ARCHIMEDES

Advanced Research Collaboration for Health Integration, Medical Exploration, and Data Synthesis

# Ethics and Data Governance Framework

Introduction to ARCHIMEDES

ARCHIMEDES is a bilingual national health data platform that provides centralized and flexible access to multi-modal health data and can be used to collect, manage, share, or perform high performance computing and analytics. ARCHIMEDES has a flexible user-centric data governance structure, enabling Data Contributors to select the tier of data governance (i.e., open, registered, or controlled) that is most appropriate for their data. All data in ARCHIMEDES has been de-identified and/or coded.

ARCHIMEDES Governance Structure

The ARCHIDEMES Steering Committee, Joint Liaison Committee, and Community Partners Committee perform portfolio-specific decision-making and advisory functions.

The Data Access Compliance Office (DACO) receives and reviews all data access requests to ensure that access decisions align with data users governance preference.

ARCHIMEDES Steering Commitee

ARCHIMEDES Joint Liaison Commitee

ARCHIMEDES Community Partners Committee

Data Access Compliance Office (DACO)
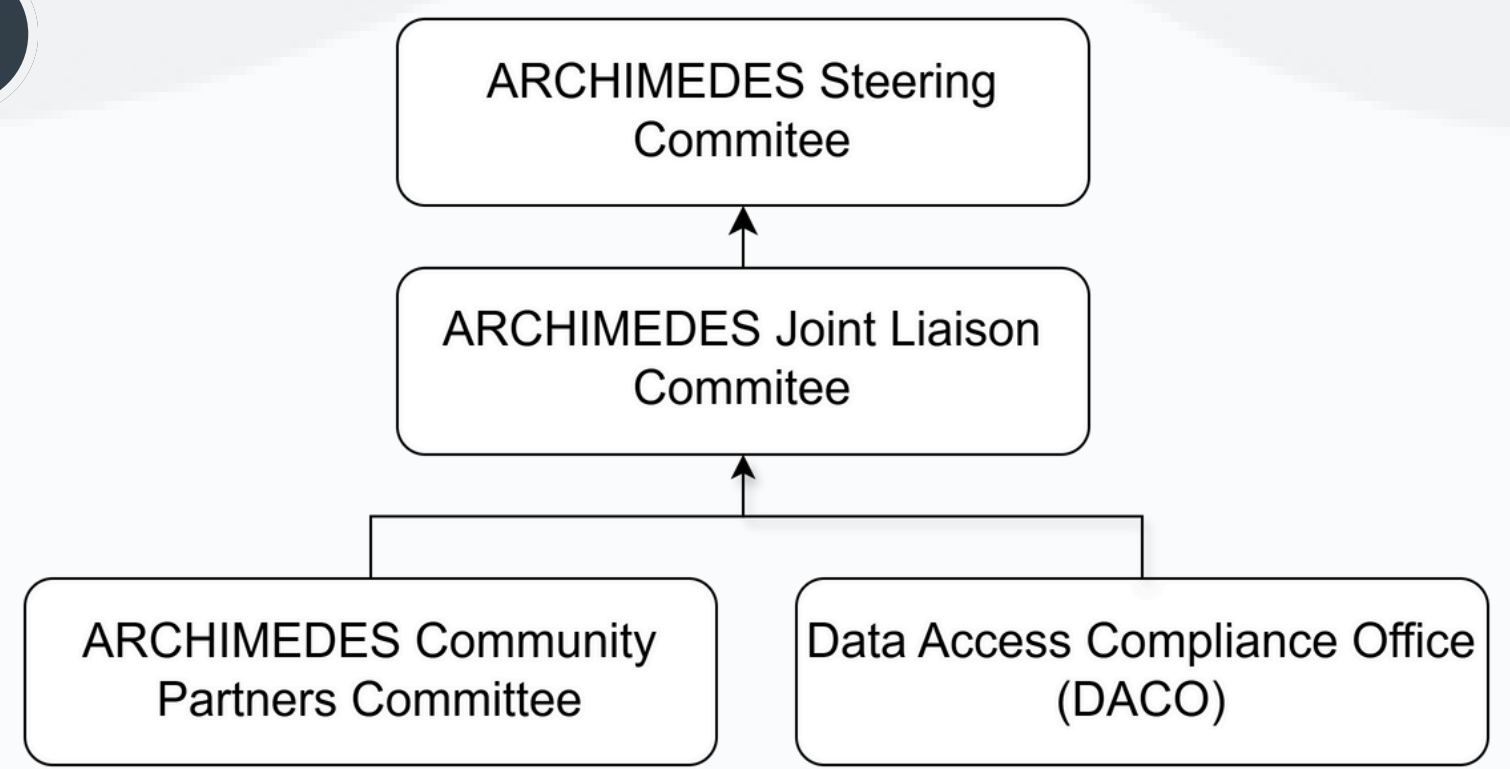
Technical Components of ARCHIMEDES

Data Ingestion

Data ingestion tools that enable credentialed users to submit data to ARCHIMEDES for private, controlled, registered, or open release.

Data Discovery Tools

Data discovery tools that enable queries across available multi-modal datasets.

User Access Tools

User authentication and access request tools, which enable credentialed users to obtain registered-access data, and apply to use controlled-access datasets.

High-Performance Computing Tools

High-performance computing capabilities, which are made available through the Digital Research Alliance Canada (DRAC) computing cluster .

Requirements to Contribute Data

Authorizations

Contributing researchers must confirm that they hold institutional and legal permissions for data sharing as described in the Data Contribution and/or Access Agreement and ARCHIMEDES policies.

Informed Consent

Informed consent forms (ICFs) must include data sharing.
The ARCHIMEDES Open and Controlled Access Consent Form Templates can be adapted to any institutional ICFs and found **here**.

Data De-Identification

ARCHIMEDES policies require all direct and indirect identifiers be removed by the data contributor prior to contribution. Technical personnel perform limited automated and manual verifications of data de-identification.

Codes, Linage Logs and GUIDS

Data Contributors are required to code their data, ARCHIMEDES will use the GUID tool to translate single-coded data into a unique long-code identifier (GUID). This enables ARCHIMEDES to link participants across studies.

Data Contribution Support Services

UOHI operates an ARCHIMEDES Ethics Helpdesk for all users to obtain information about the data governance practices of ARCHIMEDES.
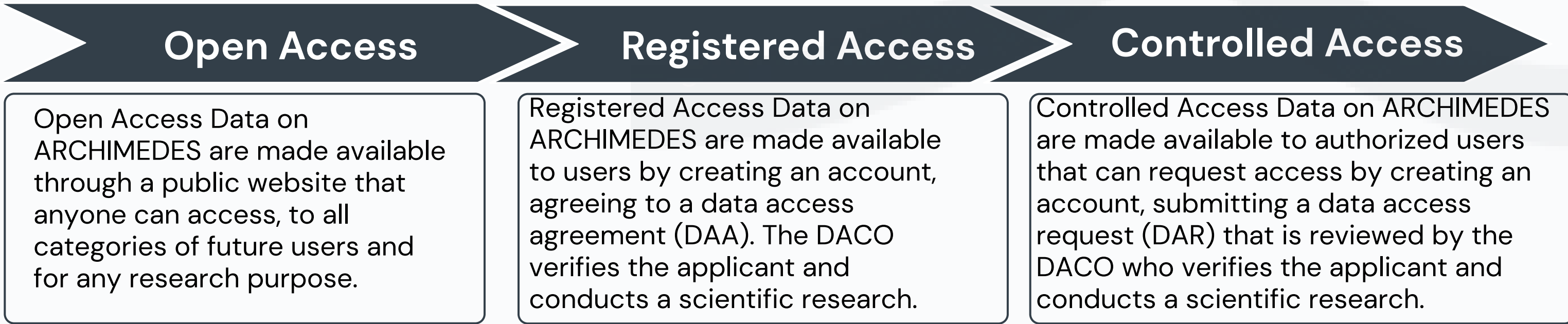
Data Contribution

Prior to contributing data to ARCHIMEDES, user institutions must complete a Data Contribution Agreement (DCA). This is a contractual agreement between the Data Contributor and the data steward (UOHI) that enables authorized Principal Investigators (PIs) at the signatory research organization to contribute data to ARCHIMEDES, as part of a specific research project.

Each Data Contributor will enter into one Data Contribution Agreement with UOHI, and can create or amend projects through the submission of a Data Contribution Form specific to that project.

The Institutional Signing Official manages the accounts and permissions assigned to its PIs and other staff members.

Data Access

ARCHIMEDES supports Data Contributors to make data available through open, registered, and controlled data access tiers.

Open Access

Open Access Data on ARCHIMEDES are made available through a public website that anyone can access, to all categories of future users and for any research purpose.

Registered Access

Registered Access Data on ARCHIMEDES are made available to users by creating an account, agreeing to a data access agreement (DAA). The DACO verifies the applicant and conducts a scientific research.

Controlled Access

Controlled Access Data on ARCHIMEDES are made available to authorized users that can request access by creating an account, submitting a data access request (DAR) that is reviewed by the DACO who verifies the applicant and conducts a scientific research.

Data Protection

Each Data Contributor that submits data to the stewardship of UOHI must ensure compliance with applicable data protection laws, including the Personal Health Information Protection Act (PHIPA), or equivalent local or sectoral data protection statute(s) that govern data collection, use, and disclosure. UOHI treats data from Data Contributors as assignments to act as a third-party-service provider.

The ARCHIMEDES Data Contribution Agreement (DCA) informs Data Contributors that the UOHI is authorized to provide notice of data breaches to regulatory authorities, affected individuals, and other third parties to mitigate the harms and other consequences.

Data Backup and Disaster Recovery Tools

Users are responsible for backing up and safely storing their own raw and derived data that is contributed to and stored in ARCHIMEDES.

- <u>Data Storage and Backup Strategy</u>: daily, weekly, and monthly backups and storage separation on dedicated storage volumes in a secured backup network.
- <u>Disaster Recovery Plan</u>: a rapid response and restoration in the event of hardware failures, software corruption, security incidents or natural disasters.
- <u>Compliance and Data Retention</u>: All retained backups are subject to encryption-at-rest, audit controls, and retention schedules.

Data Security

ARCHIMEDES applies a layered, role-based security model supported by institutional IT policies and biomedical data governance standards, with encryption, firewalls, and strong user authentication. Continuous monitoring, vulnerability audits, and secure infrastructure ensure protection against unauthorized access and system threats.