Privacy and Data Retention Policy

1. Purpose

Research Power Inc. (RPI) is committed to respecting the privacy of individuals and protecting the privacy of data and information provided to RPI in the course of our business. This policy applies to all information handled by the organization, including but not limited to data received, stored, processed, or transmitted in any form. This includes electronic data, physical documents, and other media, regardless of the format or storage method. This policy describes RPI's approach and procedures related to the collection, use, retention, and disclosure of data and information.

2. Definitions

Personal health information, as defined in the Personal Information Protection and Electronic Documents Act (Canada) and the Personal Health Information Act (Nova Scotia) means information about an individual, living or deceased, including:

(a) information concerning the physical or mental health of the individual, including information that consists of the health history of the individual's family;
(b) information concerning any health service provided to the individual;
(c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
(d) information related to the application, assessment, eligibility and provision of health care to the individual, including the identification of a person as a provider of health care to the individual;
(e) information related to payments or eligibility for health care in respect of the individual;
(f) the individual's registration information, including the individual's health-card number;
(g) information that identifies an individual's substitute decision-maker; or
(h) information that is collected incidentally to the provision of health services to the individual.

Personal information, defined in the Freedom of Information and Protection of Privacy Act (Nova Scotia) means recorded information about an identifiable individual, including

(a) the individual's name, address or telephone number,
(b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
(c) the individual's age, sex, sexual orientation,
(d) marital status or family status,
(e) an identifying number, symbol or other particular assigned to the individual,
(f) the individual's fingerprints, blood type or inheritable characteristics,
(g) information about the individual's health-care history, including a physical or mental disability,
(h) information about the individual's educational, financial, criminal or employment history,
(i) anyone else's opinions about the individual, and

(j) the individual's personal views or opinions, except if they are about someone else;

3. Informed Consent for Data Collection

RPI collects information from and on behalf of its clients to complete work as described in client contracts and service agreements. We may also collect information for other business purposes such as contacting and providing information to current and potential clients about our services or hiring and managing employees and sub-contractors.

Any information about identifiable individuals ("Personal Information" and "Personal Health Information") collected by RPI or provided to RPI in the course of its business relationships and service agreements with clients is protected. This means that, at the point of collection, individuals providing information will be informed that personal information is being collected, the purpose for which it is being collected, and that they have a right to access their information. Providing this information to individuals may be done by RPI or the client, depending on who is collecting the information.

4. Protection of Information

RPI adheres to the Privacy Management Guidelines below to protect all information, including Personal Information and Personal Health Information from loss, unauthorized access, modification, or disclosure.

Minimum Required Information Collected

RPI collects the minimum amount of information required for business purposes and, whenever possible, ensures that information collected by RPI or provided to RPI by clients does not include identifiable Personal Information or Personal Health Information (e.g., collecting an age category instead of a date of birth; using anonymous data collection; using a unique identifier specific to the project instead of a health-card number) .

Storage

RPI stores Personal Information and Personal Health Information on a secure Microsoft SharePoint/OneDrive server (for electronic information) or in a locked cabinet (for hard copy information). Microsoft servers for electronic data are located in Canada. In addition, we have implemented technological safeguards including anti-virus software, enabling multi-factor authentication, and firewalls to prevent unauthorized access to devices and electronic files.

No RPI data, including Personal Information and Personal Health Information, is permitted to be stored on local devices including computers, cell phones, and other mobile devices. The following policies apply:

- If virtual meetings (e.g., Zoom, Teams) are recorded, the recordings may be temporarily saved locally but then must be immediately moved to SharePoint/OneDrive as soon as the recording is completed.

- If RPI team members access email using their cell phone, they are not permitted to download any attachments to their phone. For secure access to RPI documents on mobile devices, staff must use the OneDrive app.

See the Data Retention section for additional details.

Disclosure

RPI will not disclose Personal Information and/or Personal Health Information to any third party, unless individuals have provided informed consent for this disclosure.

No mobile information will be shared with third parties/affiliates for marketing/promotional purposes. All other categories exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties

Access and Correction

Only RPI employees and sub-contractors that have a direct need to access information to complete their duties are provided with access to data. All RPI employees and sub-contractors of RPI sign a strict confidentiality agreement. Any employee or sub-contractor violating the terms of this agreement will be terminated.

RPI supports an individual's right to access their Personal Information and/or Personal Health Information. RPI will provide access to information following a written request from individuals.

5. Data Retention and Deletion

This section describes RPI's approach to retaining and deleting data. The objective is to ensure data is retained only for as long as necessary to meet legal, regulatory, and operational requirements and to minimize risks associated with over-retention of data, including potential cyberattacks.

Roles and Responsibilities

RPI Partner Clare Levin (Data Lead) holds primary responsibility for handling, retaining, and deleting data. These duties may also be assigned to staff as required, and staff are expected to follow the required procedures to manage data.

The Data Lead is responsible for:

- Being aware of any changes to laws or regulations related to data privacy and implementing processes to ensure compliance.
- Reviewing contracts to ensure compliance with privacy standards and protection of individualized data.
- Evaluating reported or discovered data breaches or incidents and escalating them for investigation.

- Securely archiving or deleting data at the end of its retention period, as outlined in the Data Retention and Deletion section below.

Employees and sub-contractors are responsible for:

- Adhering to this policy and ensuring that sensitive and confidential information is always protected.
- Following any additional practices or procedures that may be requested by a specific client.
- Acting with integrity and diligence when handling data and reporting any concerns or incidents to the Data Lead.

Data Retention and Deletion

RPI is committed to managing data responsibly and in compliance with applicable laws and regulations.

Upon reaching the end of the retention period, data will be securely deleted or archived as indicated in the table below. All individuals will be informed of the data retention and deletion policies and their rights to request data deletion. RPI clients may request permanent destruction of their project information (data/information provided to RPI or collected by RPI on behalf of a client) at any time.

Data	Retention Time	Archive/ Delete
Client project files	5 years	Delete
Final copies of key project documents developed by RPI (e.g., final reports, data collection tools)	Permanent	Archive
Financial files (income statements, invoices, receipts, etc.)	7 years	Delete
Annual financial reports (tax returns, final income statements)	Permanent	Archive

Secure Methods for Deleting Data

RPI is committed to securely deleting data when it is no longer needed, or its retention period expires. The approved methods for secure deletion of digital and physical data are described below.

Digital Data

- Data stored on OneDrive/SharePoint: Use secure deletion features provided by Microsoft.
- Devices no longer being used for RPI purposes: Reset the device to factory settings if it will be used for another purpose. Otherwise, physically destroy the hard drive (HDD or SSD) through shredding, pulverizing or melting.

Physical/Paper Documents

- Shredded using a professional shredding service.

6. DATA BREACH RESPONSE

RPI takes data security seriously and has procedures in place to respond promptly and effectively to any actual or suspected data breach involving Personal Information or Personal Health Information. **All team members and subcontractors are required to report any suspected data breach immediately.** If a data breach is suspected or confirmed, the following steps should be taken:

1. **Contain and Assess:** The breach will be contained to prevent further exposure or unauthorized access. RPI will assess the nature and scope of the breach, including what information was affected, how it happened, and the potential impact.

2. **Notify Affected Parties:** Individuals whose information may have been compromised will be notified as soon as possible if there is a real risk of significant harm. Notifications will include:
    a. A description of the breach
    b. The type of information involved
    c. The steps RPI is taking to address the breach
    d. Recommendations to help affected individuals protect themselves

3. **Reporting to Authorities:** RPI will report the breach and maintain a record of the breach as required under applicable laws.

4. **Corrective Action and Prevention:** RPI will investigate the root cause of the breach and implement any necessary changes to prevent recurrence. This may include updates to policies, technical safeguards, or staff training.

Policy Revision History:

DATE	DESCRIPTION OF REVISIONS	PERSON RESPONSIBLE
July 2025	Policy created	Richard Buote