THE ROYAL / LE ROYAL

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

McGill

ARCHIMEDES

Ethics and Data Governance Framework

Version 1.0

January 2026

uOttawa

INTERCONNECTOME
CŒUR-CERVEAU
BRAIN-HEART
INTERCONNECTOME

camh

1. Definitions

Authorized User: The employees, agents, or trainees of the Data User, to whom data use privileges are assigned relative to one or more Research Projects (referred to as both Authorized Personnel and Authorized Trainees).

Data Contributor: An organization that contributes data to ARCHIMEDES. The Data Contributor obtains required legal authority to contribute data (e.g., consent or other), selects a tier of data release (open or controlled), ensures the data is Coded or De-identified, and signs a Data Contribution Agreement. Data Contributors are responsible for ensuring that their authorized Principal Investigators and Contributor Users comply with applicable laws, ethics requirements and technical standards, and the terms of the Data Contribution Agreement (defined below).

Data User: An organization that receives Controlled Access data from the Data Contributor through ARCHIMEDES. Data Users are responsible for ensuring that their data usage, and that of their authorized Principal Investigators and Authorized Users, complies with applicable laws, ethics requirements, technical standards, and the terms of the Institutional Data Access Agreement (I-DAA) or Data Access Agreement (DAA) (defined below).

Coded: Direct Identifiers are removed from the data and replaced with a code. It may be possible to re-identify specific participants (i.e., the Principal Investigator retains a list that links the research participants' code names with their actual names so data can be re-linked if necessary).[1] ARCHIMEDES treats Coded data like personal information, to which data protection laws continue to apply.

Collection: A dataset, or a group of datasets, which are subject to common oversight and permissions, and generated with the intent of being analyzed, shared to the appropriate tier of access, and used together, generally at the direction of one Data Contributor's Principal Investigator. Each Collection is a subset of the data.

Contributor User: The employees, agents, or trainees of the Data Contributor, to whom data contribution privileges are assigned relative to one or more Collections (referred to as both Contributor Personnel and Contributor Trainees).

Controlled Access: Data released in Controlled Access is exclusively made available to Principal Investigators, and their Research Team, for an approved research purpose. Prospective Data Users must submit a request to access Coded data for a specific Research Project, obtain approval from the ARCHIMEDES Data Access Committee (DAC), and have their host organization conclude an I-DAA or DAA before being able to access data.

Core Permissions: To share data through ARCHIMEDES, the Data Contributor must demonstrate that it has obtained the permissions described at s. 3.2.1 for release in Open Access and at s. 3.2.2 for

[1] Government of Canada. (2022). *TCPS 2 (2022) – Glossary*. Panel on Research Ethics. https://ethics.gc.ca/eng/tcps2-eptc2_2022_glossary-glossaire.html

Controlled Access through an informed consent to research participation and ethics approval, an ethics waiver of informed consent requirement, or other legal authorization.

De-identified: Information that identifies an individual as well as information that could be used, either alone or with other information, to identify an individual based on what is reasonably foreseeable in the circumstances is removed. (Verb: to de-identify; outcome De-identified Data). In practice, de-identification is the process of transforming identifiers in a dataset so that the risk of re-identification is very low.[2]

Direct Identifier: Variables that can be used to uniquely identify an individual, with or without the use of external information (e.g., name, civic address, social insurance number).[3]

Indirect Identifier: Variables that can be used, often in combination with each other, to identify an individual and that are reasonably known by an adversary (e.g., age, profession, gender, ethnicity). [4]

Institutional Signing Official (ISO): The authorized representative identified by a Data Contributor or Data User with both the capacity and the authorization to bind that organization to contractual agreements which pertain to research, e.g. CEO, contracts officer, VP Research. An Institutional Signing Official signs contractual agreements that enable data contribution or data access on behalf of the Data Contributor or Data User.

IPC De-identification Guidelines: Information and Privacy Commissioner of Ontario's De-Identification Guidelines for Structured Data.[5]

Open Access: Data released in Open Access is made openly available through a public website that anyone can access. To use Open Access data, Open Access Users must first agree to a click-wrap terms of use that requires them to use data exclusively for research purposes, and to respect the applicable ethical and legal restrictions on data use.

Pre-clinical Data: Data that does not, and never did, relate to human research participants. To be considered Pre-clinical Data, data must not be subject to the TCPS-2 (or equivalent local research ethics requirement) nor to the Personal Health Information Protection Act, 2004 (PHIPA) (or local data protection laws). E.g. Data about non-human cell cultures, animal models data, or data about drugs or devices.

---

[2] De-Identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario, October 2025. Accessed October 17, 2025. De-identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario

[3] De-Identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario, October 2025. Accessed October 17, 2025. De-identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario

[4] De-Identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario, October 2025. Accessed October 17, 2025. De-identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario

[5] De-Identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario, October 2025. Accessed October 17, 2025. De-identification Guidelines for Structured Data | Information and Privacy Commissioner of Ontario

Principal Investigator (PI): The lead researcher responsible for the design, execution, and overall management of a Research Project. This role is central to ensuring the scientific integrity, regulatory compliance, and ethical conduct of the study. The PI is affiliated with a Data User or Data Contributor and authorized to act as an agent of the Data User or Data Contributor for the purpose of data contribution and/or access.

Private Environment: The private environment refers to the portion of ARCHIMEDES through which Data Contributors can store, analyze, and curate data related to a Collection that they have uploaded, prior to releasing it for others to use through the Open Access or Controlled Access tiers.

Research Project: A self-contained research effort, with defined aims, methods, and outputs, carried out by a Principal Investigator and their Research Team in accordance with institutional requirements. Each Research Project is described in a data access request form (DAR) and must obtain approval from the ARCHIMEDES Data Access Committee (DAC). Rights to use Controlled Access ARCHIMEDES data are allocated relative to a specific Research Project.

Research Team: For each of their Research Projects, the Principal Investigator supplies a list of members of their Research Team to the DACO (i.e., Authorized Users). Many obligations to ensure responsible data use that are detailed in applicable contracts and ARCHIMEDES policies apply to each Research Team and are assessed relative to each of their approved Research Projects. For example, data released as part of a Research Project can only be used by members of the associated Research Team, relative to the approved Research Project.

Open Access User: Individual who agrees to the Open Access Terms of Use and accesses Open Access data.

2. Introduction to ARCHIMEDES

Advanced **R**esearch **C**ollaboration for **H**ealth **I**ntegration, **M**edical **E**xploration, and **D**ata **S**ynthesis (**ARCHIMEDES**) is a health platform that can be used to collect, manage, or share data, and to perform analysis (biostatistical analyses, predictive modelling, data visualization and artificial intelligence). Our vision is to provide a bilingual national health data platform that provides centralized and flexible access to curated health data, which can be analyzed using state-of-the-art distributed computing tools. ARCHIMEDES is equipped to collect or ingest multimodal brain, heart, and mind data (e.g., behavioural data, imaging data, biobank materials data).

ARCHIMEDES enables Data Contributors to contribute Coded, De-identified, or Pre-clinical datasets so that Data Users and Open Access Users can use the data for their own research. Data Contributors select the tier of data release (i.e., open or controlled) for their data.

ARCHIMEDES is designed to support data utility, while protecting the privacy of individuals, and is based on robust informed consents (or other ethical and legal authorizations described in Section 9.1.).

1. Research participant informed consent is the primary legal authorization to contribute, use, and disclose Coded data though other legal and ethical authorizations (such as an ethics waiver of informed consent requirement, De-identification, or other enabling law) are also supported. Coded data is generally considered to be personal information and must be protected in accordance with applicable privacy laws and regulations which limit what can be done with the data. As a result, the consent and other authorizations must be robust and authorize broad permitted future research use as defined in the Core Permissions.

2. On the basis that De-identification could reduce a researcher's ability to do meaningful research, and subject to local ethics review bodies, ARCHIMEDES allows the ingestion of Coded data to maximize data utility. This approach must be clear to all research participants, ethics review bodies, Data Contributors and Data Users. These groups must also be informed (with risks disclosed in the informed consent form) that ARCHIMEDES data may be held indefinitely, used for commercial and non-commercial research purposes, and that risks of re-identification exist now and in the future, although steps have been taken technically and administratively to reduce (but not eliminate) that possibility.

3. ARCHIMEDES Data Access Compliance Office at OHIRC (DACO) reviews consents against established criteria, and the ARCHIMEDES technical team at McGill (ARCHIMEDES Technical Team) performs limited automated verification of the data ingested into ARCHIMEDES against ARCHIMEDES standards (e.g., that standard identifiers have been removed).

4. Data Contributors are accountable as custodians for contributing data and for agreeing to its downstream use and disclosure in Controlled Access or Open Access. Data Contributors will have sightline through the life of their contributed data and remain responsible for steps taken by their agents (including designated PIs) at any step.

5. To that end, for Controlled Access data, administrative and technical means keep Data Contributors apprised and accountable, facilitating their compliance with local laws and institutional requirements.

2.1. Open Access Data Release – Phased Implementation

ARCHIMEDES is introducing both Controlled Access and Open Access data release tiers through a phased implementation (as further described in s. 9, below).

At present:

- ARCHIMEDES accepts Coded and De-identified data, as well as Pre-Clinical Data, for release through its Controlled Access tier.
- ARCHIMEDES accepts Pre-clinical Data for release through its Open Access tier (according to the conditions described at Authorization E, below).

- In the future, ARCHIMEDES intends to accept Coded, De-identified, and Pre-clinical Data for release through both its Open Access and its Controlled Access tiers.

The requirements that govern the release of Coded, De-identified, and Pre-clinical Data in both Controlled Access and Open Access are nonetheless described in the Ethics and Data Governance Framework.

2.2 ARCHIMEDES Core Values

Values and Principles	Commitments associated with these values and principles
Collaboration	We will promote interdisciplinary collaboration and partnerships within Canada and internationally.
Privacy, Confidentiality, and Security	We will embed privacy, confidentiality, and security considerations in all aspects of governance and development processes.
Integrity	We will uphold ethical and research integrity standards in data acquisition, management, sharing, and analytics.
Open Science and Equity	We will promote transparency and openness of research and all its outputs to favour equitable access and reuse.
Training	We will provide and promote education and training resources that encourage robust and ethical research data management and transparent data sharing that respects privacy and research security.

2.3 ARCHIMEDES Collaborating Institutions

ARCHIMEDES is a joint scientific effort of the University of Ottawa Heart Institute (UOHI), the University of Ottawa (uOttawa) and McGill University (McGill). Ottawa Heart Institute Research Corporation (OHIRC), the research and contracts arm of the UOHI, acts as the data steward for ARCHIMEDES data and implements and oversees ARCHIMEDES's data governance practices. It is responsible for administering ARCHIMEDES' data use, contribution and access requirements and approving data contribution and access in a manner that is consistent with applicable law and this framework.

McGill develops, operationalizes and maintains the technological infrastructure and technical elements of ARCHIMEDES. Its responsibilities include hosting and managing ARCHIMEDES data and implementing reasonable technical security measures for the platform.

uOttawa provides funding for ARCHIMEDES through its grant from the Government of Canada's Canada First Research Excellence Fund for the Brain-Heart Interconnectome Program (BHI Program). It is responsible for ensuring that the BHI Program funds are used in accordance with the terms and conditions of the grant and the policies of the fund.

While OHIRC, McGill and uOttawa have distinct but complementary roles in developing and operating ARCHIMEDES, each institution ensures oversight of the overall governance and participates in defining the strategic direction of ARCHIMEDES through the governance structure of ARCHIMEDES (described below).

2.4 ARCHIMEDES Governance Structure

The ARCHIDEMES Leadership Committee, Joint Liaison Committee, and Community Partners Committee perform portfolio-specific decision-making and advisory functions as detailed below.

The Data Access Committee (DAC) oversees requests from prospective Data Users to access Controlled Access data with the administrative support of the Data Access Committee Office (DACO).

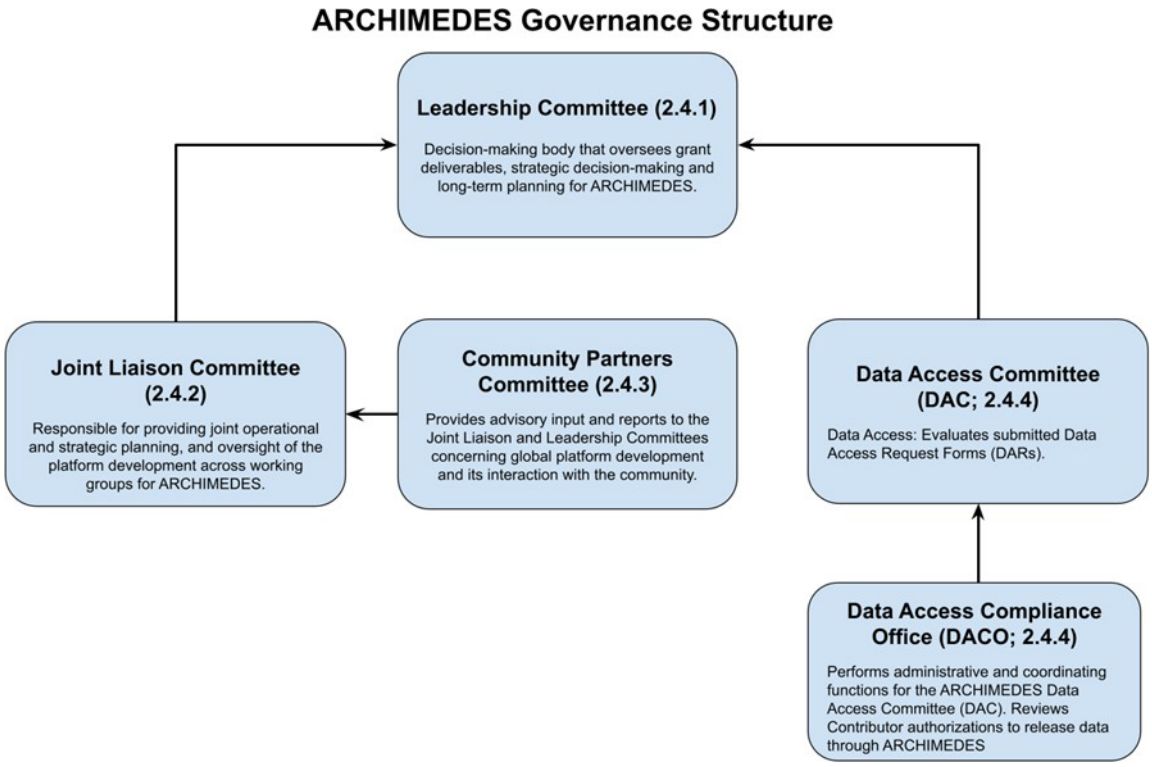

Figure 1: ARCHIMEDES Governance Structure

2.4.1 ARCHIMEDES Leadership Committee

The ARCHIMEDES Leadership Committee is the decision-making body of ARCHIMEDES and reports bi-annually to the BHI Executive Committee. It is responsible for oversight of ARCHIMEDES, strategic decision-making and long-term planning. Committee membership includes the scientific leads and senior representatives from each of uOttawa, OHIRC and McGill. Committee terms of reference can be found here.

2.4.2 ARCHIMEDES Joint Liaison Committee

The ARCHIMEDES Joint Liaison Committee ensures that the development and implementation of ARCHIMEDES will achieve the scientific goals of the BHI program. It will have cross-representation from OHIRC, McGill, and uOttawa to ensure full transparency, accountability, alignment, and continuity between collaborating institutions. The Joint Liaison Committee oversees the day-to-day operational management of all platform activities, with the oversight of the ARCHIMEDES Leadership Committee. Committee terms of reference can be found here.

2.4.3 ARCHIMEDES Community Partners Committee

The ARCHIMEDES Community Partners Committee includes stakeholders with expertise in topics that influence the successful implementation of ARCHIMEDES and its interaction with the community. The Community Partners Committee will provide advice to the Leadership Committee and to the Joint Liaison Committee, as applicable and required, on key areas that affect ARCHIMEDES, including commercialization, indigenous engagement, knowledge mobilization, open science, patient engagement, and training. This Committee reports to the ARCHIMEDES Leadership Committee. The Community Partners Committee terms of reference can be found here.

2.4.4 ARCHIMEDES Data Access Committee (DAC)

The ARCHIMEDES DAC performs oversight functions relative to requests to use Controlled Access ARCHIMEDES data. The ARCHIMEDES Data Access Committee (DAC) Terms of Reference can be found here.

The ARCHIMEDES DACO is the administrative arm of the ARCHIMEDES DAC. It coordinates the DAC review of Data Access Requests and performs select monitoring functions regarding the ongoing commitments of authorized Data Users. For data contribution, the DACO reviews the documentation demonstrating ethical and legal authority, including informed consent materials and ethics approvals, provided by Data Contributors for compatibility with ARCHIMEDES policies before authorizing data contribution. The DACO also reviews requests for Data Contributor and Data User credentials.

The procedures followed by the DACO and DAC are detailed in the “ARCHIMEDES Data Access Compliance Office (DACO) Procedures – Data Contribution,” the “ARCHIMEDES Data Access Compliance Office (DACO) Procedures – Data Access,” and the “ARCHIMEDES Data Access Committee (DAC) Terms of Reference”.

3. Ethical oversight

Ethics approval for ingestion of research participants’ data in ARCHIMEDES is sought by Data Contributors to the local REB responsible for ethics oversight of each Collection and information on the contribution to ARCHIMEDES should be provided in the research participant informed consent forms.

Ethics approval for the creation of ARCHIMEDES was obtained from Ottawa Health Science Network Research Ethics Board (OHSN-REB) Protocol ID #20250418-01H.

4. Management

ARCHIMEDES OHIRC operations, staffing and finances are managed by the ARCHIMEDES Co-Chairs. ARCHIMEDES McGill operations, staffing and finances are managed by the ARCHIMEDES McGill lead.

5. Financing

ARCHIMEDES is undertaken thanks in part to funding from uOttawa awarded by the Government of Canada's Canada First Research Excellence Fund (CFREF) for the BHI Program as well as partnership matching funds from OHIRC and in-kind data-infrastructure contributions from McGill. ARCHIMEDES builds upon the existing data-sharing infrastructure within LORIS, CBRAIN, NeuroHub, and C-BIG, with new features tailored for cardiac application within BHI.

Ongoing funding sources will be sought to ensure the financial sustainability of ARCHIMEDES.

6. Overview of Technical Elements of ARCHIMEDES

ARCHIMEDES is composed of the following major technical elements:

- **Data ingestion tools**, which enable PIs and Contributor Users to submit data to ARCHIMEDES for Controlled Access or Open Access sharing.
- **Data Query Tool (DQT)**, which enables data to be searched according to data dictionaries that are made available to Data Users and Open Access Users. This helps Data Users and Open Access Users find data that is useful to them.
- **User authentication and access request tools**, which enable prospective Data Users to apply to use Controlled Access datasets.
- **High-performance computing capabilities**, which are made available through supercomputing facilities.

The functioning of these elements is further detailed in ss. 7-9, below.

7. Overview of Data Flow in ARCHIMEDES

The following figure summarizes the key components of data flow in ARCHIMEDES, beginning with ingestion of data by Data Contributors, on through processing, access and use.

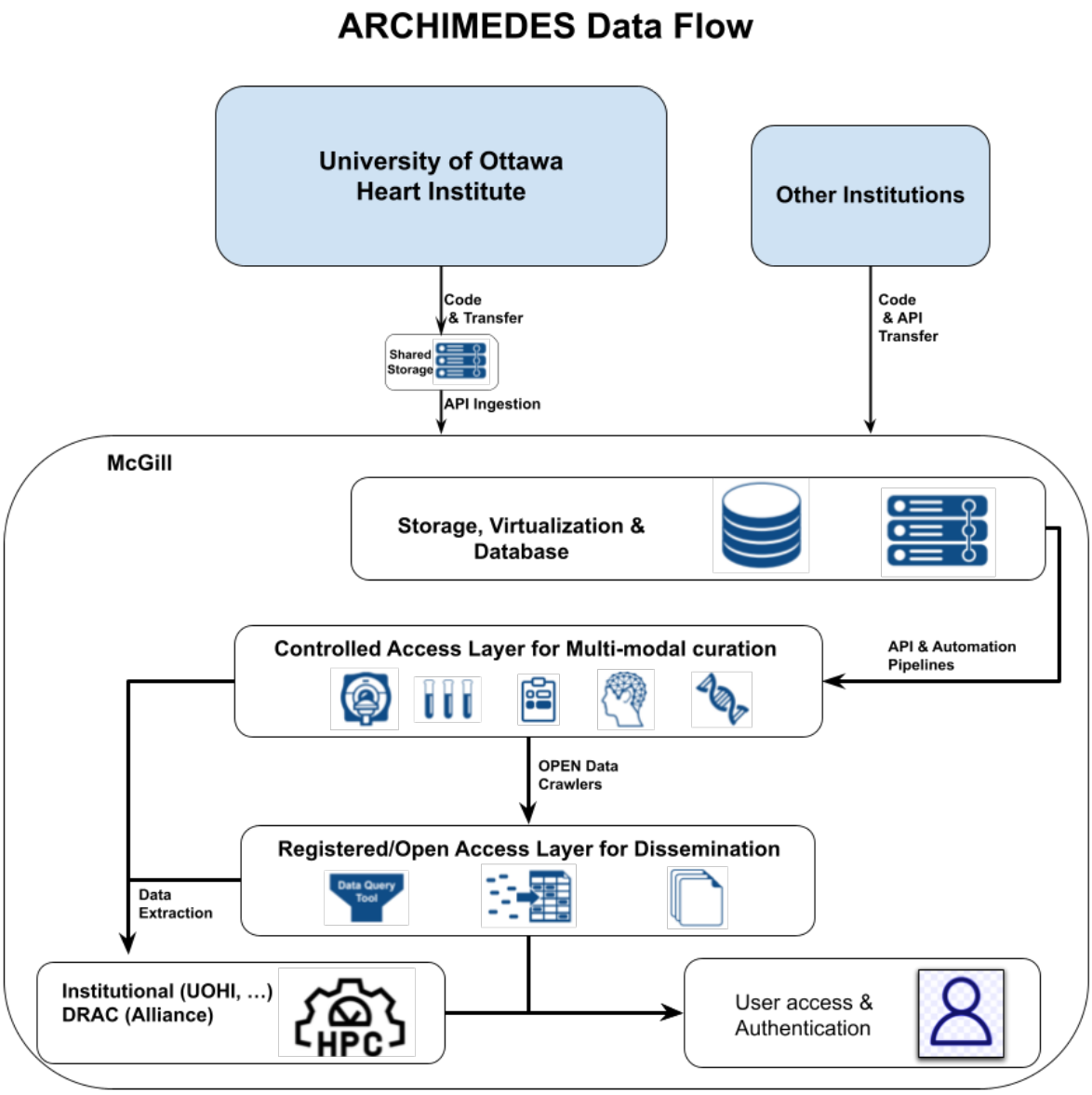

Figure 2: ARCHIMEDES Data Flow

8. Types of Data

Multimodal curated health data, including, but not limited to, behavioural data, imaging data, biomaterials data, and administrative data are available in ARCHIMEDES. This includes both data derived from human research participants, and data not derived from human research participants (i.e., Pre-Clinical Data).

9. Data Contribution

Prior to contributing data to ARCHIMEDES, each Data Contributor is required to ensure that:

- They hold the institutional, ethical, and legal authorizations required to contribute the specific data to ARCHIMEDES and release this data through Open Access or Controlled Access.
- For data that is not Preclinical Data, the data is Coded (or in some cases, it will be De-identified).

Prior to contributing data to ARCHIMEDES, Data Contributors must enter into a Data Contribution Agreement with OHIRC. This enables authorized Principal Investigators to contribute data to ARCHIMEDES by submitting a Data Contribution Form specific to a research project. All data ingested into ARCHIMEDES requires review of the Data Contribution Form by the ARCHIMEDES DACO prior to being accepted into ARCHIMEDES.

Data Contributors and their Principal Investigators are welcome to contact the ARCHIMEDES Ethics Helpdesk at OHIRC to obtain information about the data governance practices of ARCHIMEDES, and the data contribution process.

9.1. Authorizations

In contributing data to ARCHIMEDES, Data Contributors must confirm that they are authorized to share the data in the chosen tier of release as described in the Data Contribution Agreement, the Data Contribution Form, this framework, and relevant ARCHIMEDES policies.

Each Data Contributor must ensure that an appropriate ethical and legal authority supports the specific Data Contribution and provide supporting documentation. Such documentation must demonstrate that one of the following ethical-legal authorizations supports each of its acts of data contribution and data release through the Controlled Access or Open Access tiers of ARCHIMEDES:

A. **Informed consent and ethics approval:** Data Contributors have obtained the informed consent of research participants, and a research ethics board approval (or local equivalent), that authorizes data sharing according to the Core Permissions of the chosen Data Release tier.

B. **Ethics waiver of informed consent requirement**: A research ethics board (or local equivalent) has authorized the release of data, through an ethics waiver of the informed consent requirement, that authorizes data sharing according to the Core Permissions of the chosen Data Release tier.

C. **Enabling local law:** Local law allows the contribution of data to ARCHIMEDES according to the Core Permissions of the chosen Data Release tier.

D. **Data is De-Identified:** The data is De-identified in accordance with IPC De-identification Guidelines or generally accepted best practices including local legal or ethical requirements that appropriately reduce the risk of re-identification to very low. Such data can consequently be released through the chosen Data Release tier.

E. **Data is not human research participants data (i.e., is Pre-clinical Data):** The data does not, nor did it ever, constitute data relating to human research participants, or identifiable personal data, according to applicable research ethics requirements and data protection laws. This is reserved for Pre-Clinical Data such as data derived from non-human cell cultures, from testing on animal models, that relates to drugs and devices. Such data can consequently be released through the chosen Data Release tier.

The ARCHIMEDES DACO reviews the supporting documentation that demonstrate such justification prior to authorizing data ingestion, for each Collection that a Data Contributor submits to ARCHIMEDES.

The Data Contributor is ultimately responsible for ensuring such authorization complies with the applicable Core Permissions. For Controlled Access, the Data Contributor may choose to allow Principal Investigators to act on their behalf for authorizations A and B, or require Institutional Signing Official (ISO) sign off; and ISO sign off is required for authorizations C, D, and E. For Open Access, the Data Contributor's ISO must approve each authorization.

The processes used by ARCHIMEDES DACO to review the authorizations and supporting materials are further detailed in ss. 9.8. and 9.9., below, and in the DACO Procedures.

9.2. Core Permissions

The institutional, ethical, and legal authorizations supporting data contribution and data release through ARCHIMEDES must, at a minimum, permit the uses and data processing described as Core Permissions at s. 9.4.1 for Open Access or at s. 9.4.2 for Controlled Access.

The Core Permissions are the permissions that must be obtained for data to be contributed into ARCHIMEDES and released through the Controlled Access or Open Access tiers of ARCHIMEDES.

9.3. Informed Consent

Generally, Data Contributors obtain informed consent and an ethics approval, as well as anything required under local laws. Consent forms used for data collection must, at a minimum, incorporate the Core Permissions detailed at s. 9.4.1 (Open Access) or 9.4.2 (Controlled Access) to enable data contribution and sharing through ARCHIMEDES.

- **For Prospective Consent**: The ARCHIMEDES Open Access and Controlled Access Consent Form Templates, available here, provide template consent language to PIs who wish to contribute data to ARCHIMEDES in its Open Access or Controlled Access tiers of data release. These templates are suitable both for obtaining consent to the future collection and release of data (i.e., prospective consent) and for obtaining a new consent authorizing the sharing of research data collected as part of a prior study (i.e., retrospective consent) so long as reviewed and approved by the applicable local ethics board.
- **For Retrospective Consent:** The ARCHIMEDES Retrospective Consent Filter enables Data Contributors to determine whether the language of their existing informed consent forms (ICFs) is suitable to allow the contribution of data to ARCHIMEDES and, if so, at what access tier. It is a self-assessment tool that helps Data Contributors to assess which steps, if any, should be taken prior to sharing data through ARCHIMEDES.

9.4 Other Authorizations

However, other authorizations, such as an ethics waiver of the informed consent requirement, other enabling local legislation, or the contribution of data that is De-identified or Pre-Clinical Data, also constitute appropriate justifications for performing data release through ARCHIMEDES, as specified above.

As with informed consent, these authorizations must also permit the uses and data processing described as Core Permissions at s. 9.4.1 for Open Access or at s. 9.4.2 for Controlled Access.

9.4.1 Core Permissions - Open Access Data (Subject to Phased Implementation)

Subject to review and approval from the ARCHIMEDES Leadership Committee, ARCHIMEDES intends to implement the following open access data core permissions in the next phase of implementation.

To contribute data to **ARCHIMEDES (Open)**, the following permissions must be obtained, through an informed consent to research participation (or other mechanism, e.g. an ethics waiver of informed consent requirement).
Collection of study data from research participants.
Sharing of coded study data through an open-access mechanism.
International sharing of study data.
Future research on all relevant scientific research questions.
Use of the study data for commercial and non-commercial research purposes (this allows both the commercialization of downstream research outputs and research by private sector bodies).
Indefinite storage of the study data collected.
Withdrawal of study data not possible if already used or published.
There is still a residual risk that the participant may be re-identified.

9.4.2 Core Permissions - Controlled Access Data

To contribute data to **ARCHIMEDES (Controlled)**, the following permissions must be obtained, through an informed consent to research participation (or other mechanism, e.g. an ethics waiver of informed consent requirement).
Collection of study data from research participants.
Sharing of Coded study data with approved researchers through a controlled access mechanism.
International sharing of study data.
Future research on all relevant scientific research questions.
Use of the study data for commercial and non-commercial research purposes (this allows both the commercialization of downstream research outputs and research by private sector bodies).

Public sharing of anonymized or aggregated data (Optional, but recommended).
Indefinite storage of the study data collected.
Withdrawal of study data not always possible if already used or published.
There is still a residual risk that the participant may be re-identified
(RECOMMENDED) Option to transfer data to the stewardship of a different data steward, and a different data repository.

9.4.3 Removal of Select Identifiers

In contributing data, each Data Contributor is responsible for ensuring that the submitted data satisfies applicable ARCHIMEDES policies and the legal, ethical, and institutional requirements applicable, regarding data identifiability.

Data Contributors are required to remove all Direct Identifiers from submitted data prior to data contribution in ARCHIMEDES.

For Coded data, ARCHIMEDES also recommends the removal of Indirect Identifiers that create a significant risk of individual re-identification, especially those that do not contribute to the scientific utility of the data. However, final decision as to the adequacy or completeness of the removal of identifiers rests with the Data Contributor. The Data Contributor (and their Principal Investigator – having the requisite knowledge of the data and domain expertise) retains ultimate responsibility for removing identifiers as well as assessing and managing re-identification risk and ensuring research participants are adequately informed. The ARCHIMEDES Technical Team works with Principal Investigators to detect and remove common identifiers using the tools and controls detailed below, but do not confirm the adequacy or completeness of this verification and removal. These are limited administrative oversight measures that may further reduce the risk of individual re-identification occurring in practice. The responsibility for reducing the risk of re-identifiability of data nonetheless rests with the Data Contributors.

For De-identified data, the Data Contributor is responsible for De-identifying the data in accordance with IPC De-identification Guidelines or generally accepted best practices including local legal or ethical requirements.

For Pre-clinical Data, the Data Contributor is responsible for ensuring that the data does not, and never did, relate to human research participants or identifiable natural persons, and that it is out of scope of both research ethics requirements and data protection laws.

9.5 Codes and Linkage Logs

Data Contributors are required to ensure that their data is Coded prior to contributing it to ARCHIMEDES. Data Contributors replace all Direct Identifiers with a unique alphanumeric code.

Data Contributors are also responsible for retaining their own local linkage logs that enable them to determine which study records belong to each research participant, in a secure manner. If a research

participant decides to withdraw their data from ARCHIMEDES, it is the linkage log that enables Principal Investigators to request the individual-level withdrawal of data. Data Contributors that submit data on the grounds that it is De-identified (confirmed by the attestation of the Data Contributor's ISO) should generally not retain linkage logs.

9.6 Data Contribution Agreement

Data contribution to ARCHIMEDES begins with a Data Contributor entering into a Data Contribution Agreement with OHIRC.

Principal Investigators seeking to contribute a Collection to ARCHIMEDES submit a Data Contribution Form specific to that Collection, with ISO sign off when required, and supporting documentation, to the DACO for review and approval.

Data Contributors must submit a list of their authorized Principal Investigators to the DACO, and update the DACO each time they wish to add or a remove a Principal Investigator. Once the DACO approves them, Principal Investigators on the master list can create a new Collection, or amend an existing one, through the submission of a Data Contribution Form that is specific to that Collection.

Authorized Principal Investigators can perform the upload, curation, and analysis of data through ARCHIMEDES, and authorize the release of data in Open Access or Controlled Access. They can also assign permissions to Contributor Users at their institution. Such listed individuals can perform supporting activities that facilitate the upload, curation, and analysis of data in the Private Research Environment, but cannot authorize the release of data to ARCHIMEDES' Controlled Access or Open Access tier.

The Institutional Signing Officials as designated and authorized by the Data Contributor (see s. 9.1.) will have access a list of the Data Contributor's Collections (and the associated Data Contribution Forms), and will be notified each time a new Collection is created and/or is authorized for release in Open Access or Controlled Access.

The Institutional Signing Officials will also be notified each time a Principal Investigator or Contributor User is added or removed. The notification further describes their associated account permissions. The DACO operationalizes the changes to each Data Contributor's list of Principal Investigators and Contributor Users in collaboration with the ARCHIMEDES Technical Team.

9.7 Data Contribution Form

To create a new Collection, a Principal Investigator submits a Data Contribution Form that describes the nature of the Collection, the datasets in the Collection that will fall within each tier of data release, and the ethical-legal authorization for data contribution to ARCHIMEDES and the release of such data through ARCHIMEDES.

This form confirms the commitments that the Data Contributor and their PI make in contributing their data, such as ensuring that the **Core Permissions** (9.4.1. Open Access Data and 9.4.2. Controlled Access Data) have been associated to the data, that the data is Coded or De-Identified, that the Data Contributor holds the institutional, ethical, and legal authorizations required to integrate the data into ARCHIMEDES and that the Data Contributor has obtained the Core Permissions necessary to share the data through the chosen tier of release.

The data contribution form is signed by the ISO for all authorizations in the Open Access release tier and certain authorizations in the Controlled Access release tier. The Data Contributor can specify in the Data Contributor Agreement when ISO sign off is required for the Controlled Access release tier as described in s. 9.1.

9.8 Submission of Supporting Documentation

Before uploading data to ARCHIMEDES, Data Contributors must provide supporting documentation that enables the ARCHIMEDES DACO to confirm the appropriateness of intake into ARCHIMEDES and the proposed data release (see. s. 9.1, Authorizations, above).

The Data Contributor specifies its legal authorities and uploads supporting materials relevant thereto, as follows:

A. **Informed consent and ethics approval** (Provide copy of informed consent materials and ethics approval letter, for DACO evaluation).
B. **Ethics waiver of informed consent requirement** (Provide waiver letter, or other relevant document from the research ethics board, for DACO evaluation).
C. **Enabling local law** (Provide copy of enabling legal instrument, e.g., legislation, regulation, local ethics guidance, for DACO evaluation. The Data Contributor ISO must approve such a release).
D. **Data is De-identified** (The Data Contributor's ISO must approve such a release, confirming that the Data is De-identified in accordance with IPC De-identification Guidelines or generally accepted best practices including local legal or ethical requirements that appropriately reduces the risk of re-identification to very low. Provide ethics approval letter when required.).
E. **Data is not human research participants data (i.e., is Pre-clinical Data)** (The Data Contributor's ISO must approve such a release, confirming that the Data does not constitute human research participants data. This requires them to confirm that the data is not subject to PHIPA, the TCPS-2, or local data protection laws and biomedical research ethics requirements, and that it is not derived from human research participants.)

9.9 Evaluation of proposed data contributions

The ARCHIMEDES DACO conducts an administrative review of the Data Contribution Form and supporting documentation. Based on the results of this assessment, the ARCHIMEDES DACO either recommends data contribution, or recommends that additional steps be taken prior to data contribution (e.g., obtaining a new consent or an ethics waiver of the informed consent requirement). The outcome of this analysis depends on whether the materials submitted for review align with the Core Permissions (9.4.1 Open Access Data and 9.4.2 Controlled Access Data) associated to the chosen tier of data contribution.

Only data from Data Contributors recommended for contribution by the DACO will be integrated into ARCHIMEDES.

The DACO Procedures (Data Contribution) provide a more comprehensive description of its evaluation process. See the DACO Procedures (Data Contribution) here.

9.10 Data Submission

Data submission can occur once the Data Contributor and their Principal Investigator have obtained all necessary approvals for the ingestion of the data into ARCHIMEDES. Data submission is done in different steps:

1. Data is first ingested into the Private Environment of ARCHIMEDES.
2. Principal Investigator curates, validates, and prepares their data for release through the chosen release tier.
3. Principal Investigator confirms data is accurate and ready for release, at which point data is made available through the chosen release tier.

9.11 Ingestion into Private Environment

Data is first ingested into the Private Environment of ARCHIMEDES through two secure channels:

(1) SSL-encrypted transfer through the platform's web-browser interface. This method uses the RESTful API to transfer data from the Data Contributor's servers to McGill servers.

(2) encrypted data transfer through the Secure Shell File Transfer Protocol (SFTP or SSH), which enables bulk file transfer from the Data Contributor's servers to McGill servers.

Data submitted to ARCHIMEDES reside in servers located at McGill. If using DRAC HPC, Data may also be temporarily hosted on the DRAC infrastructure. A small number of the ARCHIMEDES Technical Team that perform data management, data curation, and platform administration can access it.

9.12 Preparing Data for Release

After uploading data to ARCHIMEDES, Principal Investigators and their Contributor Users can first analyze and manipulate the uploaded data in the Private Environment.

Then, PIs can initiate the release process through a formal written request that outlines the components of the dataset (e.g., specific instruments, visits, modalities, or cohorts) to be shared. Data to be released is then prepared in a secure staging environment, with or without assistance of the ARCHIMEDES Technical Team (as described below). A final written sign-off from the PI to the DACO confirms that the curated dataset is accurate and ready for release through the chosen tier. The DACO then instructs the ARCHIMEDES Technical Team to release the data.

This two-step confirmation process—initial request and final sign-off—ensures alignment with consents and ethics approvals applicable to the data, and Collection-level data contribution forms.

9.13 Data Curation and Validation

There are two main approaches to preparing data in the staging environment:

1. **Full Curation with ARCHIMEDES**
   In this model, the Principal Investigator and their authorized Contributor Users, with the assistance of ARCHIMEDES Technical Team, test and review the data within staging environments to ensure the dataset is properly curated, validated, and prepared for release

through the chosen tier.

2. **Handoff of Pre-curated Data**
   Alternatively, the Principal Investigator and their authorized Contributor Users may provide a fully curated dataset. In this case, the ARCHIMEDES Technical Team verifies that the data is structured and annotated according to ARCHIMEDES standards for release through the chosen tier.

9.14 Removing Select Identifiers (ARCHIMEDES Technical Team)

Data Contributors and their Principal Investigators possess domain-specific knowledge and expertise that is fundamental to the effective removal of identifiers. They are responsible to determine the measures and controls required to adequately mitigate the residual risk of re-identification in the chosen tier of release.

ARCHIMEDES tools and controls, administered by the ARCHIMEDES Technical Team, and described below, detect and remove common identifiers from predefined standard fields but cannot comprehensively identify all potential identifiers across diverse data structures and contexts.

- **Double-coding and GUID assignment**: For Coded data, project-level research participant codes are replaced with Globally Unique Identifiers (GUIDs), ensuring that datasets are dissociated from their original sources. For data that Data Contributors describe as De-identified, no GUID is generated. In this case, responsibility rests with the Data Contributor's ISO to confirm that the data is appropriately De-identified.
- **Removal of Indirect Identifiers for imaging data**: For certain data types, such as MRI, 'de-facing' algorithms are applied to remove facial features while maintaining anatomical integrity for downstream analyses. This is mandatory for certain access tiers (e.g., open access) and is implemented without impacting core research workflows. Other bespoke workflows will be developed in the future for commonplace data types.
- **Temporal removal of Indirect Identifiers**: Dates tied to hospital visits, assessments, or research participant birthdates are stripped or shifted.
- **Metadata sanitization**: All potentially identifying metadata fields, such as DICOM headers, are systematically scrubbed or overwritten using standardized tools like DICAT (DICOM-Anonymization Tool). Fields such as StudyDate, and BirthDate are reformatted or removed to comply with ARCHIMEDES policies and standards.

Following this processing, Data Contributors and their Principal Investigators are solely responsible to determine whether supplementary measures are required to adequately mitigate the residual risk of re-identification in the chosen tier of release.

9.15 Data Quality (ARCHIMEDES Technical Team)

Data Contributors and their Principal Investigators are responsible for the accuracy, completeness, and quality of contributed data. ARCHIMEDES quality review is conducted solely to ensure the data meets ARCHIMEDES standards.

- **Quality control and curation**: The data undergoes automated and manual validation to identify inconsistencies, missing values, or outliers, but accuracy is not guaranteed. This includes logic checks, adherence to expected value ranges, and metadata consistency across instruments and time points.

- **Review compliance with standards**: Ensure adherence to ARCHIMEDES naming conventions, and standardized schemas.

9.16 Pre-Release Verification and Validation

Prior to making the data available for release through the chosen release tier, verification and validation is performed to ensure that data is appropriately permissioned according to the release tier chosen by the Data Contributor, is GUID coded for Coded data, and is of sufficient quality meeting ARCHIMEDES standards. This is an administrative oversight process that the ARCHIMEDES Technical Team performs that may help Data Contributors reduce the risk of an unauthorized data release or re-identification.

However, this process does not confirm the adequacy of the chosen release tier, or the adequacy or completeness of the removal of identifiers or De-identification of the data. Ultimate responsibility for ensuring that data is Coded, De-identified, or is Pre-clinical Data, in accordance with applicable laws and for selecting the appropriate release tier remains with the Data Contributor.

9.17 Data Contributor Credentialing and Authentication

When creating a new Collection, authorized Principal Investigators ascribe the permissions defined in the table below to Contributor Users at their organization.

The ARCHIMEDES user management module allows Principal Investigators to create accounts that are associated to their Collection(s) in the ARCHIMEDES Private Environment. These accounts carry distinct privileges, ranging from permission to view a specific dataset, to the ability to create Collections and upload data to them to the ARCHIMEDES Private Environment, to creating additional new Contributor Users and credentials with specific privileges. Collection creation and data release privileges are restricted to PIs alone. All logins, Collection creations, data entry, data uploads, and other interactions with ARCHIMEDES are logged and are tied to the account that performs these operations.

9.18 Role Based Access Controls

Once the DACO authenticates the Contributor User and ensures that they have completed the requisite contracts and forms PIs can assign Contributor Users one or more roles. Each role has defined privileges at the site and/or project level. Roles are configurable in the system and mapped as follows:

Role	Key Permissions
Viewer	View catalog metadata and non-sensitive dataset previews.

Contributor	Upload data, submit data dictionaries, view own contributions.
Manager	Add/remove project members, approve Contributor User accounts, manage data dictionaries.
Analyst	Execute queries, submit analysis jobs, access analysis pipelines.
Principal Investigator	Ability to create new Collections, release data through ARCHIMEDES, and assign privileges in the Private Environment to Contributor Personnel and Contributor Trainees, relative to their created collections.
Institutional Signing Official	Ability to view all activity associated with the institution, including creation of new collections, release of data through ARCHIMEDES, and privileges granted in the Private Environment.

Access is further restricted to:

- Data from specified Research Projects.
- Data from specified institutions (e.g., only McGill-affiliated datasets).

10. Data Access

Data contributed to ARCHIMEDES will be made available to Open Access Users through Open Access and Data Users through Controlled Access tiers. The authorization attributed to data inform the Data Contributor's selection of the appropriate release tier (i.e., an ethical and legal justification that supports its sharing and use, such as research participant consent, an ethics waiver of informed consent requirement, or other legal authority for data release, as described at s. 9.1).

10.1 Accessing Open Access Data

Open Access data on ARCHIMEDES are made available through a public website that Open Access Users can access, to perform research on all relevant scientific research questions. Open Access Users must respect ARCHIMEDES Open Access Terms of Use, which precludes non-research uses of data and those that could harm research participants. The ARCHIMEDES DACO performs only limited monitoring of Open Access User compliance with the Open Access Terms-of-Use. The DACO has little capability to monitor compliance with the governance rules applicable to open data.

OHIRC and McGill reserve the right to cease hosting any contributed set of data through ARCHIMEDES, or making the data available to Users, where required to ensure compliance with ethical, legal, or institutional obligations. OHIRC, McGill, and uOttawa reserve the right to cease operating ARCHIMEDES where resources are no longer available to support the hosting of Data Contributor's data.

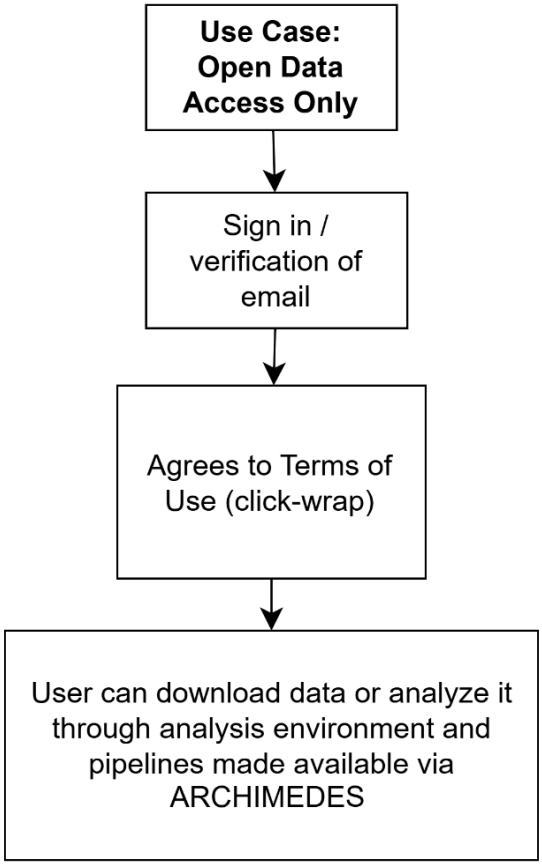

Figure 5: Open Access Workflow

10.2 Accessing Controlled Access Data

Controlled Access Data are made available through ARCHIMEDES to enable Data Users and their authorized Principal Investigators to download data for an approved research purpose. To access Controlled Access data, PIs must create an account through ARCHIMEDES and submit a data access request form (DAR). This request specifies the requested datasets, the intended purposes of their research use, and the identities of the Authorized Users that are members of the Research Team.

The ARCHIMEDES DACO receives the DAR and performs the administrative review thereof. It determines whether the applications contain the information that the ARCHIMEDES Data Access Committee (DAC) will need to perform its own substantive evaluation of the application. The DACO coordinates revisions with the applicants until it is suitable for DAC review, at which point the access request is made available to the DAC. See the DACO Procedures (Data Access) here.

The ARCHIMEDES DAC authorizes applicants for Controlled Access data where they demonstrate compliance with the terms listed in the **ARCHIMEDES Data Access Committee Evaluation Criteria**. To perform this evaluation, it uses the processes defined in the **ARCHIMEDES Data Access Committee Terms of Reference**.

OHIRC and McGill reserve the right to revoke Data User access if the Data User is found to breach the conditions of data access, or to ensure compliance with ethical, legal, or institutional obligations. uOttawa, OHIRC and McGill reserve the right to cease operating ARCHIMEDES where resources are no longer available to support Data User access to the data.

10.2.1 Controlled Access Data - Data Access Agreement

Only Principal Investigators can request access to Controlled Access Data. To do so, they must first create an account on ARCHIMEDES, submit a purpose-specific Data Access Request that justifies their intended data use to the ARCHIMEDES Data Access Compliance Office (DACO), and obtain an approval from the ARCHIMEDES Data Access Committee (DAC). Their organization must further enter into an Institutional Data Access Agreement (I-DAA) or Data Access Agreement (DAA) with OHIRC, confirming their appropriate use of the data shared with them.

To this end, Principal Investigators must create an account on ARCHIMEDES, using an institutional e-mail address that is associated to the organization that hosts them.

The Institutional Signing Official at their host research organization must complete an Institutional Data Access Agreement (I-DAA) to enable data access. This is a contractual agreement that establishes the obligations, responsibilities, and commitments of Data Users and their Principal Investigators and Authorized Users in using ARCHIMEDES Controlled Access data.

Once the I-DAA has been completed and a PI has created an account on the ARCHIMEDES, an Institutional Signing Official can allocate permissions to specific Principal Investigators at their organization. This enables those Principal Investigators to submit Data Access Requests (DARs) through ARCHIMEDES.

Simple “single-shot” DAAs are also available that govern a singular data access request. These are easier for Data Users to manage but must be replicated for each access request.

To submit a DAR, a Principal Investigator must first select the datasets they wish to access and add them to their cart on the ARCHIMEDES. They must then complete the DAR Form through ARCHIMEDES.

The DACO reviews DARs for pertinence and completeness. Incomplete DARs are returned to applicants for completion prior to DAC evaluation. Once completed, the DACO sends the DARs to the DAC for evaluation.

On receiving a DAR, the DAC convenes to review the application, during which it considers 1) whether the applicant is affiliated with a *bona fide* research organization and has sufficient research expertise to perform the proposed research, 2) whether the proposed research activities fall within-scope of the informed consents, data use conditions, and policies applicable to the data, and 3) whether the necessary supporting documentation has been provided (e.g., ethics board approvals, lists of Authorized Users). See the full DAC Evaluation Criteria found here.

The DACO communicates the decision of the DAC to the applicant. The possible outcomes are acceptance, conditional acceptance, or refusal. The decision-making process of the DAC is further detailed in the DACO Terms of Reference.

Once an applicant has received DAC approval to use data, this authorization remains valid for a period of three years, after which point it is necessary to submit another DAR to obtain continued authorization to access and use the data. In some cases, such as when the supporting ethics approval is not valid for the full access period, the period of authorization will be shorter still.

11. ARCHIMEDES Data Query Tool (DQT)

The ARCHIMEDES DQT is a data discovery tool that enables Data Users and Open Access Users to search for data that is useful for their research. This helps Data Users determine whether data that is useful for their purposes is available in Controlled Access dataset, before undertaking the procedures required to request access thereto.

12. Data Analysis

ARCHIMEDES enables Data Users to perform the analysis of data using their own local hardware and computing capabilities (i.e., through download access to data). Alternatively, it enables Data Users to perform analysis of data using dedicated third-party high-performance computing (HPC) infrastructure (i.e., supercomputing), and to analyze the data using a collection of software tools, pipelines, and APIs. The details of each method of analysis are further outlined below.

Local analysis	**ARCHIMEDES HPC**
Computing capabilities: Data Users can download data available to them to their local hardware.	**Computing capabilities:** Where Data Users instead require greater computing power, ARCHIMEDES supports data processing across High-Performance Computing (HPC). This allows Data Users to access significant computing power and storage that would not otherwise be available to them The Digital Research Alliance of Canada (DRAC) HPC allocation of ARCHIMEDES is available to Data Users, subject to the agreement with the DRAC. Use of DRAC HPC involves securely transferring data from ARCHIMEDES to DRAC's supercomputing facilities (i.e. distributed storage).
Analysis tools: This retrieval allows a researcher to analyze data with their preferred tools and hardware, so long as this analysis continues to respect the applicable data governance commitments.	**Analysis tools:** ARCHIMEDES supplies Data Users with analysis tools (i.e., software, algorithms, and pipelines) created by the scientific community. Users can leverage these tools when they analyze data through HPC. The ARCHIMEDES Technical Team receives analysis tools from community contributors and performs a reasonable information security assessment and basic verifications of their functioning and fitness. It provides no guarantees regarding their non-infringement of intellectual property rights (IPRs), nor their serviceability or good functioning. Data Users will agree through click-wrap ToS that these tools are provided without warranties nor guarantees.

	ARCHIMEDES integrates with other open-source tools, e.g., Jupyter Notebooks, DataLad, and Zenodo. These tools enable Data Users to analyze data through HPC using their own code, or that of third parties.

12.1 Community Contribution of Analysis Tools

ARCHIMEDES enables members of the wider research community to contribute data analysis tools to its library of analysis tools. PIs and Authorized Users can analyze ARCHIMEDES data using these community-contributed tools, when analyzing the Data through supercomputing facilities.

Community members that contribute a tool to ARCHIMEDES are required to provide information used to validate its appropriateness and agree to abide by a Tool Contributor Code of Conduct.

13. Data Protection

Each Data Contributor that contributes data to the ARCHIMEDES platform must ensure compliance with the data protection laws applicable, including the Personal Health Information Protection Act, 2004 (PHIPA), or the equivalent local or sectoral data protection statute(s) that govern their data collection, use, and disclosure.

In the context of PHIPA, OHIRC is acting as an agent on behalf of the Data Contributor for data ingestion. OHIRC, as Data Contributor's agent, bears the contractually assigned responsibilities for discharging the data stewardship functions detailed in this Governance Framework and in the Data Contribution Agreement. In OHIRC's agreement with McGill, McGill bears the contractually assigned responsibilities for discharging the technical and data management functions central to ARCHIMEDES and described in this Governance Framework.

OHIRC then performs administrative oversight, as described above, prior to releasing data based on the informed consent or other authorization. It nonetheless remains the sole obligation of Data Users to ensure their respect for privacy and data protection laws and related laws applicable to their activities and comply with the Data Access Agreement.

UOHI Privacy Office is responsible for all aspects of privacy compliance within the administrative structure of ARCHIMEDES.

13.1 Re-identification Risk

Data Contributor PIs contributing data to ARCHIMEDES do so in accordance with their local ethical and legal requirements and ARCHIMEDES standards, primarily based on research participant consent or an ethics waiver of informed consent requirement to share data that has been treated to remove all Direct Identifiers, and may include the removal of some (but not all) Indirect Identifiers. While this reduces the risk of individual re-identification, it does not eliminate it. Such data is often still identifiable personal information. This approach was chosen to achieve an optimal balance between research participant privacy and maintaining the scientific utility of the data.

In some cases, Data Contributors will contribute data based on another suitable authorization (i.e., enabling local law), on the grounds that the data are De-identified in accordance with IPC De-identification Guidelines or generally accepted best practices including local legal or ethical requirements that appropriately reduce risk of re-identification to very low, or on the grounds that

the data are Pre-clinical Data. If relying on De-identification, the Data Contributor's ISO must confirm that they have completed the required De-identification process and that the data has a very low risk of re-identifiability at the time of data ingestion.

OHIRC nonetheless treats all ARCHIMEDES-hosted data as though it were identifiable personal information:

- In hosting the data, ARCHIMEDES applies security safeguards and access controls that are reasonable to the storage of identifiable personal data.
- Research participants provide consent on the basis that some measures have been taken to remove select identifiers, are aware that given the broad scope of data sharing including internationally, for commercial purposes and for an indefinite timeframe, there is a possibility of re-identification.

13.2 Data Breach Notification

Data Contributors and Data Users must provide a written notice to the UOHI Privacy Office of any potential, suspected or actual data breaches which may affect ARCHIMEDES data.
UOHI Privacy Office is responsible for providing notice of data breaches to regulatory authorities, affected individuals, and other third parties, as might be required by applicable law to mitigate the harms and other consequences that such breaches cause to affected individuals. It also is responsible to provide notice to Data Contributors of data breaches that are known or suspected to have affected their contributed data. In practice, the original Data Contributor is responsible for informing affected individuals and ensure compliance with applicable data protection laws. Confirmed and material security or privacy incidents affecting ARCHIMEDES or Data, along with remedial actions taken, will be promptly reported to the Leadership Committee.

OHIRC and McGill will reasonably cooperate with the affected Data Contributor, and the breaching Data User, to enact measures required to mitigate the harms that the data breach has caused, which can include providing notice to relevant privacy regulators as permitted or required by law.

14. Data Backup and Disaster Recovery

Data Contributors are responsible for backing up and safely storing their Collection. Routine backups are implemented by ARCHIMEDES Technical Team but due to the distributed nature of the ARCHIMEDES platform, we cannot guarantee that lost data can always be recovered.

14.1 Data Storage and Backup Strategy

Central data storage and backup operations for ARCHIMEDES are managed by the ARCHIMEDES Technical Team within a secure virtual infrastructure. Access to data is strictly controlled and limited to designated ARCHIMEDES Technical Team users authenticated through secure credentials and operating within approved Virtual Machines (VMs).

A multi-tiered backup strategy ensures high availability, data integrity, and long-term recoverability.

All backup operations are logged and routinely validated to ensure data fidelity.

14.2 Disaster Recovery and Business Continuity

A Disaster Recovery Plan (DRP) defines protocols for rapid response and restoration in the event of hardware failures, software corruption, security incidents, or natural disasters.

14.3 Compliance and Data Retention

Backup and recovery procedures align with McGill policies and applicable laws. All retained backups are subject to encryption-at-rest, audit controls, and retention schedules defined in data contribution agreements or ethics protocols.

Future enhancements include the integration of immutable storage layers, cloud-based replication (as appropriate), and expanded automation for faster disaster response.

15. IT Security

The ARCHIMEDES platform adopts a layered and proportionate security strategy to mitigate risks of unauthorized access, data loss, and misuse. These measures are aligned with McGill's IT policies and informed by leading practices in biomedical research data governance. Access to sensitive systems and datasets is controlled through granular permission settings, allowing administrators to manage roles at the level of individual Collections, data modalities, workflows, and modules. Collection-based access control lists (ACLs) are actively being developed to further enhance user-level segmentation and data protection.

Security measures are enforced at both the application and infrastructure levels. All network traffic to ARCHIMEDES is encrypted using SSL/TLS, and access to servers is restricted via closed ports, firewall rules (including Firewall), and IP-level blocking tools such as Fail2Ban. User authentication practices include strong password enforcement, credential rotation, and optional two-factor authentication (2FA). Regular credential verification ensures that only appropriate persons retain access. Server infrastructure is hosted in physically secure, access-controlled environments at the McGill Centre for Integrative Neuroscience (MCIN), protected with clear protocols, response timelines, and around-the-clock automated monitoring using Nagios.

Codebase security is maintained through continuous integration testing, routine audits, and manual reviews of any changes that involve data access, storage, or user input. McGill personnel conduct ongoing security research and log any findings in a shared vulnerability database to ensure rapid mitigation of potential threats. Application-level protections include input sanitization, CSP headers, and role-based content filtering to reduce the risk of XSS, CSRF, and injection attacks.

A robust backup and recovery strategy further safeguards ARCHIMEDES data assets (implemented through McGill). This includes daily incremental and weekly full offsite backups of both virtual machines and databases, retained for up to six months to ensure recoverability. Restoration procedures are clearly defined in the event of hardware, storage, or system failure, and are tested routinely. ARCHIMEDES enforces a multi-layered security model designed to support sensitive data processing across DRAC's High-Performance Computing infrastructure. The platform leverages containerized workflows that isolate user processes and ensure reproducibility while limiting system exposure. All user access is authenticated and controlled through role-based permissions, with support for secure login protocols and credential expiration policies. Data transfers to and from

ARCHIMEDES are encrypted and staged in secure, access-controlled environments. DRAC centers implement their own rigorous physical and network security measures, including firewall protection, system auditing, and intrusion detection. The platform also maintains audit trails for all data and job activity, ensuring traceability and compliance with institutional and national data protection policies. While full automation of data pipelines is still under development, ARCHIMEDES's flexible API design supports secure, modular integration with external systems and tools without compromising its strict compliance posture.

16. Intellectual Property

ARCHIMEDES has adopted an open science strategy that maximizes the availability of data hosted through ARCHIMEDES, and that of derived datasets, for future research use where appropriate and in accordance with research participant consent and applicable privacy laws.

Data Users and Open Access Users must refrain from asserting Intellectual Property Rights (IPRs) in a manner that could preclude researchers from using or accessing data and other outputs hosted on ARCHIMEDES, or that could restrict ARCHIMEDES from sharing those outputs openly, as permitted by the respective Data Contributor.

OHIRC and McGill do not exercise the IPRs associated to the data hosted on ARCHIMEDES, nor to datasets derived the hosted data, except as is required to preserve the openness of data and of the other research outputs that are hosted on ARCHIMEDES.

17. Return of Individual Results, Material Incidental Findings, and Derived Datasets

The Data Contributor is responsible for discharging its ethical-legal obligations to return individual results and/or material incidental findings (MIFs) to research participants, where applicable.

Data Users and Open Access Users that access data on ARCHIMEDES are neither required, nor expected, to return individual-level research results or MIFs to OHIRC, nor to the original Data Contributors or research participants. OHIRC will not process the return of research results, or MIFs, to the Data Contributor or research participants.

OHIRC accepts the contribution of derived datasets to ARCHIMEDES according to the same conditions as other forms of Data Contribution. However, the choice whether to contribute derived datasets to ARCHIMEDES is left to the discretion of Data Users and Open Access Users that generate such derived datasets.

18. Data Withdrawal, Correction and Access

The ARCHIMEDES DACO accepts data withdrawal requests from the Data Contributors that first deposited the data to ARCHIMEDES. Requests to withdraw data can be made at the level of the dataset (i.e., requesting the withdrawal of the entire dataset), or at the level of the individual record.

The Data Contributor is responsible for retaining the linkage log that associates the ARCHIMEDES GUID to their own original copies of the research data (exception: De-identified Data). The Data Contributor must retain this linkage log to be able to request data withdrawal, correction and access at the level of the individual record. In the case of data withdrawal, it will only be possible to request the removal of entire datasets without the linkage log. Data that has already been shared through

ARCHIMEDES to a Data User or an Open Access User cannot be removed or destroyed to preserve the scientific integrity of the analysis.

Research participants have the right to withdraw their consent, to make a request to correct and to access their data in ARCHIMEDES. However, ARCHIMEDES DACO cannot accept data withdrawal, corrections and access requests directly from research participants that contributed their data to Research Projects hosted through ARCHIMEDES. Research participants must instead make their request with the original Data Contributor, who is responsible to respond to research participants and to explain any limitations on their rights of withdrawal.

19. Database Decommissioning and Changes in Data Stewardship

Data housed in ARCHIMEDES is under the data stewardship of OHIRC. The technological infrastructure to support ARCHIMEDES is developed and implemented by McGill.

If ARCHIMEDES were to be discontinued at any time in the future, the ARCHIMEDES Leadership Committee will decide on the transfer or closure of the database.

Efforts will be made to transfer data to a third party that contractually agrees to respect the same conditions as ARCHIMEDES. If this occurs, the Data Contributors will be notified, as will the OHSN-REB. Data Contributors will have the choice to withdraw their data.

20. Approval and Review

The Leadership Committee approved this Framework on January 12, 2026, and will ensure its continuing review on a yearly basis. A thorough revision of this Framework will be undertaken every 5 years. In addition, any revision and/or amendment made to this Framework must be approved by the Leadership Committee and the OHSN-REB prior to implementation. Changes will be prospective, will be communicated to Data Contributors and Data Users on the ARCHIMEDES website and will not, except in exceptional circumstances, require individual re-consenting or amendments to signed agreements.