resigning or being terminated, suspended or disciplined.

Note: A Serious Occurrence Report should also be submitted (e.g., Any complaint made by or about a client, or any other serious occurrence concerning a client, that is considered to be of a serious nature). Refer to AD 05 *Serious Occurrence Policy.*

31. Before March 31st of each year, the Chief Executive Officer will report the following to the IPC:
    - Requests for access or corrections to records (number, timelines, responses including refusals)
    - Privacy breaches resulting from theft, loss or unauthorized use or disclosure (number and type)
    - Use and disclosure outside of the scope of the provider's information practices (number and type)
    - The number of times Contact Brant received a statement of disagreement after a correction was refused
    - The number of times Contact Brant responded within 30 days and the number of times the deadline was extended to 90 days or less.

32. The CEO will report any breach of privacy and follow-up to the Board of Directors at the next Board meeting. The Board will address whether any further responses and actions are required.

33. The Chief Executive Officer will:
    - At least annually audit information and security practices to ensure that policies are up to date.
    - Ensure employees, students and volunteers are aware of their duties through initial and then annual review of policies, including the Privacy and Confidentiality Policy.
    - Also maintain the confidentiality of employee information; the release of information to a third party will only be done with the written authorization of the employee, unless legislation requires otherwise.