MLSC Biobank FY26 - Data Storage Request for Proposal (RFP)

Ends on Fri, Mar 6, 2026 11:59 PM

Centralized Data Storage, Curation, and Access Platform for the Biobank Program

1. Background and Purpose The MLSC Biobank Program is a multi-institutional initiative designed to support biomedical research through the centralized management of biospecimen-associated clinical, molecular, and longitudinal data. The program seeks to enable secure data ingestion, harmonization, long-term stewardship, and governed access to support discovery, translational research, and clinical innovation. The Biobank Program is soliciting proposals from qualified vendors to provide a secure, scalable, and compliant data storage and curation platform that will serve as the central data infrastructure for the program.

2. Scope of Work The selected vendor will be responsible for providing and maintaining an end-to-end data platform with the following capabilities.

A. Data Ingestion and Integration

- Secure ingestion of multi-modal data, including clinical, demographic, pathology, imaging, laboratory, molecular, and longitudinal data.
- Support for data submissions from multiple contributing institutions using standardized formats.
- Validation, quality control, and error reporting at data intake.

B. Data Storage and Infrastructure

- Cloud-based or hybrid infrastructure capable of scaling with program growth.
- Secure storage architecture with redundancy, backup, and disaster recovery.
- Persistent identifiers and traceability linking datasets to biospecimens without direct identifiers.
- Logical separation of datasets by project or access tier as required.

C. Data Curation and Harmonization

- Data cleaning, normalization, and harmonization across sites and data types.
- Support for standard ontologies, controlled vocabularies, and metadata schemas where applicable.
- Maintenance of data dictionaries, provenance records, and version history.
- Ongoing curation as new data are generated or updated.

D. Data Governance and Access Enablement

- Tools to support controlled data access workflows aligned with program policies.
- Role-based access control, audit logs, and usage monitoring.
- Ability to enforce data use limitations, consent-based restrictions, and withdrawal requirements.

- Support for tiered access models for academic, nonprofit, and commercial users.

E. Program Support and Collaboration

- Dedicated technical and project management support.
- Coordination with the Biobank Program team and participating institutions.
- Support for onboarding new data contributors and downstream users.
- Participation in governance or advisory meetings as requested.

3. Vendor Qualifications Responding vendors should demonstrate:

- Experience supporting large-scale biomedical data platforms, biobanks, or research consortia.
- Expertise in secure data management and curation.
- Experience working with academic medical centers, research institutions, or public-sector entities.
- Robust data security, privacy, and compliance practices.
- Operational stability to support a multi-year engagement.

4. Proposal Requirements Proposals must include the following sections:

1. Company overview and relevant experience
2. Technical architecture and infrastructure description
3. Approach to data ingestion, curation, harmonization, and governance
4. Security, privacy, and compliance framework
5. Implementation plan and timeline
6. Pricing structure and cost transparency
7. References from comparable programs

5. Evaluation Criteria Proposals will be evaluated based on:

- Alignment with program goals and scope
- Technical robustness, scalability, and flexibility
- Experience with similar initiatives
- Strength of data governance, security, and stewardship
- Cost effectiveness and long-term sustainability

6. Anticipated Timeline

- RFP release: 1.26.26
- Proposal submission deadline: 2.27.26

7. Submission Instructions

Proposals should be submitted electronically via Submittable. Selected proposals may be invited to interview.

8. Term

The engagement will be for a five (5) year term with options to renew

9. Contact For questions regarding this RFP, contact: BioBank@masslifesciences.com This solicitation does not constitute an obligation to fund any proposals. The MLSC reserves the right to modify or cancel this RFP at any time and may request further clarifications or conduct interviews as part of the selection process.

Appendix :

Security, Privacy, and Compliance Requirements

Vendors must demonstrate, as applicable:

Security

- HIPAA-compliant data handling and storage

- Encryption in transit and at rest
- Role-based access control and audit logging
- Incident response and breach notification procedures

Privacy

- Separation of direct identifiers from research datasets
- Support for data use limitations and withdrawal workflows
- Data provenance and traceability

Compliance and Standards

- SOC 2 Type II or equivalent
- ISO 27001 or equivalent
- Clear documentation of subcontractors and cloud providers

Business Continuity

- Disaster recovery and backup strategy
- Defined service-level commitments

Manage Collaborators

Thank you for your interest in the MLSC Biobank Program

Please read the scope of work prior to submitting the proposal.

Requirements

Proposal Requirements

Responding organizations must submit a complete proposal that addresses the following elements. Proposals that do not include all required components may be considered non-responsive.

Section 1: Vendor Information

Legal Name of Organization (required)

Primary Point of Contact Name (required)

First Name (required)

Last Name (required)

Primary Point of Contact Email (required)

email@example.com

Primary Point of Contact Phone (required)

Company Website (required)

example.com

Headquarters Location (required)

Country (required)

Select...

Address (required)

Address Line 2 (optional)

City (required)

State, Province, or Region (required)

Zip or Postal Code (required)

Headquarters Year Founded (required)

Section 2: Organizational Experience

Describe your company's experience supporting biomedical data platforms, biobanks, or large-scale research consortia. (required)

Limit: 250 words

Provide examples of comparable projects, including scope, scale, and duration. (required)

Limit: 250 words

Identify experience working with academic medical centers, research institutions, or public-sector entities. (required)

Limit: 250 words

Section 3: Technical Architecture

Describe the proposed technical architecture for data storage and management. (required)

Limit: 500 words

Indicate whether the platform is cloud-based, hybrid, or other. (required)

- ◯ Cloud-based
- ◯ Hybrid
- ◯ Other

Describe scalability, redundancy, backup, and disaster recovery capabilities. (required)

Limit: 500 words

Describe how persistent identifiers and traceability are maintained. (required)

Limit: 250 words

Section 4: Data Ingestion and Integration

Describe your approach to secure data ingestion from multiple institutions. (required)

Limit: 250 words

List supported data types and formats. (required)

Limit: 250 words

Describe validation, quality control, and error handling at data intake. (required)

Limit: 250 words

Describe onboarding workflows for new data contributors. (required)

Limit: 250 words

Section 5: Data Curation and Harmonization

Describe your approach to data cleaning, normalization, and harmonization. (required)

Limit: 500 words

Identify supported ontologies, metadata standards, or data models. (required)

Limit: 250 words

Describe how data dictionaries, provenance, and versioning are maintained. (required)

Limit: 250 words

Describe ongoing curation and update processes. (required)

Limit: 250 words

Section 6: Data Governance and Access Controls

Describe role-based access controls and audit logging capabilities. (required)

Limit: 250 words

Describe tools supporting controlled data access and usage monitoring. (required)

Limit: 250 words

Describe how data use limitations and withdrawal requirements are enforced. (required)

Limit: 250 words

Describe support for tiered access models. (required)

Limit: 250 words

Section 7: Security, Privacy, and Compliance

Describe your security framework and certifications. (required)

Limit: 250 words

Describe encryption practices for data in transit and at rest. (required)

Limit: 250 words

Describe incident response and breach notification procedures. (required)

Limit: 250 words

Identify any subcontractors or cloud service providers. (required)

Limit: 250 words

Section 8: Implementation Plan

Proposed implementation timeline from contract execution to go-live. (required)

Limit: 250 words

Key milestones and dependencies. (required)

Limit: 250 words

Staffing and project management approach. (required)

Limit: 250 words

Section 9: Pricing and Cost Structure

Describe your pricing model. (required)

Limit: 250 words

Provide a detailed cost breakdown. (required)

Limit: 500 words

Identify any optional or variable costs. (required)

Limit: 250 words

10. References

Provide at least three references from comparable programs. (required)

Choose File

Upload a file. No files have been attached yet.

Acceptable file types: .csv, .doc, .docx, .odt, .pdf, .rtf, .txt, .wpd, .wpf, .gif, .jpg, .jpeg, .png, .svg, .tif, .tiff

Please combine multiple files.

Certifications Upload

Upload relevant security or compliance documentation (if applicable).

Choose File

Upload a file. No files have been attached yet.

Acceptable file types: .csv, .doc, .docx, .odt, .pdf, .rtf, .txt, .wpd, .wpf, .gif, .jpg, .jpeg, .png, .svg, .tif, .tiff

Please combine multiple files.

Save Draft Apply

Drafts may be visible to the administrators of this program.